anno XXXII
numero 3-4
2021

TORINO MEDICA

comunicazione
informazione
formazione

LA RIVISTA DELL'ORDINE DEI MEDICI CHIRURGHI E ODONTOIATRI DELLA PROVINCIA DI TORINO

SICUREZZA DEI DATI IN SANITÀ

La leggerezza è nella nostra natura.

Per il tuo benessere quotidiano scegli l'acqua più leggera d'Europa.

Residuo fisso 14 mg/l	Sodio 0,88 mg/l	Durezza 0,60 °f

	residuo fisso in mg/l	sodio in mg/l	durezza in °f
Lauretana	**14**	**0,88**	**0,60**
Monte Rosa	16,1	1,2	0,64
S.Bernardo	34,1	0,8	2,5
Acqua Eva	45	0,3	4,2
Levissima	80	2,1	5,7
Acqua Panna	141	6,6	10,7
Fiuggi	142	7,3	8
Smeraldina	157	29	N.D.
Nestlè Vera Fonte In Bosco	162	2	N.D.
Rocchetta	181	3,87	N.D.
San Benedetto Primavera	313	4,1	N.D.
Evian	345	6,5	N.D.
Vitasnella	418	3,7	N.D.

Il residuo fisso, il sodio e la durezza di alcune note acque oligominerali (residuo fisso <500 mg/l) commercializzate nel territorio nazionale.

LAURETANA®

L'acqua più leggera d'Europa

consigliata a chi si vuole bene

Segui la leggerezza www.lauretana.com

Sommario
numero 3-4_2021

La Rivista è inviata a tutti gli iscritti all'Ordine dei Medici Chirurghi e degli Odontoiatri di Torino e provincia.

omceo-to.it
facebook.com/omceoTorino
@OmceoTo

Per l'invio di proposte, contributi, segnalazioni e per informazioni è possibile scrivere alla redazione all'indirizzo:
torinomedica@omceo.to.it

Direzione, Redazione
Corso Francia 8
10143 Torino
Tel. 011 58151.11 r.a.
Fax 011 505323
torino.medica@omceo.to.it
www.omceo.to.it

Presidente
Guido GIUSTETTO

Vice Presidente
Guido REGIS

Segretaria
Rosella ZERBI

Tesoriere
Emanuele STRAMIGNONI

Consiglieri
Domenico Bertero
Patrizia Biancucci (Od.)
Tiziana Borsatti
Vincenzo Michele Crupi (Od.)
Gianluigi D'Agostino
Riccardo Falcetta
Riccardo Faletti
Gilberto Fiore
Ivana Garione
Aldo Mozzone
Fernando Mujà
Angelica Salvadori
Renato Turra
Roberto Venesia

Commissione Odontoiatri
Presidente:
Gianluigi D'AGOSTINO
Patrizia BIANCUCCI
Vincenzo Michele CRUPI

Revisori dei Conti
Presidente:
Tonini Maurizio
Alessandra TARASCHI
componente
Giorgio VISCA
componente
Chiara DACOMO
supplente

TORINO MEDICA
Editore:
OMCeO Torino

Direttore responsabile:
Rosa Revellino

Collaborazione redazionale:
Il Pensiero Scientifico Editore

Aut. del Tribunale di Torino
793 del 12-01-1953

Per spazi pubblicitari: SGI Srl Via Pomaro 3 - 10136 Torino
Tel. 011 359908 - Fax 011 3290679 - e-mail: info@sgi.to.it - www.sgi.to.it
Grafica e Design SGI Srl

Chiuso in redazione il 10-12-2021

COMUNICAZIONE, INFORMAZIONE, FORMAZIONE.
VOGLIAMO MIGLIORARE

Guido Giustetto
Presidente OMCeO Torino

Cambiamento:
Atto ed effetto del diventare diverso.
Scalda i cuori, e in alcuni casi li terrorizza.

Su questo numero anticipiamo ai nostri iscritti la scelta di un cambiamento. Che come tutti i cambiamenti richiede impegno e programmazione.

Abbiamo deciso di orientare la nostra comunicazione verso un sistema di aggiornamento e approfondimento in cui vengano trattati temi specifici che riguardano la Professione attraverso la lente dell'etica e della deontologia.

Il progetto è una rivista digitale che analizzerà, con un taglio interdisciplinare e dialettico, alcuni dei principali temi che interessano l'attività dei Colleghi: tra i più importanti **l'etica e la deontologia, il rapporto tra le professioni, la relazione di cura, la comunicazione clinica, la responsabilità professionale, la formazione continua, il conflitto di interesse**.

Gli argomenti saranno sviluppati da studiosi nazionali e internazionali e seguiranno una periodicità di continuo aggiornamento e sviluppo critico. L'attesa e l'ambizione è offrire un punto di riferimento culturale di alto profilo per i nostri iscritti e per tutti i professionisti sanitari.

Inoltre gli approfondimenti potranno diventare anche percorsi specifici di formazione professionale in modalità FAD con accreditamento ECM.

Sono tre le direttrici progettuali da cui siamo partiti:

- Individuare contenuti più vicini agli interessi e ai bisogni della Professione;
- scegliere uno stile multicanale che integri on line e off line, digitale e cartaceo, in modo programmato e sostenibile;
- individuare le necessità di formazione e informazione dei nostri iscritti.

In questo scenario non dimentichiamo però l'importanza della traccia scritta, della carta stampata. Soprattutto nella scelta di una comunicazione multicanale, mantenere un supporto cartaceo darà massimo valore e memoria ai contenuti che proporremo: i temi più interessanti sviluppati periodicamente sulla rivista digitale saranno raccolti in 3/4 pubblicazioni cartacee annue che saranno inviate ai Colleghi che ne farannno richiesta.

Anche il sito istituzionale sarà integrato in questo cambiamento, offrendo una nuova sezione dedicata esclusivamente ai diversi contributi dei nostri iscritti, alle loro riflessioni, proposte e interventi. La nuova sezione avrà l'obiettivo di essere un tramite per l'ascolto e mantenere viva e dinamica quella trama di memorie, testimonianze e contributi che da sempre ha caratterizzato una parte della comunicazione del nostro Ordine.

Abbiamo deciso di avviare questo nuovo progetto di comunicazione e formazione per offrire una risposta alle domande e ai dubbi della Professione. Soprattutto per il nostro Ordine oggi è importante trovare l'equilibrio migliore tra innovazione e cultura attraverso i suoi canali di comunicazione. Questo non significa accantonare una tradizione, che ci ha restituito grande valore, ma al contrario renderla contemporanea e attenta alle trasformazioni in atto nel mondo della cultura medica.

Questo numero chiude quindi un lungo e glorioso ciclo della Rivista di Torino Medica per come l'abbiamo letta e seguita con interesse fino ad oggi.

Cogliamo l'occasione per esprimere un vivo ringraziamento al gruppo di redazione e in particolare al Direttore Dott. Mario Nejrotti che in tutti questi anni ha portato avanti Torino Medica con grande impegno e valore.

introduzione al focus

Su questo ultimo Focus vi proponiamo un tema fondamentale e articolato su cui torneremo nei prossimi mesi: la sicurezza dei dati in ambito sanitario. Un tema sfaccettato e spesso carico di ambiguità che iniziamo a trattare qui come inizio di un lungo percorso.
Il segreto professionale e la riservatezza dei dati personali sono due cardini del rapporto tra il medico e il paziente e su questi si basa la fiducia reciproca e l'alleanza di cura; nel dispiegarsi di questa relazione vengono continuamente raccolte e registrate informazioni sensibili, legittimamente prodotte dai due interlocutori.
L'OMCeO di Torino ha scritto alla Regione per richiedere - anche a tutela dei propri iscritti - di essere informato sulle modalità con le quali è stata impostata e avviene la protezione dei dati sanitari degli assistiti del servizio sanitario regionale.
Al 15 Dicembre non è pervenuta alcuna risposta.

Prot.32967/21 del 15/11/2021 - P - Ordine dei Medici Chirurghi e degli Odontoiatri della Provincia di Torino.

ORDINE DEI MEDICI CHIRURGHI E DEGLI ODONTOIATRI
DELLA PROVINCIA DI TORINO

C.so Fiume 8 - 10143 Torino - Tel. 011 58 15 111 Fax. 011.50 63 23
Web: www.omceo-to.it cod. fisc. 01111330013
e-mail: segreteria.amministrativa@omceo-to.it
pec: segreteria.to@pec.omceo.it

Egregio Assessore alla Sanità, Livelli
essenziali di assistenza, Edilizia sanitaria
della Regione Piemonte
dott. Luigi Genesio Icardi

assessore.sanita@cert.regione.piemonte.it

Oggetto: sicurezza della conservazione dei dati sanitari nelle strutture informatiche della Regione Piemonte

Il segreto professionale e la riservatezza dei dati personali sono due cardini del rapporto tra il medico e il paziente e su questi si basa la fiducia reciproca e l'alleanza di cura; nel dispiegarsi di questa relazione vengono continuamente raccolte e registrate informazioni sensibili, legittimamente prodotte dai due interlocutori.
Della conservazione e del trattamento di questi dati il medico è l'unico responsabile, finché essi rimangono nella sua esclusiva disposizione. Quando questi, con il consenso del paziente, sono necessariamente condivisi con o in banche dati gestite da altre entità, come avviene per la prescrizione di farmaci o di accertamenti diagnostici, o nel caso della COVID per la richiesta di tamponi o per la prenotazione e registrazione di vaccinazioni, il medico ha l'obbligo deontologico (richiamato dall'art. 11, terzo comma, del vigente Codice di Deontologia Medica) di accertarsi che anche in queste sedi sia tutelata la riservatezza e la sicurezza dei dati stessi.

La grave violazione della sicurezza dei dati sanitari subita nell'estate scorsa dal sistema informatico della Regione Lazio induce questo Ordine, anche a tutela dei propri iscritti, a richiedere di essere informato sulle modalità con le quali è stata impostata e avviene la protezione dei dati sanitari degli assistiti del servizio sanitario regionale.
In particolare, si chiede di avere informazioni di dettaglio sui seguenti punti:

- modalità di accesso ai locali dove avviene lo storage dei server e dei sistemi di backup primari;
- frequenza e modalità di implementazione dei backup primari (full, incrementali, e snapshot on-line e/o off-line);
- frequenza e modalità di implementazione di eventuali backup secondari su sedi remote, localizzati in paesi UE (full, incrementali, e snapshot on-line e/o off-line);
- presenza di eventuali sistemi di alert che avvisino sul buon fine o meno dei singoli backup;
- politiche di rete, esistenza di eventuali VLAN dedicate esclusivamente ai sistemi di backup;
- eventuale presenza di piattaforme proattive di sicurezza che analizzino i processi dei singoli client;
- modalità di gestione del telelavoro, uso di VPN con certificati e/o sistemi di sicurezza tramite secure-gateway o simili;
- politiche di resilienza/complessità delle password e eventuale autenticazione a due fattori nel caso di filesystem in cloud;
- politiche di accesso ai files e dei privilegi dei singoli utenti di dominio.

Ringraziando per il cortese riscontro l'occasione è gradita per porgere i più cordiali saluti

IL PRESIDENTE DELL'ORDINE
Dott. Guido Giustetto

Codice di Deontologia medica

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.

Art. 78

Tecnologie informatiche

Il medico, nell'uso degli strumenti informatici, garantisce l'acquisizione del consenso, la tutela della riservatezza, la pertinenza dei dati raccolti e, per quanto di propria competenza, la sicurezza delle tecniche.
Il medico, nell'uso di tecnologie di informazione e comunicazione di dati clinici, persegue l'appropriatezza clinica e adotta le proprie decisioni nel rispetto degli eventuali contributi multidisciplinari, garantendo la consapevole partecipazione della persona assistita.
Il medico, nell'utilizzo delle tecnologie di informazione e comunicazione a fini di prevenzione, diagnosi, cura o sorveglianza clinica, o tali da influire sulle prestazioni dell'uomo, si attiene ai criteri di proporzionalità, appropriatezza, efficacia e sicurezza, nel rispetto dei diritti della persona e degli indirizzi applicativi allegati.

SICUREZZA DEI DATI IN SANITÀ

Deontologia e tutela dei dati sanitari

Angelica Salvadori
MMG, Consigliera OMCeO Torino

La prima cosa che faccio quando arrivo in studio è accendere il computer. E con questo gesto apro, in qualche modo inconsapevole, una finestra, anzi una porta attraverso la quale, nel corso della giornata, i dati dei miei pazienti potranno essere disseminati in molte direzioni.

Mi metto in grado, cioè, di operare un grande scambio di informazioni, naturalmente attenendomi alle norme vigenti in materia, tra i dati contenuti nel mio computer e tutta una serie di sistemi: ad esempio, mi metto in collegamento con il SAR (Sistema di Accoglienza Regionale) della Regione Piemonte e il SAC (Sistema di Accoglienza Centrale) quando compilo in modalità informatica una ricetta dematerializzata contenente prescrizioni farmaceutiche e specialistiche, mi collego con AURA (Archivio Unico Regionale degli Assistiti della Regione Piemonte) se emerge l'esigenza di un aggiornamento dell'anagrafe degli assistiti, mi connetto con l'INPS (Istituto Nazionale della Previdenza Sociale) quando rilascio un certificato di malattia, oppure con l'INAIL (Istituto Nazionale per l'Assicurazione contro gli Infortuni sul Lavoro) se devo certificare un infortunio lavorativo, con il CSI Piemonte (Consorzio per il Sistema Informativo) se devo vedere ▶

l'esito di un tampone per la Covid 19, se devo richiederne uno, se devo verificare l'inizio o la fine di una quarantena o di un isolamento, se devo vedere se un paziente è vaccinato. E questo vale non solo per me, medico di medicina generale, ma per tutti i medici convenzionati con il SSN, per i medici specialisti ospedalieri e, per alcuni aspetti, anche per i medici liberi professionisti. Se i medici, forse, non sempre sono consapevoli di tutto quello che mettono in moto, viene da chiedersi: e i cittadini? Hanno una percezione corretta di tutte le strade che possono prendere i loro dati sanitari?

La medicina, si sa, non ha confini e la tecnologia applicata alla medicina ancora di meno. E proprio per questa continua evoluzione, il nostro Codice di Deontologia medica del 2014 ha previsto espressamente alcuni articoli che si riferiscono all'uso delle tecnologie informatiche in ambito sanitario, nell'ottica di individuare precauzioni da tenere presenti e prescrizioni da osservare per garantire ai cittadini la riservatezza delle informazioni da loro fornite e la sicurezza a questo fine delle tecnologie utilizzate.

D'altra parte le persone chiedono quotidianamente di interfacciarsi con i medici utilizzando strumenti informatici di diversi tipi, il più delle volte informali: posta elettronica, instant messaging o teleconsulti perché ritenuti più rapidi, più facilmente accessibili, più "smart". Una risposta corretta, e non scontata, a questa pressione ci pone questioni bioetiche e deontologiche nuove su cui riflettere. E allora, come procedere?

Proprio nell'ottica di questo cambiamento inarrestabile, dobbiamo chiederci se gli attuali articoli del nostro Codice siano ancora attuali o se necessitino di una revisione e di una integrazione in quanto non più sufficienti e corrispondenti alla realtà che stiamo vivendo; oppure anche solo domandarci se nella nostra pratica quotidiana sia così semplice mettere in atto le precauzioni e le prescrizioni indicate.

Per fare degli esempi: solo noi medici dobbiamo acquisire il consenso al trattamento dei dati nell'utilizzo di qualsiasi strumento informatico? Dati che, come ci ha insegnato la recente pandemia da Covid 19, vengono poi inglobati in sistemi aziendali e regionali sui quali non abbiamo alcun controllo. Come possiamo riuscire ad eliminare ogni forma di discriminazione nell'uso delle tecnologie informatiche? Dovrebbero entrare in campo strategie governative con l'obiettivo di formare i cittadini all'uso efficace, consapevole e partecipato di tali strumenti. I criteri di proporzionalità, appropriatezza, efficacia e sicurezza sono sempre i medesimi per qualsiasi strumento informatico decidiamo di utilizzare o possono essere diversi? Cambiano o dovrebbero cambiare se usiamo un social media, se usiamo un sistema di messaggistica, se usiamo un sistema di posta elettronica? Tali questioni necessitano di un'analisi di ampio respiro che coinvolga ed integri più livelli, a partire dai professionisti sanitari, insieme a figure multidisciplinari che sappiano orientare in ambito formativo, tecnico-ingegneristico, legislativo ed economico i medici e i cittadini, utilizzatori di tali tecnologie, spesso inconsapevoli delle molte implicazioni.

La pervasività dell'ICT (Information and Communication Technologies) impone un'azione di controllo da parte dei medici con la finalità non di arrestare un processo in continuo divenire, ma con l'obiettivo di continuare a tutelare la salute come finalità dell'intervento medico.

La sicurezza dei dati sanitari

Ing. Andrea Gelpi
Specializzato in sicurezza delle informazioni, membro di Security Brokers
Vicepresidente Sicurdott

La sicurezza dei dati presenti nei sistemi informatici è da tempo un nodo cruciale di tutte le nuove applicazioni. La normativa sulla protezione dei dati se ne occupa da oltre 25 anni, e dà indicazioni su come tutelare i dati anche sanitari sia in ambito pubblico che professionale. Tuttavia sono quasi giornaliere le notizie di problemi e violazioni alle banche dati. La pirateria informatica è sempre più agguerrita, organizzata e ben preparata.

I dati sanitari, come altri, sono appetibili per molti motivi, comprese varie forme di ricatti. Questi dati risultano ancora poco protetti. Troppo spesso la pirateria riesce ad arrivare ai dati e fare danni molto gravi, che in almeno un caso ha portato alla morte di un paziente.

Nell'articolo si affronta la situazione della (in)sicurezza nel mondo e in Italia, con particolare attenzione ai dati sanitari, ma non solo. Sono date indicazioni sui principali problemi, sugli attacchi e che cosa interessa ai criminali. Si affrontano poi gli strumenti di comunicazione, in particolare i social network e i servizi gratuiti per gli utenti finali, soprattutto quando si trattano dati sanitari o altri dati "particolari" degli utenti. Si parla, infine, del baratto di dati personali, da parte delle multinazionali dell'informatica.

CHE COSA È LA SICUREZZA DEI DATI E PERCHÉ È IMPORTANTE

Sempre più dati e informazioni vengono immessi nei sistemi informatici, creando banche dati sempre più grandi e ricche di informazioni. Avere accesso a queste informazioni oggi significa avere potere in quanto si può sfruttare l'informazione a proprio vantaggio in svariati modi. Chi detiene le informazioni le può trasformare in qualcos'altro, per esempio:

- vantaggi competitivi rispetto ai concorrenti
- gestione di informazioni critiche/sensibili
- trasformazione in denaro con vari metodi
- uso improprio dei dati (malavita)

Le informazioni sugli individui sono appetibili per il marketing. Poter fare marketing mirato è molto più redditizio che tentare a caso nel mucchio. Alla maggior parte delle persone la troppa pubblicità infastidisce, ma se invece è mirata, cioè propone oggetti o servizi che interessano, è tollerata e aumenta la probabilità che venga guardata e che il soggetto compri.

Le grandi multinazionali dell'informatica raccolgono una quantità enorme di informazioni sulle persone, informazioni che poi vengono correlate con altre per creare dei profili che vengono poi o venduti o utilizzati in vari modi. Molti servizi gestiti da queste multinazionali sono apparentemente gratuiti. L'uso del motore di ricerca Google è gratuito, ma è esperienza di chiunque abbia fatto una ricerca su un argomento specifico, che dopo poco tutta la pubblicità appare evidentemente correlata a quella ricerca. La stessa cosa capita con i social network. Facebook fa vedere solo i post che ritiene siano d'interesse per ciascuno di noi, sulla base di "profili creati ad hoc. Lo stesso vale per i post sponsorizzati", quelli che le aziende inviano "a pagamento" come pubblicità mirata. L'uso di Facebook e altri social come WhatsApp è gratuito, ma le società che li gestiscono sono miliardarie. Come fanno? Semplice: utilizzano le informazioni sugli utenti, immesse volontariamente o ricavate da algoritmi.

Ma c'è di più. Queste società hanno accesso ai dati non solo direttamente, con un nostro consenso, ma anche indirettamente accedendo a dati di altre società - anche se su uno smartphone il sistema di localizzazione (GPS) è spento - è possibile conoscere comunque la posizione approssimata del dispositivo tramite la sua connessione alla rete telefonica mobile. Infatti le informazioni sulla posizione dell'antenna utilizzata dal dispositivo sono a disposizione non solo degli operatori di telecomunicazioni. Un altro esempio: Google usa un *DeviceId*, cioè un identificatore univoco per ogni dispositivo. Utilizzando un qualsiasi servizio di Google, questa potrà sempre sapere di chi è e che cosa sta facendo e dove è il dispositivo. Prova ne è che alcuni anni fa Google ha sottoscritto un accordo con l'FBI americano per fornire, su richiesta, le generalità dell'utilizzatore e la posizione di qualsiasi dispositivo mobile presente nei dintorni di qualche grave avvenimento (ad esempio un omicidio). Correlando quindi informazioni di natura differente è possibile aggirare alcune delle limitazioni che gli utenti utilizzano.

C'è chi dice che non ha nulla da nascondere e che le preoccupazioni sono inutili. Sarebbe vero se ci si limitasse al marketing, ma i dati raccolti dalle multinazionali servono e vengono utilizzati anche per tante altre finalità, fra le quali informazioni di natura politica ed economica, non sempre esatte, se non volutamente false. In altre parole quei dati vengono usati per orientare a proprio piacimento le persone, anche dal punto di vista politico. Che molte elezioni siano state influenzate da dati più o meno corretti è ormai noto. Identico discorso si può fare per la pandemia in atto e i vaccini.

PERCHÉ I DATI INTERESSANO ALLA CRIMINALITÀ E COME VENGONO SFRUTTATI

La pirateria informatica sta facendo soldi a palate con attacchi che hanno una percentuale di riuscita in crescita di circa il 15% annuo. I danni stimati da Clusit[1] per l'Italia ammontano già oggi ad una manovra finanziaria e i dati dicono che sono in crescita e potrebbero arrivare in pochi anni a superare i 20 miliardi di euro (si veda il Rapporto Clusit 2021 pg. 12 e 13).

Clusit è un'associazione che raccoglie esperti e aziende sui temi della sicurezza delle informazioni. Collabora con associazioni simili sparse per tutta Europa, con ENISA (European Network and Information Security Agency) e con altre realtà che si occupano degli stessi temi. In Italia collabora con molti enti governativi, università e aziende.[2] La tutela dei dati, in particolar modo quelli legati allo stato di salute delle persone, sono da decenni al centro delle normative sulla cosiddetta privacy. Vengono infatti definiti come dati "particolari", la cui raccolta, gestione e conservazione è soggetta a norme molto stringenti, in particolare per la sicurezza.

Clusit è un'associazione che raccoglie esperti e aziende sui temi della sicurezza delle informazioni. Collabora con associazioni simili sparse per tutta Europa

Purtroppo i dati disponibili sulla rete, relativi ad incidenti di sicurezza, ci dicono che proprio i dati sanitari non sono poi così ben protetti come sarebbe necessario.

Ogni anno si assiste a un aumento dei casi noti di attacchi riusciti, con danni anche notevoli sia in termini d'immagine che di costi. Infatti il tempo e i costi per ripristinare il funzionamento dei sistemi è spesso molto alto. Vanno infatti messi in conto tempi di fermo delle attività, del personale collaboratore, in certi casi addirittura a casa, ma pagato. Costi di tecnici specializzati nel recupero dei dati. Senza citare l'obbligatorietà di autodenuncia al Garante per i dati personali, che può portare a ispezioni e possibili sanzioni.

Purtroppo ancora oggi gli investimenti in sistemi di sicurezza vengono visti solo come costi e quindi limitati il più possibile. Se invece ci si rendesse conto che si tratta di investimenti, che hanno un loro ritorno in diminuzione dei rischi d'incidenti e quindi permettono un domani di risparmiare sia tempo che denaro, molti incidenti potrebbero essere limitati se non evitati.

VIOLAZIONI DI DATI NEL MONDO E IN ITALIA

Vediamo di seguito alcuni dati presi dal Rapporto Clusit 2021 sulla sicurezza ICT in Italia[3] che riporta dati relativi al 2020.

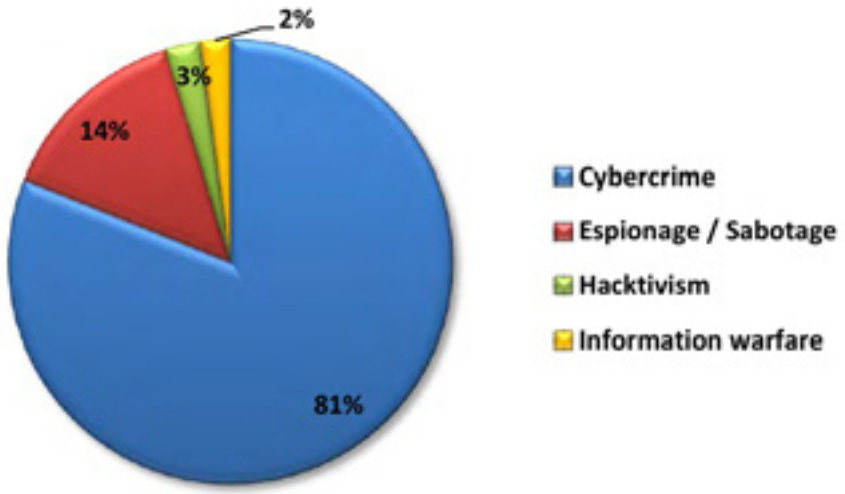
Il rapporto da sempre suddivide gli attacchi riusciti in quattro categorie:

- Crimini informatici (Cybercrime)
- Attivisti
- Spionaggio/sabotaggio
- Guerra d'informazione

Nel 2020 tutte queste categorie, ad eccezione degli attivisti che sono rimasti costanti, sono cresciute in media del 12%. Gli attacchi riusciti verso strutture con dati sanitari sono cresciuti nel 2020 del 6% circa. I dati sanitari sono fra le categorie più colpite (al terzo posto con il 12% del totale) e con un maggior incremento nel 2020. Nelle due figure che seguono si può notare la differenza fra i dati "globali" e quelli relativi ai soli dati sanitari. La quantità di attacchi riusciti di Cybercrime è decisamente più alta nel mondo sanitario, superando abbondantemente il 90% di successo! Ciò indica inequivocabilmente che tali dati sono ancora oggi troppo poco protetti.

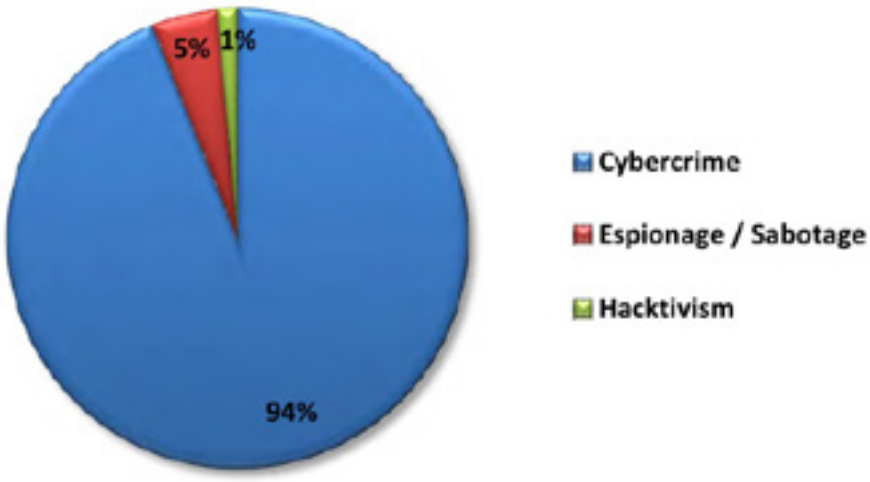
1. clusit.it
2. clusit.it/chi-siamo/
3. clusit.it/rapporto-clusit/

Tipologia e distribuzione degli attaccanti (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Attaccanti vs Healthcare (2020)

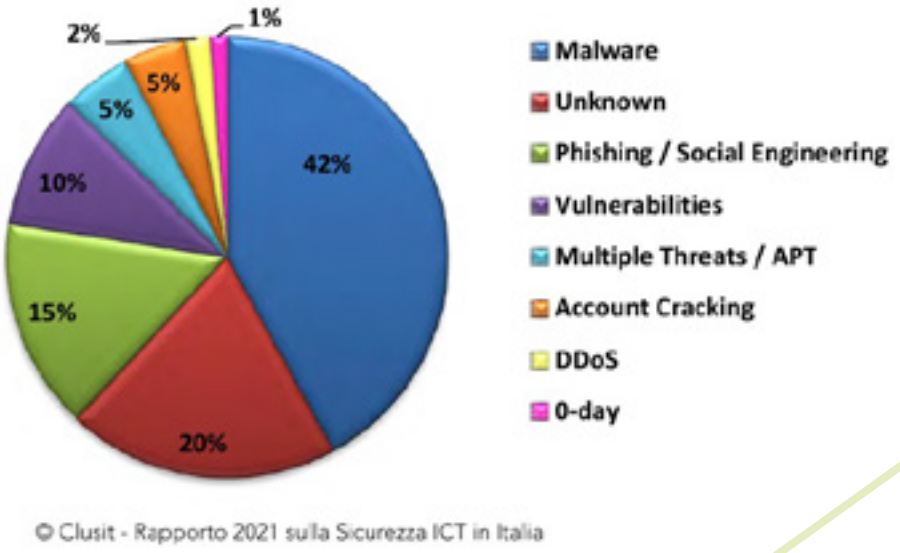


© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Guardando le tecniche usate per gli attacchi si nota come le principali siano poche e ben conosciute.

I malware[4] continuano a farla da padrone, nonostante esistano da decenni sistemi di protezione, che però sembra non siano più all'altezza. Anche la fetta delle vulnerabilità (10%) è ancora alta e denota una insufficiente attenzione al problema della sicurezza dei dati.

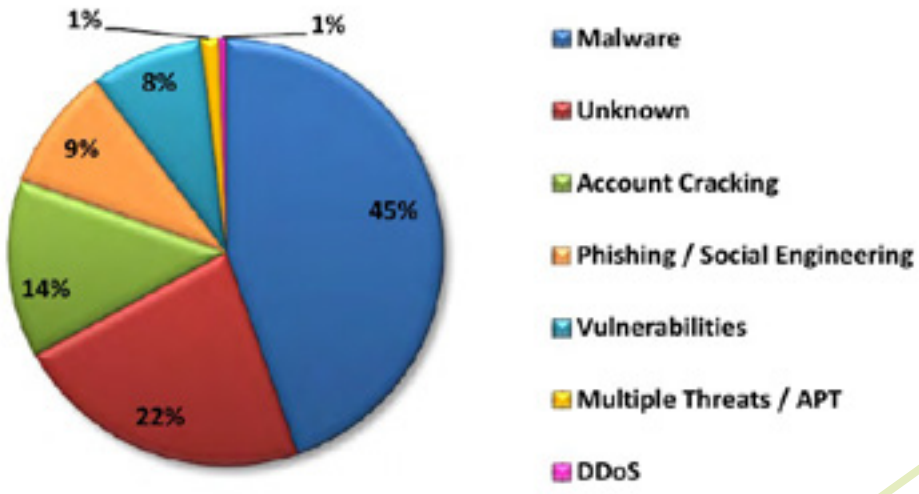
Tipologia e distribuzione delle tecniche di attacco (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

Se guardiamo il solo mondo dei dati sanitari le cose cambiano poco, malware e vulnerabilità superano il 50% degli attacchi riusciti. Cioè un attacco su due potrebbe essere evitato.

Tecniche vs Healthcare (2020)



© Clusit - Rapporto 2021 sulla Sicurezza ICT in Italia

4. it.wikipedia.org/wiki/Malware

Per quanto riguarda i malware si nota che nel 2020 due terzi degli attacchi riusciti sono stati eseguiti con i famigerati ransomware[5], vediamo come funzionano.

In passato questi malware una volta entrati su un sistema tramite un allegato a una mail o tramite una pagina web di un sito compromesso, o tramite campagne d'attacco mirate o altre vulnerabilità che danno accesso alla postazione dell'utente o a un server, si limitavano a cifrare[6], cioè rendere illeggibili, tutti i documenti a cui riuscivano ad arrivare, non solo quelli presenti sul sistema colpito, ma anche su tutti i sistemi raggiungibili tramite la rete. Poi veniva chiesto un riscatto per fornire la chiave necessaria per rimettere in chiaro i dati. Oggi questi malware si sono evoluti e i danni che riescono a provocare possono essere notevoli. Prima di cifrare i dati ne fanno una copia all'esterno per creare problemi d'immagine, per cercare di propagare il malware mediante mail reali, e per ricattare ulteriormente la vittima, oppure semplicemente venduti sul mercato nero dove altri gruppi troveranno modo di utilizzarli per fare soldi. Vengono cifrati oltre ai dati anche gli eventuali salvataggi dei dati stessi e sono cancellati i punti di ripristino. Insomma fanno di tutto per rendere molto complicato il recupero dei dati. Poi chiedono una somma di denaro in cambio della restituzione dei dati.

La cifra richiesta dipende dal tipo di vittima. Più è in vista ed importante o più i dati sono delicati più la richiesta è alta. Nel 2020 un'azienda italiana ha ricevuto una richiesta di riscatto di oltre 1 milione di euro! Pagare in questi casi vuol dire rendersi complici di un illecito e, avendo a che fare con criminali, non si ha alcuna certezza di riottenere i propri dati. Infatti circa il 40% di chi paga non riottiene i suoi dati, ma viene invece inserito dai criminali nell'elenco dei buoni pagatori e quindi aumenta la probabilità di essere colpito da altri attacchi e/o da altri gruppi criminali. L'unica vera strategia è avere un backup dei dati che non sia stato toccato dal ransomware, da cui ripristinare i dati. Va tenuto però presente che i malviventi avranno prelevato documenti che useranno per cercare di convincere altri ad aprire un qualche allegato contenente il malware. Tale tecnica ha una buona percentuale di successo, in quanto la mail arriva da un contatto noto con un testo che potrebbe essere veritiero. Va fatta molta attenzione per molto tempo dopo un attacco ransomware, in quanto arriveranno mail fasulle, ma difficili da distinguere da quelle lecite. Ecco perché servono nuovi strumenti di protezione diversi dai normali antimalware (antivirus). Va notato che l'uso dei dati da parte della pirateria ha un impatto notevole sulla privacy, ancor più se si tratta di dati particolari, ad esempio quelli sanitari. Il Garante può sanzionare anche pesantemente situazioni in cui i dati sono stati resi pubblici da malviventi. È imperativo cercare di evitare situazioni del genere. Gli attacchi ransomware verso strutture che gestiscono dati sanitari hanno, purtroppo ripercussioni anche gravi sulla salute delle persone. Nel 2020 in alcuni ospedali americani alcuni interventi chirurgici a pazienti (compresi interventi programmati al cuore) sono stati rinviati a causa dell'impossibilità di accedere ai dati a causa di un attacco informatico di tipo ransomware[7], ma in Germania il 9/10 settembre 2020 all'ospedale universitario di Dusseldorf una paziente è morta a causa di un attacco ransomware che ha bloccato il pronto soccorso[8]. Questo viene considerato il primo caso di decesso a causa di un attacco informatico. L'attacco all'ospedale di Dusseldorf ha sfruttato una vulnerabilità nota da febbraio (ben 7 mesi prima) che non era stata sanata.

L'attacco e la morte della paziente erano quindi prevenibili, nel senso che si sapeva cosa e come fare per evitarli. In questo specifico caso le forze dell'ordine hanno contattato i criminali segnalando che avevano colpito il Pronto soccorso di un grosso ospedale e i

5. it.wikipedia.org/wiki/Ransomware
6. it.wikipedia.org/wiki/Crittografia
7. https://hitconsultant.net/2021/01/05/death-by-ransomware-healthcare-cybersecurity/#.YUnN1yXOOJA
8. https://www.technologyreview.com/2020/09/18/1008582/a-patient-has-died-after-ransomware-hackers-hit-a-german-hospital/

criminali hanno fornito gratuitamente la chiave per decifrare tutti i dati, ma per quella paziente era ormai tardi.

Come fanno i criminali a inviare malware e altri attacchi senza essere individuati facilmente? Sono pochi, pochissimi coloro che vengono individuati e arrestati. La maggior parte degli attacchi viene gestita tramite dispositivi di vittime inconsapevoli di essere nelle mani di criminali (i tecnici li chiamano zombie). Nel mondo ci sono milioni di dispositivi, molti di privati cittadini, violati da pirati informatici, che vengono usati per rimbalzare malware e attacchi di vario tipo. Ciò rende quindi molto più complicato, se non impossibile, risalire al pirata che, ben nascosto, gestisce la sua attività. Il pirata di turno si nasconde ulteriormente utilizzando pochi sistemi che funzionano come centri di comando e controllo, a cui vengono inviati comandi che vengono poi rimbalzati ai dispositivi violati che eseguono materialmente l'attacco. Riuscire a ricostruire una di queste reti, che può contare anche milioni di PC, è complicato, anche perché quasi sempre si ha a che fare con dispositivi posti in Stati differenti e non esiste ancora una normativa internazionale che permetta un'indagine veloce e puntuale.

Sempre nel 2020 la quantità di mail legittime scambiate sui temi della pandemia ha raggiunto quasi il 10% del totale. Da marzo 2020 molte sono state le mail di spam[9] contenenti allegati malevoli o con link a siti compromessi. La maggior parte di queste mail hanno delle caratteristiche in comune. Arrivano apparentemente da fonti ufficiali (ma l'indirizzo è falso), cercano di catturare l'attenzione del lettore (si cerca di far sì che l'utente apra e legga la mail), e nel messaggio si cerca di far leva sull'urgenza in modo da ottenere un più alto tasso di successo (se non c'è il tempo per riflettere è più facile fidarsi di quello che si legge). Queste caratteristiche portano gli utenti ad aprire allegati o a seguire link contenti malware, con una maggior probabilità.

In campo sanitario sono girate mail apparentemente provenienti dall'Organizzazione Mondiale della Sanità che avvisavano di nuovi cluster di contagi, allegando un documento di presunte nuove norme di prevenzione. Ovviamente l'allegato conteneva malware o puntava ad esso (cioè conteneva un link verso il malware). Per concludere il tema delle mail malevoli, queste sono dal punto di vista tecnico indistinguibili da quelle legittime. La differenza sta nel contenuto e sta alla nostra capacità di capire se si tratta di mail legittima o meno. La tecnologia aiuta, ma è necessario passare da normali antivirus a tecnologie nuove e più aggressive. Dal Rapporto Clusit 2021 Pg. 167: "10 marzo 2020 - Un rapporto di Palo Alto Networks ha rilevato che l'83% dei dispositivi di medical imaging negli Stati Uniti utilizza sistemi operativi obsoleti. Ciò rappresenta un aumento del 56% in due anni, che può essere in parte attribuito alla mancanza del supporto di Microsoft per Windows 7 giunto a fine vita nel gennaio 2020. Il rapporto ha analizzato un perimetro composto da 1,2 milioni di dispositivi IoT[10] in migliaia di infrastrutture IT e sanitarie ubicate negli Stati Uniti. I ricercatori hanno anche rilevato come nel 98% dei casi il traffico inviato dai dispositivi IoT non venga crittografato.[11] Il report punta anche l'attenzione sul fatto che le apparecchiature vulnerabili non sono correttamente installate nell'ambito di sezioni di rete segregate tramite VLAN[12], essendo quindi facilmente raggiungibili da dispositivi PC e server adibiti a scopi ben diversi."

9. it.wikipedia.org/wiki/Spam

10. it.wikipedia.org/wiki/Internet_delle_cose

11. unit42.paloaltonetworks.com: 2020 Unit 42 IoT Threat Report

- www.wired.com: Most Medical Imaging Devices Run Outdated Operating Systems

- www.theregister.co.uk: The Internet of Things is a security nightmare reveals latest real-world analysis: unencrypted traffic, network crossover, vulnerable OSes

12. it.wikipedia.org/wiki/VLAN

COME RISPETTARE LE NORME DEL GDPR E METTERE AL SICURO I DATI

Abbiamo visto diversi problemi, ma come ci si può difendere concretamente e come si fa a rispettare le indicazioni del GDPR sul trattamento dei dati personali?

Vediamo alcuni semplici consigli utili per migliorare la sicurezza e il rispetto delle norme.

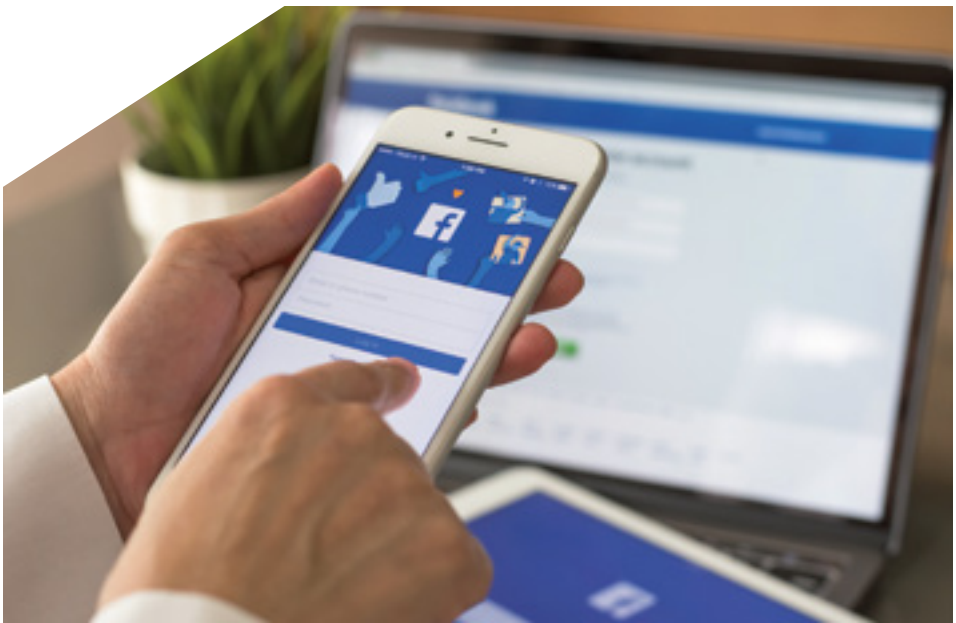
Partiamo proprio dalla mail dicendo che l'utilizzo di servizi di posta elettronica gratuiti (es. gMail) non vanno bene in quanto il servizio è solo in apparenza gratuito. In realtà chi lo offre guadagna dalla rivendita dei contenuti, ufficialmente anonimizzati. Ad esempio gMail utilizza i contenuti delle mail sia ricevute che spedite per ricavarne informazioni utili per terzi. È esperienza comune che se si legge o si spedisce una mail con un certo contenuto, dopo non molto tempo sui siti visitati comparirà pubblicità legata a quel contenuto.

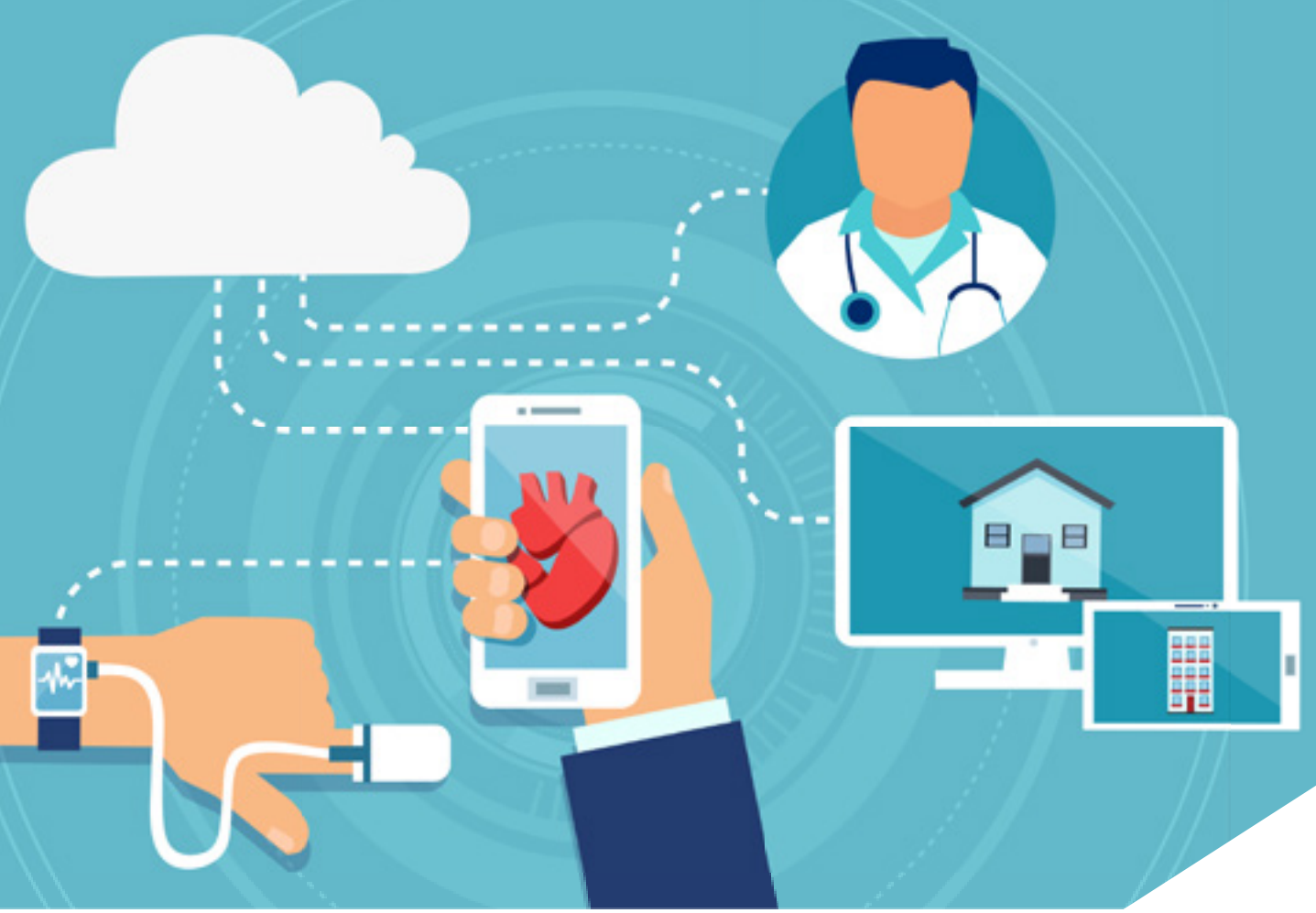
Quindi l'utilizzo di fornitori di posta elettronica che offrono il servizio gratuitamente non dà una ragionevole garanzia sulla sicurezza dei contenuti.

Va inoltre tenuto presente che Google correla informazioni ottenute da un dispositivo con altre informazioni dello stesso utente o dello stesso dispositivo. Infatti nell'informativa privacy di Google si legge: "Quando non esegui l'accesso a un account Google, archiviamo le informazioni che raccogliamo tramite identificatori univoci legati al browser, all'applicazione o al dispositivo che stai utilizzando." Queste informazioni possono essere collegate a quella di un qualsiasi altro servizio di Google. Lo stesso principio funziona anche con altri grandi multinazionali dell'informatica, come Facebook, WhatsApp e tutti i social network in genere. Nel caso di Facebook va ricordato che, alla creazione di un account, fra le condizioni del servizio c'è scritto che tutti i contenuti una volta immessi possono essere utilizzati da Facebook. Nel mondo ad oggi ci sono più di 2 miliardi di utenti, che pubblicano informazioni, foto e altro. Facebook fa vedere solo i contenuti che ritiene d'interesse in base ad un profilo dell'utente, basato sui contenuti pubblicati, i like, commenti scritti e altri servizi utilizzati. Questo ci dice che tutte le informazioni inserite vanno ad alimentare profili che vengono poi utilizzati anche per veicolare contenuti sponsorizzati. In altre parole l'uso di Facebook, WhatsApp e altri social network non sembra appropriato per lo scambio di informazioni sanitarie, in particolare fra medici e pazienti. Non c'è infatti nessuna garanzia che tali informazioni non vengano utilizzate o per la generazione di profili o veicolate in qualche modo a terzi anche se anonimizzate.

La stessa cosa vale per altri servizi gratuiti, ad esempio WeTransfer, in quanto ancora una volta non si ha alcuna garanzia sulla riservatezza dei dati trasferiti.

Ricordo che trattandosi di dati particolari il GDPR ne vieta espressamente la comunicazione e diffusione a persone non espressamente autorizzate.





COME SI FA ALLORA A TRASFERIRE INFORMAZIONI SANITARIE FRA MEDICI, STRUTTURE OSPEDALIERE E PAZIENTI?

Per rispettare le norme e per garantire un'adeguata sicurezza, l'unico metodo ad oggi sicuro è l'uso della cifratura dei dati prima dell'invio. Un sistema comodo e a basso costo per trasferire dati cifrati è l'uso di prodotti come ad esempio WinZip, che non è gratuito, ma va pagato entro 3 settimane dal primo utilizzo. Il costo è veramente contenuto, poche decine di euro una tantum. WinZip permette di comprimere dati e cifrarli in modo che solo il destinatario di quei dati possa accedervi. Il file così ottenuto può essere scambiato con qualsiasi mezzo, sia posta elettronica, che social network. Al momento questo è l'unico modo sicuro che rispetta anche le indicazioni del GDPR.

Si stanno sempre più diffondendo l'utilizzo di servizi cloud, vedi Dropbox, GDrive e simili. Su tutti questi servizi vale lo stesso identico discorso fatto poco sopra. Da inizio estate 2021 Google e Amazon hanno introdotto la possibilità di utilizzare i loro sistemi cloud cifrando i dati con chiavi in esclusivo possesso dell'utente. In questo caso i dati memorizzati sui sistemi cloud sono al sicuro, sia da occhi indiscreti, che da eventuali malware. Tuttavia se i dati sono cifrati non è più possibile utilizzare i servizi online come ad esempio Office 365 che può essere molto comodo per la condivisione di dati e informazioni.[13] Purtroppo la sicurezza delle informazioni non va molto d'accordo con la comodità di molti servizi.

13. https://thehackernews.com/2021/06/google-workspace-now-offers-client-side.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+TheHackersNews+%28The+Hackers+News+-+Cyber+Security+Blog%29&_m=3n.009a.2505.cs0ao0cwrw.1l5m

PUNTI CRITICI NELL'USO DI STRUMENTI DI COMUNICAZIONE E SUI SOCIAL

Alcuni punti importanti.

a) Quando viene installato un nuovo sistema, far verificare che siano state cambiate le credenziali d'accesso al sistema. Mai lasciare quelle fornite dalla fabbrica, in quanto sono facilmente reperibili sui manuali, oggi in rete. Le nuove credenziali devono essere robuste e non parole facili da indovinare.

b) Andrebbe verificato prima di acquistare un dispositivo che questo permetta l'accesso solo mediante delle credenziali, soprattutto se dovrà essere installato ed esposto sulla rete Internet.

c) Va chiesto ai tecnici di verificare che non rimangano disponibili accessi da remoto mediante protocolli obsoleti o non più sicuri, come ad esempio Telnet.

d) Privilegiare sempre dispositivi che usano la cifratura nelle comunicazioni. Si ricordi che nel caso di dati sanitari la cifratura è necessaria per rispettare il GDPR.

e) Evitare il più possibile di collegare dispositivi direttamente alla rete Internet. Se possibile è sempre meglio mettere in mezzo un qualche sistema che faccia da ponte e che provveda a separare il traffico del dispositivo da quello della rete. Questo dovrebbe essere sempre fatto, ad esempio, per gli apparati elettromedicali.

f) Far controllare periodicamente se esistono aggiornamenti software per i dispositivi in uso. Per i dispositivi che trattano dati sanitari tale misura era considerata minima dalla precedente normativa sulla protezione dei dati personali (Dlgs. 196/03). Ora vengono richieste misure "adeguate". Pertanto gli aggiornamenti se disponibili vanno programmati ed eseguiti periodicamente.

g) Se la struttura è sufficientemente grande è opportuno dotarsi di certificazioni come ad esempio la ISO 27001 ed eseguire dei "penetration test"[14] annualmente.

Parlando di cloud, la tendenza delle aziende è di togliere i dati particolari dal cloud e riportarli in casa. Per ciò che rimane sul cloud si sta spingendo sempre più verso la cifratura del dato e il controllo di chi vi accede. Tuttavia questi passaggi avvengono lentamente in quanto pare manchino risorse, sia umane che finanziare oltre a esperienza nella gestione della sicurezza nel cloud. Nel 2020 solo il settore dei dati sanitari ha aumentato la propria presenza nel cloud. Gli altri settori l'hanno diminuita a causa di incidenti avvenuti negli anni precedenti. I più comuni sono stati danni dovuti a phishing[15] e ransomware che hanno superato il 50% degli incidenti registrati nel 2019 e anche nel 2020.

In conclusione, la sicurezza delle informazioni, soprattutto quelle sanitarie, risulta insufficiente. È una questione di tempo e altri incidenti capiteranno a tutti, se non si provvede ad aumentare le misure di sicurezza. Spendere in sicurezza non è un costo, ma un investimento che ha un alto ritorno (ROI) in prevenzione dai danni. L'errore più grande che si può fare è pensare di essere a posto, di avere i propri dati al sicuro. Questo non è mai vero! Tutti i dati esposti in qualche modo sulla rete sono a rischio e i malviventi hanno troppa fantasia, tralasciando gli errori umani di chi opera sui dati! Molta strada c'è ancora da fare.

14. it.wikipedia.org/wiki/Penetration_test
15. it.wikipedia.org/wiki/Phishing

LA SICUREZZA DEI DATI PERSONALI NELLA PRATICA MEDICA

Manlio Cammarata
giornalista specializzato in informatica giuridica e diritto delle tecnologie

Può sembrare inappropriato o superfluo parlare ai medici di protezione dei dati personali, poiché il segreto sulle condizioni di un paziente è un pilastro della professione. Tuttavia l'uso generalizzato di sistemi informatici e una pesante normativa specifica, che si accumula da più di un quarto di secolo, impongono una ricognizione almeno sugli aspetti generali della protezione dei dati, in particolare per la parte relativa alla sicurezza.

La sicurezza dei dati (personali e non) deve essere guardata sotto due aspetti: tecnico e giuridico. L'aspetto tecnico si articola nella cura del "ciclo di vita" del dato: riservatezza, integrità, resilienza dei sistemi di conservazione ed elaborazione; poi il tracciamento delle operazioni compiute sul dato (chi ha fatto cosa e quando), le procedure di recupero e *disaster recovery* in caso di incidenti...

L'aspetto giuridico è speculare a quello tecnico e altrettanto complesso. Riguarda da una parte gli obblighi di protezione di natura tecnica, e dall'altra una serie di adempimenti, spesso di natura sostanzialmente burocratica, che coinvolgono il titolare del trattamento e le persone che operano sotto la sua autorità, oltre ai soggetti - diversi dai pazienti - da quali riceve o ai quali deve trasmettere i dati.

L'adozione e la documentazione delle procedure di trattamento dei dati personali e delle misure di sicurezza obbligatorie richiedono le competenze coordinate di un tecnico e di un esperto di diritto, soprattutto se sono presenti "dati particolari", come quelli relativi allo stato di salute.

La normativa sulla protezione dei dati personali è vasta e complessa. Le disposizioni fondamentali sono contenute nel **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)**, meglio noto come GDPR (*General Data Protection Regulation*); al GDPR si aggiunge il **Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 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** (noto come *Codice privacy*).

La normativa italiana sulla protezione dei dati personali è contenuta in tre distinti provvedimenti: il GDPR europeo, il Codice privacy aggiornato e il decreto legislativo di adeguamento del Codice stesso al GPR, per un totale di oltre 80.000 parole

Già dai titoli chilometrici si intuisce la complessità della normativa. Alcuni dati approssimativi sono utili per intuirne le dimensioni: il GDPR si compone di circa 30.000 parole; il Codice "adeguato" al GDPR arriva a 27.000. A questi testi di base si devono aggiungere i "considerando" del Regolamento UE, che conta circa 24.000 parole.

In sostanza la normativa italiana sulla protezione dei dati personali è contenuta in tre distinti provvedimenti: il GDPR europeo, il Codice privacy aggiornato e il decreto legislativo di adeguamento del Codice stesso al GPR, per un totale di oltre 80.000 parole. E si deve ancora aggiungere la valanga di provvedimenti del Garante, che si accumulano dal 1997 e hanno raggiunto un numero ormai incalcolabile.

Il mancato rispetto delle disposizioni comporta l'applicazione di sanzioni amministrative anche molto pesanti e, in alcuni casi, anche penali. Oltre, naturalmente, all'obbligo di risarcimento di eventuali danni in sede civile.

Infine va tenuto presente che le norme di cui parliamo non sono sulla privacy (intesa come riservatezza e come controllo sulle informazioni che riguardano una persona), ma sul trattamento dei dati personali. La protezione della vita privata è un effetto (non sempre raggiunto) della protezione dei dati. E questo aiuta a capire perché molte disposizioni appaiono meri adempimenti burocratici.

PER CAPIRE LE NORME

Prima di affrontare nelle linee essenziali il problema della protezione dei dati personali (e soprattutto dei dati che interessano il medico - dati "particolari"), è utile fissare l'esatto significato dei termini usati dalle norme. Qui ci limitiamo a poche definizioni essenziali.

Dato personale[I]. Qualsiasi informazione che riguarda una persona identificata o identificabile (il dato anonimo o anonimizzato non è un dato personale, ma lo è il dato "pseudonimizzato", perché dallo pseudonimo si può risalire all'identità della persona).

Spesso, soprattutto nelle cronache giornalistiche, i dati personali vengono indicati come "dati sensibili". È un errore che può causare malintesi anche gravi, perché nella normativa sono chiamati "sensibili" quelli che il GDPR definisce come "dati particolari".

Dato particolare[II]. È un dato la cui conoscenza da parte di altri può recare un grave pregiudizio per l'interessato. Per esempio le opinioni politiche, la religione, l'orientamento sessuale e tutte le informazioni relative allo stato di salute. Il trattamento dei dati particolari è vietato in linea di principio, ma con numerose eccezioni, in particolare quando è previsto da norme di legge o con il consenso informato dell'interessato. Ed è soggetto a particolari cautele di riservatezza e di sicurezza.

In conclusione, secondo l'attuale normativa, ci sono due classi di dati: a) dati personali e b) dati particolari.

Trattamento[III]. Qualsiasi operazione o insieme di operazioni compiute su un dato o su un insieme di dati personali. Attenzione: la semplice registrazione di un dato personale su un foglio di carta costituisce "trattamento", e ricade nelle previsioni della normativa, solo se il dato è destinato a essere inserito in un archivio (cartaceo o automatizzato).

Interessato. La persona fisica, identificata o identificabile, alla quale si riferisce il dato personale.

Titolare del trattamento[IV]. La persona, fisica o giuridica, che dispone dei dati e determina i fini e le modalità del trattamento.

Responsabile del trattamento[V]. È un soggetto esterno all'organizzazione del Titolare, al quale il Titolare stesso affida una o più operazioni di trattamento. Può essere una persona fisica o un'azienda, deve ricevere istruzioni specifiche ed è soggetto al controllo da parte del Titolare.

Responsabile della protezione dei dati[VI]. Noto come "DPO" (*Data Protection Officer*), è un soggetto che ha il compito di consigliare il Titolare, controllare la regolarità dei trattamenti e dell'efficacia delle misure di protezione dei dati e di verificarne l'applicazione. Può essere un dipendente, un consulente esterno o anche una società. È il punto di contatto tra il Titolare e il Garante per la protezione dei dati personali. È nelle sue competenze anche la formazione (obbligatoria) del personale addetto al trattamento dei dati. In ogni caso, la responsabilità per i trattamenti resta in capo al Titolare.

Attenzione: è importante non confondere il Responsabile del trattamento con il Responsabile della protezione. Il primo tratta i dati per conto del Titolare, il secondo si occupa della protezione dei dati stessi.

Garante per la protezione dei dati personali[VII]. È una "autorità di controllo indipendente", inserita nel nostro ordinamento dall'Unione europea. Ha diversi compiti. Per quello che ci riguarda in questa sede, verifica la regolarità dei trattamenti e sanziona le infrazioni. Inoltre emana provvedimenti che interpretano e applicano le norme del GDPR e del Codice italiano. ▶

I. GDPR Art. 4. «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 rife-rimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on-line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;»

II. GDPR, art 9. «1. È vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convin-zioni 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 perso-na.»

III. GDPR, art. 4. «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la struttura-zione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;»

IV. GDPR, art, 4. «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o in-sieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trat-tamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici appli-cabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;»

V. GDPR, art. 4 «la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;»

VI. GDPR art. 37. «1. Il titolare del trattamento e il responsabile del trattamento designano sistematicamente un respon-sabile della protezione dei dati ogniqualvolta:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su lar-ga scala; oppure

c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su lar-ga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.»

VII. Alle autorità di controllo sono dedicati gli articoli da 51 a 84 del GDPR e al Garante italiano gli articoli da 153 a 160 del Codice.

I PRINCÌPI FONDAMENTALI DELLA PROTEZIONE DEI DATI

In ambito medico, e cioè in qualsiasi struttura ospedaliera, RSA, ambulatorio del medico di base o del libero professionista, sono trattati sistematicamente soprattutto dati "particolari". Perciò è necessario rispettare scrupolosamente tutte le disposizioni, in particolare quelle relative alle misure di sicurezza, oltre ai principi generali che il GDPR elenca all'art. 5. È opportuno leggere con attenzione il testo di questo articolo, perché intorno ai "principi" ruotano tutti i meccanismi di protezione dei dati. Infatti i provvedimenti sanzionatori del Garante della protezione dei dati personali sono spesso motivati dal mancato rispetto di uno o più principi.

Articolo 5: Principi applicabili al trattamento di dati personali

1. I dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);

In ambito medico, e cioè in qualsiasi struttura ospedaliera, RSA, ambulatorio del medico di base o del libero professionista, sono trattati sistematicamente soprattutto dati "particolari"

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);

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 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»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).

In sintesi, i princìpi sono i seguenti:

a) liceità, correttezza e trasparenza

b) limitazione della finalità

c) minimizzazione dei dati

d) esattezza

e) limitazione della conservazione

f) integrità e riservatezza

g) responsabilizzazione

In genere i Titolari pongono attenzione soprattutto ai punti a) e f) e si preoccupano per il punto g), che comporta in primo luogo la necessità di documentare per iscritto i criteri seguiti nel trattamento ed eventuali eventi avversi (che impongono ulteriori adempimenti).

L'esperienza indica che sono i punti b), c) ed e) quelli che provocano più spesso situazioni… imbarazzanti.

Infatti sono abbastanza frequenti i casi di trattamento per fini non previsti all'atto della raccolta dei dati e spesso si raccolgono più dati di quelli strettamente necessari, o si conservano anche quando non servono più per le finalità stabilite all'inizio.

La lettera f) presenta un aspetto critico, da considerare con attenzione: la normativa precedente al GDPR elencava una serie di "misure minime" (davvero minime, ma illustrate da un "documento programmatico sulla sicurezza"), il cui rispetto documentato poteva bastare in prima battuta a escludere una responsabilità del Titolare; ora la norma parla di "misure adeguate". Che significa "adeguate"? Significa che, se si è verificato un incidente, le misure non erano "adeguate" (se lo fossero state l'incidente non si sarebbe verificato!). E tocca al Titolare dimostrare il contrario, come si evince dal secondo comma dello stesso articolo, che sancisce il principio di "responsabilizzazione".

INFORMAZIONI, CONSENSO INFORMATO E DIRITTI DELL'INTERESSATO

Come abbiamo visto, il trattamento di dati personali è lecito se (fra l'altro) si verificano almeno una delle condizioni essenziali: a) il Titolare è soggetto a un obbligo legale, b) è necessario per l'esecuzione di un contratto e c) se c'è il consenso informato e documentato o documentabile dell'Interessato.

Quest'ultimo è un aspetto critico, soprattutto quando sono trattati, come nel caso delle attività sanitarie, dati "particolari". È un campo nel quale sono frequenti gli interventi sanzionatori del Garante: il consenso può definirsi "informato" quando le informazioni sono complete e comprensibili da parte dell'Interessato. In genere si fa ricorso a formulari, predisposti dal singolo Titolare o da associazioni di categoria. Occorre prestare molta attenzione alla completezza delle informazioni: si devono specificare, fra l'altro, i soggetti ai quali i dati possono o devono essere comunicati (aziende sanitarie, strutture regionali, Ministero della salute…).

Consensi separati devono essere richiesti per trattamenti non necessari (per quelli necessari non occorre il consenso). Si deve tenere sempre presente che, per la normativa, l'Interessato è "padrone assoluto" dei propri dati, con effetti a volte discutibili. Per esempio, è noto che l'Interessato può negare il consenso all'inserimento di informazioni nel FSE (fascicolo sanitario elettronico), al punto che persino il medico di base può essere all'oscuro del fatto che un suo paziente è affetto da AIDS.

Infine si deve ricordare che l'Interessato ha il diritto di sapere tutto sui propri dati personali, dalla loro origine alle modalità di trattamento e conservazione. Inoltre ha sempre il diritto di opporsi al trattamento, di chiedere la cancellazione o la correzione di dati, e infine di rivolgersi al Garante nel caso in cui ritenga che i suoi dati non siano trattati in modo corretto[VIII].

CHI È IL TITOLARE DEL TRATTAMENTO?

Capire chi è il Titolare di un trattamento è essenziale per l'attribuzione dei compiti e delle responsabilità per i diversi trattamenti. Nel caso della libera professione in uno studio privato, è chiaro che il titolare del trattamento è il medico. Ma il medico, in molti casi, trasmette le informazioni (ridotte al minimo indispensabile secondo il principio di minimizzazione dei dati) ad altri soggetti, per esempio a un laboratorio di analisi cliniche. E di questo deve tenere conto nel rendere le informazioni, anche se non richiedono un consenso specifico.

Nella sanità pubblica la situazione è più complicata. La titolarità dei dati personali che tratta il medico di base è, in linea di principio, in capo alla ASL o ai servizi della Regione, o anche al Ministero della salute. Dunque il medico riveste la funzione di Responsabile del trattamento e dovrebbe ricevere istruzioni (e subire i controlli) da parte di tali strutture. Tuttavia raccoglie e tratta direttamente alcuni dati dei suoi pazienti, per i quali sarebbe Titolare di un proprio trattamento. Il condizionale è dovuto al fatto che la situazione è diversa da una Regione all'altra e, in qualche caso, piuttosto confusa.

Ma anche a livello nazionale non è facile districarsi tra norme e attribuzioni. Per esempio, dei dati contenuti nel FSE sono titolari il Ministero della salute, le Regioni e le ASL. A chi spetta rendere le informazioni e acquisire e documentare il consenso, verificare l'esattezza dei dati, soddisfare le richieste di rettifica o cancellazione? Ogni Regione ha le sue regole e non sempre sono facilmente accessibili ai cittadini-pazienti, oltre che agli operatori sanitari.

VIII. GDPR, articoli da 12 a 21.

Non finisce qui, perché il GDPR e il Codice contengono una serie di norme specifiche per i trattamenti di dati relativi alla salute. L'esame di queste norme richiederebbe un discorso a sé. Qui basta ricordare che il divieto di trattare i dati particolari non si applica «quando 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…»[IX].

QUANDO È OBBLIGATORIA LA NOMINA DEL RESPONSABILE DELLA PROTEZIONE?

La nomina del Responsabile della protezione dei dati[X] di solito indicato come "DPO" (*Data Protection Officer*) è sempre obbligatoria per gli enti pubblici e, in determinati casi, per i privati, quando il trattamento comporta "il monitoraggio regolare e sistematico degli interessati su larga scala". Inoltre - questo è il punto che ci interessa - quando "le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9", cioè anche i dati sulla salute.

La nomina del Responsabile della protezione dei datiX di solito indicato come "DPO" (Data Protection Officer) è sempre obbligatoria per gli enti pubblici e, in determinati casi, per i privati

Questo non significa che ogni medico sia obbligato a designare un DPO: il singolo professionista o il medico di base non trattano dati "su vasta scala", mentre il problema si pone per gli studi in cui operano più medici, oltre che per le strutture sanitarie pubbliche e private (poliambulatori e simili), in cui ci sono molti pazienti e diverse persone che trattano i dati (con le relative conseguenze anche sull'identificazione del Titolare, sugli incarichi ai Responsabili del trattamento, sulla formazione eccetera).

In questi casi, anche se le dimensioni dell'organizzazione non sono tali da configurare trattamenti "su vasta scala", la nomina del DPO è fortemente consigliata. Il numero e la complessità degli adempimenti è tale da richiedere l'opera di un esperto di diritto ben ferrato in materia di protezione dai dati. E l'esperto di diritto deve lavorare a stretto contatto con un esperto di sicurezza informatica, per tutto quello che riguarda la protezione "tecnica" dei dati.

La nomina del DPO non è un mero adempimento burocratico. Il comma 5 dell'art. 37 del Regolamento specifica che "Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39". Se si verifica un incidente che mette a rischio la protezione dei dati, la responsabilità è sempre del Titolare, anche per avere scelto un DPO privo delle qualità professionali richieste per tale compito.

I (LARGHI) CONFINI DELLA SICUREZZA DEI DATI

Siamo così giunti al nocciolo della questione: la sicurezza dei dati. Abbiamo visto che i dati devono essere trattati con modalità che ne assicurino la riservatezza, la protezione da alterazioni, perdite o cancellazioni fortuite. I "nemici" della protezione dei dati appartengono a due diverse categorie: a) i nemici interni, cioè coloro che, per negligenza più

IX. GDPR, art. 9, comma 2, lettera h.

X. GDPR, articoli 37, 38 e 39.

che per malafede, lasciano che le informazioni siano alla portata di chi non è autorizzato a trattarle o ne provochino l'alterazione o la distruzione e b) i nemici esterni, cioè quella che viene generalmente definita come "pirateria informatica" e che provoca danni gravissimi, anche su larga scala, come si è visto, purtroppo, nel corso della pandemia da Covid-19.

La vulnerabilità dei sistemi informatici, anche di quelli non deputati al trattamento di dati personali, è un problema del nostro tempo e lo sarà ancora a lungo. Le dimensioni e la complessità dei sistemi hanno raggiunto livelli critici, tali che per la protezione sono necessarie sofisticate misure tecnologiche e competenze professionali altissime. Le notizie che si susseguono di attacchi su vasta scala, che mettono in crisi funzioni essenziali della società (come la distribuzione dell'energia elettrica, per fare un solo esempio) devono essere prese in considerazione con la massima serietà. E devono convincere all'adozione di misure preventive. Queste non impongono solo l'adozione di "barriere" tecnologiche, ma anche un'attenzione maniacale al rigore delle procedure e alla formazione degli addetti. La distrazione non è ammessa, la superficialità è criminale.

Occorre diffondere la "cultura della sicurezza", tenendo presente che per ogni "incidente" provocato dall'esterno c'è una responsabilità all'interno dell'organizzazione colpita. Per esempio, nel caso di un ormai purtroppo comune attacco *ransomware*, che causa l'impossibilità di accedere ai dati, l'unica soluzione per ripristinare la normale attività in tempi ragionevoli è la disponibilità di copie di sicurezza *off-line* del software e dei dati. *Off-line* significa che le copie devono essere custodite su sistemi non raggiungibili dall'esterno e non direttamente collegate ai sistemi che devono essere protetti. E che devono essere aggiornate periodicamente secondo schemi ben noti agli esperti di sicurezza.

Un discorso a parte merita il dilemma tra trattamenti manuali (carta e penna, per intenderci) e trattamenti informatici. Nei trattamenti cartacei il punto essenziale è che nessun documento che riporti dati sensibili deve essere lasciato alla vista di estranei o comunque facilmente accessibile. Cassetti e schedari sempre chiusi a chiave, istruzioni scritte per persone eventualmente abilitate a consultare i documenti. La stanza in cui siano presenti documenti cartacei con dati personali di uno o più pazienti, in assenza del medico o di un suo ▶

incaricato, deve essere chiusa a chiave ed è necessario documentare i nominativi delle persone che possono accedervi (e impartire loro, per iscritto, le istruzioni per la protezione dei dati, l'obbligo di chiusura della stanza ecc.). Alla fine dei conti, i trattamenti informatici sono più semplici. Basta infatti l'uso di password (da cambiare periodicamente), assegnate alle persone che sono autorizzate all'accesso, ed eventualmente all'inserimento e alla modifica dei dati. È necessaria anche la documentazione automatica di chi ha fatto cosa (i cosiddetti *log*) per ottenere un adeguato livello di protezione del dati.

In ogni caso è importante la formazione del personale. Soprattutto in una struttura più grande dello studio di uno o due professionisti, come un poliambulatorio, fino al grande ospedale, le persone che trattano dati sanitari possono essere molte e devono essere a conoscenza delle procedure (e del rischio elevato) nel trattamento di dati "particolari". Si deve sempre considerare che un *data breach*, cioè una violazione dei dati può avere conseguenze devastanti.

Un dettaglio importante: qualsiasi violazione della riservatezza dei dati, reale o anche solo potenziale, deve essere notificata al Garante e ai singoli interessati e può portare a sanzioni, anche penali nei casi in cui si verifichi un danno per gli Interessati.

La protezione dei dati deve essere sempre *by design* e *by default*. Significa che i sistemi e le procedure devono essere progettati e impiegati in funzione della sicurezza. Un esempio: la corrispondenza tra medico e paziente con l'uso di sistemi non sicuri, come i *social* o la posta elettronica affidata a Gmail[XI] o altri sevizi gratuiti offerti dalle *big tech*, sono di per sé procedure a rischio, quindi costituiscono violazioni delle regole sulla protezione dei dati e possono essere sanzionate dal Garante, anche se non si verificano incidenti.

In conclusione, il medico ha una particolare responsabilità nella protezione dei dati personali dei pazienti e deve seguire procedure abbastanza complesse per proteggerli. E per proteggere se stesso dal rischio di grattacapi e sanzioni. Il consiglio, come sempre, è di dedicare qualche ora allo studio della normativa e rivolgersi a un esperto di sicurezza per l'organizzazione dello studio professionale (per non parlare di una struttura più complessa). Sarebbe compito delle Regioni e delle strutture territoriali, in quanto Titolari di molti trattamenti, svolgere regolarmente programmi di informazione e formazione dei medici sulla protezione dei dati personali.

MEDICI E TECNOLOGIA. COMPORTAMENTI E STRUMENTI APPROPRIATI

Michele Bottari
Cofondatore del gruppo EXIT - Mi riprendo la privacy!

LO SMARTPHONE: LA RIVOLUZIONE TECNOLOGICA (QUASI) INVISIBILE

Lo smartphone è lo strumento più tecnologico mai creato. O, almeno, è il migliore tra quelli che gli umani possono permettersi. Vi permette di telefonare, come i cellulari di penultima generazione, ma anche di andare su Internet; di messaggiare a costo zero con testi, immagini, video e videochiamate; di registrare le conversazioni o i concerti; di fotografare e fare video, con una qualità che pochi anni fa nemmeno immaginavate[1]; di illuminare una stanza buia a giorno; di scansionare documenti; di avere una vita sociale artificiale; di controllare il vostro percorso, quanti chilometri avete fatto e di trovare una strada; di sapere l'orario di chiusura del negozio dove vi state recando; di riconoscere una costellazione in cielo.

E tutto questo, lo fa gratis, o compreso nel costo del vostro abbonamento. Come è possibile che tutto questo ci piova dal cielo gratis? La risposta non è immediata, e, per averla, dobbiamo rovesciare il concetto di proprietà: lo smartphone che abbiamo acquistato, talvolta a caro prezzo, non è nostro, ma ci è stato assegnato, diciamo, in comodato. Prima di tutto non è l'esito di una libera scelta: quanti di noi si possono permettere, al giorno d'oggi, di non avere il telefonino intelligente? Senza di esso, non riusciremmo a effettuare le operazioni di banca sul nostro conto corrente, non potremmo esercitare la nostra identità digitale attraverso lo SPID, e di conseguenza non potremmo interagire con la Pubblica Amministrazione. Senza di esso saremmo letteralmente tagliati fuori dai contesti sociali, le mamme della scuola elementare, gli amici del calcetto, che ormai comunicano solo via chat di gruppo, ovviamente con strumenti proprietari che fanno commercio di dati.

1. Un esempio, il film Unsane, del 2018, diretto da Steven Soderbergh, con protagonista Claire Foy, ha una particolarità: le sue riprese sono state effettuate interamente con uno smartphone. E si tratta di una pellicola di buon livello tecnico, per quanto riguarda la fotografia. https://www.badtaste.it/cinema/video/unsane-trailer-steven-soderbergh-claire-foy/

In secondo luogo, non possiamo fare niente, con essi, se non all'interno di un percorso tecnologico estremamente limitato, da cui non è possibile uscire, e che comporta il drenaggio totale di tutti i nostri dati, soprattutto dei dati di coloro con cui siamo in contatto. E questo, per una persona che lavora in un ambito delicato, che ha a che fare con dati estremamente sensibili dei propri utenti (è questo il caso dei medici), è un problema legale e deontologico assolutamente sottovalutato.

Ma dietro lo smartphone c'è un mondo di servizi che sta ridisegnando l'economia mondiale. Nei primi anni 2010, alla presentazione dell'iPhone, Apple introdusse sì sul mercato uno strumento concreto, di quelli che si possono toccare, diciamo. Ma il grosso dell'investimento, da lì e per gli anni a venire, sarebbe stato nella creazione di un ecosistema che fungesse da supporto per i (presunti) possessori dello smartphone. Fu ulteriormente sviluppato così iTunes (che era già in essere per i PC), e successivamente iCloud. Quest'ultimo servizio oggi comprende praticamente tutta la personalità di un utente Apple: i servizi Mail, Contatti, Calendario, backup automatico, il tutto sincronizzato automaticamente. Al primo avvio del dispositivo, si dà sostanzialmente l'incarico a Apple di amministrare tutta la nostra vita. Da ora e per sempre.

Siccome i dispositivi della mela erano (e sono rimasti) piuttosto costosi, era rimasta scoperta una 'piccola' categoria di utenti, più dell'80% della popolazione mondiale. In questa nicchia, si buttò a pesce un altro colosso del Web, Google, con la creazione del sistema operativo Android, che da allora equipaggiò la quasi totalità degli smartphone non-Apple. Ovviamente, Google replicò l'azione del concorrente, creando il proprio ecosistema di raccolta dati, la Google Suite, comprendente Gmail, Drive, e tutto ciò che può servire all'utente Android, aggiungendo Google Maps, strumento che di lì a poco avrebbe sostituito i navigatori che equipaggiavano quasi tutte le automobili del mondo, ovvero Garmin e TomTom.

Dietro lo smartphone c'è un mondo di servizi che sta ridisegnando l'economia mondiale

Naturalmente, i profitti di queste due aziende, da allora, diventarono esorbitanti, dando luogo alla formazione di ricchezze mai viste in precedenza. Ricchezze che si possono spiegare soltanto con una massiccia e costante messa a frutto di dati personali, prelevati dagli smartphone senza una completa comprensione da parte dell'utente. Nella spartizione del bottino della raccolta di dati, consistente in svariate migliaia di miliardi di euro l'anno (sull'entità di queste cifre parleremo in seguito), ad Apple e Google si aggregarono presto Amazon (massimo operatore nel settore dell'e-commerce e dei servizi web alle aziende), Facebook, regina incontrastata dei social-media, Microsoft (regina incontrastata del software per PC), più alcune aziende con sede in Cina, territorio non coperto dai colossi sopra nominati. Per questa allegra compagnia è stato da noi coniato il termine "Bestia", date le sinistre somiglianze con l'essere malvagio dipinto da San Giovanni nella sua Apocalisse.

Queste aziende prelevano tutti i nostri dati, li danno in pasto alle loro intelligenze artificiali e li monetizzano fornendo pubblicità sempre più mirate e personalizzate. Lo scopo di tutto ciò è semplicemente incrementare un archivio (database) con una serie di dossier dettagliati su ognuno di noi, per scopi commerciali.

Il risultato di questo dominio è già oggi devastante. Questa pratica sta portando alla distruzione dell'economia, del lavoro e dell'ambiente, con la rottura dei meccanismi delicati che regolano i sistemi complessi in cui viviamo. Molti temono che si possa instaurare un controllo politico o poliziesco, a partire proprio dal possesso di questi dati. Analizziamo le conseguenze dell'onnipervasività di questo uso di dati sulla privacy e sulle conseguenze penali e civili di chi si rende responsabile di questo prelievo. E comunque, non è nostra intenzione analizzare l'aspetto del controllo politico, pur importante e fondato, in questa trattazione. Ciò che ci interessa è verificare le conseguenze dell'onnipervasività di questo prelievo sulla privacy e sulle conseguenze penali e civili di chi si rende responsabile di questo prelievo.

STRUMENTI SENZA CULTURA

Chiunque si metta alla guida di un autoveicolo senza la patente rischia conseguenze penali piuttosto pesanti. Questo fatto è interiorizzato da tutti, ed è giustificato dal pericolo che comporta l'uso improprio o imperito di una vettura per se stessi e per gli altri. Ma per lo smartphone, strumento anche più pericoloso dell'automobile[2], non è richiesto alcun documento di attestazione di abilità. Eppure i genitori lo comprano, o lo fanno usare ai bambini, ormai di qualunque età.

E questo è solo l'aspetto più imbarazzante e pericoloso di una mancanza di cultura, diffusa ormai a tutte le persone, a qualunque latitudine. Quando una classe politica comunica via social con i propri elettori, quando la campagne informative di intere istituzioni sono portate avanti a colpi di post su Facebook o su Twitter, significa che non è affatto chiaro il fatto che si tratta di canali web privati, proprietari, il cui scopo è quello di fare profitti su una pratica che ha chiari sospetti di illegalità: quella della raccolta dati in violazione di qualunque principio di riservatezza.

Medici, avvocati, fiscalisti, ingegneri, e molte altre categorie professionali, scambiano informazioni con i propri clienti, pazienti, assistiti, usando canali di messaggistica e posta elettronica i cui titolari incamerano dati sensibili con estrema voracità, mettendo a repentaglio la riservatezza di tutte queste persone.

Sono passati poco più di dieci anni da quando questi strumenti hanno iniziato a invadere la nostra vita, ma sembrano passati secoli. L'autorità acquisita, senza costrutto, da Facebook, Twitter e compagnia bella è indiscussa. Spesso, si parla di violazioni di regolamenti interni di queste piattaforme, come se fossero delle vere e proprie violazioni di legge. Nel contempo, prassi assolutamente scriteriate, come fotografare i propri figli minori, ed esporli al pubblico, magari nudi, al mare, intenti a fare il bagnetto, sono ampiamente in uso, alimentando le bacheche personali di milioni di pedofili. Ma questo fatto non danneggia la politica commerciale del social-medium, e quindi non è severamente vietata.

Questa mancanza di cultura è dovuta, evidentemente, all'ascesa di questi servizi, che è stata troppo veloce e possente, per poter essere controbilanciata da un'adeguata crescita della consapevolezza di questi mezzi. Per cui, il professionista che si trovi a interagire con i cittadini, troverà davanti a sé persone non assolutamente avvezze all'uso di questi strumenti, e da loro certo non arriverà alcun tipo di precauzione in termini di privacy. Sta dunque al professionista adottare, e in certi termini imporre, l'uso di canali sicuri per inviare documenti sensibili, come ricette, referti…, la cui divulgazione costituirebbe un danno alla riservatezza della persona.

2. Si vedano le voci di Wikipedia Italia relative a fenomeni come cyberbullismo (https://it.wikipedia.org/wiki/Cyberbullismo), revenge porn (https://it.wikipedia.org/wiki/Revenge_porn). Si veda inoltre la sequenza di morti sospette, ritenute istigate da una sfida (challenge) circolante sul social medium cine se TikTok (https://www.panorama.it/news/black-challenge-come-funziona-il-gioco-che-ha-ucciso-igor-maj)

UN BUSINESS DI PROPORZIONI COLOSSALI

La Bestia, dicevamo, è costituita da un ridotto numero di aziende, i cui fatturati, profitti, e capitalizzazioni stanno crescendo in maniera esponenziale, divorando l'economia tradizionale. Qualcuno lo chiama il 'capitalismo della sorveglianza' [3]

Symbol	Company	Cap Rank 10-11-21	Market Cap 10-11-21
AAPL	Apple	1	2,360.7
MSFT	Microsoft	2	2,211.1
GOOGL	Alphabet	3	1,852.0
AMZN	Amazon	4	1,644.1
FB	Facebook	5	917.6
TSLA	Tesla	6	784.0
BRK.A	Berkshire Hathaway	7	636.1
TSM	Taiwan Semiconductor	8	571.8
NVDA	NVIDIA	9	517.4
JPM	JPMorgan Chase	10	497.9

La figura qui sopra mostra la classifica, a ottobre 2021, delle prime dieci aziende del mondo per *market cap*, ovvero per valore del capitale azionario. Questa classifica mostra molto del sistema economico che attualmente domina il mondo. Su dieci aziende, otto sono del comparto tecnologico/web, e solo due (la Berkshire Hataway e la JP Morgan) fanno parte del settore della finanza. Questo significa che Wall Street non è riuscita a papparsi Silicon Valley, ma che è avvenuto invece il contrario.

Le corporation tecnologiche occupano le prime sei posizioni, le prime quattro posizioni implicano valori di capitale tra i 1500 e i 2400 miliardi di dollari. L'insorgenza di questi poteri rappresenta una debacle totale della politica, che non riesce nemmeno a far pagare loro le tasse, nonostante gli utili da capogiro che queste generano in tutti i paesi del mondo. Ma soprattutto, gli Stati nazionali non riescono a tutelare la privacy dei propri cittadini, visto che queste aziende traggono il loro potere e il loro denaro dalla più palese e clamorosa violazione della riservatezza che si sia mai vista.

La questione presenta problemi in molteplici direzioni. Innanzitutto è sempre un male che i dati siano travasati verso server dall'altra parte dell'Atlantico, e quindi fuori della giurisdizione di Italia e Unione Europea. Questo semplicemente perché non è necessario, e il non-necessario, in termini di riservatezza, è un pericolo.

3. *Shoshana Zuboff: Il capitalismo della sorveglianza -Il futuro dell'umanità nell'era dei nuovi poteri, Luiss University Press, 2019*. La sociologa statunitense traccia con precisione i tratti di questa nuova, formidabile macchina da soldi. Un'architettura di sorveglianza, ubi-qua e sempre all'erta, che analizza e indirizza il nostro comportamento per fare gli interessi di questi colossi. Un potere enorme che sfida la democrazia e la libertà. Zuboff, curiosamente, commette l'ingenuità (o la colpevole malizia) di assolvere Apple (che invece, per noi è tra le principali responsabili, se non la principale in assoluto) da questo esercizio di dominio. Ma, a parte questo, il suo è uno spaccato illuminante di come la Bestia sia riuscita, gradualmente, a prendere in mano il nostro destino.

Le aziende della Bestia non hanno il diritto di avere accesso a questi dati, perché non sono né benevoli, né sicure. Sulla benevolenza: vi è evidenza di strategie precise di invadere a gamba tesa la sanità pubblica, come al solito con un dispiegamento di risorse finanziarie che renderà difficile contrastarle. A ben vedere, questo è il mestiere della Bestia, entrare a gamba tesa nei settori economici, e spaccarli. Queste aziende hanno scardinato interi settori economici, dando gratuitamente servizi che, fino al giorno prima, i concorrenti distribuivano a pagamento. E la qualità è addirittura maggiore.

La sanità è notoriamente un affare da miliardi di euro, è quasi inutile dirlo, ma ha sempre contato sulla professionalità dei suoi operatori, fatto che rende piuttosto difficile scalzarli dalle loro competenze. A differenza del passato, invece, ora la Bestia può contare su un mix di 5G, ovvero Internet decente in ogni parte del globo, Internet delle Cose (in particolare i dispositivi *wearable*), e Intelligenza Artificiale. Questo rende possibile una trasformazione tecnologica del settore sanitario.

Molte funzioni sanitarie chiave stanno iniziando a utilizzare l'intelligenza artificiale per determinare potenziali diagnosi e decidere la prognosi per un paziente. Un ausilio in più, naturalmente, ma anche un problema di svilimento delle capacità professionali. Ma la scommessa della Bestia sembra puntare sui *wearable*: utilizzando soluzioni indossabili, braccialetti o smartwatch, la Bestia può monitorare i pazienti e raccogliere dati per migliorare l'assistenza personalizzata e preventiva.

L'involuzione del settore ci viene confermata da Wired, nell'articolo *Come l'intelligenza artificiale rivoluzionerà il sistema sanitario*[4], che ci informa che Google e Apple sono in prima linea nella ricerca sulla sanità. Ma ci dice anche, tra le righe, che l'intelligenza artificiale sarà usata per fare diagnosi più rapidamente, e che il futuro vedrà "assistenti virtuali alimentati a intelligenza artificiale." Le intenzioni della Bestia sono più chiare nell'intervista ad Amy Webb[5], professoressa di previsione strategica alla New York University, che prevede che i colossi tech "smantelleranno il settore della sanità, anzi, lo stanno già facendo." Le loro strategie comprendono l'apertura di cliniche, lo sviluppo di dispositivi per il fitness (i cosiddetti indossabili, di cui abbiamo detto sopra) in grado di monitorare i dati sulla salute e la creazione di team specializzati. "Le tech company," dice Webb, "godono di un vantaggio che i player del settore sanitario non hanno: le questioni normative a cui i player tradizionali devono far fronte non valgono allo stesso modo per loro," (qualcuno ricorda Uber contro i tassisti?), per esempio le norme che tutelano la privacy dei pazienti. Si inizia dagli USA, dove c'è terreno facile, ma poi arriverà anche da noi.

Anche sulla sicurezza dei dati all'interno dei server della Bestia ci sarebbe da ridire: molte persone si affidano ai servizi di chat, posta elettronica, cloud di Amazon, Apple, Facebook, Google nella convinzione che, essendo all'interno di aziende notevolmente capitalizzate, i dati siano intrinsecamente sicuri. Ciò non risponde a verità: molto spesso questi dati sono messi a disposizione dalle piattaforma per scopi di mero lucro. È stato il caso di Cambridge Analytica, l'azienda che, nel 2016, fu in grado di manipolare i risultati elettorali delle elezioni presidenziali americane e del referendum britannico sull'uscita dall'UE. Il metodo utilizzato usava il *data mining*, combinato con gli studi della psicometria, lo studio dei comportamenti umani, per individuarne una precisa personalità ed impacchettare messaggi estremamente precisi che colpirono le loro debolezze e paure. Fu accertato l'uso da parte dell'azienda delle informazioni personali su 87 milioni di utenti, soprattutto statunitensi, prelevate da Facebook, senza autorizzazione. Facebook, in realtà, aveva saputo di questa violazione della sicurezza per due anni, ma non fece nulla per proteggere i suoi utenti.

4. Wired: Come l'intelligenza artificiale rivoluzionerà il sistema sanitario

https://www.wired.it/scienza/medicina/2019/02/28/intelligenza-artificiale-sistema-sanitario/

5. Business Insider: A top expert on disruption explains how Amazon, Google, and Apple will 'completely dismantle' the healthcare in-dustry - and says the wheels are already in motion

https://www.businessinsider.com/how-tech-giants-will-dismantle-healthcare-industry-quantitative-futurist-2020-1?r=US&IR=T

Tutto ciò dimostra che la delega data a uno di questi colossi, per la protezione dei dati dei nostri utenti, è certamente pericolosa. Nessuna di queste aziende userà la propria potenza per la tutela dei dati, dal momento che è proprio sul commercio di questi dati, con ogni mezzo, lecito o illecito, che si fondano i loro faraonici profitti.

LA SITUAZIONE DI CHI OPERA CON DATI SENSIBILI (OVVERO: COSA POSSONO FARE I MEDICI)

Il medico, e più generalmente qualunque operatore professionale che si trovi a gestire dati sensibili dei suoi utenti è tra l'incudine e il martello. Da un lato, le sempre più pressanti disposizioni legislative spingono a una tutela sempre più esasperata della privacy, dall'altro, le tecnologie di fatto obbligatorie per tutta l'utenza, e quindi anche per la categoria, sono in agguato, pronte a drenare quantità inimmaginabili di dati sensibili, come sono quelli relativi alla salute. Questo fatto rende i medici responsabili, di fronte alla legge, ma anche di fronte alla propria coscienza. Lo scopo di questi suggerimenti è fornire strumenti per evitare di essere complici del gigantesco, illegale, sistematico furto di dati che caratterizza questa nostra bizzarra epoca.

Prima di tutto, è bene avere una mentalità attenta e flessibile, evitando gli estremismi. Gli errori da evitare sono sostanzialmente due.

ERRORE N. 1: RIFIUTARE LA TECNOLOGIA

Ragioniamo su alcuni strumenti per evitare di essere complici del gigantesco, illegale, sistematico furto di dati che caratterizza questa nostra bizzarra epoca

Non è possibile stare fuori dal tracciamento della Bestia semplicemente ignorando i moderni strumenti, ne va della nostra vita sociale, ma anche del nostro lavoro, specialmente per chi lavora a contatto con una molteplicità di pazienti, abituati (anche se non consapevoli) ad aver a che fare con la tecnologia. Rifiutarsi di adottare strumenti come le chat, le email, i servizi online, avrebbe conseguenze negative non indifferenti. Siamo completamente immersi nella tecnologia, e rifiutarla porta all'isolamento, sia nei confronti dei pazienti, che ne fanno largo uso, sia nei confronti dei pari, che ostacolerebbe il confronto e la formazione. Occorre, al contrario, un comportamento più attivo, cioè: conoscere profondamente questo diabolico strumento, e prendere le adeguate contromisure per evitare pericoli. È scomodo, ma non abbiamo altra scelta.

ERRORE N. 2: AFFIDARSI ALLA LEGGE

La seconda tentazione a cui non dobbiamo cedere è quella del rispetto pedissequo della legge, primo perché non è sufficiente, secondo perché la burocratizzazione del lavoro che ne seguirebbe, renderebbe impossibile essere efficaci e professionali. Pensare di governare le fughe di dati, semplicemente seguendo la legge, è illusorio: i dati su di noi, e sui nostri contatti, sono talmente mescolati, disaggregati e non localizzabili, perchè è impossibile che lo Stato possa attuare concretamente una politica di privacy per legge. I governi sono due passi indietro rispetto alla Bestia, per motivi strutturali (la tecnologia si evolve troppo velocemente perché le leggi possano seguirla).

Le ridicole e borboniche leggi sulla tutela della privacy (come il GDPR) non possono difendere i professionisti e i medici dalle aziende del Web che si fondano sul prelievo dei dati. Il GDPR si limita sostanzialmente a imporre una serie di inutili e gravosi appesantimenti burocratici. La Bestia, invece, sta ancora ridendo: è da quando è nata che ci fa firmare scartoffie piene di avvisi, che nessuno ha mai letto ma che l'hanno protetta finora. Per lei, basta cambiare qualche parola e il gioco è fatto.

PROTEGGERE I VOSTRI DISPOSITIVI

Veniamo ora alle azioni concrete per proteggere i dati dei pazienti, in maniera attiva. La prima cosa da fare è rendere sicuri i dispositivi che possono contenere i loro dati. Si tratta del PC e del telefonino.

Crittografia

Occorre fare in modo che i dispositivi che conservano i dati dei pazienti siano realmente sicuri. La soluzione migliore consiste nella crittografia. La crittografia del dispositivo mette tutti i file in un formato che non può essere compreso senza prima decifrarli con la chiave corretta, la vostra password o un'analisi di un vostro dato biometrico (impronta digitale, scansione della retina...). La crittografia è una forma di sicurezza davvero tosta, lo dimostra il fatto che le autorità statali di tutto il mondo fanno enormi pressioni sulle società della Bestia nel tentativo di scoraggiarne l'uso.

Per il telefonino

Trovate le opzioni di cifratura sotto i menu Impostazioni -> Sicurezza, dove troverete le opzioni per proteggere i dati su smartphone e scheda microSD, se il dispositivo dispone di uno slot. La crittografia può richiedere un po' di tempo, quindi è meglio iniziare il processo con una batteria piena e un sacco di tempo libero.

Per il PC

Cercate tra le opzioni la parola 'crittografia' e seguite le istruzioni.

Password non troppo deboli

Assieme a blocca-schermo e crittografia, è necessario l'uso di una password forte. Come regola generale, un mix di maiuscole-minuscole, numeri e caratteri speciali (dove consentito) rende la password più sicura. Più lunga è, meglio è. 8 caratteri sono davvero troppo pochi, spostarli fino a 12 o 16 li rende molto più difficili da indovinare.

Una password sicura è un buon inizio, e non deve essere la stessa che usate per altri servizio, come accesso al PC, alla banca, alla casella di posta. Se qualcuno viola un sito in cui siete registrasti con utente e password, può provare a usare questi dati per collegarsi ad altri servizi di cui usufruite, quindi non è molto sicuro affidarsi alla stessa password per tutti i vostri account, app e siti web.

Ricordarsi tante password forti e lunghe è un'impresa titanica, ma potete sempre usare un'app come Keepass DX o TinyKeePass, che offrono una selezione di funzionalità per una maggiore sicurezza, tra cui opzioni di archiviazione sicura delle password, autenticazione a due fattori e supporto multidispositivo.

CANALI DI COMUNICAZIONE E STORAGE DEI DOCUMENTI

Spesso ci si affida alle piattaforme per tutta una serie di servizi che sono comodi e fruibili, come il servizio di posta Gmail, il servizio di messaggistica WhatsApp, il servizio di cloud Google Drive o iCloud. Niente di più sbagliato: affidare a operatori come Google o Apple la posta elettronica, le ricerche web, il calendario, il navigatore satellitare, la traduzione di lingue, la condivisione documenti, foto e video... non è una politica di privacy sana, per i motivi che abbiamo detto sopra: i dati non devono lasciare il dispositivo in cui sono stati caricati, e se avete per forza bisogno di spedirli (anche sul cloud) dovete trovare tecnologie sicure e nelle vostre mani, o in quelle del tecnico che vi segue.

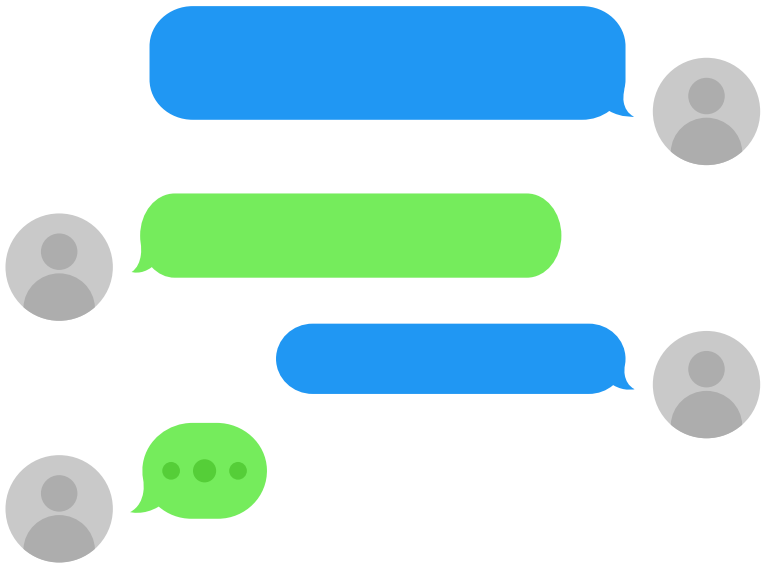
Il guaio è che, per quasi tutti i servizi elencati, Google, Apple, Facebook si collocano ai primi posti per popolarità e qualità. E tutto viene offerto gratis. Per questo rinunciarvi è dannatamente difficile. Il lavoro dovrà essere lento e progressivo. Ricordate che spiare i nostri comportamenti è un business colossale, quindi non è possibile che questi colossi non approfittino della possibilità che date loro. Lo fanno e basta.

Cercate un servizio di posta elettronica di una community web di cui vi fidate, e anche se l'interfaccia web non è proprio il migliore, cercate di adattarvi. Ci sono servizi poco conosciuti ma efficaci, come per esempio PronMail. I server di ProtonMail sono in Svizzera, paese noto per il rispetto della privacy, per cui è improbabile che le autorità possano avere accesso ai dati degli utenti. Ma la caratteristica più convincente è che tutte le email sono blindate con crittografia end-to-end: non possono quindi essere lette o usate se non da chi le invia e le riceve. Quindi, quand'anche il gestore del servizio cedesse alle pressioni delle autorità, non avrebbe comunque accesso al contenuto delle email.

La crittografia presuppone una collaborazione crittografica con tutti i vostri contatti. Se il livello tecnologico di voi e dei vostri utenti/pazienti non è elevato, forse si tratta di una soluzione un po' difficile

Non è comunque una passeggiata: la crittografia presuppone una collaborazione crittografica con tutti i vostri contatti. Se il livello tecnologico di voi e dei vostri utenti/pazienti non è elevato, forse si tratta di una soluzione un po' difficile.

OwnCloud e Nextcloud sono suite di software client-server per la creazione di servizi di hosting di file e il loro utilizzo. Sono funzionalmente molto simili al famoso Dropbox, con la principale differenza funzionale che il software dal lato Server è free, consentendo in tal modo a chiunque di installarla e gestirla gratuitamente su un server privato. Hanno anche estensioni che gli consentono di funzionare come Google Drive, con la modifica dei documenti on line, la sincronizzazione di calendari e contatti e altro ancora.



Ma ci vuole una quantità non trascurabile di setup, manutenzione e risorse sul server. Inoltre la sicurezza deve esser gestita con attenzione. Quindi vi si chiede di fare uno sforzo: non aderire a una piattaforma cloud, ma costruire e gestire la vostra piattaforma cloud privata. Non è necessario farlo da soli: lo si può fare per lo studio associato, oppure assieme ai colleghi.

Se non è possibile rinunciare ai messaggi brevi sullo smartphone dei pazienti, bisogna sapere che WhatsApp è il sistema meno sicuro e più invasivo in circolazione. Purtroppo, è anche il più usato, quindi aspettatiamoci molte pressioni da parte dei pazienti per essere informati con questo canale. Anche qui, sarebbe un grave errore far circolare informazioni, o peggio ancora documenti, sensibili su questo canale. Telegram e ancor più Signal sono soluzioni migliori, ma non risolvono il problema. Telegram è un'azienda privata come WhatsApp, anche se a minor rischio monopolio, e Signal è una Onlus, che però potrebbe da un giorno all'altro cambiare proprietario e politica di privacy.

Ancora una volta, la soluzione migliore è adottare un proprio server, anche cooperativo, e installare un sistema di comunicazione libero, come XMPP, in modo che tutti i dati rimangano sotto controllo. Occorrerà imporre agli utenti l'installazione di una App per leggere e scrivere i messaggi, ma è una soluzione praticabile.

FARSI AIUTARE

Per conoscere le opportunità, ci sono numerose comunità in rete che offrono informazioni sui sistemi liberi più efficaci. EXIT (www.3x1t.org) è una di queste.

Il passaggio a sistemi liberi non è facile. Occorre investire del denaro in un tecnico che appronti l'hardware e il software necessari. Ovviamente, più numerosa è la comunità professionale che farà riferimento a un server e a un tecnico, minori saranno i costi. Ma ne vale davvero la pena.

L'avanzata della rischiosa e zoppicante combinazione tra Big Data e Algoritmi-Machine Learning

Francesco Del Zotti*
Medicina Generale Verona
Membro esperto della Commissione Information Communication Technology (FNOMCeO)
Vice-Presidente di SicurDott.

* Si ringrazia il Dott. Francesco Del Zotti per aver coordinato questo Focus dal punto di vista scientifico.

Siamo così immersi da anni nella "medicina in Rete" da aver difficoltà a percepirla.

Ricordiamo la famosa storiella di David Foster Wallace

Ci sono due pesci che nuotano e a un certo punto incontrano un pesce anziano che va nella direzione opposta, fa un cenno di saluto e dice: "Salve, ragazzi. Com'è l'acqua?". I due pesci giovani nuotano un altro po', poi uno guarda l'altro e fa: "Che cavolo è l'acqua?"

Oggi il centro non è più la relazione ma il dato, prodotto reso merce fluida, capace di andare in ogni direzione ed in mano ai detentori di chi lo domina, nel pubblico o in grosse corporazioni private

Non si tratta solo di un'ignoranza cognitiva. Se non percepiremo bene le correnti e la temperatura di quest'acqua potremmo finire come nell'apologo di Noam Chomsky: la rana contenta di essere riscaldata, gradualmente, per finire bollita. Ci descrive la grande capacità di adattamento e di non-reazione dell'uomo moderno a situazioni che sembrano vantaggiose o piacevoli (e spesso così appare la Medicina in Rete) ma che nel medio-lungo periodo finiscono per essere spiacevoli e dannose: tutto ciò senza reagire o reagendo solo quando ormai è troppo tardi.

Per millenni, sino ad una quindicina di anni fa, il medico ed il paziente si incontravano in luoghi fisici appartati e con le regole ferree del rapporto fiduciario e del non passaggio di dati all'infuori della relazione diadica. Oggi il centro non è più la relazione ma il dato, prodotto reso merce fluida, capace di andare in ogni direzione ed in mano ai detentori di chi lo domina, nel pubblico o in grosse corporazioni private. Questa "datizzazione" della medicina equivale in qualche modo allo *ius primae noctis* di antica memoria: il medico ed il paziente possono anche incontrarsi in un luogo apparentemente appartato (l'ambulatorio, la stanza in ospedale, il domicilio), ma lo possono fare se nello stesso tempo ne lasciano traccia documentale ad esempio in cartelle computerizzate con ampi spazi condivisi con i grandi gestori dei dati, o, per fare un altro esempio, con gli assistenti vocali accesi e sempre connessi con la casa madre.

Di fronte a questi processi in cui siamo immersi, probabilmente abbiamo bisogno di una scossa, ad esempio fornita da alcuni casi emblematici e clamorosi.

Presentiamo un caso di studio: lo Score Narxcare, negli Sati Uniti, in cui si verifica l'incrocio moltiplicatore di rischi di tre "protagonisti" della datizzazione: Big data medici, Big data non-medici, Machine Learning.

La storia di Naxcare riportata dalla rivista online Wired. La terapia negata a Kathrin, una donna sofferente per endometriosi

Un algoritmo per il rischio di tossicodipendenza è diventato fondamentale per il modo in cui gli Stati Uniti gestiscono la crisi degli oppioidi.

Una storia emblematica raccontata su Wired, qui sintetizzata, spiega bene i baratri in cui ci può condurre la fiducia eccessiva nell'abbinata algoritmi + Big data[1].

Una donna di 32anni, di nome Kathryn, una sera del 2020 è andata al Pronto Soccorso di un ospedale statunitense del Michigan, in preda a dolori atroci, dovuti all'endometriosi. Nell'ospedale le avevano praticato oppioidi endovena; le avevano detto che le avrebbero fornito questa terapia fino a quando la crisi non fosse passata.

Al quarto giorno di ricovero la paziente notò un brusco cambiamento. Le comunicarono che non avrebbero più continuato l'oppioide in vena e in più dichiararono: "Lei non si rende conto di quanto è alto il suo punteggio in cartella, legato a certe prescrizioni".

La paziente, dimessa e ancora dolorante iniziò a chiedersi aquale tipo di punteggio e di prescrizioni si riferivano i medici. Circa due settimane dopo, Kathryn ricevette una lettera dal suo ginecologo in cui si affermava che egli interrompeva la loro relazione professionale; ciò a causa di un report del Database Narx Care.

1. https://www.wired.com/story/opioid-drug-addiction-algorithm-chronic-pain/

Kathrin alla ricerca via web di notizie sullo Score Narxcare

Kathrin allora si lanciò nell'esplorazione del Web e scoprì che si trattava di un algoritmo legato ad un'azienda, Appriss, che stava assumendo un ruolo centrale e nazionale nella lotta alle overdose da oppioidi. Appriss è un'azienda sviluppatasi negli anni '90. Un primo suo prodotto fu un software che forniva un avviso automatico alle vittime di reati ed ad altri «cittadini preoccupati» in vista dell'imminente rilascio dal carcere di un detenuto. Quindi il campo di interesse dell'azienda si è spostato alla sanità.

Prima ha creato banche dati per il monitoraggio delle prescrizioni; quindi Appriss nel 2014 ha acquistato, dall'Associazione Nazionale dei gestori delle Farmacie, l'algoritmo allora più comunemente usato per prevedere chi era più a rischio di «abuso di sostanze controllate».

L'azienda Appriss è largamente sostenuta finanziariamente, direttamente o indirettamente, dal Dipartimento di Giustizia. Il Governo federale e soprattutto il Ministero della Giustizia hanno investito milioni di dollari nello sviluppo e mantenimento di un grande database delle ricette ed in particolare di ricette sotto particolare controllo, come gli oppioidi.

L'azienda di NarxCare, il suo Algoritmo di Machine Learning (ML) ed il collegamento a vari Database medici e non medici.

Appriss nel tempo aveva collegato tra loro svariati database regionali e nazionali ed in più aveva connesso il tutto ad un sistema di Intelligenza Artificiale, di Machine Learning.

Quindi NarxCare era divenuta la piattaforma ufficiale per medici, farmacisti, ospedali. E da allora è difficile per i professionisti non tenere in conto il punteggio NarxCare, anche perché se non ne tengono conto potrebbero incorrere in provvedimenti giudiziari tali da compromettere la loro stessa persistenza nella professione. Secondo i giornalisti di Wired questo punteggio a sua volta dipende da altre delicate informazioni mediche e non che il Database è capace di interfacciare: dati medici amministrativi, dati derivanti dalle cartelle mediche computerizzate, dati dai Pronto Soccorso, e dati dal casellario giudiziario. In alcuni Stati, poi, sia la polizia sia altri organi inquirenti possono avere accesso a queste informazioni mediche riservate.

Ad ogni statunitense uno score NarxCare

Cosi Kathrin viene a scoprire che a quasi tutti gli statunitensi è assegnato un punteggio che presume di valutare il rischio di uso incontrollato degli oppioidi e che sugli operatori sanitari grava lo sguardo delle autorità in grado di giudicare quanto il singolo operatore osserva e rispetta questo punteggio. Appriss ormai è la leader della gestione di questi database di prescrizioni statali. L'azienda Appriss è convinta che un punteggio del suo algoritmo Narx Care non sia destinato a sostituire la diagnosi di un medico. Ma, come detto, se i medici ignorano questo score lo fanno a loro rischio e pericolo. In effetti, quasi tutti gli stati degli USA ora utilizzano il software Appriss per gestire i propri programmi di monitoraggio dei farmaci da prescrizione e la maggior parte richiede per legge a medici e farmacisti di consultarli quando prescrivono sostanze controllate (e gli oppioidi in primis).

Kathrin, consumatrice non abituale di oppioidi, scopre il motivo del suo score elevato

Kathrin ha cercato di andare a fondo, anche online, a questo suo punteggio: ella usava gli oppioidi sporadicamente e non riteneva di esserne dipendente. Tutt'al più aveva a volte richiesto una prescrizione per una benzodiazepina, per il trattamento del disturbo da stress post-traumatico.

Al momento del suo ricovero in ospedale, Kathryn possedeva due cani retriever a pelo piatto, Bear e Moose. Era abitudine della signora adottare sempre cani particolarmente fragili e malati. A questi due cani erano stati prescritti oppioidi, benzodiazepine e persino barbiturici dai loro veterinari. Ebbene, le prescrizioni per gli animali sono poste sotto il nome del loro proprietario. Quindi, a NarxCare sembrava che Kathryn stesse vedendo molti medici per diversi delicati farmaci, alcuni a dosaggi elevati, e in maniera continuata.

NarxCare e le imperfezioni del suo Algoritmo di ML

L'attribuire alla padrona i farmaci dei suoi cani potrebbe sembrare una sbavatura rispetto ad un software e un database peraltro efficace. Ma secondo molti ricercatori sia NarxCare che altri algoritmi per screening come questo sono profondamente imperfetti.

Secondo dati statistici, il 20% dei pazienti che hanno maggiori probabilità di essere contrassegnati come consumatori dipendenti da oppioidi ha in realtà il cancro, che spesso richiede la visita di più specialisti. E molte delle *red flag* che aumentano i punteggi di rischio di una persona sono semplicemente degli attributi dei pazienti più vulnerabili e complessi dal punto di vista medico; con l'aggravante che non poche volte ciò fa sì che a quei gruppi venga negato il trattamento del dolore con oppioidi.

L'Intelligenza Artificiale dietro NaxCare: tra imperfezioni e segreto industriale

L'attribuire alla padrona i farmaci dei suoi cani potrebbe sembrare una sbavatura rispetto ad un software e un database peraltro "efficace. Ma secondo molti ricercatori NarxCare e altri algoritmi per screening come questo sono profondamente imperfetti

L'intelligenza artificiale che genera il punteggio di rischio di overdose di NarxCare è, per molti critici, basata su una metodologia per certi versi inquietante. Secondo vari studiosi questo sistema di Score e di IA non è validato da ricerche soggette a *peer-review*. Si tratta di un sistema minato da opacità che almeno in parte dipendono dal fatto di essere un sistema proprietario, che come tutti i sistemi proprietari si trincera dietro il diritto a difendere il segreto industriale. Negli ultimi due anni, la giurista Jennifer Oliva, direttrice del Center for Health and Pharmaceutical Law presso la Seton Hall University, ha deciso di esaminare NarxCare alla luce di queste apprensioni. In un importante articolo pubblicato su una rivista forense, dal titolo "Dosing Discrimination", sostiene che molti dei dati che NarxCare afferma di tracciare possono semplicemente ricondursi alle disuguaglianze associate a razza, classe e genere, diseguaglianze che il sistema rischia di peggiorare ulteriormente.

Come ho detto molte volte nella mia ricerca, la cosa più terrificante della piattaforma di valutazione del rischio di Appriss è il fatto che i suoi algoritmi sono proprietari e, di conseguenza, non c'è modo di convalidarli esternamente.

Il risultato di tutto ciò dice l'esperto Prof Stefan Kertesz, di Harvard, è che:

L'algoritmo sembra organizzato per convincere i clinici che qualsiasi persona con un problema medico più importante può recare ai medici il maggiore peso e rischio di responsabilità legale. E in questo modo esso potrebbe incentivare l'abbandono dei pazienti che hanno i problemi più seri.

E tutto ciò secondo lo studioso può condurre pazienti con dolore serio e senza dipendenza ad abbandonare il farmaco con il conseguente rischio di passare a farmaci più rischiosi prelevati dal mercato illegale o persino al suicidio; e d'altra parte si sa che l'interruzione di queste prescrizioni è associato al rischio triplicato di morte per overdose.

Il paradosso della buprenorfina

Un'ennesima situazione paradossale legata allo score NarxCare è la seguente: ai pazienti che cercano di disintossicarsi viene prescritta la terapia *gold standard* in tali circostanze: la buprenorfina. Siccome questa molecola è a sua volta un oppioide, essa può innalzare lo score NarxCare, al punto tale da essere negata a chi vuole disintossicarsi.

Un sondaggio tra i pazienti i cui fornitori hanno controllato questi sistemi ha rilevato che più del 40% dei pazienti con prescrizione di buprenorfina hanno riferito di essere stati umiliati o hanno subito tagli nelle prescrizioni, il che ha aumentato il dolore e ridotto la qualità della vita.

La Prof. Kilby e la sua ricerca che smonta e rimonta l'algoritmo di Machine learning NarxCare.

Quando un membro della sua famiglia, un medico del sud rurale, le disse quanto fosse difficile prendere decisioni sulla prescrizione di oppioidi in una comunità devastata dalle overdose, Kilby, allora giovane studiosa di economia del Mit, decise di studiare il dilemma del medico valutando l'ipotesi per cui un maggiore controllo sulla prescrizione di oppioidi potesse eventualmente influire effettivamente sui pazienti. Per tenere traccia dei risultati sulla salute, ella utilizzò i dati sulle richieste di indennizzo di 38 stati che avevano implementato database di monitoraggio delle prescrizioni in momenti diversi tra il 2004 e il 2014. Aveva previsto che la riduzione delle prescrizioni avrebbe aumentato la produttività e la salute. In effetti, secondo Kilby la sua ricerca sorprendentemente le dimostrò che la riduzione delle prescrizioni mediche di oppioidi portò sia ad un aumento delle spese mediche, sia a livelli più elevati di dolore nei pazienti ospedalizzati e a più giorni lavorativi persi. Ella ha dichiarato:

Un sondaggio tra i pazienti i cui fornitori hanno controllato questi sistemi ha rilevato che più del 40% dei pazienti con prescrizione di buprenorfina hanno riferito di essere stati umiliati o hanno subito tagli nelle prescrizioni, il che ha aumentato il dolore e ridotto la qualità della vita

Si tratta di persone che probabilmente stanno perdendo l'accesso agli oppioidi, che stanno lottando di più per tornare al lavoro dopo gli infortuni e lottano per ottenere un trattamento del dolore.

Così, alla fine degli anni 2010, dopo essere diventata assistente professore alla Northeastern University, decise di simulare il modello di apprendimento automatico che genera la misura algoritmica più sofisticata di NarxCare, l'Overdose Risk Score. Sebbene Appriss non abbia reso pubblici i fattori che sono entrati nel suo algoritmo, Kilby ha decodificato ciò che poteva. Non avendo accesso ai dati del registro dei farmaci da prescrizione, Kilby ha deciso di utilizzare i dati anonimizzati sulle richieste di indennizzo dell'assicurazione sanitaria, una fonte che è alla base di tutti gli altri algoritmi di apprendimento automatico pubblicati, che prevedono il rischio di oppioidi. Usando all'incirca lo stesso metodo che Appriss espone nei resoconti del proprio lavoro di apprendimento automatico, ella ha addestrato il suo modello mostrandogli casistiche di persone a cui era stato diagnosticato un disturbo da abuso di oppiacei dopo aver ricevuto una prescrizione di oppiacei. Quello che Kilby ha scoperto è che il modello di NarxCare condivide una limitazione essenziale con il suo algoritmo:

Il problema con tutti questi algoritmi, compreso quello che ho sviluppato», dice Kilby, «è la precisione».

Il set di dati completo di Kilby includeva i file di circa 7 milioni di persone che erano assicurate dai loro datori di lavoro tra il 2005 e il 2012. Il risultato è stato che l'algoritmo di Kilby ha generato un gran numero di risultati sia falsi positivi che falsi negativi, anche quando ha impostato i suoi parametri in modo così rigoroso che qualcuno doveva ottenere un

punteggio pari o superiore al 99° percentile per essere considerato ad alto rischio. Questo dipende dal fatto che su quei vari milioni di pazienti del database solo 23mila avevano segni di dipendenza da oppiodi: una proporzione che rende più deboli le previsioni. «Non c'è alcuna correlazione tra la probabilità di essere considerati ad alto rischio dall'algoritmo e la riduzione della probabilità di sviluppare un disturbo da uso di oppiacei», spiega Kilby. Non solo, se l'algoritmo ha accumulato una lunga serie temporale di dati su quel paziente ha molto più probabilità di "marchiarlo" come dipendente da oppioidi rispetto al paziente su cui l'algoritmo ha pochi dati. In altre parole, l'algoritmo essenzialmente non può fare ciò che afferma: ovvero determinare se scrivere o negare la prossima prescrizione di qualcuno altererà la loro traiettoria in termini di dipendenza.

Nel suo articolo "Dosing Discrimination", su algoritmi come NarxCare, Jennifer Oliva descrive una serie di casi simili a quelli di Kathryn e in cui alle persone sono stati negati gli oppioidi a causa di traumi sessuali e altri fattori potenzialmente fuorvianti. La domanda più grande, ovviamente, è se gli algoritmi debbano essere utilizzati per determinare il rischio di dipendenza. L'autrice dichiara: «Non penserei ai soli algoritmi». Al contrario, durante la crisi delle overdose negli USA, i politici si sono concentrati soprattutto nel loro uso per la riduzione del consumo di oppiacei per uso medico. La stessa Apriss ha riconosciuto la necessità di non limitarsi alla dimostrata riduzione di consumo di oppioidi indotta da NarxCare (NarxCare ha accelerato il calo della prescrizione di oppioidi in sei stati di circa il 10%), ma di ricercare evidenze ancora non chiarite: sulla mortalità, sulla qualità di vita dei pazienti che vanno sotto il vaglio del loro Score. E in effetti una recente ricerca conferma che la "grey literature" sui sistemi di Score legati al consumo di oppioidi ribadisce la prevalente mancanza di studi ben controllati.

L'attuale situazione di Kathrin

Non appena Kathryn ha capito cosa era successo, ha iniziato a tentare di cancellare dal mondo onli-ne almeno in parte il dato non veritiero dell'abuso cronico di oppioidi. Ha avuto poco successo; anzi ogni volta che si reca in una farmacia e da un medico si vede soggetta allo scrutinio critico di chi osserva il suo Score. A questo proposito ha dichiarato: «Il loro comportamento è cambiato. Non vi è una relazione di cura, simpatetica, ma un rapporto come tra sospetta e detective; una sorta di inquisizione». Per Kathryn, l'effetto di NarxCare sulla sua qualità di vita e sulla sua salute è stato piuttosto netto. Ella dichiara: «A parte il mio psichiatra, non ho un dottore che mi segua, a causa del mio punteggio». Si preoccupa di cosa farà la prossima volta che la sua endometriosi si riaccenderà o si presenterà un'altra emergenza, e ancora lotta per ottenere farmaci per curare il suo dolore. E non sono solo in difetto le prescrizioni per il dolore di Kathryn. Alcuni stati hanno riconosciuto il problema delle prescrizioni veterinarie erroneamente identificate e richiedono a NarxCare di contrassegnarle con un'impronta di zampa o un'icona di animale sugli schermi degli operatori sanitari.

Questa storia può essere tipica degli USA, ma non dell'Italia?

Lo score NarxCare sembra una versione ridotta e specializzata del più famoso "sistema di credito sociale" della Cina (https://it.wikipedia.org/wiki/ Sistema_di_credito_sociale) Si potrebbe obiettare che questi sistemi telematici così pervasivi sono tipici delle grandi potenze e che in Italia non possono esistere simili esempi. Purtroppo non è così. Non tutti riflettono su un dato di fatto: le ULSS, le Regioni ed il Ministero delle Finanze da molti anni hanno una delle concentrazioni di dati sanitari (ricette, FSE…) tra le più alte di Europa. E anche da noi si sono sviluppati degli Score discutibili, all'incrocio tra big data istituzionali e algoritmi di Intelligenza artificiale. Di alcuni siamo venuti a conoscenza; ma chissà quanti altri sono già in funzione mentre i pazienti ed i medici sono inconsapevoli di essi.

L'intelligenza semantica usata per alleggerire le priorità per test e visite indicate dai MMG?

Un primo esempio è a carattere locale. Nel 2018 viene alla ribalta lo scandalo della ULS veneta in cui si sembra che si sia adoperato un software di intelligenza semantica per validare le **priorità** impostate dal MMG nelle richieste di test diagnostici e visite.

La magistratura indagò sul caso. Dalla lettura dei quotidiani dell'epoca si legge che questo software, in più di 44 mila ricette, avrebbe cambiato i codici di priorità più urgenti scritti dai MMG in codici meno urgenti. Si veda ad esempio l'articolo: ***Venezia, il software rinviava le visite urgenti dei malati di tumore. E 28 di loro sono morti.***[2]

L'algoritmo SAVIO dell'Inps bloccato dal Garante

Nello stesso anno, il 2018, giunse su tutti i quoiditiani la notizia di uno scandalo che questa volta riguardava L'INPS. Ecco la notizia: ***Garante Privacy 'No a profilazione lavoratori con sistema di data mining dell'Inps per le visite fiscali.***

2. https://corrieredelveneto.corriere.it/venezia-mestre/cronaca/18_novembre_28/rinviate-visite-200-pazienti-oncologiciil-software-ammorbidiva-urgenze-9af4a4d0-f27d-11e8-b0d6-71c84bf2718d.shtm

Il Garante della Privacy Soro allora ha bloccato l'introduzione di un algoritmo di *data mining* per la programmazione mirata delle visite fiscali da parte dell'Inps, di nome SAVIO. Questo algoritmo, basato anche sui big data dei "certificati per malattia" in mano a Inps, aveva l'obiettivo di individuare preventivamente possibili assenze ingiustificate dal lavoro per malattia. Secondo il Garante il modello messo a punto e adottato negli ultimi anni dall'Istituto realizza "una vera e propria profilazione dei lavoratori interessati", non conforme al nuovo Regolamento europeo (GDPR), anche perché operante non solo all'insaputa dei lavoratori interessati ma anche in assenza di precauzioni e garanzie specifiche volte ad evitare, ad esempio, che inesattezze nei dati raccolti o incongruenze nella logica degli algoritmi utilizzati, inducano decisioni erronee con impatti negativi sui singoli.

L'Istituto tra l'altro in quella circostanza non aveva notificato all'Autorità l'adozione di un tale meccanismo di data mining, basato sulla profilazione. L'algoritmo, introdotto cinque anni prima, pur non prendendo in considerazione la diagnosi dell'episodio di "malattia", comunque trattava il numero e la durata degli episodi di assenza per malattia, entrambi dati medici sensibili; più precisamente, dalle parole di SORO: ***il dato stesso dell'assenza dal lavoro per malattia costituisce dato sulla salute.***

Emerge il possibile bavaglio al Garante della Privacy: dovrà solo usare il suo potere dopo le iniziative del Governo, di Regioni ed Enti pubblici.

Secondo il decreto "Capienze" Secondo il decreto, le Pubbliche amministrazione potranno trattare i dati personali anche senza un'apposita legge di autorizzazione

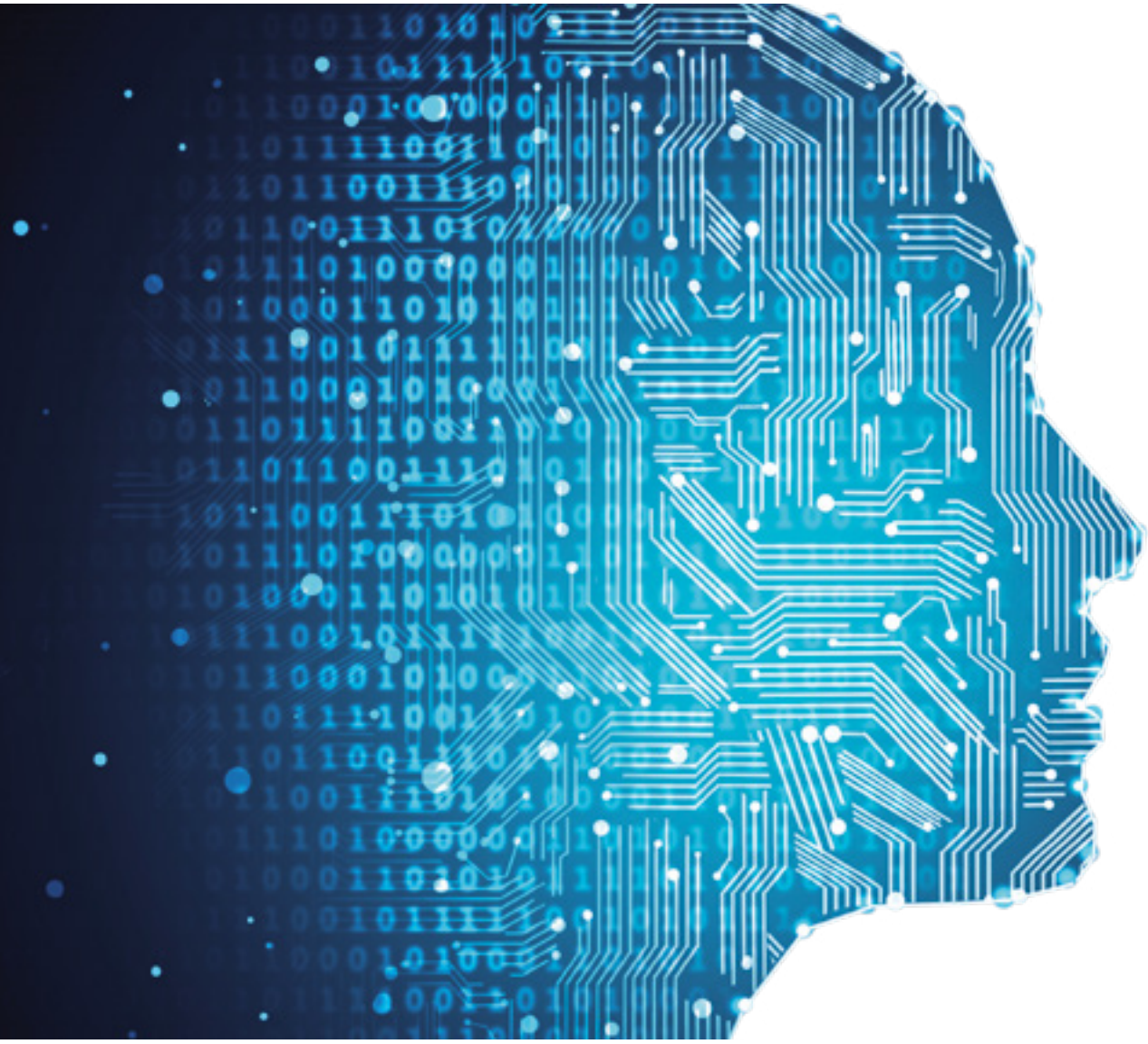
Si dirà, in fondo sono tentativi, abortiti, del 2018. Oggi l'Italia seguirebbe in campo sanitario il rigore del regolamento europeo GDPR. Ebbene, con Covid-19 molti freni si sono allentati e ai medici in molte regioni è stata consentita, ad esempio la spedizione delle ricette per normali email di provider proprietari e spesso extra-UE. Ed inoltre, nel settembre 2021, lo Stato sta favorendo una nuova norma inserita nel Decreto "Capienze", che salta il ruolo preliminare del Garante della Privacy. Secondo il decreto, le Pubbliche amministrazione potranno trattare i dati personali anche senza un'apposita legge di autorizzazione.

E leggiamo sul sito de Il Fatto Quotidiano le dichiarazioni rispettivamente di due illustri giuristi. La prima del giurista Resta: ***Le amministrazioni devono comunque rendere conto della congruità del trattamento"***; la seconda di Sarzana: ***La norma va circoscritta, ci sono rischi di abusi.***

Ma anche a livello europeo...

Ma anche a livello europeo avanzano big data e algoritmi istituzionali e si fanno scelte che vanno in contraddizione con lo stesso GDPR. Ad esempio il bollettino online specializzato in sicurezza Techcrunch[3] ci ricorda che mentre la UE ha consigliato ai suoi parlamentari e ai suoi burocrati di usare l'App cifrata e indipendente della fondazione "Signal" (al posto ad esempio di WhatsApp), nello stesso tempo essa sta mettendo in atto leggi che compromettono la cifratura, così come ci ricorda il comunicato congiunto dei provider europei di aziende di App e servizi email o Cloud con cifratura seria.

3. https://techcrunch.com/2021/01/27/protonmail-threema-tresorit-and-tutanota-warn-eu-lawmakers-against-anti-encryption-push/



Conclusioni

Questi esempi di difettoso e rischioso potere della combinazione di Algoritmi di Intelligenza Artificiale e Big Data in mano ad importanti aziende private o istituzioni pubbliche ci ricordano l'avvertimento della matematica Cathy O'Neil, che dopo essere stata consulente di aziende simili ha deciso di passare alla contro-informazione e nella sua importante opera, *Weapons of Math Destruction*, ha scritto:

La matematica sposata alla tecnologia riusciva a moltiplicare il caos e le sventure, alimentando o rendendo più efficienti sistemi che - ora lo capivo- erano malati... molti di questi modelli avevano codificato il pregiudizio umano, l'incomprensione e l'errore sistematico nei software che controllano ogni giorno di più le nostre vite. Come fossero divinità questi modelli matematici erano misteriosi e i loro meccanismi invisibili tranne che ai sommi sacerdoti della materia: matematici ed informatici.

Secondo l'autrice i giudizi degli algoritmi da lei studiati, anche se sbagliati o pericolosi, sono spesso incontestabili e senza appello, visto che chi li contesta è chiamato a fornire dimostrazioni di livello decisamente superiore rispetto agli stessi algoritmi. Le tecnologie basate su intelligenza artificiale potrebbero essere utili in alcuni contesti difficili (rifugiati, Paesi in via di sviluppo, zone isolate con pochi medici). Ma anche in questo caso bisognerà evitare un rischio di asimmetria a cui l'autrice si riferisce: la medicina impersonale dei grandi numeri e degli automatismi potrebbe essere destinata ai pazienti poveri, mentre solo agli abbienti sarebbe fornita una medicina sartoriale, personalizzata, dal contatto umano, anche fatto di strette di mano e di esame obiettivo.

I medici si trovano di fronte a un bivio: usare il comprensibile fatalismo o chiedere di partecipare più attivamente al cambiamento. La prima scelta, ovvero l'accettare il nuovo ordine del cambiamento, è la più comoda vista anche la potenza di fuoco di chi oggi comanda l'informatica e la telematica e viste le complessità. E questa comodità è sposata da non pochi operatori. In effetti chi l'avrebbe detto che i medici, dopo una storia professionale di 2300 anni di rapporto diadico fiduciario e solo dopo pochi decenni alla nascita delle riforma sanitaria nel 1978 (basata sulla partecipazione democratica nel "territorio" e nel "distretto"), sarebbero stati indotti a spedire alla Regione e allo Stato non solo le loro ricette online, ma persino la lista delle malattie, ed i problemi più rilevanti e più intimi dei pazienti?

I medici si trovano di fronte ad un bivio: usare il comprensibile fatalismo o chiedere di partecipare più attivamente al cambiamento

Noi medici rischiamo così di dimenticare alcuni fondamenti della deontologia professionale e nello stesso tempo alcuni imperativi categorici che ci hanno sempre sospinto all'autonomia dal potere. Viene opportuno a questo punto citare il recente lavoro di uno storico statunitense il prof Timothy Snyder[4]:

Se gli avvocati avessero seguito la regola del non processo senza tribunale, se i medici avessero praticato la regola di nessun intervento senza consenso, se gli imprenditori avessero approvato il divieto della schiavitù, se i burocrati avessero rifiutare di partecipare alle relative procedure burocratiche del regime nazista che implicavano omicidi, sarebbe stato molto più difficile il commettere le atrocità con cui lo ricordiamo. L'etica professionale deve guidarci proprio quando ci dicono che la situazione è eccezionale.

Per fortuna la sudditanza dal potere commerciale-industriale intorno ai dati è di scala molto diversa da quella del periodo oscuro ricordato da Snyder. Ma lo storico vuole metterci in guardia rispetto a certa analoga passività che come professionisti mettiamo in atto rispetto all'ideologia del momento, del "progresso ad ogni costo", come la seguente sua frase meglio mette in luce:

Se i membri delle professioni confondono la loro etica specifica con le emozioni del momento, tuttavia, possono trovarsi a dire e fare cose che in precedenza avrebbero potuto ritenere inimmaginabili.

I medici ed i cittadini si sentono soverchiati dallo sviluppo dei grandi database e dalle Reti in Medicina. Per evitare sentimenti negativi e mantenere la lucidità che serve per migliorare la nostra vita di medici e pazienti in Rete, credo che sia utile anche richiamare la dimensione storico-antropologica della Rete.

4. Timothy Snyder: 20 lezioni per la democrazia dalle malattie della politica - Rizzoli, 2017.

Abbiamo pensato che la Rete fosse la semplice evoluzione e arricchimento tecnologico del Personal Computer. No, Internet ha significato un cambio antropologico di gran lunga maggiore di quell'arricchimento. In effetti, spesso dimentichiamo che la storia della Rete nasce negli anni '50 nell'ambiente militare. Vi è stato solo un periodo, quello del primo Web, in cui abbiamo avuto una Rete basata più sulla collaborazione tra tanti nodi periferici che su alcuni grandi nodi centrali. Nell'ultimo decennio stiamo tornando al controllo centralizzato di grandi server appartenenti o a stati e regioni o a grandi aziende multinazionali. La tendenza attuale purtroppo sfavorisce la tradizione della cultura della medicina del territorio, vicina ai quartieri e ai nuclei familiari o di vicinato.

Questa centralizzazione chiede ai medici di aderire al modello di co-controllo dall'alto dei cittadini e pazienti. Alla fine di questo articolo, i medici possono, comprensibilmente, sentirsi troppo piccoli rispetto alla potenza dei nuovi meccanismi in mano a vecchi e nuovi poteri. Può vincere la pesantezza del fatalismo. Per recuperare la leggerezza dovremo tornare alla prima immagine dell'articolo, dei pesci nell'acqua. Anche le pesanti mante giganti sono capaci a volte di staccarsi dal mare in tempesta, per osservarlo da fuori. Ma anche gruppetti dei piccoli "pesce rondine" sono capaci di volare sull'acqua anche per 400-500 metri e magari darsi uno sguardo l'un altro. Ecco, analogamente, in questo momento più che imporsi o imporre cambiamenti su *Big data* e *Big interest*, ci serve una prima consapevolezza, un nuovo sguardo.

Bibliografia e sitografia

https://www.wired.com/story/opioid-drug-addiction-algorithm-chronic-pain/

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3768774

https://corrieredelveneto.corriere.it/venezia-mestre/cronaca/18_novembre_28/rinviate-visite-200-pazienti-oncologiciil-software-ammorbidiva-urgenze-9af4a4d0-f27d-11e8-b0d6-71c84bf2718d.shtml

https://www.privacyitalia.eu/garante-privacy-no-a-profilazione-lavoratori-con-sistema-dimining-dellinps-per-le-visite-fiscali/8705/

https://techcrunch.com/2021/01/27/protonmail-threema-tresorit-and-tutanota-warn-eulawmakers-against-anti-encryption-push/.

Cathy O' Neal "Weapons of Math destruction" (ed italiana: Armi di distruzione matematica, 2017, Bompiani, Milano).

Timothy Snyder: 20 lezioni per la democrazia dalle malattie della politica - Rizzoli, 2017.

(Beaulieu T, Knight R, Nolan S, Quick O, Ti L. Artificial intelligence interventions focused on opioid use disorders: A review of the gray literature. Am J Drug Alcohol Abuse. 2021 Jan 2;47(1):26-42. doi: 10.1080/00952990.2020.1817466. Epub 2020 Oct 2. PMID: 33006905.

Letture consigliate

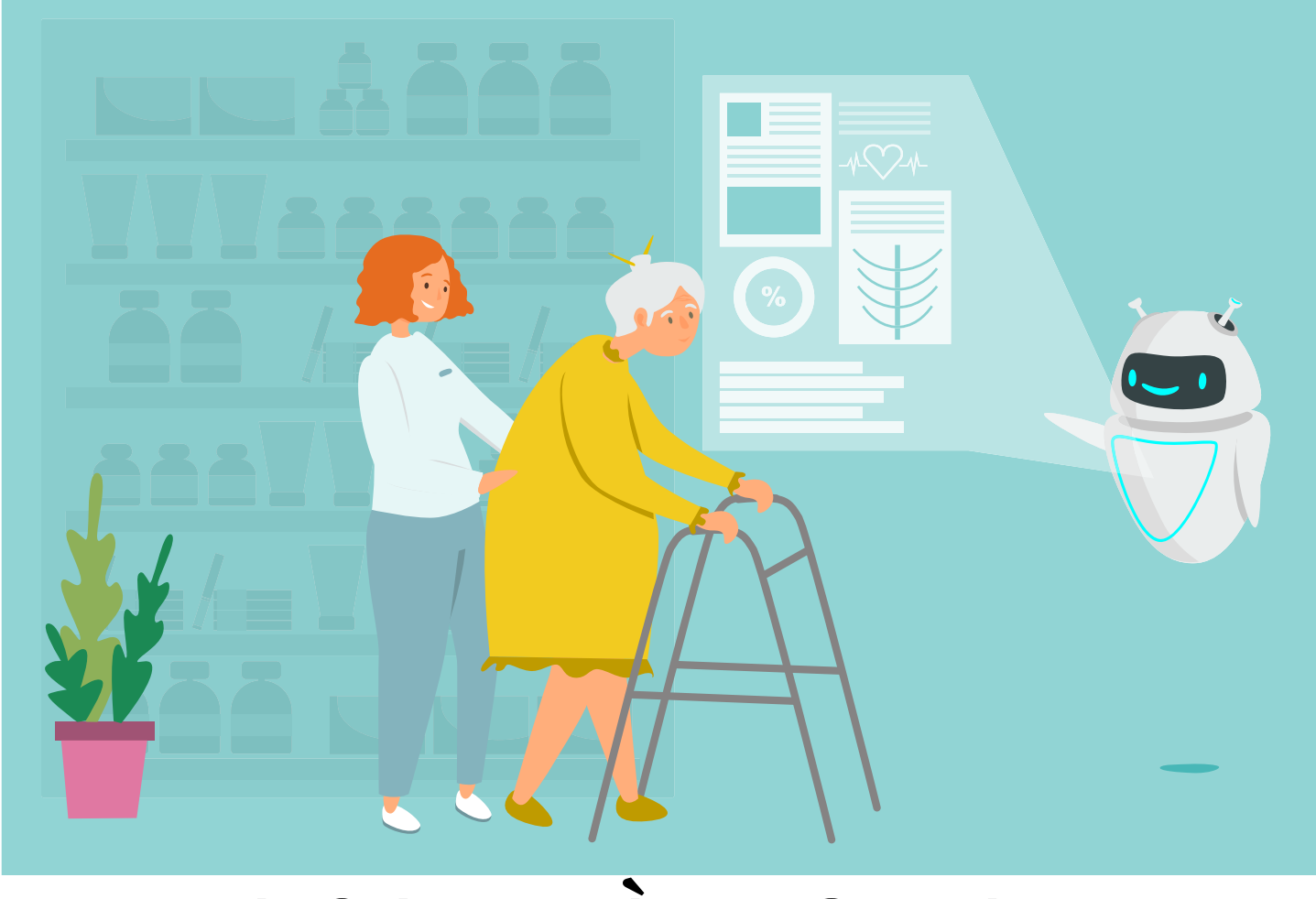
Veronica Barassi **I FIGLI DELL'ALGORITMO. Sorvegliati, tracciati, profilati dalla nascita** - Luiss Editore, 2021

Michele Bottari **COME SOPRAVVIVERE NELL'ERA DIGITALE. Uscire dalla dipendenza dello smartphone, ribellarsi al commercio dei dati personali, riprendersi la rete** - Ediz. Terra Nuova, 2019

Manlo Cammarata **IL FURBOFONO** - Editore Tabulas, 2019

Luciano Floridi e Federico Cabitza **INTELLIGENZA ARTIFICIALE: L'USO DELLE NUOVE MACCHINE** - Giunti Editore 2021

David Lyon **LA CULTURA DELLA SORVEGLIANZA** - Luiss Editore, 2020



LA SANITÀ DIGITALE DAL PUNTO DI VISTA DEI CITTADINI

Claudio Destri
Presidente SicurDott

SicurDott ETS è un'associazione civica nata nel febbraio 2018 con l'obiettivo di aggiornare i cittadini sul loro diritto ad una telematica sanitaria sicura e di qualità, che li veda attivamente partecipi. Vuole dare voce ai tanti cittadini e alle persone in difficoltà che spesso per tanti motivi non hanno espressione.

Stiamo vivendo in un periodo storico fatto di superficiale mancanza di senso civico a tutti i livelli. Essa si accompagna ad una quota crescente di deresponsabilizzazione delle istituzioni, a svantaggio soprattutto delle fasce deboli, su cui si scarica l'apparente praticità e democraticità delle applicazioni, che di fatto delegano l'onere del controllo ai cittadini a fronte di un effimero reale potere di riscontro e azione nella propria situazione sanitaria.

Lo scopo dell'APS SicurDott ETS è dar vita a esperienze innovative di formazione e informazione indipendente sull'uso consapevole della Rete e dei Sistemi in sanità; favorire lo sviluppo dei migliori mezzi informatici e ingegneristici tali per cui si abbia da una parte la migliore possibilità di comunicare e analizzare in rete dati medici e dall'altra la qualità e modernità massima dei sistemi per proteggere la riservatezza delle comunicazioni tra medico e paziente, e tra medico e medico, dietro autorizzazione del paziente.

Al fine di perseguire gli scopi istituzionali l'Associazione:

a) Promuove l'alfabetizzazione su Internet e sulle reti in sanità, con particolare riguardo a sicurezza e privacy.

b) Richiede l'autenticità giuridica della firma digitale e identità digitale accreditate, che qualificano un cittadino o un medico, per andare oltre le autenticazioni deboli (quali user-id e PW);

c) Richiede un serio sistema di archiviazione di documenti digitali immodificabili secondo quanto previsto dal Codice per l'Amministrazione Digitale (CAD) con la promozione di controlli sui Server che ospitano i database;

d) Promuove l'architettura dei sistemi telematici che siano costruiti con i criteri della *privacy by design* e *privacy by default*;

e) Promuove nell'analisi dei dati un sistema di anonimizzazione di qualità' e di ricorrere all'analisi di dati nominativi solo quando è strettamente necessario;

f) Promuove la creazione di portali sanitari, ecosistemi protetti e chiusi, ove si possono scambiare informazioni in maniera sicura tra medico e paziente;

g) Promuove tra i medici, operatori sanitari e istituzioni sanitarie il rispetto delle modalità formali migliori, in termini etici e giuridici, della raccolta del Consenso Informato;

h) Promuove il Diritto dei cittadini ad informazioni personalizzate e non propagandistiche sulla modalità di interazione in rete con le istituzioni sanitarie; favorire una informazione che deve essere personalizzata e adattata a età, classe sociale, morbilità e grado di fragilità del singolo paziente. Favorire la formazione dei cittadini verso le nuove tecnologie/apparecchiature per una corretta conoscenza - scelta - utilizzo delle stesse;

i) Diffonde il Regolamento Europeo sulla Privacy ed eventuali successive normative con specifica delle figure professionali collegate: consapevolezza, oneri attuali da applicare e nuovi vincoli;

j) Cerca di essere funzione di raccordo a 360° e collaborazione tra Associazioni dei Consumatori, e le Authority (in particolare Garante della Privacy e l'Agenzia per l'Italia digitale, AGID), con gli Ordini e Associazioni Professionali (in particolare di medici, di Ingegneri, di Avvocati, di Giuristi, di informatici, ecc.) e raccordo con analoghe associazioni nazionali ed europee e con tutta la società civile. L'Associazione al riguardo promuove convegni, svolge attività formative, di ricerca, stipula convenzioni e svolge ogni altra attività purché congruente rispetto ai propri scopi.

La sanità italiana a causa all'emergenza sanitaria legata al COVID-19 mentre accelera il ritmo dell'innovazione digitale in sanità, ha evidenziato lacune e ritardi nel nostro Servizio sanitario nazionale. Nella maggior parte dei nuovi servizi il cittadino/utente diviene parte fondamentale in fase di accesso e gestione senza che ci si chieda se ha le capacità/competenze.

Un esempio di deresponsabilizzazione è l'applicazione di controllo del sistema di trasmissione del monitoraggio dei dati di funzionamento di un pacemaker che permetterebbe all'utente (spesso anziano) di verificarne il funzionamento: anche qui vige l'onere di controllo per il cittadino, nel mentre si verifica che più volte il Centro specialistico non si è accorto per mesi di non ricevere i dati.

È fuori dubbio che le soluzioni di intelligenza artificiale potranno avere un ruolo fondamentale nelle situazioni di emergenza, consentendo di rendere i processi delle aziende sanitarie più efficienti, aiutando a personalizzare le cure e cosi renderle più efficaci, anche attraverso la riduzione della probabilità di errori clinici. Abbiamo usato il condizionale visto che le realizzazioni di Intelligenza Artificiale in Medicina sono ancora poche e con alcuni importanti difetti o limitazioni.

Un'altra questione delicata riguarda la diffusione di dati medici sensibili all'interfaccia onnipresente dei CUP telematici. In effetti al medico viene ingiunto di apporre sulle richieste di esami o visite il quesito diagnostico. Non si comprende il motivo per cui tutti i quesiti siano controllati da personale non sanitario. È un vulnus che richiederà una iniziativa ad hoc della nostra associazione ed una richiesta di riflessione che rivolgeremo sia alle istituzioni che alle categorie professionali. Vi è necessita di comunicazione/informazione su canali telematici riservati da creare per comunicazioni medico-medico che contrasti questa lievitazione di uscita impropria dei dati dei pazienti verso personale non qualificato, Il che mette a rischio la sfera privata e crea talvolta presupposti discriminatori.

A questo punto sorgono spontanee alcune domande:

- I cittadini/utenti sono e saranno in grado di usufruire e gestire tali servizi così strutturati o ci sarà una autoesclusione di estese fasce della popolazione?
- Esiste un "monitoraggio in itinere" che valuta le questioni che sorgono e che, considerando l'utenza, modifica il servizio per garantirne il reale e corretto utilizzo?
- Si è pensato a come far "crescere" l'informatizzazione della cittadinanza, senza basarsi esclusivamente sull'utilizzo dello smartphone come indice dell'informatizzazione stessa?
- E i nostri dati sono trattati e conservati in maniera sicura, alla luce degli ultimi attacchi informatici alle aziende sanitarie?
- Il personale delle aziende sanitarie è formato nei confronti dei problemi di Cyber security e dispone di soluzioni adeguate?
- E a questo proposito vi è stata una sufficiente protezione ad hoc del telelavoro o lavoro agile, in particolare riferimento all'accesso da parte del personale dell'azienda o a reti non protette o a strumenti e device personali non sufficientemente sicuri?

La pandemia è arrivata in un momento cruciale della digitalizzazione in Italia, il sistema sanitario nazionale era pronto, ma mancava lo slancio iniziale. Se per certi versi essa se ha aumentato la velocità dei passaggi e di uso di comunicazioni di dati a distanza, d'altra parte ha bloccato lo sviluppo di tecnologia della sicurezza e la nuova gestione delle regole ad hoc, di cui una medicina in Rete partita spesso "insicura" aveva da anni bisogno.

Evidentemente, i vantaggi della trasformazione digitale della sanità sono per molti ma non per tutti, e sono comunque accompagnati da alcuni effetti collaterali. Il problema più grosso era e rimane il *digital divide*: una grossa fetta della popolazione non si è ancora familiarizzata con le tecnologie digitali e pertanto non ha accesso a servizi come il fascicolo sanitario elettronico oppure non ha i mezzi necessari per utilizzarli (non tutti hanno un computer o uno smartphone in casa). Le cause principali, infatti, sono l'età e le disparità socioeconomiche. Da un punto di vista clinico, poi, la sanità digitale comporta una trasformazione del rapporto medico-paziente e non sappiamo ancora quali siano gli effetti a lungo termine sull'efficacia del processo diagnostico.

Se da un lato la digitalizzazione ci ha permesso di adattarci alla pandemia, dall'altro ha anche creato nuove difficoltà a livello di sicurezza informatica e protezione dei dati personali.

Quindi la digitalizzazione dell'assistenza sanitaria implica una nuova sfida a livello di sicurezza informatica: una nuova categoria di dati sensibili sta migrando da offline a online, presentando tutta una serie inedita di problematiche:

- Il Medico di Medicina Generale dovrebbe coordinare e gestire la raccolta in segretezza e sicurezza dettata dal suo giuramento di Ippocrate dei dati del paziente. Gli attuali standard di sicurezza digitale gli danno questa tranquillità?
- Per quanto riguarda i dati sanitari del cittadino: chi è responsabile dei sistemi di raccolta, trasferimento e conservazione e garantisce che le protezioni sono adeguate per impedire il danneggiamento o il furto dei dati?

- I tagli avvenuti nella sanità negli ultimi anni hanno avuto un impatto enorme, mentre parallelamente cresce l'offerta e la potenza dei servizi sanitari privati che arrivano là dove si esauriscono le risorse del settore pubblico; e il cittadino si trova nel mezzo tra due realtà che stanno digitalizzandosi.
- A quali minacce informatiche ci esponiamo utilizzando la sanità digitale pervasa tra faciloneria, sottovalutazione e ignoranza tecnologica?

Uno dei punti emergenti è nella non focalizzazione della medicina digitale sui principali consumatori di servizi: gli anziani ed i fragili. In effetti le procedure necessarie, ed in particolare la necessità di uso frequente di smartphone e di Applicazioni, sono più consone al giovane adulto social-like, che all'anziano abituato alla solidità del cartaceo.

Ad esempio, il recente passaggio obbligatorio allo SPID o CIE per poter utilizzare la sanità a chilometro zero (dematerializzazione delle ricette e visualizzazione del FSEr) ha reso sempre più dipendente l'anziano dai propri figli o care-giver.

In effetti per molti anziani non ambulabili diventa complesso attivare lo SPID o CIE vista la necessità di recarsi di persona agli uffici addetti. Né bisogna tacere che una volta intrapreso l'iter bisogna attendere tempi tecnici non brevi (mesi). E tutto ciò con l'aggravante che non esiste possibilità di delega, da parte dell'anziano. Eppure già esistono modelli basati sulla delega, per la gestione telematica, dall'anziano al care-giver: ad esempio in Trentino e recentemente in certe procedure INPS.

La richiesta obbligatoria di SPID ha spinto molti care-giver a passi indietro: non più uso della applicazione ma ritorno alle telefonate o alla preparazione di email non sicure, ad esempio per richiedere farmaci.

Queste zoppie o arretramenti delle proposte telematiche delle regioni contengono anche un altro pericolo; quello di non fare intravedere altri tipi di avanzamenti della cultura digitale dei cittadini e dei medici (in particolare dei Mmg). Ad esempio vari software di cartella clinica contengono uno spazio inziale (box o cassetto) condiviso tra medici e pazienti. Sono ecosistemi protetti (server sicuri) ove ad esempio il paziente può richiedere/ricevere le ricette ripetute o caricare dei referti. L'impressione è che sia le istituzioni sia le softwarehouse non abbiano divulgato queste potenzialità. Si tratta di una possibilità almeno complementare ai progetti regionali e statali di FSEr.

La richiesta obbligatoria di SPID ha spinto molti care-giver a passi indietro: non più uso della applicazione ma ritorno alle telefonate o alla preparazione di email non sicure, ad esempio per richiedere farmaci cronici

L'emergenza Covid19 ha costretto i Medici di medicina generale (Mmg) a ridurre i flussi di pazienti presso lo studio e aumentare la propria reperibilità telefonica e l'uso contemporaneo un po' confondente di più canali comunicativi, al posto del contatto diretto: sms, messaggistica, email…

C'è da segnalare che mentre le soluzioni regionali e delle softwarehouse delle cartelle mostrano difetti o incompletezze, avanzano iniziative legate ad uso individualistico di piattaforme di messaggistica (soprattutto whatsApp). Come soci di SicurDott abbiamo ricevuto segnalazioni di iniziative da parte dei care-giver che tendono ad evitare le visite dirette attraverso l'invio al medico di risultati di ogni sorta (referti, foto). La telemedicina, con l'emergenza sanitaria legata al Covid, ha registrato un vero e proprio boom di interesse fra gli operatori del settore. Ma bisogna porre attenzione: la Telemedicina fa esplodere le possibilità di diagnosi e monitoraggio, ma questa pletora di novità può mettere in difficoltà gli stessi operatori del settore perché bypassati da Algoritmi e intelligenze artificiali poco attendibili e definiti.

Se una persona ha un problema di salute e chiede la soluzione in rete ottiene tramite un'applicazione di intelligenza artificiale una risposta "generalizzata" basata su statistiche, perché il sistema che sta alla base dell'AI non è personalizzato. Non ha ad esempio il "Patient Summary", il quadro clinico personalizzato che ha il Medico di Famiglia, basato sia sulla conoscenza delle patologie e sulle familiarità correlate ma anche sugli aspetti di

vita privata che condizionano il vissuto del paziente, ottenuti nella relazione Medico - paziente, costruita sulla fiducia e sul segreto professionale. La questione della "cessione totale" - verso Server istituzionali esterni - delle informazioni intorno ai propri pazienti raccolte dal Medico di famiglia è oggetto anche di contraddittorio etico legato alla delicatezza dei dati raccolti e al segreto professionale del Medico stesso.

In conclusione

Bisogna a questo punto ribadire che la nostra Associazione, pur consapevole dei seri difetti dell'attuale sanità digitale, è del tutto favorevole alla possibilità di partecipazione all'innovazione, purché essa coltivi l'armonia delle due facce:

- la diffusione oculata di dati medici;
- lo sviluppo giuridico e tecnologico di saldi elementi di sicurezza e di conservazione di confidenzialità nel mondo della Rete.

L'APS SicurDott ETS già nel 2018 aveva le idee chiare su quello che poteva essere, ed in parte è, la sanità digitale ma i nostri interlocutori istituzionali spesso non hanno ascoltato le nostre motivate perplessità pur essendo da noi espresse come critiche costruttive, con delle indicazioni attuative tecnicamente provate ed espresse da riconosciuti esperti a livello nazionale ed internazionale dei vari settori (medico, organizzativo, tecnologico, sicurezza informatica).

Adesso speriamo che aumenti la consapevolezza dei crescenti problemi dell'attuale sanità digitale: ci riferiamo agli hackeraggi (anche di interi server regionali: vedi la debacle da ramsoware di Laziocrea), alle disfunzioni tecniche e gli insuccessi di vari progetti. Queste preoccupanti emergenze non possono non condurre ad un vasto progetto, per cittadini e medici, di alfabetizzazione sull'uso consapevole di Internet e delle reti in sanità, con particolare riguardo alla sicurezza e privacy e alla reale "cittadinanza digitale".

PANDEMIA, TELEMEDICINA E TUTELA DEI DATI

Daniele Iselle
Vice Presidente dell'Unione Parkinsoniani di Verona o.d.v.

La pandemia Covid-19 ha prodotto un impatto durissimo sull'erogazione di prestazioni sanitarie. Il report del GIMBE 1/2021[1] ha effettuato un confronto del numero di prestazioni sanitarie erogate in Italia nel 2020 rispetto al 2019. È stato rilevato un impatto pesantissimo: un totale di 1,3 milioni di ricoveri e 144,5 milioni di prestazioni di specialistica ambulatoriale in meno.

L'Associazione Nazionale Francese Parkinson, in collaborazione con un Centro Parkinson hanno effettuato uno studio[2] mediante un sondaggio online su oltre 4700 pazienti.

Questi i risultati: la fisioterapia è stata interrotta nell'88,6% dei pazienti ed il 40,9% riportava un peggioramento dei sintomi. Sulla base del questionario, il dolore (9,3%), la rigidità (9,1%) e il tremore (8,5%) erano i tre sintomi più frequentemente peggiorati. Sulla base dell'autovalutazione effettuata, i sintomi motori rappresentavano il dominio più colpito, seguito dal dolore e dallo stato psichico.

L'Università Cattolica di Milano, in partnership con Confederazione Parkinson Italia e Fresco Parkinson Institute, ha a sua volta promosso uno studio[3] indirizzato ad approfondire l'impatto della pandemia Covid-19 sul percorso assistenziale e sulle condizioni psico-sociali delle persone con Parkinson in Italia.

I risultati dello studio hanno evidenziato come, a causa dei provvedimenti di lockdown sanitario, un gran numero di malati di Parkinson abbia incontrato difficoltà di accedere alle cure. Ben il 66% ha dichiarato di avere interrotto per lunghi periodi le attività di riabilitazione, il 55% ha ricevuto disdette da parte delle strutture sanitarie o dei medici per visite mediche programmate, mentre il 29% ha cancellato personalmente le prenotazioni per paura di contrarre il virus. Il 26% ha avuto problemi nel contattare il proprio medico di famiglia e il 23% ha registrato analoghe difficoltà a mettersi in contatto con il proprio neurologo. Sul piano psico-sociale, un Parkinsoniano su due ha vissuto un aggravamento del senso di solitudine e di un complessivo peggioramento della qualità della vita.

Appare quindi evidente come la telemedicina rappresenti una risorsa decisiva per la ripartenza dell'assistenza sanitaria, tramite il ricorso a tecnologie innovative, in particolare alle Information and Communication Technologies (ICT), in situazioni in cui il professionista della salute e il paziente (o due professionisti) non si trovano nella stessa località.

Riguardo alle attività ambulatoriali le interazioni a distanza tra sanitari e assistiti possono avvenire nei seguenti tre modi:

Televisita: consiste in una interazione a distanza tra il medico e il paziente con l'eventuale presenza di un caregiver; può dar luogo alla prescrizione di farmaci accertamenti diagnostici o di terapie.

Durante la Televisita un operatore sanitario che si trovi vicino al paziente può assistere il medico.

Se tale visita anche a distanza garantisce tutti i requisiti di quella erogata in presenza può essere considerata come prestazione specialistica ai sensi della normativa vigente.

1. Fabbri M, et al. A French survey on the lockdown consequences of COVID-19 pandemic in Parkinson's disease. The ERCOPARK study. Parkinsonism Relat Disord. 2021 Jul 13;89:128-133.

2. https://www.tecnomedicina.it/vivere-il-parkinson-al-tempo-del-covid-19

3. https://www.salute.gov.it/portale/ehealth/dettaglioContenutiEHealth.jsp?lingua=italiano&id=5525&area=eHealth&menu=telemedicina

Teleconsulto: consiste in un'interazione consulenza a distanza tra due medici che può portare ad una indicazione diagnostica e/o di una scelta terapeutica senza la presenza fisica del paziente. Questa attività viene considerata come parte integrante dell'attività lavorativa dei medici e degli specialisti e come quella effettuata in presenza non necessita di una remunerazione a prestazione e pertanto di una tariffa ad hoc;

Telecooperazione: consiste nell'assistenza fornita da un medico o altro operatore sanitario ad un altro medico o altro operatore sanitario impegnato in un atto sanitario. Questa attività, a seconda dei casi, può essere ricondotta ad una delle precedenti in particolare ad una visita multidisciplinare o ad un teleconsulto.

TELEMEDICINA

CLASSIFICAZIONE		AMBITO	PAZIENTI		RELAZIONE
TELEMEDICINA SPECIALISTICA	TELE VISITA	sanitario	Può essere rivolta a patologie acute, croniche, a situazioni di post-acuzie	Presenza attiva del Paziente	B2C B2B2C
	TELE CONSULTO			Assenza del Paziente	B2B
	TELE COOPERAZIONE SANITARIA			Presenza del Paziente, *in tempo reale*	B2B2C
TELE SALUTE		sanitario	E' prevalentemente rivolta a patologie croniche	Presenza attiva del Paziente	B2C B2B2C
TELE ASSISTENZA		socio-assistenziale	Può essere rivolta ad anziani e fragili e diversamente abili		

* B2B: individua la relazione tra medici

B2B2C: individua la relazione tra un medico e un paziente mediata attraverso un operatore sanitario

B2C: individua la relazione tra medico e paziente

Tabella estratta dal documento "Telemedicina. Linee di indirizzo nazionale" del Ministero della Salute

Nel periodo pandemico e per far fronte alle difficoltà dei pazienti parkinsoniani e rispettive famiglie, la Confederazione Parkinson Italia Onlus e ParkinsonCare hanno messo a disposizione l'accesso gratuito alla teleassistenza infermieristica specializzata. Gratuiti anche i video consulti con i neurologi dell'Istituto Neurologico Carlo Besta di Milano e con fisioterapisti, logopedisti, terapisti occupazionali, neuropsicologi e neurologi del Fresco Parkinson Institute ed altri neurologi volontari.

"La teleassistenza si è rivelata una soluzione geniale - ha dichiarato Giangi Milesi presidente della Confederazione Parkinson Italia, che ha spiegato - *Mentre il sistema sanitario fronteggia l'emergenza Covid 19 con cambiamenti importanti e repentini, le persone con Parkinson, spesso sole, restano profondamente disorientate. ParkinsonCare diventa per loro una rassicurante bussola per navigare nel sistema sanitario in tempesta".* Anche il quadro di riferimento regolatorio ha avuto una accelerazione. A livello nazionale il CSS ha approvato le linee guida nazionali sulla telemedicina[4] e le regioni,

4. http://www.statoregioni.it/it/conferenza-stato-regioni/sedute-2020/seduta-del-17122020/atti/repertorio-atto-n-215csr/

in data 17/12/2020, hanno siglato l'accordo[5] sulle indicazioni nazionali per l'erogazione delle relative prestazioni. La telemedicina è una risorsa non solo per i pazienti, ma anche per i medici. Lo conferma un'indagine del Centro studi del sindacato e dell'Osservatorio innovazione digitale in sanità del Politecnico di Milano.

"L'88% dei medici ha dichiarato di essere interessato ad utilizzare il teleconsulto con gli specialisti, il 60% la tele-cooperazione (MMG-Specialista-paziente), il 74% le risorse destinate alla tele-salute, il 72% quelle per la tele-assistenza.[6]*"*

Nel Piano Nazionale di Ripresa e Resilienza PNRR - noto anche come NEXT GENERATION ITALIA- la Missione Salute viene divisa in componenti ed è focalizzata su due elementi:

- il primo è un cambio di paradigma nell'assistenza sociosanitaria basato sullo sviluppo di una rete territoriale che consenta una vera vicinanza alle persone secondo un percorso integrato che parte dalla casa come primo luogo di cura per arrivare alle Case della comunità e quindi alla rete ospedaliera;
- il secondo elemento è dato dall'ammodernamento delle dotazioni tecnologiche del SSN.

Specificatamente la prima componente - Assistenza di prossimità e telemedicina - mira a potenziare e riorientare il SSN verso un modello incentrato sui territori e sulle reti di assistenza socio-sanitaria a superare la frammentazione e il divario strutturale tra i diversi sistemi sanitari regionali garantendo omogeneità nell'erogazione dei Livelli Essenziali di Assistenza LEA a potenziare la prevenzione e l'assistenza territoriale, migliorando la capacità di integrare servizi ospedalieri servizi sanitari locali e servizi sociali. La seconda componente - innovazione ricerca e digitalizzazione dell'assistenza sanitaria - è finalizzata a promuovere la diffusione di strumenti e attività di telemedicina a rafforzare i sistemi informativi sanitari e gli strumenti digitali a tutti i livelli del SSN a partire dalla diffusione ancora limitata e disomogenea della cartella clinica elettronica. Rilevanti investimenti sono quindi destinati all'ammodernamento delle apparecchiature e alla realizzazione di ospedali sicuri tecnologici e sostenibili. Vedremo se il Governo e le Regioni saranno in grado di attuare questo ambizioso progetto.

Non mancano però dubbi e le riserve[7] sull'efficacia e sicurezza di questo metodo innovativo.

I requisiti che le strutture sanitarie sono chiamate a rispettare nell'erogazione dei servizi di telemedicina sono molto impegnativi e, ove non adeguatamente garantiti, possono dare adito a nuove e ulteriori forme di responsabilità medica

Il Garante della Privacy ha espresso da un lato apprezzamento sulla nuova tecnologia, ma anche preoccupazione per la tutela di un bene irrinunciabile qual è la tutela dei dati personali sensibili.

Per fare chiarezza sulle modalità applicative, il Garante, con provvedimento n. 55 del 7 marzo 2019 aveva già fornito: *"Chiarimenti sull'applicazione della disciplina per il trattamento dei dati relativi alla salute in ambito sanitario"*[8].

I medici possono trattare i dati dei pazienti, per finalità di cura, senza dover richiedere il loro consenso, ma devono comunque fornire loro informazioni complete sull'uso dei dati. Il medico che opera come libero professionista non è tenuto a nominare il Responsabile della protezione dati. Tutti gli operatori del settore dovranno tenere un registro dei trattamenti dei dati.

5. http://www.quotidianosanita.it/lavoro-e-professioni/articolo.php?articolo_id=86020.
6. https://www.ordinemedicimodena.it/assets/Uploads/Documento-Ordine-dei-Medici-Telemedicina-31.7.2020.pdf
7. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942
8. https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9091942

È invece richiesto il consenso, o una differente base giuridica, quando tali trattamenti non sono strettamente necessari per le finalità di cura, anche quando sono effettuati da professionisti della sanità. Ne sono un esempio i trattamenti di dati sulla salute connessi all'uso di "App" mediche (ad eccezione di quelle per la telemedicina), quelli effettuati per la fidelizzazione della clientela (come quelli praticati da alcune farmacie o parafarmacie), oppure per finalità promozionali, commerciali o elettorali.

L'Autorità ricorda che, sulla base dell'attuale normativa che regola il settore, permane la necessità di acquisire il consenso anche per il trattamento dei dati relativo al fascicolo sanitario elettronico, o per la consultazione dei referti online.

Il garante non si è limitato a dare indicazioni operative a tutela della privacy, ma ha applicato nei confronti dei trasgressori anche ingiunzioni e sanzioni pecuniarie[9].

I requisiti che le strutture sanitarie sono chiamate a rispettare nell'erogazione dei servizi di telemedicina sono molto impegnativi e, ove non adeguatamente garantiti, possono dare adito a nuove e ulteriori forme di responsabilità medica[10].

In Veneto il rapporto tra strutture sanitarie e paziente è gestito mediante il "*Sanità km zero Fascicolo*"[11], che permette di visualizzare e scaricare, senza alcun limite di tempo e da qualsiasi dispositivo, referti e altri documenti sanitari, prodotti da qualsiasi azienda sanitaria ed ospedaliera regionale. In realtà però, solo le strutture ospedaliere pubbliche alimentano la banca dati e permettono l'accesso, mentre alcune strutture ospedaliere private convenzionate non sono ancora collegate. Il pagamento del ticket sanitario on line è ancora incompleto.

La Regione Veneto, più in generale, nel farsi parte attiva in questo processo di cambiamento, ha disposto con Delibera della Giunta Regionale n. 568 del 5 maggio 2020 l'attivazione dei servizi di telemedicina presso le Aziende sanitarie e il contestuale monitoraggio di Azienda Zero per la definizione degli standard e dei requisiti organizzativi, operativi e tecnologici coerenti con la normativa nazionale sull'assistenza sanitaria a distanza.

Con successiva DGR n. 383 del 30 marzo 2021 ha approvato il Progetto per l'erogazione del servizio di Telemedicina ai pazienti affetti da Sclerosi Multipla.

Nell'allegato alla già menzionata delibera, la regione Veneto, individua anche i limiti della Telemedicina.

Essa non sostituisce la medicina tradizionale, ma la affianca e la integra con nuovi canali di comunicazione e tecnologie innovative con l'obiettivo di migliorare l'assistenza sanitaria e aiutare i cittadini ad accedere ed ottenere le migliori cure possibili.

Secondo la Regione, esistono tuttavia ancora oggi delle limitazioni culturali e tecnico-strutturali che rendono problematica una rapida applicazione della Telemedicina nella routine clinica che possiamo così sintetizzare:

- Non adeguata preparazione culturale sia del paziente e dei caregivers da un lato che degli operatori sanitari dall'altro;
- I pazienti che rifiutano a priori la televista sono la netta maggioranza;
- La televisita viene erroneamente percepita come un distacco - un abbandono da parte del medico;
- Anche molti operatori sanitari vivono la telemedicina come uno svilimento dell'atto medico.

È pertanto necessario avviare una campagna formativa e informativa rivolta al personale sanitario e alla popolazione generale.

9. Ordinanza ingiunzione nei confronti di Azienda Unità Sanitaria Locale Toscana Sud Est - 17 di-cembre 2020 [9529527]; Ordinanza ingiunzione nei confronti di Asl Ferrara: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1368946

10. https://www.studiocataldi.it/articoli/40733-responsabilita-medica-telemedicina-nel-ssn.asp#par6

11. https://sanitakmzerofascicolo.it/.

La Regione rileva poi difficoltà tecniche.

- Molti pazienti, soprattutto quelli di una certa età, non possiedono o non sanno usare il computer o spesso hanno computer obsoleti privi di webcam.
- I pazienti con più alta disabilità - difficoltà motorie agli arti superiori necessitano della presenza di un caregiver per gestire lo strumento informatico; lo stesso vale per i pazienti con deficit cognitivi.
- La rete internet dei pazienti è molto frequentemente instabile; può anche succedere che in alcune zone territoriale sia assente. La rete intranet dell'Azienda Ospedaliera è spesso lenta per il sovraccarico dovuto all'eccesso di collegamenti diurni.
- La mancanza di un contatto diretto con il medico può aumentare il percepito di una medicina non aderente al territorio e lontana dalle esigenze della popolazione.
- Il medico rischia di apparire come un burocrate della medicina e il rapporto medico-paziente potrebbe risentirne in modo negativo compromettendo l'aderenza alle terapie e ai monitoraggi soprattutto nelle malattie croniche.

La complicazione data dall'obbligo di SPIDè stata in parte risolta dall'INPS con la delega dell'identità digitale. La delega è lo strumento tramite cui gli utenti impossibilitati a utilizzare in autonomia i servizi online dell'INPS possono delegare una persona di fiducia all'esercizio dei propri diritti nei confronti dell'Istituto

Il rapporto medico di base - paziente è invece gestito mediante una app su smartphone *"App Sanità km zero Ricette"*[12].

Fermo restando che per utilizzare questi servizi è necessario un certo grado di competenza informatica, non così diffusa soprattutto nella popolazione anziana, si rileva che dal primo ottobre 2021 è entrata in vigore la legge per effetto della quale non è più possibile accedere ai servizi dei portali pubblici con credenziali diverse da SPID o CIE. (Decreto Semplificazioni - DL 16 luglio 2020, n. 76, convertito, con modificazioni, dalla L. 11 settembre 2020, n. 120)[13].

L'entrata in vigore di tale norma ha comportato un passo avanti sulla unificazione delle modalità di accesso ai servizi pubblici on line, ma un peggioramento significativo sul livello di accessibilità ai servizi on line in quanto l'utilizzo di SPID è notevolmente complicato e farraginoso.

Come è noto, l'accessibilità ai servizi con SPID, avviene su tre livelli:

Livello 1 - accesso mediante la combinazione di nome utente e password.

Livello 2 - accesso di livello 1, seguito dall'inserimento di una password monouso generata tramite SMS, app o token/dispositivo dedicato.

Livello 3 - accesso tramite smart card e password.

Ebbene, l'accesso ai servizi sanitari avviene esclusivamente a livello 2 e quindi, ogni volta che si accede, occorre inserire username e password ed attivare l'accesso monouso tramite sms, app, o token sul cellulare e questo complica, al netto dei frequenti malfunzionamenti, le modalità di utilizzo del servizio.

Appare altresì difficile, se non impossibile, utilizzare SPID senza essere in possesso e saper usare un cellulare.

12. https://salute.regione.veneto.it/web/fser/cittadino/app-sanita-km-zero

13. Ai fini dell'attuazione dell'articolo 64, comma 3-bis, secondo periodo, del decreto legislativo 7 marzo 2005, n. 82, come modificato dal comma 1, lettera e), numero 6), dal 28 febbraio 2021, **è fatto divieto** ai soggetti di cui all'articolo 2, comma 2, lettera a) del predetto decreto legislativo n. 82 del 2005 **di rilasciare o rinnovare credenziali per l'identificazione e l'accesso dei cittadini ai propri servizi in rete, diverse da SPID, CIE o CNS, fermo restando l'utilizzo di quelle già rilasciate fino alla loro naturale scadenza e, comunque, non oltre il 30 settembre 2021.**

La complicazione data dall'obbligo di SPID è stata in parte risolta dall'INPS con la delega dell'identità digitale. La delega è lo strumento tramite cui gli utenti impossibilitati a utilizzare in autonomia i servizi online dell'INPS possono delegare una persona di fiducia all'esercizio dei propri diritti nei confronti dell'Istituto. È anche lo strumento attraverso il quale i tutori, i curatori, gli amministratori di sostegno e gli esercenti la potestà genitoriale possono esercitare i diritti dei rispettivi soggetti rappresentati e dei minori.

Ma in telemedicina questo è possibile? Sembra proprio di no.

Il rigore applicato agli accessi mediante SPID trova riscontro nella pratica? Per esempio, quasi sempre il rapporto medico di base, paziente e farmacia avviene *"informalmente"* con l'utilizzo di whatsapp, sms, posta elettronica ordinaria, comunicazione telefonica...

Quasi mai i pazienti, e spesso anche i medici di base, sedotti dalla semplicità d'uso della messaggistica istantanea sono consapevoli delle conseguenze che tale utilizzo può comportare, in materia di privacy e di sicurezza delle informazioni.

Senza pretesa di completezza, potrebbe ad esempio accadere che:

- i dati sanitari trasmessi ai cellulari dei medici circolanti all'interno delle chat o e-mail vengano intercettati da attacchi informatici;
- in caso di utilizzo della messaggistica da parte del medico o del personale sanitario, il paziente - che per semplicità pretende dal medico l'utilizzo di tali forme di comunicazione - potrebbe non aver espresso preventivamente il consenso al trattamento dei propri dati tramite strumenti tecnologici e, in secondo luogo, potrebbe essere danneggiato da un utilizzo illecito degli stessi da parte di soggetti terzi. In questa situazione, il personale sanitario è il primo ad essere sottoposto a responsabilità, così come la struttura di riferimento;

- per effetto di *"contenziosi giudiziari"* familiari, il paziente potrebbe chiedere il tracciamento dei propri dati. In tale situazione, potrebbe emergere un utilizzo illecito dei dati da parte del personale sanitario che il paziente non aveva autorizzato. Infatti, i dati sanitari dei pazienti potrebbero trovarsi non solo all'interno dei sistemi offerti dalla Regione Veneto come sopra illustrati, ma anche all'interno del telefono di diversi medici e/o infermieri o nei server di posta privata degli stessi;
- alcune di queste applicazioni (whatsapp, mail, sms...) potrebbero avere dei server collocati al di fuori dall'Unione europea. In tal caso si configura un trasferimento dei dati all'estero, il quale, nel rispetto della normativa prevista dal GDPR, potrebbe avvenire solo con il consenso dell'interessato.

Al di là del rispetto delle leggi, ovviamente doveroso, si pone sempre il problema di trovare un giusto equilibrio tra esigenza di riservatezza e semplicità di utilizzo dei mezzi informatici.

Anche lo strumento del consenso presenta dei limiti enormi: ad esempio ogni volta che si utilizza il motore di ricerca Google ci viene chiesto di esprimere il consenso. Ma quanti di noi hanno mai letto le chilometriche pagine contenenti le condizioni del servizio. Ed anche se le leggessimo e non fossimo d'accordo possiamo rinunciare al servizio. Direi proprio di no, nessuno rinuncia e quindi il consenso diventa - in concreto - un'autorizzazione inconsapevole.

Ho effettuato una veloce ricerca nelle banche dati giuridiche ed ho scoperto che la fattispecie *"autorizzazione inconsapevole"* non esiste. Mi sono ricordato la profezia di George Orwell nel romanzo "1984": ***"a un tempo in cui il pensiero è libero, quando gli uomini sono differenti l'uno dall'altro e non vivono soli (...) a un tempo in cui esiste la verità e quel che è fatto non può essere disfatto dall'età del livellamento, dall'età della solitudine, dall'età del Grande Fratello, dall'età del Bispensiero".***

IL FASCICOLO SANITARIO ELETTRONICO: UNA CHIMERA RASSICURANTE?

Intervista al dott. Francesco Del Zotti
a cura della redazione di Torino Medica

La digitalizzazione del settore sanitario è uno strumento fondamentale per avere un SSN con modelli di assistenza più efficienti, sostenibili e partecipati.

Tra le applicazioni più innovative e interessanti nell'ambito della sanità digitale e della *connected care*, trova sicuramente il suo posto d'eccezione il Fascicolo Sanitario Elettronico (FSE), nato dal processo di dematerializzazione della documentazione sanitaria che ha investito, a partire dal 2011, anche le cartelle cliniche, le prescrizioni e i referti.

Il FSE dovrebbe essere lo strumento attraverso il quale il cittadino può tracciare e consultare tutta la storia della propria vita sanitaria, condividendola con i professionisti sanitari per garantire un servizio più efficace ed efficiente.

In molte regioni medici e pazienti però non usano il fascicolo. Ma allora quanti sono quelli che davvero utilizzano il fascicolo sanitario elettronico?

Vediamo per esempio alla fine del secondo trimestre del 2021, quanti medici di medicina generale e pediatri di libera scelta hanno utilizzato il FSE rispetto al numero di medici abilitato all'uso.

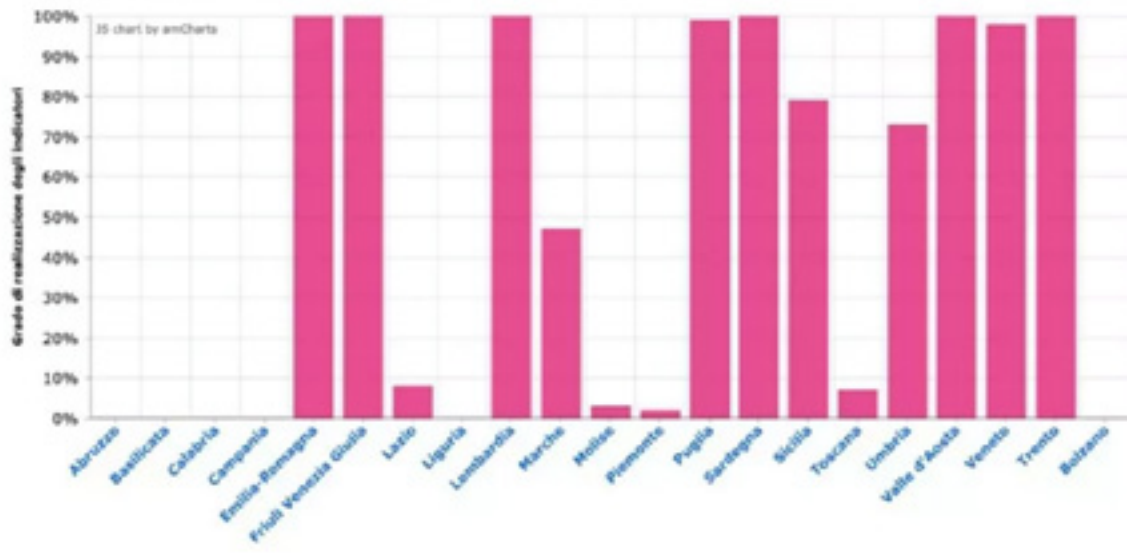


Grafico 2. Medici e pediatri che hanno utilizzato il Fse – Fonte: Agid Il trimestre 2021

Come si vede, in 6 regioni su 21 i livelli di utilizzo sono praticamente pari a zero. Solo in Emilia Romagna, Friuli Venezia Giulia, Lombardia, Sardegna, Valle d'Aosta e la provincia autonoma di Trento la percentuale arriva al 100%.

Le percentuali di utilizzo da parte dei medici crollano se, invece, si guarda un preciso indicatore: il numero di *Patient summary* forniti dai medici rispetto al numero complessivo di FSE attivati. Quasi tutte le regioni registrano percentuali pari a zero, tranne il Friuli Venezia Giulia, la Sicilia, l'Umbria e la Valle d'Aosta.

Da una recente analisi dell'Osservatorio Innovazione Digitale in Sanità del Politecnico di Milano, ricordiamo, inoltre, che in Italia non più del 60% dei medici specialisti e dei medici di medicina generale ha sufficienti competenze digitali di base, legate all'uso di strumenti digitali nella vita quotidiana. Ma la percentuale scende al 4% se si considera il raggiungimento di un livello soddisfacente in tutte le aree delle competenze digitali professionali (le cosiddette eHealth Competences).

Alla luce di questa riflessione generale abbiamo deciso di chiedere un approfondimento al Dott. Francesco Del Zotti, medico di medicina generale, nominato membro esperto della Commissione Information Communication Technology della FNOMCeO.

Dott. Del Zotti, da tempo lei studia e analizza la questione del FSE. Partiamo dalle origini?

La concreta attuazione del fascicolo sanitario elettronico non risulta, al livello nazionale, ancora pienamente realizzata e, nelle regioni che già da tempo hanno implementato tale procedura, i sistemi meriterebbero forse una revisione, in termini non solo di efficienza operativa, ma anche di logiche di archiviazione e di utilizzo.

Ad esempio, da più parti i sistemi fondati sulla prevalente circolazione degli statici Pdf. Oppure FSE eventualmente basati sulle SOLE codifiche: vengono posti in discussione e si evidenziano i rischi di una limitazione del ragionamento clinico legati ad una chiusura precoce dei problemi, nonché ad una

visione limitata a brevi e fissi codici, in una Rete che è da almeno 10 anni in grado di processare sia testi liberi, sia audio che video.

La sfida quindi diventa duplice: realizzare le basi di un sistema informatico che garantisca al cittadino l'utilizzo delle informazioni e ottimizzarlo al passo dell'evoluzione delle nuove tecnologie informatiche.

Se si vuole avviare una rivoluzione epocale dal punto di vista informatico, allora bisogna assumersi in pieno la responsabilità di mettere in campo le energie necessarie per questa scelta e mettere i medici nelle condizioni di poter lavorare in modo corretto.

Dott. Del Zotti, ci può quindi dare un'istantanea reale, tra benefici e rischi del FSE?

In primo luogo essendo digitale e disponibile online sulla rete elettronica, il Fascicolo Elettronico sarà fruibile, in qualsiasi momento e attraverso qualunque dispositivo, da ogni soggetto abilitato ad accedervi.

Ogni fascicolo potrebbe essere sempre aggiornato all'ultimo "episodio clinico" che il paziente, o chi per lui, avrà caricato sul sistema. Tutto ciò dovrebbe fornire la possibilità di realizzare una più stretta collaborazione tra medici di famiglia, medici di continuità assistenziale, reparti e aziende ospedaliere diversi.

Ciò dovrebbe comportare una semplificazione della situazione odierna, in cui un paziente può arrivare ad avere anche più di 20 cartelle cliniche diverse (una per ogni reparto in cui è stato ricoverato). Ne deriverebbe un risparmio da parte dell'assistito di tempo e di certo si eviterebbero spostamenti per il recupero dei documenti. Vi è poi la possibilità di un una ricetta completamente dematerializzata, senza la necessità di ritirare fogli cartacei del medico: con il ritiro dei farmaci direttamente in farmacia usando la tessera sanitaria o lo smartphone, cosa che già avviene in alcune regioni.

L'assistito avrà anche la possibilità di avere la sua storia clinica sempre e ovunque permettendo a chi lo prenderà in cura di avere un accesso veloce e diretto alle informazioni necessarie.

Così dovrebbe beneficiarne anche la collaborazione tra Medici di Medicina Generale, Medici Specialisti e Pazienti, che comunque devono effettuare una scelta preliminare: aderire o non aderire al fascicolo (consenso o dissenso informato). Se il paziente decide di aderire dovrà decidere se in toto o parzialmente, ad esempio esercitando il diritto all'oscuramento di alcuni dati: e ciò solo nel caso in cui le regioni avranno realizzato una flessibilità tecnica del FSE, che oggi spesso ancora non si vede all'orizzonte. Le migliori modalità per concedere da parte dei pazienti il consenso alla regione e ai medici, sia le regole in forza delle quali essi possano esercitare l'esercizio del diritto all'oscuramento sono soggette a valutazioni legali e tecniche non ancora ben risolte in maniera univoca. Inoltre, tra i vantaggi, ricordiamo che l'accumulo di dati elettronici (Big Data) può favorire la ricerca statistico-epidemiologica. Ma si badi bene: per abilitare questa funzione di ricerca non servono i dati nominativi, ma sono più che sufficienti dati anonimizzati, mentre a volte si ha la sensazione che alcune istituzioni pubbliche (sanitarie e non) spingano verso la (eccessiva) raccolta a strascico di dati nominativi, vista come unica pre-condizione per poter effettuare valutazioni di ricerca pubblica.

Pensiamo però adesso al reale buon funzionamento degli allineamenti previsti.

Servono tempo, denaro e grandi capacità tecniche e manageriali per allineare i diversi tipi di dati, le diverse cartelle, le diverse aree geografiche intra-regionali ed extra-regionali (anche perché si è permessa un'architettura del FSE su base regionale più che statale). Se uno di questi fattori non funziona, vi è crisi dell'intero apparato, che tra l'altro non potrebbe più usare agevolmente le procedure precedenti, su carta o su Personal computer del medico o del reparto.

Un secondo aspetto critico riguarda l'utilizzo di "identificatori forti". Sino a poco tempo fa il medico ed il paziente erano identificabili con la firma per esteso su documenti cartacei.

Invece, attualmente siamo in una situazione rischiosa di passaggio, ove non poche volte la persona-paziente o la persona-medico vengono riconosciute dal sistema o con identificatori deboli (*User* e *Password*). In verità aumentano le realtà sanitarie in cui si concede "l'identità digitale" ai medici e pazienti ad es mediante lo SPID; ma esse sono ancora poco diffuse e tecnicamente poco fruibili.

Lo Spid, tra l'altro, presenta non poche difficoltà logistiche e di fruibilità in particolare per i pazienti anziani o fragili.

Un altro aspetto importante: Privacy e dati sensibili.

Quello di difendere insieme sia la segretezza dei dati del paziente sia, quando opportuno per il paziente, la trasmissione ad altri operatori sanitari, è un tema importante attuale: si tratta di dati sensibili e riservati di cui il paziente è il titolare ultimo.

In realtà la Rete attuale, anche quella più "protetta", è esposta ad un rischio: a fronte di una grande semplicità e velocità della trasmissione e viaggio dei dati in Centri di Raccolta (regionali o statali), esistono ancora, in tutto il mondo, e anche nei sistemi più avanzati, comprovati rischi non trascurabili nelle fasi di trasferimento e conservazione, con possibilità che vi sia danno o da sguardi indiscreti o da azioni criminali (intrusione, visione non-autorizzata, manipolazione, furto dei dati), come il recente caso di LAZIOcrea dimostra. Esistono norme tecniche e giuridiche per ridurre i rischi sopra descritti, modalità che comunque necessitano di volontà politica, investimenti tecnologici, finanziamenti per la formazione del personale e degli stessi utenti.

Inoltre, non sempre sono ben chiarite ai medici ed ai pazienti le regole ed i meccanismi di inserimento-esclusione di certe patologie nel FSE. Per quanto riguarda l'inserimento di informazioni particolarmente delicate (ad es: presenza di Aids, o uso di alcolici, aborti) sarà necessario ottenere un ulteriore consenso specifico e dovrà essere garantita la possibilità di "oscurare" alcuni dati o documenti sanitari che non si intenda far confluire nel dossier; ma ciò dipende, come già detto, anche da specifici investimenti tecnologici e formativi. Esistono poi malattie delicate ma che sembrano non rientrare nell'elenco precedente; ad esempio: epatite virale, tumore, TBC.

Riguardo alle misure di sicurezza (come proteggere i dati elettronici da furti o da sguardi indiscreti nelle reti di Computer) sarà obbligatorio per le strutture sanitarie comunicare sia il luogo fisico sia le modalità di tenuta nei Computer sia (e immediatamente) all'Autorità Garante eventuali casi di *"data breach"* (violazioni o incidenti informatici, come attacchi, accessi abusivi, perdita, furto).

Il paziente inoltre dovrebbe avere la possibilità di tener traccia di tutti gli accessi eseguiti dai vari operatori sul proprio dossier (il cosiddetto "Log"). L'accesso al dossier ospedaliero o al FSE sarà comunque consentito, oltre che al paziente, solo al personale sanitario coinvolto negli episodi di cura; e dovranno essere individuati criteri per rendere segreti (cifratura) i dati sensibili.

Aggiungiamo che il paziente-cittadino il più delle volte non è stato opportunamente formato per accedere, consultare e quindi usare le informazioni del suo FSE.

C'è quindi una reale difficoltà di interpretazione dei dati sia per chi li deve organizzare a fini clinici sia per chi li deve leggere come utente.

Ma quindi il FSE fa davvero risparmiare?

Sempre di più leggiamo sui giornali che la ricetta dematerializzata, il FSE, ed il Patient summary permetteranno forti risparmi. La velocità con cui le autorità stanno propugnando queste novità e la possibilità che le regioni perdano forti incentivi se non aderiscono a questi progetti in una data scadenza stanno alimentando un pericoloso sillogismo: i vantaggi economici sono "sicuramente scontati".

Al di là degli esempi europei negativi (si veda per esempio lo stop al progetto inglese "Care Data" di alcuni anni fa), quando si deve fare un bilancio tra vantaggi e costi, bisogna mettere nel computo una serie di effetti negativi non ben previsti dai progetti:

1. quanto costa per il singolo ambulatorio o per la singola struttura tenere aggiornati e sicuri il proprio PC, router, server, cloud? Quanto costa la formazione dei medici e del personale per evitare le frequenti trappole tese dagli hacker? E quanto costa alle Medicine di gruppo l'eventuale attivazione del DPO?
2. quanto costa l'eventuale compromissione del rapporto fiduciario ad opera dei non piccoli rischi e difetti dello sharing dei dati sensibili?
3. quanto costa il discreto disturbo del lavoro dei MMG e della relazione medico-paziente ad opera di piattaforme telematiche a volte non ergonomiche (si veda in caso dell'esposto alla magistratura di un gruppo di MMG di una regione italiana, a causa di perdite dati e non poche interruzioni del lavoro)?
4. è stato infine soppesato il rapporto costi-benefici rispetto a più agili alternative praticabili?

Ad esempio la gestione di una "tessera sanitaria" evoluta che sia gestita dai pazienti e non dalle istituzioni (vedi ad es. il sistema svizzero *lifepassport*); o ad esempio il sistema *MedicAlert*, basato su braccialetti o collari di metallo, con incise poche fondamentali notizie, promosso tra l'altro dal noto guru della Sicurezza l'ing. prof. Ross Anderson: esso avrebbe il vantaggio di essere utilizzabile in tutto il globo, anche nelle realtà senza PC e senza Rete. Né, infine, è da tacere una modalità alternativa o almeno complementare al FSE: l'attivazione nelle cartelle computerizzate dei MMG di aree di interazione attiva, e cifrate, tra pazienti e loro MMG. Esistono intanto dei primi "esperimenti" in tal senso di alcune aziende di cartelle computerizzate usate da molti MMG. Bisogna informare i pazienti di queste possibilità; ed è necessario che le istituzioni incoraggino in tutti i modi sia le s*oftware house* sia gli stessi MMG.

Come ha già evidenziato in più occasioni dal Professor Coiera (Coiera E. (2011) *"Do we need a national electronic summary care record?" MJA 2011; 194 (2): 90-92)* possiamo codificare in modo schematico alcune osservazioni sul FSE che sono anche le criticità di fondo:

- lo sharing del Patient summary a volte sembra essere priorità politica e tecnica più che clinica;
- nel caso di "estrattori automatizzati" si incorre in ovvie imprecisioni dell'automatismo e rischi simili a quelli dei piloti che, "drogati"dagli automatismi, scordano il come manovrare la cloche;
- se l'aggiornamento è "manuale": la manutenzione costante della lista problemi da parte dei MMG implica molto tempo perso e sottratto ad attività cliniche e relazionali importanti;
- pensiamo ai rischi anche di Pronto Soccorso e specialisti che si affidino a Patient summary incompleti (per dati cruciali o con pletora di problemi piccoli o vecchi, non "puliti";
- Non da ultimo i rischi da centralizzazione snaturante delle cure.

Parliamo adesso di un aspetto fondamentale proprio sul piano della relazione medico-paziente: il Consenso informato.

Questo è uno dei passaggi più importanti. A livello internazionale sono state individuate due strategie: una è quella del sistema *Opt-out* e l'altro è quello del sistema *Opt-in*.

Facciamo l'esempio della legislazione per i trapianti d'organo:

• **Opt-out**: è legato a legislazioni favorevoli ad una pratica (ad es. favorevole ai trapianti di organo), ove il cittadino che vuole restarne fuori con un no, deve espressamente inviare un modulo sottoscritto di suo pugno;

• **Opt-in**: in questo caso il cittadino può entrare nella lista dei donatori solo se espressamente sottoscrive un modulo in cui dichiara il suo sì.

In alcune realtà come l'Inghilterra, per il "Patient summary" tempo fa è stato usato il sistema opt-out. Ciò ha comportato gravi problemi e gravi accuse, al punto da dare costringere le autorità a congelare l'avvio del FSE. Ha fatto scandalo la richiesta di opt-out a cittadini inglesi attraverso semplici depliant, che magari neanche arrivavano nella buca postale dei cittadini che avevano peraltro bloccato la pubblicità in cassetta (BMJ Mccartney,2014).

La legge europea del GDPR del FSE prevede un consenso per *opt-in*, raccolto in maniera non equivoca ed esplicita e possibilmente scritta o con SPID. Ma alcuni report su ciò che sta succedendo nei luoghi in cui si acquisisce il consenso scritto (strutture amministrative ospedaliere o di Asl; farmacie; alcuni ambulatori medici) fanno pensare che esista il concreto rischio di usare tappe forzate che possono sincopare il tempo necessario per un realmente consapevole opt in. Gli ultimi regolamenti attuativi in diverse regioni hanno permesso il solo consenso orale del paziente; questo allentamento è stato favorito altresì dal Covid.

L'*opt-in* costa più tempo rispetto all'opt-out, e impiega maggiori risorse (ad es. per preparare moduli scritti, o per la formazione *ad hoc* a favore di moduli comunicativi orali comprensibili, completi e corretti in termini relazionali), ma alla lunga è nettamente superiore.

In buona sostanza serve attivare un filone di ricerca nel campo degli aspetti etici, relazionali, educativi per dare vita ad un consenso informato dinamico.

Io ritengo che ci voglia un approccio davvero multidisciplinare che metta nelle condizioni di creare una rete di lavoro per la raccolta del consenso. Non è necessario che tutto il lavoro di raccolta informazioni e aggiornamento proconsenso venga svolto solo dal medico, con il rischio di forzature snaturanti la Professione e con la sottrazione di tempo alla relazione clinica.

Per concludere la medicina fiduciaria, ippocratica, funziona da 2400 anni; non saranno i soli 50 anni di Internet, costellati ultimamente da gravi incertezze sul livello democratico e di sicurezza delle attuali reti, a cancellare Ippocrate. La Rete deve adattarsi a questa lunga storia e non si deve pretendere che sia la professione medica a piegarsi al suo sviluppo, spesso precipitoso ed informe.

Credo che sia fondamentale studiare un sistema di apertura e consultazione del FSE che permetta di uscire dalla logica per cui è la raccolta del dato che viene messo al centro, e non la relazione personale medico-paziente.

Sarebbe necessario fondare dei Comitati Etici ad hoc che riflettano sull'uso delle informazioni e dei dati stessi.

A mio avviso è necessario coniugare lo sviluppo della medicina in Rete con l'approccio analitico-anamnestico e relazionale, piuttosto che quello archivistico, perché spesso la grande quantità di dati inficia sia la lucidità clinica sia l'armoniosa comunicazione medico paziente.

Dott. Del Zotti, ma allora di chi è il dato sanitario e cosa può produrre come effetto sui cittadini non "educati"?

La questione è delicata. Ad esempio può avere risvolti a volte drammatici ciò che avanza: la fruizione diretta delle banche-dati da parte del cittadino, con tempi e modi che a volte precedono la stessa comunicazione medico-paziente. È già successo, ad esempio, con il venire a conoscenza, in anteprima da parte del paziente, di una diagnosi di tumore maligno: in questi casi il paziente è stato deprivato della necessaria protezione della relazione con il suo medico. Non possiamo lasciare che un processo pericoloso vada in autonomia, senza analisi, senza interventi strutturati.

Ripeto l'importanza di attivare Comitati Etici che studino da vicino il problema, come normalmente si fa per la sperimentazione farmacologica. Che creino un vero e proprio processo a partire dai processi reali e non dagli obiettivi attesi dai tecnologi.

Io immagino gruppi di ricerca seri in cui si attivi un confronto interdisciplinare, tra medici, filosofi, giornalisti,giuristi e pazienti esperti…insomma una comune area di ricerca approfondita, equipaggiata e partecipata.

Regioni e Stato hanno il dovere di seguire e sostenere questi Comitati Etici, visto che hanno voluto questo cambiamento epocale. A questo punto devono farsi carico di fornire tutti gli strumenti per affrontarlo, senza aspettarsi che i medici risolvano tutto da soli.

Sanità SOTTO ATTACCO

LE PRIORITÀ PER LA RESILIENZA E LA SICUREZZA DELLA SANITÀ DIGITALE E DEI DATI DEI PAZIENTI. UNO SGUARDO DAGLI STATI UNITI ALL'EUROPA.

Laura Tonon, *Il Pensiero Scientifico Editore*

"È in corso un potente attacco al Ced regionale. I sistemi informatici sono tutti disattivati compresi quelli del portale Salute Lazio e della rete vaccinale". "È un attacco senza precedenti per il sistema informatico". Ancora: "Un attacco clamoroso". Sono alcuni dei tweet dell'assessore regionale alla Sanità del Lazio, Alessio D'Amato. Era il primo giorno di agosto che si prospettava essere un mese particolarmente "caldo". Solo tre mesi prima, a maggio, c'erano stati altri tre massicci attacchi informatici alle strutture sanitarie in tre differenti paesi: Irlanda, Canada, Nuova Zelanda. Il personale degli ospedali era stato costretto a tornare all'uso di carta e penna, interventi chirurgici ed esami diagnostici bloccati. "I responsabili non si preoccupano del grave impatto che un atto del genere può avere sui pazienti che necessitano di cure e sulla privacy di coloro le cui informazioni private sono state rubate. Gli attacchi ransomware sono crimini spregevoli, soprattutto quando prendono di mira infrastrutture sanitarie critiche e dati sensibili dei pazienti", scriveva nel comunicato stampa il governo irlandese che dall'oggi al domani si è trovato a dover chiudere temporaneamente i sistemi informatici dell'Health Service Executive, compreso quello del portale del programma vaccinale in corso. "Un'interruzione di tale portata dei servizi per la salute è da condannare, ancor di più in questo momento di emergenza sanitaria per la pandemia. C'è il rischio che i dati sanitari e di altro genere dei pazienti vengano impropriamente utilizzati".

AMBIENTI E DATI A RISCHIO, SOTTO RISCATTO

Il comune denominatore di questi attacchi è il *ransomware*, virus informatico molto insidioso che una volta penetrato nel dispositivo ne blocca le funzioni e rende illeggibili i file cambiandone il formato con l'esplicita intimidazione di cancellarli se non viene pagato un riscatto ("ransom" in inglese significa "riscatto", "ware" sta per software). È la stessa tipologia dei virus dell'attacco passato alla storia con il nome di *WannaCry* che a maggio del 2017 aveva bloccato la sanità britannica causando dei danni di 92 milioni di sterline e con essa a molte altre organizzazioni e aziende dislocate in un centinaio di paesi: oltre 230mila i computer fermati quasi in contemporanea dallo stesso ransomware in tutto il

mondo. L'importo di riscatto per ciascun computer era inizialmente l'equivalente di 275 euro in bitcoin che raddoppiava se non veniva pagato entro pochi giorni[1].

Gli autori dell'attacco informatico irlandese avevano chiesto 16 milioni di euro minacciando di rilasciare i dati rubati sul dark web, per scopi illeciti. Stando alle dichiarazioni ufficiale il Governo irlandese non ha ceduto. Anche alla Regione Lazio era stato richiesto un riscatto. "Hello Lazio! I vostri file sono stati criptati. Per favore non cercate di modificarli o rinominarli, potrebbe portare a una perdita dei dati", era il messaggio che compariva negli schermi dei computer della Regione. A seguire il link per il pagamento del riscatto con le istruzioni per ottenere lo sblocco. Non è noto se la Regione Lazio abbia pagato[2].

"Si stima che nel 2020 i proventi da estorsioni informatiche abbiano raggiunto i 350 milioni di dollari nel mondo, considerando soltanto gli incidenti noti (molti preferiscono non rendere pubblico l'attacco). Una situazione insostenibile che sta spingendo i Governi dei principali Paesi a prendere misure drastiche per ridurre la portata del problema", ha riportato Elena Vaciago, Associate Research Manager di The Innovation Group sulla cybersecurity, all'ultimo Digital Italy Summit[3]. "Il ransomware, utilizzato a scopo di lucro, può infettare anche i sistemi di controllo industriale, diventando quindi una potenziale arma distruttiva. Un esempio dei pericoli che corrono oggi quanti collegano infrastrutture critiche a Internet (di solito per ottenere incrementi di efficienza e di operatività) viene da incidenti come quello avvenuto lo scorso marzo a Colonial Pipeline, il più grande oleodotto degli Stati Uniti, utilizzato per rifornire di carburante tutta la East Cost americana".

CYBERATTACCHI DIETRO L'ANGOLO

Negli ultimi anni gli attacchi informatici a infrastrutture nazionali e ambienti industriali sono cresciuti a tassi preoccupanti, e ancor di più con la pandemia COVID-19 che ha portato a un più ampio utilizzo del digitale sia nel settore pubblico (dalle amministrazioni pubbliche alla scuola e alla sanità) che in quello privato. Per gli hacker questo ha significato avere più ambienti digitali critici attaccabili. Secondo i dati pubblicati a giugno 2021 da ENISA, l'agenzia europea per la cybersecurity, gli attacchi significativi a infrastrutture critiche sarebbero stati 304 nel 2020, contro i 146 del 2019. Le cyber minacce agli ospedali e sistemi di cura sarebbero cresciute del 47%, spesso accompagnate da note di riscatto (ransomware) per il ripristino dei dati cifrati. Altre fonti indicano che in piena emergenza sanitaria gli attacchi a tema COVID-19 indirizzati alle strutture sanitarie si sono divisi tra tentativi di estorsione di denaro (55%) e tentativi di spionaggio ai danni di centri di ricerca sui vaccini per l'acquisizione di informazioni rilevanti (45%)[4].

L'analista di mercato sui trend dell'innovazione digitale -Elena Vaciago- aggiunge che "siamo arrivati a una situazione in cui nel mondo, ogni ora, si verificano tra i 5 e i 10mila attacchi informatici. Le minacce di cybersecurity sono in continua evoluzione: viene creato un nuovo malware su scala globale ogni mezzo secondo. Gli aggressori sfruttano sempre di più automatismi per lanciare i propri attacchi, mentre i meccanismi di difesa e *cyber threat intelligence* sono ancora, per la maggior parte, manuali. Tutto questo crea un'asimmetria che nel tempo diventa sempre più difficile da superare".

1. Frediani C. Cybercrime. Attacchi globali, conseguenze locali. Milano: Ulrico Hoepli Editore, 2019.

2. Carboni K. È scaduto (senza conseguenze) l'ultimatum dato alla Regione Lazio dai criminali informatici. Wired, 9 settembre 2021.

3. Vaciago E. Reimaging resilience after disruption: ridurre il rischio cyber nell'industria 4.0. Digital Italy Summit 2021 La resilienza del digitale, Roma 18-20 ottobre 2021.

4. Rapporto Clusit 2021 - Edizione di ottobre 2021. https://clusit.it/rapporto-clusit/

Che i cyberattacchi sarebbero aumentati durante la pandemia era stato previsto da tutti i servizi segreti del mondo. La National Security Agency statunitense aveva allertato i sistemi informativi sanitari che trattano dati sensibili dei cittadini. "In realtà, non possiamo escludere che nel nostro Paese vi siano state diverse aggressioni oltre quella alla Regione Lazio. Chi viene attaccato tendenzialmente cerca di non renderlo pubblico e di limitarsi a comunicarlo alle istituzioni preposte. La direttiva europea NIS ha infatti introdotto l'obbligo di notifica degli incidenti informatici con impatto rilevante al fine di poter predisporre delle difese in caso di attacchi simili", spiega a Torino Medica Andrea Rossetti, professore associato di filosofia del diritto all'Università di Milano Bicocca, dove tiene anche i corsi di "Informatica giuridica"

"Quindi brancoliamo un po' nel buio. Non sappiamo con precisione quante aziende ospedaliere e sanitarie siano state attaccate e secondo quali modalità, e quanti dati sanitari siano stati sottratti. L'attacco alla Regione Lazio è diventato inevitabilmente pubblico perché ha bloccato l'intero sistema informatico ma ci sono altre aggressioni che possono essere altrettanto pericolose, in termini di sottrazione di dati sanitari, che passano inosservate perché si misurano in furti di pochi byte quotidiani ma ripetuti. Essendo attacchi a bassa intensità è difficile intercettarli in un flusso quotidiano di svariati gigabyte".

AL CUORE DELLA SICUREZZA INFORMATICA

I cyberattacchi rientrano nella top five della classifica dei principali rischi globali per il breve termine del World Economic Forum. Lo sono sia per i furti d'identità e di denaro (82% degli interpellati) sia per l'impatto sulle infrastrutture (80%). Secondo il Global Risks Report potrebbe costare al pianeta circa 3mila miliardi di dollari, più o meno l'equivalente del PIL del Regno Unito. Gli autori degli attacchi usano tecniche sempre più sofisticate, studiate appositamente per eludere i rilevamenti. Tali tecniche consentono anche di accelerare la velocità degli attacchi per impedire di attuare delle contromisure difensive.

Potenziare la tecnologia per alzare il livello di sicurezza è di certo una strada da intraprendere per prevenire future aggressioni e salvaguardare la sicurezza delle informazioni sensibili. Ma non è la sola. "Le aziende sono oggi consapevoli del fatto che non è sufficiente adottare la giusta tecnologia: vanno anche modificati i processi e formate le persone. Questo è ancora più vero quando si parla di sicurezza di sistemi di controllo industriale, apparati gestiti tipicamente da personale con poche o nulle competenze in ambito di cybersecurity", ha commentato Elena Vaciago[3]. "Un piano di cybersecurity, per essere efficace, deve infatti riguardare tutti gli asset e deve fruire della collaborazione di tutte le persone: nei settori più avanzati, sono oggi realizzati anche dei Security Operations Center in grado di monitorare contemporaneamente gli 'ambienti' a rischio, inviare alert, consolidare informazioni sulle minacce che sempre attraversano le barriere tra i due mondi. Questi team sanno inoltre che non basta aver predisposto misure di sicurezza: serve uno sforzo continuativo, di riconoscimento di incidenti, di monitoraggio di anomalie. Ed è molto importante essere pronti ad affrontare un eventuale incidente, aver testato la propria capacità di risposta in modo proattivo".

"L'unica cosa che può davvero fare la differenza è fare cultura della sicurezza tra tutti gli utenti come del resto viene previsto dalla stessa normativa. Molti dimenticano che oltre agli aspetti tecnologici ci sono quelli giuridici", aggiunge Rossetti. Il regolamento europeo in materia di protezione dei dati personali GDPR[5] include anche un'appropriata formazione al personale che ha accesso permanente o regolare ai dati personali e la promozione della sensibilizzazione del pubblico riguardo ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali. Speciale attenzione viene data alle informazioni particolarmente sensibili come quelle sanitarie che possono riguardare la vita delle persone.

3. Vaciago E. Reimaging resilience after disruption: ridurre il rischio cyber nell'industria 4.0. Digital Italy Summit 2021 La resilienza del digitale, Roma 18-20 ottobre 2021.

5. Regolamento generale sulla protezione dei dati. Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016.

La protezione dei dati personali dei pazienti è sempre più prioritaria con la progressiva digitalizzazione della sanità e dell'assistenza sociosanitaria. La Commissione Europea ha presentano l'ambiziosa iniziativa che vuole arrivare entro il 2025 alla creazione di uno spazio comune europeo di dati sanitari[6]: spazio che migliorerà l'accesso a diversi tipi di dati sanitari (fascicoli sanitari elettronici, dati genomici, dati presi dai registri dei pazienti) e il loro scambio, non solo per sostenere l'erogazione dei servizi sanitari (il cosiddetto uso primario dei dati) ma anche a fini di ricerca e di elaborazione di politiche in ambito sanitario (il cosiddetto uso secondario dei dati). Se da un lato come si legge nelle pagine web della Commissione Europea "la sanità e l'assistenza digitali sono innovative e possono migliorare l'accesso all'assistenza e la qualità delle cure, ma anche aumentare l'efficienza complessiva del settore sanitario", dall'altro è assodato che le infrastrutture digitali sono facilmente hackerabili e la sanità è uno dei principali bersagli.

LA STRATEGIA DI SICUREZZA INFORMATICA DELL'UNIONE EUROPEA

La direttiva NIS per una risposta unitaria e per migliorare la cyber resilienza

Uno dei primi tentativi di migliorare il livello di difesa delle infrastrutture critiche degli Stati membri in modo omogeneo è rappresentato dalla Direttiva NIS adottata dall'Unione Europea a luglio 2016. Nel 2018 l'Italia ha recepito la direttiva NIS con il Decreto legislativo n.65/2018 pubblicato sulla *Gazzetta Ufficiale*. In quanto erogatrice di servizi essenziali la sanità rientra nell'ambito di applicazione della Direttiva NIS.
In sintesi la Direttiva NIS obbliga gli Stati membri ad adottare una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi, definendone sia gli obiettivi sia le misure strategiche e regolamentari, e a identificare i settori di servizi da considerarsi essenziali per il mantenimento di attività sociali ed economiche fondamentali (healthcare incluso). Gli Stati membri devono anche provvedere affinché gli operatori di tali servizi essenziali adottino misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza delle reti e dei sistemi informativi che usano nelle loro operazioni. Inoltre, la Direttiva richiede l'istituzione di un gruppo di cooperazione per agevolare un'azione condivisa e uno scambio di informazioni tra gli Stati membri e di una rete di gruppi di intervento per la sicurezza informatica in caso di incidente (rete CSIRT).
Buone le intenzioni ma a distanza di due anni era emerso una divergenza tra gli approcci degli Stati membri nell'attuazione della Direttiva con il rischio di non raggiungere l'obiettivo di un potenziamento omogeneo della sicurezza su tutto il territorio europeo. Per esempio, in alcuni Stati membri, alcuni ospedali non sono stati inclusi tra gli operatori sottoposti all'obbligo di adottare le misure di sicurezza imposte dalla Direttiva NIS, esponendoli a un rischio più alto di minacce. Alla fine 2020 la Commissione Europea ha presentato una proposta di revisione della Direttiva NIS, denominata NIS 2, che è ancora in fase di lavorazione e andrà a sostituire la prima versione.
Altre normative europee rilevanti per sicurezza informatica per la sanità e l'*ehealth* sono il Regolamento 2016/679 GDPR che detta i requisiti per sicurezza del trattamento di dati personali secondo i principi di "integrità" e "riservatezza" e il nuovo Regolamento 2017/745 sui dispositivi medici che impone obblighi di sicurezza chiave, rilevanti anche sotto un aspetto cybersecurity, per fabbricanti ed operatori economici sanitari.

Fonte: Agendagitale.eu

6. Commissione Europea. Spazio europeo dei dati sanitari. Pubblicato sul sito www.ec.europa.eu

IL VALORE DEI DATI SANITARI

Nel 2019, prima della pandemia, gli hacker aveva colpito l'American Medical Collection Agency (Amca), una società che fornisce servizi finanziari a una serie di strutture mediche statunitensi: più di 24 milioni di file e cartelle cliniche sottratte. Queste cartelle cliniche hanno valore nel mercato illegale del dark web dove, secondo un rapporto di Experian, possono essere vendute da 1 a 1000 dollari ciascuna in base a quanto sono complete[7]. I dati delle cartelle cliniche dei pazienti possono anche essere utilizzati per creare kit di identità che valgono fino a 2000 dollari.

I dati sanitari valgono molto nel *dark web*, dove vengono organizzate delle aste. Non è però escluso - considera Rossetti - che questi dati in grandi quantità abbiano "valore" solo per scopi illeciti; tra i player possono esserci per esempio le aziende farmaceutiche che possono estrapolare sistemi di Intelligenza Artificiale informazioni di rilievo per la ricerca e sviluppo. "Anche i dati sanitari dei singoli cittadini hanno un valore. Per esempio collegare dei dati sanitari a una singola persona può avere delle ripercussioni nella stipula di un'assicurazione medica o nella selezione dei dipendenti. Circolano già notizie che negli Stati Uniti ci siano delle società che acquistano i dati sanitari dei singoli cittadini per poi venderli a società terze per questi scopi. "Negli Stati Uniti non c'è una legge federale sul trattamento dei dati e solo pochi Paesi hanno una normativa per la protezione dei dati. Laddove questa normativa manca è legittimo vendere e comprare questi dati senza alcuna protezione dei cittadini".

Negli Stati Uniti è centrale l'autonomia dei privati e la libertà individuale: essenzialmente i dati appartengono a chi li usa senza una tutela della privacy per i dati sanitari. La tutela della privacy è attribuita principalmente alla Federal Trade Commission, la commissione per il commercio federale per la quale tale tutela è un'estensione della tutela del consumatore e della legittimità delle pratiche commerciali. Ma dei passi in avanti verso il modello del GDPR europeo per la protezione dei dati personali si stanno facendo. A gennaio 2020 è entrato in vigore il California Consumer Privacy Act che impone dei limiti giuridici a tutela della privacy per le grandi aziende. Per esempio, quelle che vendono dati dei consumatori a terzi ora sono obbligate ad informare i proprietari dei dati e a dare la possibilità di rinunciare alla vendita *"Do Not Sell My Personal Information"*.

La normativa federale che regola specificamente i dati sanitari dei privati è l'*Health Insurance Portability and Accountability Act* (HIPAA) del 1996 che definisce i requisiti per il trattamento dei dati. L'HIPAA compliance deve essere parte integrante della cultura aziendale di ogni entità che opera nel settore sanitario al fine di garantire la privacy, la sicurezza e l'integrità dei dati sanitari protetti[2]. Benché si tratti di una legge con sanzioni ben definite, le imprese statunitensi che producono e forniscono dispositivi IoT al settore non hanno alcun obbligo di compliance. A febbraio di quest'anno 2021 Center for Democracy & Techonology e l'e-Health Initiative hanno lanciato il Consumer *Privacy Framework* che fornisce supporto alla legge con nuove regole per tutti gli enti coinvolti nel trattamento dei dati sanitari alla luce, anche, dei sempre crescenti cyber attacchi ai database sanitari.

LA PROTEZIONE DEI DATI DENTRO E FUORI I CONFINI NAZIONALI

Nei primi anni del nuovo secolo è nato il concetto di "sovranità digitale" come la capacità di determinare autonomamente le proprie norme e la capacità di agire di conseguenza. "Quello della sovranità digitale europea è tra i temi più discussi degli ultimi mesi per quanto concerne la direzione geopolitica della Commissione europea annunciata dalla presidente Ursula von der Leyen", scrive Carolina Polito, research assistant presso il Centre for European Policy Studies, sulla rivista dell'Istituto Affari Generali[8]. "Le conseguenze della pandemia di COVID-19 hanno contribuito a rendere centrale questo dibattito. La pandemia ha fatto emergere quanto le società siano ▶

7. Hackers are stealing millions of medical records - and selling them on the dark web. CBS News, 14 febbraio 2019.

2. Carboni K. È scaduto (senza conseguenze) l'ultimatum dato alla Regione Lazio dai criminali informatici. Wired, 9 settembre 2021.

8. Polito C. La governance globale dei dati e la sovranità digitale europea. IAI Papers 21 l 11 Marzo 2021

drammaticamente dipendenti dai dati, dalla stabilità dei network e, più in generale, dalla digitalizzazione. La pandemia ha quindi fortemente rafforzato in Europa la convinzione di come sia urgente raggiungere un'autonomia strategica nello sviluppare soluzioni digitali in linea con i principi e i valori fondanti dell'Unione e della conseguente necessità di un crescente impegno in termini di investimenti e di sforzo normativo".

Collegandosi alla definizione di sovranità digitale di Pierre Bellanger, CEO della stazione radio francese Skyrock, quale "controllo del nostro presente e del nostro futuro così come si manifestano e si orientano per mezzo dell'uso delle tecnologie e delle reti informatiche", Rossetti commenta che la ricerca della sovranità digitale sia un obiettivo che non deve essere perseguito solo dallo Stato ma che deve essere condiviso da aziende e dai singoli utenti della rete, intesi come cittadini e come utenti-consumatori[9]. Negli ultimi dieci anni, infatti, è radicalmente cambiata la percezione delle piattaforme social da parte dei singoli utenti-consumatori: inizialmente venivano percepite come spazi di comunicazione globale che permettono di restare in contatto con gli altri utenti, invece adesso vengono percepite come "luoghi" in cui si è persa la capacità di proteggere i dati di coloro che sono interconnessi e con essa la possibilità di tutelare efficacemente i loro diritti.

"La sovranità digitale si connette strettamente alla direttiva europea NIS e alla nozione di perimetro cybernetico" dice Rossetti. "Alla base vi è la convinzione che i dati dei cittadini italiani debbano restare italiani però molto spesso questi dati arrivano in nazioni dove non c'è nessuna protezione di tipo legale. Prima del regolamento europeo GDPR i dati venivano sottoposti a 'trattamenti' che potevano potenzialmente pregiudicare i diritti. Il compito primario dello Stato è quello di proteggere le reti delle infrastrutture critiche (aerei, treni, energia elettrica, gas, sanità) da cui dipende il funzionamento stesso della società. Ma per farlo serve un coordinamento quantomeno a livello europeo. Negli ultimi anni l'Unione Europea ha lavorato in questa direzione cercando di coordinare queste azioni. Per ora molte di esse sono solo sulla carta, perché l'attuazione non si può fare con la bacchetta magica un giorno con l'altro, però direi che le linee sono tracciate e mi sembra anche che siano anche ben tracciate".

BEST PRACTICE PER LA SICUREZZA

"Attualmente una delle minacce più diffuse è il ransomware di cui gli ospedali sono trai target più critici. Negli Stati Uniti - spiega a *Torino Medica* Sara Rampazzi, ricercatrice e assistant professor al Department of computer and information science and engineering della University of Florida - la regolamentazione della sicurezza informatica degli ospedali si divide tra le norme adottate internamente dai singoli ospedali e le guideline prodotte dalle agenzie governative sulle buone pratiche per la gestione delle minacce".

Una prima raccomandazione per mettere in sicurezza l'infrastruttura IT dell'ospedale e per proteggersi dalle minacce nel tempo è la configurazione e protezione della rete informatica dell'ospedale affinché sia il più possibile blindata e isolata. Tutte le apparecchiature sensibili o essenziali e i dispositivi medici per i pazienti collegati alla rete dell'ospedale devono essere protetti in via prioritaria. E per farlo serve isolare dall'esterno la rete per renderla impermeabile agli attacchi, in particolare gli ambienti più critici.

9. Rossetti A. Sovranità digitale? Difenderla per non perdere quella politica. Red open letter, 18 novembre 2019.

Le linee di indirizzo includono anche la dotazione di un responsabile e di un protocollo per la sicurezza informatica. La figura del responsabile è diversa da quella dell'IT management. Il suo ruolo è specifico per la sicurezza informatica. Deve quindi occuparsi del mantenimento della rete ospedaliera e dell'accesso e dei privilegi di accesso ai dispositivi medici ad essa collegati e dell'implementazione di un protocollo per il personale dell'ospedale affinché sia in grado di intercettare e riportare prontamente eventuali anomalie che possono essere spia di un attacco. "In un ospedale cecoslovacco[10], l'attacco era partito da un allegato aperto in una mail di un impiegato con il suo computer che era collegato alla rete dell'ospedale. Il ransomware ha causato una reazione a catena tale per cui l'intero ospedale è andato in shutdown. Il personale sanitario non sapeva cosa fare né a chi rivolgersi" ricorda la ricercatrice.

Fondamentale, se non indispensabile, per prevenire le minacce è la formazione del personale sanitario. "Le persone devono apprendere di non effettuare determinate operazioni apparentemente normali ma che espongono la rete al rischio di attacchi, come per esempio salvare le password in posti facilmente accessibili o riutilizzare la stessa password per diverse attività anche al di fuori dell'ospedale, accedere alla rete con il proprio personal computer, scaricare dei software o aggiornarli. Solo se ben istruito sulle pratiche di sicurezza il personale sanitario può aiutare a prevenire certe modalità di attacco. E inoltre viene messo nelle condizioni di sapere come e a chi riportare eventuali malfunzionamenti e quali azioni intraprendere subito".

Infine, per contenere i danni in caso di cyberattacco, al management della sicurezza spetta il compito di implementare dei protocolli di salvaguardia, come per esempio isolare la rete interna e i dispostivi medici collegati ai pazienti, eseguire regolarmente i backup affinché i dati dei pazienti siano recuperabili nel caso in cui si dovessero perdere; implementare gruppi di continuità per l'energia e altre azioni per contenere questo tipo di minacce.

"Queste best practice non valgono solo per disastri informatici - sottolinea Rampazzi - ma anche per qualsiasi tipo di emergenza che interessi i dispositivi medici e i dati personali sanitari. Tutto il personale deve essere consapevole di come gestire un'emergenza. Un engagement della sicurezza è essenziale".

REGOLE ESSENZIALI DI SICUREZZA INFORMATICA NEI SERVIZI SANITARI

La check list dell'Istituto Superiore di Sanità

Per incrementare il più possibile la difesa da possibili attacchi informatici e con essa la protezione dei dati sensibili il Gruppo di Studio Nazionale sulla Cybersecurity nei servizi sanitari dell'Istituto Superiore di Sanità ha prodotto un documento di indirizzo rivolto sia al personale sia ai gestori del sistema informatico delle strutture sanitarie. La prima parte include un semplice elenco, valido in generale per qualsiasi utilizzo di computer connesso in internet, di comportamenti corretti e scorretti ai fini della propria sicurezza; la seconda invece raccoglie le buone pratiche per i gestori e responsabili di unità organizzative sia amministrative che operative.
"Tale suddivisione - viene spiegato nell'introduzione alle buone pratiche - è stata pensata al solo scopo di facilitare la lettura del presente documento anche a persone che non abbiamo specifiche conoscenze tecniche e non indica affatto una priorità di importanza o di urgenza. La sicurezza informatica è un problema complesso che richiede specifiche soluzioni tecnologiche ed organizzative e non può essere improvvisata. Essa deve essere sempre affrontata durante il progetto dei sistemi informativi e adottando opportune tecniche di gestione dei sistemi durante tutta la loro vita. Tuttavia, comportamenti non adeguati degli utilizzatori semplificano gli attacchi anche a sistemi informativi che offrono una sicurezza elevata. È quindi necessario che il comportamento degli utilizzatori non generi situazioni pericolose che riducono la sicurezza intrinseca di un sistema mettendo in pericolo sia il sistema che i dati che esso gestisce. Per ottenere un contrasto e una prevenzione efficaci degli attacchi, le regole di buon comportamento devono essere diffuse e adottate da tutto il personale delle strutture sanitarie".

Bibliografia
- Istituto Superiore di Sanità. Buone pratiche per la sicurezza informatica nei servizi sanitari. Pubblicato il 17 giugno 2019.

10. Brno University Hospital ransomware attack (2020). Pubblicato su https://cyberlaw.ccdcoe.org/

GOVERNARE LE VULNERABILITÀ DEI DISPOSITIVI MEDICI

La protezione della rete ospedaliera e l'aderenza alle normative e alle linee di indirizzo sono, dunque, i presupposti da cui partire per gestire in maniera efficiente tanto i servizi erogati quanto l'attività clinica, chirurgica e diagnostica svolta all'interno dell'ospedale nonché quella amministrativa. A questo si aggiunge la manutenzione dei device medicali e il loro aggiornamento, aggiunge Sara Rampazzi. Negli anni si è infatti assistito a un importante incremento nel numero di dispositivi medici (*medical devices*) disponibili sul mercato che però, essendo interconnessi tramite internet e nella rete ospedaliera, sono potenzialmente vulnerabili. Ma un eventuale attacco informatico (*medical devices hijacking*) potrebbe alterare la funzionalità di dispositivi medici mettendo in pericolo sicurezza e salute dei pazienti.

Negli Stati Uniti i requisiti per la sicurezza dei device medici è materia della FDA, l'autorità statunitense incaricata della salute pubblica che emana, pubblica la valutazione clinica, alla produzione, al confezionamento alla etichettatura e alla sorveglianza dopo l'immissione in commercio. La FDA è stata la prima a mettere in campo delle misure di tipo regolamentare la sicurezza dei medical device. Ha emanato la prima guidance nel 2005, e a seguire nel 2014 e 2016 da altri due documenti riguardanti la sorveglianza pre- e post-marketing della sicurezza informatica nei dispositivi medici.

"Una delle principali criticità è l'aggiornamento dei dispositivi medici quando vengono individuate delle falle. Ogni aggiornamento deve essere condotto e pianificato mantenendo gli standard di sicurezza" spiega la ricercatrice. Solo per fare un esempio, nel 2017, la FDA si era espressa in merito alle potenziali vulnerabilità associate al trasmettitore di un defibrillatore impiantabile che consentiva al dispositivo di inviare dati sulle funzioni vitali del paziente e di modificare parte dei parametri del dispositivo[11]. A causa di una falla c'era il rischio di un attacco e manomissione del software da parte degli hacker. La FDA aveva richiesto allo sviluppatore di correggere la vulnerabilità e agli utilizzatori di aggiornarne il software con versione modificata. Nel 2019 la stessa Autorità ha avvertito dei potenziali rischi di cybersicurezza di alcuni tipi di pompe per insulina tali da impedirne l'erogazione[12].

"L'FDA regola l'insieme delle attività che ne derivano. Ma a monte deve esserci una sinergia tra i tre attori che devono coordinare le proprie mansioni e i propri sforzi per la sicurezza: il regolatorio, il produttore e l'utilizzatore, cioè l'operatore sanitario e il paziente", spiega la ricercatrice. "L'FDA controlla gli standard di sicurezza, il produttore deve occuparsi della manutenzione e degli aggiornamenti dei dispositivi, l'ospedale deve regolare l'accesso a questi dispositivi e controllare che venga fatto tutto correttamente. Si deve quindi creare una sorta di lavoro a catena. Dopo ogni aggiornamento o modifica il dispositivo medico deve essere nuovamente approvato dal regolatorio. L'intero processo può richiedere un lungo periodo, anche di anni, che necessariamente deve essere supportato e controllato dall'FDA per garantire la sicurezza del prodotto medicale in questo lasso di tempo".

11. Implantable Cardiac Devices and Merlin@home Transmitter by St. Jude Medical: FDA Safety Communication - Cybersecurity Vulnerabilities Identified. Asah.org 18 gennaio 2017.

12. US Food & Drug Administration. Certain Medtronic MiniMed Insulin Pumps Have Potential Cybersecurity Risks: FDA Safety Communication. Fda.gov 27 giugno 2019.

COME PROTEGGERE LA CATENA DEL FREDDO DEI VACCINI?

La ricerca preventiva delle vulnerabilità

Prevenire è meglio che curare. Una delle migliori forme di prevenzione è formare il personale e i cittadini a non aprire inconsapevolmente delle falle agli hacker. Anche tenere copie aggiornate dei dati con backup continui, backup periodici e completi, e in generale rafforzare i sistemi di sicurezza informatica per ridurre al minimo i punti di accesso ai dati critici o ai processi il cui arresto comporterebbe gravi danni. Altro fronte è sicuramente quello della ricerca di base e applicata, per essere pronti a intercettare o a prevedere le vulnerabilità delle reti delle infrastrutture o dei processi e dispositivi controllati da software e hardware presenti ormai ovunque, che sono un potenziale bersaglio del cyber attacco. Nei laboratori del *Department of Computer and Information Science and Engineering*, alla *University of Michigan*, **Sara Rampazzi** si occupa delle interferenze esterne che possono causare il malfunzionamento di un dispositivo. Indentificare le vulnerabilità alle interferenze attribuibili alla fabbricazione del dispositivo può rilevarsi utile anche per prevenire intrusioni malevole e attacchi informatici criminali. Le ricerche condotte in passato sulle interferenze elettromagnetiche che alterano il controllo della temperatura delle incubatrici sono servite a Rampazzi per intercettare i punti di fragilità nella catena del freddo nei vaccini per il COVID-19. La catena del freddo è una componente essenziale della supply chain perché deve assicurare la corretta e sicura conservazione dei vaccini in ambienti a temperatura controllata. Proprio questa fase della distribuzione dei vaccini è un potenziale bersaglio degli hacker. A dicembre 2020 l'IBM aveva individuato una campagna di phishing che aveva preso di mira organizzazioni associate allo sviluppo della catena del freddo nei vaccini per il COVID-19[1]. Insieme ai colleghi della University of Michigan la ricercatrice italiana[2] ha verificato che il modo migliore per prevenire l'interruzione della catena del freddo dei vaccini è progettare sensori resistenti alle interferenze elettromagnetiche intenzionali. Quale misura temporanea ha suggerito l'implementazione di semplici controlli amministrativi, come il controllo dell'accesso fisico ai display della temperatura.

Bibliografia
1. Frediani C. Catena del freddo dei vaccini, cybercriminali e cyberspie. Il manifesto in rete, 14 Dicembre 2020.
2. Long Y, Rampazzi S, Sugawara T, Fu K. Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats. Biomed Instrum Technol 2021; 55: 112-7.

OLTRE LA SICUREZZA, IL VALORE DELL'INNOVAZIONE

Anche il Regolamento europeo 2017/745 sui dispositivi medicali, entrato in vigore a maggio, promuove questa cooperazione - e non solo ai fine della cybersicurezza ma anche di ricerca e appropriatezza. Il regolamento modifica le norme che disciplinano il sistema dei dispositivi medici, tenendo conto degli sviluppi degli ultimi vent'anni, con l'obiettivo di garantire un quadro normativo solido, idoneo a mantenere un elevato livello di sicurezza. Tra le diverse modifiche introdotte, commenta Luciana Ballini, presidente dell'Assemblea Plenaria EUnetHTA, in un'intervista sulla governance dei dispositivi medici in Italia[13], vi è infatti l'obbligo di fornire dati clinici di sicurezza ed efficacia al fine di ottenere l'autorizzazione al commercio dei dispositivi ad alto rischio. "Ci sarà quindi l'opportunità di migliorare e ottimizzare i processi di autorizzazione alle sperimentazioni cliniche, oltre che di stabilire collaborazioni più strutturate e maggiormente presidiate e trasparenti tra sviluppatori di dispositivi medici e utilizzatori (professionisti e pazienti). Il nuovo regolamento europeo non richiede dati comparativi di efficacia e sicurezza, necessari per stabilire il valore aggiunto, ma una precoce collaborazione consente di raccogliere dati che soddisfino i requisiti sia degli enti regolatori che dei sistemi sanitari, velocizzando i tempi di valutazione e di accesso alle innovazioni. Un secondo elemento molto rilevante è l'obbligo di tracciabilità dei dispositivi che potrà incentivare l'ammodernamento degli strumenti informativi necessario a rispettare tale obbligo e a potenziare il nostro sistema di vigilanza e sicurezza dei dispositivi medici".

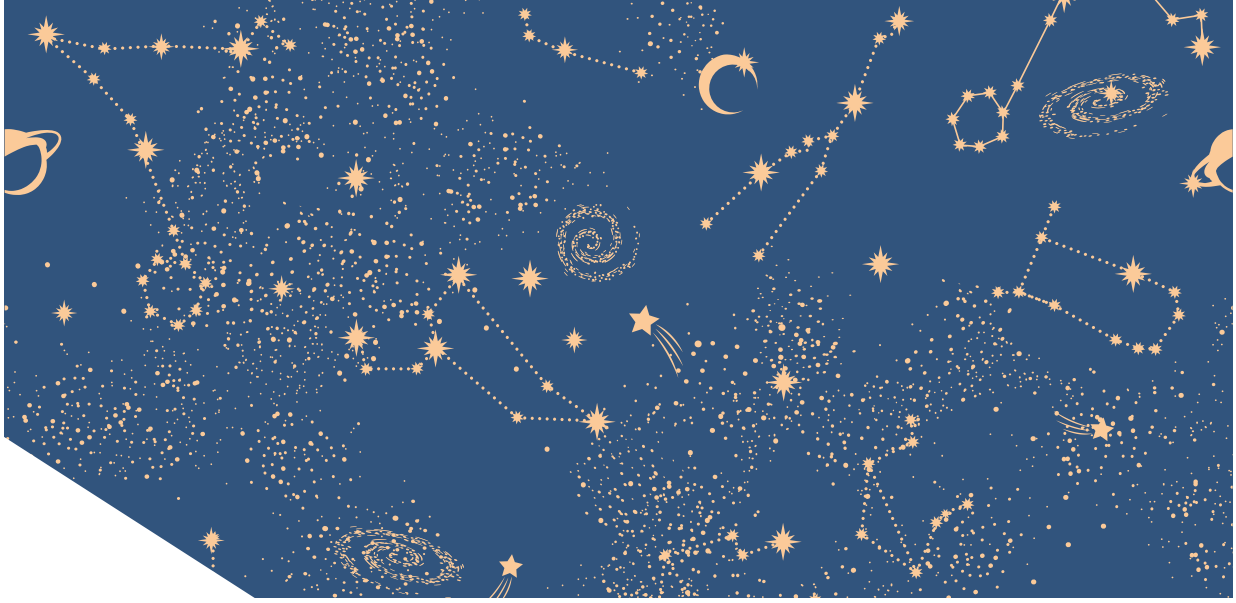
"La sfida sta nel cambiamento nei contenuti delle relazioni. I produttori non possono aspettarsi un riconoscimento di merito basato solo sulla potenzialità teorica dei propri prodotti ma dovranno costruire una base scientifica solida. Il sistema sanitario dovrà dimostrare di conoscere a fondo i propri bisogni, e quindi di riconoscere tempestivamente l'innovazione, assumendosi anche la responsabilità di esprimere una committenza. L'impegno congiunto verso un'offerta di valore consentirà una domanda in grado di sostenere l'innovazione, anche attraverso la necessaria flessibilità nelle diverse fasi di sviluppo dall'utilizzo sperimentale all'utilizzo consolidato nella pratica clinica".

RIPRENDERE A GUARDARE LE STELLE

La digitalizzazione della sanità e di tutte le infrastrutture della società come ogni innovazione e rivoluzione impone delle riflessioni sulla sicurezza e sulla gestione del rischio, e valutazione attenta della posta in gioco. Per esempio trovare un punto di equilibrio tra costi e valore aggiunto di provata efficacia, tra interessi di mercato e data privacy, tra vulnerabilità e robustezza.

Da anni il sociologo Evgeny Morozov, uno degli intellettuali di riferimento in merito al dibattito sugli effetti politici e sociali dello sviluppo della tecnologia, denuncia il capitalismo tecnologico in cui i dati personali dei cittadini vengono gestiti da altri e diventano merce: "In assenza dei nostri dati - afferma - le aziende non potrebbero fornire servizi, sviluppare tecnologie di intelligenza artificiale. Noi siamo fonti di dati, ma non abbiamo le infrastrutture per gestirli e così vengono sfruttati dalle industrie informatiche. Che li acquisiscono e li vendono". Morozov ha una posizione critica e in controtendenza rispetto al comune ottimismo sulle potenzialità democratizzanti di internet. Ma parlarne e aprire un dialogo può fare la differenza. Non si tratta di criticare o rifiutare l'innovazione o la tecnologia ma di essere consapevoli dei rischi e dei potenziali danni derivanti dall'impiego di nuovi strumenti e applicazioni.

13. Intervista a Luciana Ballini. La governance dei dispositivi medici in Italia analisi e prospettive. Policy and Pro-curement in Healthcare, 24 marzo 2020.



In un editoriale sulla medicina digitale del 2018, ormai datato (forse), *The Lancet* scriveva[14] che senza un quadro chiaro per differenziare i prodotti digitali efficaci dall'opportunismo commerciale, le aziende, i medici e i policy maker faticheranno per garantire quel livello di evidenze richiesto per realizzare il potenziale della medicina digitale. I rischi della medicina digitale, in particolare l'uso dell'Intelligenza Artificiale negli interventi sanitari, sono preoccupanti. Continuare a sostenere l'eccezionalità digitale e non riuscire a valutare in modo solido gli interventi sanitari digitali presenta il rischio maggiore per i pazienti e i sistemi sanitari".

Quello che serve innanzitutto è la fiducia nel saper gestire l'incertezza. All'inaugurazione del Digital Italy Summit 2021 - La resilienza del digitale, Luciano Floridi, professore ordinario di Filosofia ed etica dell'informazione alla University of Oxford, ha parlato di rivoluzione digitale quale cambio di paradigma. Già negli anni Novanta il digitale ha fatto il suo ingresso nel mondo reale e si parlava delle necessità di adeguarsi, di cambiare e di acquisire nuove competenze. "Esserne consapevoli è fondamentale per capire di non versare altro latte sul latte già versato. Quando infatti un paradigma cambia in maniera così profonda l'errore comune è quello di guardare e affidarsi a soluzioni passate che hanno funzionato. Ma un cambio di paradigma significa chiudere un capitolo riconoscendo i progressi compiuti e aprire uno nuovo capitolo da scrivere. Questo non vuol dire gettare tutto e ricominciare daccapo, significa piuttosto costruire su quanto è già stato fatto di buono - dalla pubblica amministrazione alla Unione europea fino ai finanziamenti". Il rischio per Floridi è "pensare che questo cambio di paradigma richieda una trasformazione radicale per poi proseguire sulla stessa strada come se nulla fosse avvenuto. Questa è la ricetta per il disastro: continueremo a versare quel latte che abbiamo versato in passato".

"La nuova sfida non è l'innovazione digitale ma la *governance* del digitale. Cioè in quale direzione oggi vogliamo andare come società, come azienda, come ambiente? Lo Stato, l'azienda e la complessità sono come la barca di Platone che deve essere pilotata. Nei dialoghi filosofici in 'La Repubblica' Platone scrive che tra i tanti marinai ce n'è uno che guarda le stelle, è il filosofo che conosce la *techne* e naviga conoscendo le correnti e seguendo una rotta che gli è chiara per raggiungere il punto di arrivo. La governance non è semplicemente l'estensione della coperta novecentesca, cioè fare sì che tanto tutto cambi affinché nulla cambi. Vuol dire anche saper gestire l'incertezza ma in vista di qualcosa di profondo".

Questo cambio di paradigma, dunque, vuol dire ripensare in profondità la nostra concettualizzazione della società, del mondo aziendale, della produzione, della formazione. Si tratta di governare anche la complessità poiché entrano in gioco diversi elementi interconnessi. Per questo serve più collaborazione e cooperazione, conclude Floridi. Ma per fare questo serve più politica che è fatta di compromessi (quelli buoni). Una politica che deve tornare a guardare le stelle parafrasando la frase di Dante "E quindi uscimmo a *rivedere* le stelle". "È la politica con la 'p' maiuscola, quella di Platone, quella che ti dice in che modo gestire o non gestire questa particolare barca in cui siamo".

14. Editorial. Is digital medicine different? The Lancet 2009; 392: 95.

GLOSSARIO

Bitcoin è una criptovaluta e un sistema di pagamento valutario internazionale creato nel 2009 da un anonimo inventore, noto con lo pseudonimo di Satoshi Nakamoto, che sviluppò un'idea da lui stesso presentata su Internet a fine 2008. Sono monete virtuali che circolano solo in rete attraverso informazioni scritte su un grande database condiviso, la blockchain. Nate come mezzo di pagamento anonimo, sono diventati anche una riserva di valore (e quindi un bene di investimento). A dieci mesi dalla sua nascita il valore di un bitcoin era stato calcolato di 0,00076 $ utilizzando un'equazione che include il costo dell'elettricità per far funzionare un computer che ha generato i bitcoin. Oggi il tasso di cambio che si calcola sulla base della domanda e dell'offerta sui vari exchange in cui il bitcoin viene contrattato è arrivato a 63.143,70 $ (tasso aggiornato al 25 ottobre 2021).

Cyberattacco o **attacco informatico** è definito dalla National Initiative For Cybersecurity Careers And Studies come il tentativo di ottenere accesso non autorizzato a servizi, risorse o informazioni di sistema e/o di comprometterne l'integrità, e in generale consiste nell'atto intenzionale di tentare di eludere uno o più servizi di sicurezza o controlli di un sistema informativo digitale per alterare la riservatezza, integrità e disponibilità dei dati.

Dark Web è la parte del web normalmente non accessibile se non attraverso specifici software, configurazioni e accessi autorizzativi. È solo una piccola parte del deep web, la parte di web che non è indicizzata da motori di ricerca, sebbene talvolta il termine deep web venga usato erroneamente per riferirsi al solo dark web. All'interno del dark web dove sono presenti attività criminali e mercati illegali (droghe, sostante stupefacenti, passaporti, carte di indentità e molto altro tra cui anche i codici per la generazione di falsi certificati e green pass). Secondo una ricerca di Swascan l'Italia è la seconda nazione al mondo ad essere colpita dal commercio illegale di dati e credenziali in Europa.

Firewall originariamente il termine si riferiva a un muro destinato a confinare un incendio all'interno di un edificio. Alla fine degli anni Ottanta viene applicato alla tecnologia di rete per indicare quelle componenti hardware e/o software che permettono di monitorare il traffico in entrata e in uscita della rete. Il firewall costituisce una barriera perimetrale di una rete di computer e può anche fornire una protezione in termini di sicurezza informatica da cyber minacce. Ma quest'ultime hanno raggiunto un grado di evoluzione molto più elevato rispetto a quello dei sistemi di difesa passiva tradizionali (firewall e antivirus).

Malware o software malevolo è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema informatico (computer, reti, tablet, dispositivi mobili, ecc.) assumendone il controllo parziale delle operazioni del dispositivo e interferendo con il normale funzionamento. I malware possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.

Ransomware è il virus del riscatto. Non è altro che un tipo di malware che limita l'accesso del dispositivo che infetta, richiedendo un riscatto (*ransom* in inglese) da pagare per rimuovere la limitazione. Alcuni ransomware bloccano il sistema e chiedono un riscatto per sbloccare il sistema, altri invece cifrano i file della vittima utente chiedendo di pagare per riportare i file cifrati in chiaro. Comunemente la somma del riscatto viene versata in bitcoin.

L'intelligenza artificiale rappresenta un rischio sovrano per la sicurezza nazionale?

Enrico Coiera
Direttore del Center for Health Informatics
presso l'Australian Institute of Health Innovation

L'intelligenza artificiale è già una realtà concreta anche nei sistemi sanitari e della ricerca. La pandemia COVID-19 ha contribuito ad accelerare sia l'adozione del digitale sia l'impiego di sistemi di intelligenza artificiale e machine learning nella clinica e nella ricerca e sviluppo dei farmaci. In tutto il mondo il livello di interesse e di investimento nell'intelligenza artificiale in ambito sanitario è enorme. Tuttavia l'uso di questi sistemi non è esente da criticità, soprattutto dal punto di vista etico e di affidabilità, e anche di sicurezza.

Questo mondo emergente in cui l'intelligenza artificiale fa parte dell'assistenza sanitaria quotidiana è un mondo in cui medici e pazienti devono essere formati per utilizzare la tecnologia in modo sicuro ed efficace. E anche un mondo in cui viene richiesta una governance per guidare la trasformazione del Paese verso l'innovazione e digitalizzazione in modo responsabile, nel rispetto dei diritti umani e dei valori democratici.

In questo commento Enrico Coiera, direttore del Center for Health Informatics presso l'Australian Institute of Health Innovation, Macquarie University, e rappresentante dell'Australia Global Partnership on AI, invita a non focalizzarsi solo sulla sicurezza informatica che è diventata prioritaria con la crescita esponenziale in emergenza COVID-19 degli attacchi informatici ai dati personali dei cittadini. Dove deve investire la nazione: nella cyber sicurezza o nello sviluppo, analisi e test dell'AI onshore? Anche un Paese come l'Australia che è produttore primario di dati e importatore di algoritmi potrebbe non essere un posto sicuro.

Con il documentario Netflix, "The social dilemma", tutti parlano di quanto l'intelligenza artificiale (AI) influisca sulla nostra vita privata. Ma se invece stessimo perdendo d'occhio il problema, ben più grande, della sicurezza nazionale?

Con una popolazione che conta 26 milioni di abitanti, l'Australia produce una enorme quantità di dati ma, allo stesso tempo, ha poco controllo su come questi vengano utilizzati dai programmatori esteri di AI. Gli australiani si sono ritrovati ai margini di una frenetica competizione a livello mondiale per valutare chi riuscisse a utilizzare al meglio le AI per il riconoscimento facciale, per guidare le nostre macchine, per indovinare quello che guarderemo, ascolteremo e acquisteremo, e addirittura con chi dovremmo stringere amicizia. Ma meno conosciuta è l'influenza dell'AI su infrastrutture critiche come quelle dell'energia, delle telecomunicazioni e della sanità. Eppure, chiunque abbia il controllo su questi algoritmi ha controllo sul mondo.

Dal momento in cui influenzano già così tanti aspetti della nostra società, gli algoritmi per l'AI rappresentano il punto perfetto su cui intervenire qualora l'intenzione fosse quella di modificare il modo in cui un Paese agisce o di interferire con la sua sicurezza. Il Ministro degli Interni Peter Dutton ha di recente sollevato la questione, ma concentrarsi solamente sulla difesa cibernetica è l'approccio più adatto?

La protezione delle infrastrutture sanitarie essenziali

La natura della minaccia è chiara ed esiste. Se la maggior parte delle informazioni cui accedono i cittadini di un Paese deriva da fonti online che possono essere manipolate da organizzazioni o nazioni estere, il Paese in questione corre il rischio di un'interferenza diretta.

Vi sono, infatti, ampie evidenze a livello mondiale di come i social media siano stati utilizzati come fossero delle armi da attori politici ostili proprio in questo modo, per manipolare la percezione pubblica e i voti.

Per quanto riguarda l'ambito sanitario, i social media sono stati manipolati per amplificare i messaggi no vax e in questo momento stiamo assistendo alla promozione dell'opinione pubblica contro il vaccino anti COVID-19. La conseguente diffusione di false credenze può portare le persone a evitare la vaccinazione, con il potenziale rischio di allontanare ulteriormente l'ottenimento di una vera immunità di gregge.

L'argomentazione sulla sicurezza nazionale è a sua volta molto convincente. Gli attacchi alle infrastrutture legate all'informazione di altri paesi da parte di attori esteri rappresentano già un luogo comune. Ne sono un esempio gli attacchi "denial of service", per i quali il sistema del computer riceve una moltitudine di messaggi online che portano alla chiusura delle stesse. Il Parlamento è già stato vittima di questo tipo di attacchi.

Gli algoritmi offrono una strada differente. Le AI create con competenze di alta specificità tecnica sono notoriamente ben poco trasparenti sul perché operino in un certo modo e può essere molto difficile rilevare eventuali design malevoli. Gli algoritmi trasformano i dati in azioni, per esempio controllando l'attività di reti energetiche e di telecomunicazione. Se si riesce a interferire con il funzionamento degli algoritmi in questione, è possibile modificare radicalmente il loro modo di operare.

Nel 2017 la Food and Drug Administration statunitense ha richiesto la sostituzione di 460.000 pacemaker per evitare che gli algoritmi di questi potessero essere controllati in modo tale da fare scaricare la batteria o innescare un ritmo cardiaco pericoloso. Allo stesso modo, è possibile provocare dei blackout interferendo con le impostazioni di controllo del software connesso ai generatori della corrente.

È evidente che i paesi devono studiare delle strategie per proteggere le infrastrutture critiche da attacchi algoritmici. La relativa assenza d'investimento in AI dell'Australia mette il Paese in una posizione pericolosa.

I confini per un controllo sovrano sugli algoritmi

Cosa può fare l'Australia per garantire il nostro controllo sovrano sugli algoritmi? Non ha senso costruire barriere digitali attorno a un Paese in un contesto di economia mondiale, ma possiamo e dobbiamo fare maggiore attenzione. Anche se molte nazioni diffidano della Huawei per operazioni relative alla costruzione delle infrastrutture per le telecomunicazioni, hanno comunque concesso a Facebook di entrare nel loro territorio senza alcuna restrizione.

Alcuni paesi decideranno di non potersi più permettere di esternalizzare sistemi AI da applicare in infrastrutture critiche quali le telecomunicazioni, l'acqua, la corrente o il settore militare. La Cina ha inserito anche i social media in questa categoria.

L'Australia dovrà garantire che i sistemi di AI applicati alla sanità e ad altri settori fondamentali siano adeguati e sicuri da utilizzare, quindi ci devono essere una qualche forma di regolamentazione, localizzazione per un utilizzo interno e, in alcuni casi, uno sviluppo della tecnologia partendo da zero con un lavoro onshore che abbia luogo dentro il Paese.

Tutto ciò significa che l'Australia necessita di profonda competenza in AI, con una forza-lavoro che non sia solo esperta nello sviluppare algoritmi ma anche nel testarli, certificarli e calibrarli. Non avere il controllo sui nostri algoritmi significa che stiamo comunicando decisioni interne riguardanti le nostre infrastrutture più critiche a enti internazionali esterni.

Sfortunatamente, mentre alcuni paesi stanno investendo significativamente sulle AI, l'Australia al momento sembra ampiamente a proprio agio nel rappresentare uno dei principali paesi produttori di dati e importatore di algoritmi relativi al loro utilizzo. Per qualsiasi Paese che tenga alla propria sicurezza, probabilmente questa non è una situazione ideale in cui rimanere.

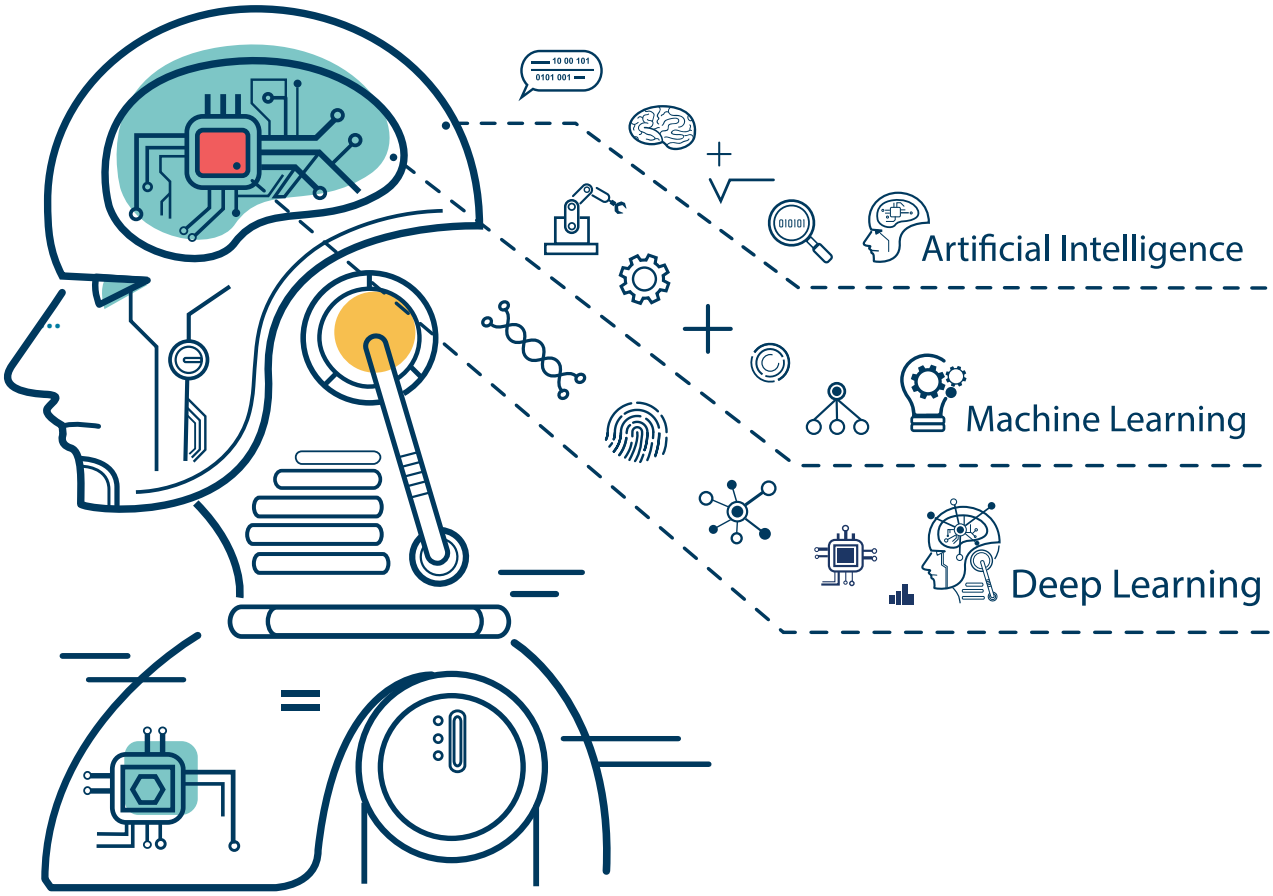
Tra il dire e il fare AI in medicina.

UNA PROPOSTA DI APPROCCIO PRAGMATICO

Prof. Federico Cabitza
Dipartimento di Informatica, Sistemistica e Comunicazione
Università degli Studi di Milano-Bicocca, Milano, Italia
IRCCS Istituto Ortopedico Galeazzi, Milano, Italia

L'interesse per l'applicazione di tecniche di machine learning (ML) alla medicina sta aumentando costantemente. Questo è dovuto anche grazie alla capacità di questi sistemi di fornire indicazioni e suggerimenti molto accurati in diversi contesti, tra cui soprattutto quelli in cui la decisione medica è basata principalmente (anche se non unicamente) su immagini in formato digitale e grandi quantità di dati strutturati. Tuttavia, garantire anche in ambito clinico le notevoli prestazioni che sono osservate in contesti sperimentali e in laboratorio è molto difficile. Questa difficoltà è stata chiamata "l'ultimo miglio dell'implementazione": questa espressione indica aspetti molto complessi relativi al trasferimento di innovazioni tecnologiche alla pratica clinica che riguardano anche le modalità più efficaci per gestire il cambiamento di processi e pratiche che le nuove tecnologie possono promuovere e rendere possibile. Queste modalità non sono solo di carattere tecnico e infrastrutturale, cioè non riguardano solo, ad esempio, standard di codifica e interoperabilità, o investimenti in nuovi dispositivi, applicazioni e reti informatiche; esse sono anche socio-tecniche e organizzative, in quanto riguardano sia la riprogettazione di processi aziendali (con la conseguente trasformazione di alcune pratiche abituali e flussi informativi), che la diffusione di una cultura della valutazione orientata a capire cosa sia utile fare per migliorare i processi sanitari e, possibilmente, l'esito dei trattamenti e delle cure.

In medicina si sta osservando, anche sulla letteratura specialistica ad alto impatto, un crescente interesse degli operatori del settore per sistemi informatici di classificazione "di nuova generazione", assimilati spesso a sistemi in grado di esibire una qualche forma di intelligenza artificiale (IA). Tali sistemi si distinguono da quelli delle generazioni precedenti (ad esempio, dai "sistemi esperti" della fine del secolo scorso) perché integrano modelli computazionali e statistici costruiti automaticamente a partire da grandi quantità di esempi tramite metodi e tecniche dette di "apprendimento automatico" (o machine learning); in particolare, quando questi modelli sono "reti neurali artificiali multistrato", si usa l'espressione "deep learning" per denotare una classe particolare di modelli (e relative tecniche) del machine learning che ottiene prestazioni particolarmente accurate nel caso di immagini e dati non strutturati (cioè scritti in linguaggio naturale). La accuratezza osservata di questi sistemi, e riportata in studi in larga parte di carattere retrospettivo su



compiti di natura quasi esclusivamente diagnostica o prognostica, suggerisce di considerare il loro impiego come sistemi a supporto delle decisioni nella pratica clinica, al punto di cura ("point of care"). Gli autori di diverse rassegne sistematiche e meta-analisi (ad esempio,[1]) riportano risultati che permettono di sostenere che questi sistemi esibiscono prestazioni confrontabili in termini di accuratezza con i migliori diagnosti umani; questo avviene in riferimento a una ampia serie di metodiche di diagnostica per immagini. Da una parte, però, non bisogna sottovalutare il fatto che i sistemi analizzati siano raramente usati su dati di provenienza clinica, ma siano bensì testati su dati di cui è sempre garantita una altissima qualità e che spesso non sono troppo diversi dagli esempi usati per sviluppare questi sistemi (validazione interna). D'altro canto, queste prestazioni suggeriscono comunque un ampio potenziale di efficientamento dei processi sanitari, soprattutto in termini di velocità e quindi di flusso di servizi erogati; e di democratizzazione di cure ad alto livello. In particolare, quest'ultimo obiettivo sarebbe raggiunto perché i sistemi sviluppati con la collaborazione di subspecialisti, e confrontabili con le prestazioni di questi ultimi, potranno essere usati anche in centri minori o di assistenza primaria, o perfino in autonomia da parte dai pazienti stessi, a cui fossero impartite istruzioni molto semplici, per certi test di screening (si pensi al caso di melanomi cutanei). In questo contesto generale, vi è comunque da considerare il grande punto interrogativo della effettiva *robustezza* di questi sistemi, cioè della loro capacità di esibire prestazioni simili in contesti anche molto diversi da quelli per i quali sono stati originariamente sviluppati, e con dati non troppo simili a quelli con cui sono stati validati e certificati[2,3]: in altre parole, bisogna considerare il caso della relativa scarsità di studi di "validazione esterna" di sistemi di IA medica, di cui non è facilmente valutabile la robustezza. Ed eppure, anche rimuovendo dall'attuale disamina la questione della robustezza, rimane comunque un punto su cui vorrei soffermarmi. Gran parte del dibattito attuale sull'importanza dei sistemi di IA medica ruota intorno a valutazioni della loro prestazione, come questa è riconducibile al mero conto degli errori, in cui eventualmente si distingue tra falsi negativi e falsi positivi (come si fa riportando sensitività e specificità); in altre parole, in larga parte ci si limita a considerare questi siste-

mi come elementi isolati e che sono applicati su dati retrospettivi, cioè raccolti per scopi secondari rispetto alla cura dei pazienti ed estratti, dopo opportune elaborazioni, dalle reali condizioni di produzione e consumo, cioè dalla pratica clinica. A tal fine, è grande la varietà delle tecniche e delle metriche con cui il tasso di errore di questi sistemi, o il suo complemento, l'accuratezza, è calcolato e riportato: una delle metriche più note a riguardo è l'area sotto la curva ROC. Questa metrica vuole rappresentare in termini probabilistici la capacità discriminativa di un sistema di classificazione binaria ma, nonostante la popolarità che le deriva dall'essere citata in centinaia se non migliaia di articoli scientifici, soffre di numerosi difetti: tra questi, ricordiamo quelli di non considerare la prevalenza della classe di maggiore rilievo clinico, o il peso di diversi tipi di errore, o il limite di non permettere un confronto oggettivo tra metodi alternativi[4]. Oltre alla suddetta "babele" metrica, gran parte degli studi che riportano i risultati di studi sulla IA medica sono caratterizzati da approcci superficiali relativamente alla fase di raccolta e "ingegnerizzazione" dei dati, oppure relativamente alla fase di validazione, in cui gli autori si limitano a riportare misure di accuratezza classificatoria senza valutare il ruolo dell'incertezza nella definizione delle loro stime[5]. Così facendo si ignora il fattore più importante in ambito di IA medica, soprattutto quando questa è costruita con tecniche di machine learning di tipo "supervisionato", cioè a partire da dati di cui è già nota la caratteristica che questi sistemi devono predire o produrre: la loro capacità di migliorare la prestazione delle squadre di clinici che le useranno su dati reali (real-world) al letto del paziente, e quindi di migliorare la qualità delle cure e degli esiti[6]. Se stimare quest'ultima capacità diviene l'obiettivo primario della ricerca nell'ambito della IA Medica, ecco che un nuovo ruolo può emergere dal panorama della scienza dei dati e dell'informatica medica: l'ingegnere informatico *interazionista*. Costui dovrebbe occuparsi di valutare l'uso e l'usabilità, la sicurezza e l'utilità, di questi supporti computazionali alla decisione medica, soprattutto nei contesti reali in cui i medici interagiscono con tali strumenti, durante cioè il loro lavoro di tutti i giorni. Per illustrare questo punto, faccio riferimento ad un costrutto di analisi, che è tanto semplice quanto potente nel permetterci di descrivere molti contesti in cui questi sistemi sono usati, come è stato proposto dal noto esperto di informatica medica, il prof. Enrico Coiera[7]: l'*ultimo miglio dell'implementazione* della IA medica. In questo ultimo miglio, che altri chiamano fase di "messa a terra", altri golfo esistente tra "sviluppo" e "operatività" (dev/op), io ho proposto di vedere due "iati" (vedasi **Figura 1**, basata su[8]): lo *iato della fiducia (del medico)* e lo *iato dell'esperienza (della macchina)*. Il primo iato, tra medico e macchina, è necessario coprirlo o presidiarlo se vogliamo che i sistemi di supporto decisionale siano effettivamente usati dagli operatori sanitari, così da concretizzare il loro potenziale di riduzione dell'errore medico e di efficientamento. Il secondo iato è invece ciò che deve percorrere il dato prodotto dal medico perché esso informi lo sviluppo di questi sistemi: lo iato dell'esperienza riguarda quindi tutti i processi con cui si raccolgono le grandi quantità di dati di cui le tecniche di machine learning hanno bisogno, e in cui si garantisce la loro qualità, cioè veridicità ed esattezza, che è necessaria affinché le macchine non apprendano distorsioni di giudizio (bias) e non finiscano per reiterare interpretazioni discriminatorie o di dubbia attendibilità in funzione delle caratteristiche dei soggetti coinvolti. Lo iato della fiducia riguarda quindi aspetti di ingegneria dell'usabilità e di ergonomia cognitiva che sono relativamente poco studiati dalle comunità scientifiche di riferimento (cioè quella degli sviluppatori di IA, o quella dei medici utilizzatori), e che non riguardano solo i modi migliori per garantire efficienza ed efficacia di questi sistemi ma anche la soddisfazione degli utenti e l'utilità delle informazioni che i sistemi forniscono loro. L'informatività dell'output delle macchine è, ad esempio, incrementata programmando, e configurando opportunamente, funzionalità grazie alle quali questi sistemi sono in grado di fornire spiegazioni (explanations, come sono chiamate nell'ambito della cosiddetta explainable AI[9]) plausibili per ciascuna delle raccomandazioni o suggerimenti che essi producono; o funzionalità che permettano agli utenti di esplorare diverse alternative e quindi essere supportati anche in ragionamenti di tipo *causale* o *controfattuali*, cioè, del tipo "cosa

Figura 1.
Schema concettuale dell'ultimo miglio della Intelligenza Artificiale Medica.
Adattato da [8]

succederebbe o che tipo di caso sarebbe se un certo dato o aspetto fosse così anziché come è". È questo iato della fiducia che deve essere presidiato anche per mitigare il rischio relativo a molti problemi di distorsione cognitiva, tra i quali citiamo quello noto con il termine di *automation bias*[10] che occorre ogniqualvolta un decisore umano si fida eccessivamente del supporto alle decisioni (anche quando quest'ultimo si sbaglia); o per garantire sicurezza (sia nel senso di cybersecurity che di patient safety) in tutti i casi in cui i fattori umani, ad esempio la tendenza al disapprendimento (deskilling[11]) o ai comportamenti opportunistici (come ad esempio in ambito di sovradiagnosi[12] e di medicina difensiva) sono presenti, o predominanti. Il secondo iato, quello dell'esperienza, riguarda invece i processi di raccolta dei dati e di loro etichettamento o meglio di "annotazione", come si chiama il processo di assegnazione di un valore vero di riferimento ai casi che devono essere appresi dai sistemi computazionali di apprendimento automatico. Anche tale iato nasconde delle insidie, spesso sottovalutate: ad esempio, la variabilità osservazionale (che è tanto maggiore quanto è più ampio il disaccordo tra i valutatori coinvolti) [13]; o la deriva concettuale (anche detta "concept drift"), cioè la modifica nel tempo del fenotipo da diagnosticare o su cui prendere decisioni di varia natura. Il "ponte" che può metaforicamente ricoprire questo iato necessita di un approccio genuinamente multidisciplinare (vedasi **Figura 2**), dove diversi aspetti siano considerati come parte di un tutto, per superare l'ostacolo più importante, o almeno quello che precede tutti gli altri: il fatto che nessun sistema computazionale può produrre in *output* risultati migliori o di maggiore attendibilità dei dati di *input*. Questo fatto, per quanto ovvio, è così importante che spesso si cita a riguardo il noto adagio inglese, "garbage in, garbage out": se entra in ingresso spazzatura, in uscita non si può che ottenere spazzatura. A riguardo, è necessario ripensare il modo in cui progettiamo e valutiamo questi sistemi, ed è quindi necessario concepire e consolidare nuove metodologie da adottare anche come base per le procedure di validazione e certificazione del software come dispositivo medico[14].

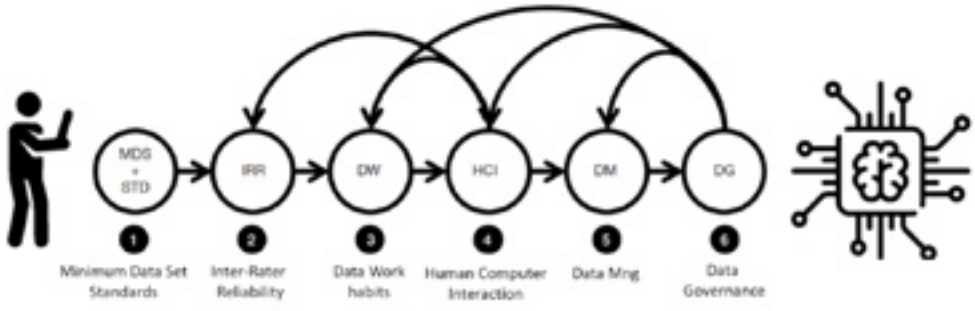


Figura 2.
Schema concettuale degli ambiti di ricerca che incidono sullo iato della esperienza della macchina.
Adattato da [8]

Il famoso progettista di sistemi di IA, Andrew Ng, ha recentemente[1] proposto di abbandonare un approccio basato sui modelli, fino ad oggi egemonico nel panorama degli studi IA, per iniziare a concentrarsi su un approccio alternativo, uno "basato sui dati", cioè che consideri prioritario curare ogni aspetto, compresa la trasparenza, dei processi di produzione del dato di partenza, e garantire la loro qualità e attendibilità, come propongono anche i promotori delle data *nutrition labels*[2] e dei *data sheet*[15]. Allo stesso modo, anche noi nel nostro piccolo[16], abbiamo recentemente parlato di un *approccio prospettivista* allo sviluppo della IA, in cui sia valorizzata, anziché negata, la ricchezza del dato medico, anche nella sua intrinseca ambiguità e complessità; e non solo nelle fasi di raccolta del dato, ma anche in quello di sviluppo dei modelli computazionali. La sfida non è quindi quella di rendere la medicina più razionale e standardizzata per mezzo delle nuove macchine a supporto delle decisioni, cioè spingere gli uomini a comportarsi come macchine. Al contrario, medici e ingegneri informatici, comprese nuove figure più focalizzate sulla qualità del rapporto essere umano-macchina, devono collaborare per rendere possibile la creazione di strumenti adeguati e affidabili (anche nel senso di *trustworthy*, cioè degni di fiducia) che i medici possano utilizzare per fronteggiare la sfide poste dalla loro professione al crescere della complessità dei casi di una popolazione destinata ad esibire un sempre maggiore tasso di invecchiamento e cronicità; cioè sviluppare macchine che aiutano gli esseri umani ad essere tali.

1. https://www.youtube.com/watch?v=06-AZXmwHjo
2. https://datanutrition.org/

Bibliografia

[1] Liu, X., Faes, L., Kale, A. U., Wagner, S. K., Fu, D. J., Bruynseels, A., ... & Denniston, A. K. (2019). A comparison of deep learning performance against health-care professionals in detecting diseases from medical imaging: a systematic review and meta-analysis. *The lancet digital health*, 1(6), e271-e297.

[2] Cabitza, F., Campagner, A., Soares, F., de Guadiana-Romualdo, L. G., Challa, F., Sulejmani, A., ... & Carobene, A. (2021). The importance of being external. methodological insights for the external validation of machine learning models in medicine. *Computer Methods and Programs in Biomedicine, 208*, 106288.

[3] Coiera, E., Ammenwerth, E., Georgiou, A., & Magrabi, F. (2018). Does health informatics have a replication crisis?. *Journal of the American Medical Informatics Association, 25*(8), 963-968.

[4] Carrington, A. M., Fieguth, P. W., Qazi, H., Holzinger, A., Chen, H. H., Mayr, F., & Manuel, D. G. (2020). A new concordant partial AUC and partial c statistic for imbalanced data in the evaluation of machine learning algorithms. *BMC medical informatics and decision making*, 20(1), 1-12.

[5] Cabitza, F., & Campagner, A. (2021). The need to separate the wheat from the chaff in medical informatics. Introducing a comprehensive checklist for the (self)-assessment of medical AI studies *International Journal of Medical Informatics*. Volume 153, September 2021, 104510

[6] Cabitza, F., & Zeitoun, J. D. (2019). The proof of the pudding: in praise of a culture of real-world validation for medical artificial intelligence. *Annals of translational medicine*, 7(8).

[7] Coiera, E. (2019). The last mile: where artificial intelligence meets reality. *Journal of medical Internet research*, 21(11), e16323.

[8] Cabitza, F., Campagner, A., & Balsano, C. (2020). Bridging the "last mile" gap between AI implementation and operation:"data awareness" that matters. *Annals of translational medicine, 8*(7).

[9] Holzinger, A., Langs, G., Denk, H., Zatloukal, K., & Müller, H. (2019). Causability and explainability of artificial intelligence in medicine. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 9(4), e1312.

[10] Lyell, D., Magrabi, F., Raban, M. Z., Pont, L. G., Baysari, M. T., Day, R. O., & Coiera, E. (2017). Automation bias in electronic prescribing. *BMC medical informatics and decision making, 17*(1), 1-10.

[11] Cabitza, F., Rasoini, R., & Gensini, G. F. (2017). Unintended consequences of machine learning in medicine. *Jama, 318*(6), 517-518.

[12] Vogt, H., Green, S., Ekstrøm, C. T., & Brodersen, J. (2019). How precision medicine and screening with big data could increase overdiagnosis. *Bmj, 366*.

[13] Cabitza, F., Campagner, A., & Sconfienza, L. M. (2020). As if sand were stone. New concepts and metrics to probe the ground on which to build trustable AI. *BMC Medical Informatics and Decision Making, 20*(1), 1-21.

[14] Harvey, H., & Cabitza, F. (2018). Algorithms are the new drugs? Reflections for a culture of impact assessment and vigilance. MCCSIS. IADIS International Conference ICT, Society and Human Beings.

[15] Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Iii, H. D., & Crawford, K. (2021). Datasheets for datasets. *Communications of the ACM, 64*(12), 86-92.

[16] Basile, V., Cabitza F., Campagner A., Fell, M. (2021) Toward a Perspectivist Turn in Ground Truthing for Predictive Computing arXiv:2109.04270v1 [cs.LG] for this version) https://arxiv.org/abs/2109.04270

ECM ieri, oggi in epoca di COVID e domani

Aldo Mozzone
Consigliere OMCEO Torino
Coordinatore Commissione Formazione Permanente e Accreditamento Formativo
Andrea Pizzini
Segretario della Scuola Piemontese di Medicina Generale
Componente Commissione Formazione Permanente e Accreditamento Formativo

La pandemia da COVID ha influito profondamente sulla scelta delle tecniche didattiche utilizzate per la formazione e per la conseguente acquisizione dei crediti ECM.

Fermo restando il ruolo vincolante della formazione per la nostra professione (**BOX 1**), le difficoltà logistiche e le stesse norme ministeriali (ad esempio il DPCM del 14 gennaio 2021) hanno fortemente ridimensionato le attività in presenza (ovvero la formazione residenziale quale quella fornita con congressi, convegni, corsi di formazione in aula) e incentivato per contro le attività a distanza (**Formazione a Distanza sincrona**, mediante piattaforme digitali, e **asincrona**, erogata con corsi preregistrati). Ciò sfruttando le potenzialità proprie della FAD che è in grado di ovviare, e con costi contenuti, alla necessità di essere presenti in una determinata sede ed in un preciso spazio temporale e di essere fruibile contemporaneamente da un elevato numero di partecipanti. Abbiamo assistito in questi mesi al diffondersi di eventi come audio o video conferenze, corsi online, webinar (seminari via web), che hanno consentito di mantenere comunque viva la formazione. Piattaforme come Cisco Webex, Skype, Zoom e altre ancora, sono divenute uno strumento ormai imprescindibile per incontri formativi di varia durata e con numeri sempre più ampi di utenti. È stato cioè necessario spaziare tra le varie modalità didattiche previste per la formazione professionale (**BOX 2**), al fine di garantire comunque in epoca emergenziale l'aggiornamento continuo del medico.

I **limiti della FAD** sono altrettanto noti. Prima di tutto è fortemente penalizzata la possibilità di interagire tra formatori e discenti con la conseguente perdita dei vantaggi legati alla possibilità di un continuo feedback tra gli attori. In secondo luogo è molto più difficile adottare quelle tecniche didattiche come i lavori di gruppo che consentono di apprendere attivamente. Anche gli strumenti di verifica della produttiva partecipazione e dell'acquisito apprendimento sono più difficilmente utilizzabili e perdono efficacia sia formativa che certificativa. In ultimo la FAD richiede strumenti informatici (hardware, collegamenti) e una dimestichezza con essi che non è necessariamente patrimonio di tutti i colleghi, in particolare dei meno giovani.

Anche la **didattica tutoriale** e altre tecniche di formazione sul campo (che prevedono ad esempio la costituzione di gruppi di confronto tra pari), che si svolgono inevitabilmente nei luoghi di lavoro, sono risultate pesantemente condizionate dalle limitazioni negli accessi a reparti ospedalieri e ambulatori, mentre, per contro, molti colleghi sono stati costretti ad operare sul campo (ad esempio nelle Unità Speciali di Continuità Assistenziale, USCA) ed a maturare in autonomia alcune competenze necessarie per poter svolgere l'importante incarico ricevuto.

BOX 1

Nella Comunicazione n. 115/2020 la FNOMCEO ricorda che **ai sensi dell'art. 16-quater del D.Lgs. 502/30.12.1992 e s. m.**:

- la partecipazione alle attività di formazione continua costituisce requisito indispensabile per svolgere attività professionale, in qualità di dipendente o libero professionista, per conto delle aziende ospedaliere, delle università, delle aziende sanitarie locali e delle strutture sanitarie private;
- i contratti collettivi nazionali di lavoro del personale dipendente e convenzionato prevedono specifici elementi di penalizzazione, anche di natura economica, per il personale che nel triennio non abbia conseguito il minimo di crediti formativi stabilito dalla Commissione Nazionale per la Formazione Continua;
- per le strutture sanitarie private l'adempimento, da parte del personale sanitario dipendente o convenzionato che operi nella struttura, dell'obbligo di partecipazione alla formazione continua e la maturazione dei crediti nel triennio costituiscono requisito essenziale per il conseguimento o la conservazione dell'accreditamento da parte del Servizio Sanitario Nazionale.

BOX 2

ECM: TIPOLOGIE DIDATTICHE PREVISTE IN BASE ALL'ACCORDO STATO-REGIONI DEL 2.2.2017

Al fine di garantire un quadro completo ed armonico che permetta di comprendere le diverse possibili modalità di formazione/apprendimento utilizzabili sono state identificate le seguenti 11 tipologie:

1. FORMAZIONE RESIDENZIALE CLASSICA (RES)
2. CONVEGNI, CONGRESSI, SIMPOSI E CONFERENZE (RES)
3. VIDEOCONFERENZA (RES)
4. TRAINING INDIVIDUALIZZATO (FSC)
5. GRUPPI DI MIGLIORAMENTO (FSC)
6. ATTIVITÀ DI RICERCA (FSC)
7. FAD CON STRUMENTI INFORMATICI / CARTACEI (FAD)
8. E-LEARNING (FAD)
9. FAD SINCRONA (FAD)
10. FORMAZIONE BLENDED
11. DOCENZA, TUTORING E ALTRO

DAL PUNTO DI VISTA DEI PROVIDER

Dal marzo del 2020 si sono improvvisamente interrotte tutte le attività formative in presenza che erano la maggior parte delle attività formative programmate, per passare ad attività a distanza mediante l'uso della tecnologia digitale.

I provider si sono così visti costretti a riorganizzare il piano formativo previsto passando attraverso tre fasi:

1. **FASE 1:** rapidamente sona stati costretti a trasformare in Webinar i corsi residenziali già programmati e che non era più possibile svolgere per il lockdown, riorganizzando, e per molti realizzando, le piattaforme digitali per la FAD.
2. **FASE 2:** tutti i progetti formativi si sono dovuti organizzare con modalità a distanza, creando progetti dedicati alla FAD. Le difficoltà sono state numerose, sia per le procedure ECM diverse da quelle previste per la formazione residenziale, sia per la non abitudine dei docenti a tale modalità di formazione (alcuni non erano in grado di svolgere la docenza o per motivi di carenze di competenze tecnico/informatiche, o per la difficoltà di svolgere il proprio ruolo in una modalità che non prevede il contatto docente/discente tradizionale) ed in ultimo per la non conoscenza da parte dei partecipanti alla formazione delle modalità di svolgimento degli eventi a distanza e delle procedure di registrazione, partecipazione (deve rimanere collegato almeno per il 70% del periodo) e svolgimento delle pratiche ECM: il discente, finito l'evento, ha tempo 3 giorni per compilare il questionario di Gradimento ed il Test di autovalutazione. Per quest'ultimo, in caso di non raggiungimento del LAP minimo, il discente ha a disposizione 5 tentativi, previa visione del registrato dell'evento.
3. **FASE 3:** è l'attuale momento storico in cui vi è la possibilità di ritornare a svolgere eventi in presenza con tuttavia nuove regole di svolgimento. La formazione quindi oggi si svolge con la maggior parte degli eventi a distanza, avendo oramai acquisito una buona confidenza con le caratteristiche di questa modalità di formazione, ed una quota crescente di formazione residenziale e formazione sul campo. Qualora si rendesse necessario, i provider dovranno comunque essere pronti a ritrasformare tali eventi in presenza in eventi a distanza.

La formazione a distanza ha alcune caratteristiche:

- si inizia con la registrazione all'evento: la maggior parte dei partecipanti (più del 60%) sceglie di iscriversi nell'ultima settimana dall'evento. Questo rende complessa l'organizzazione e la programmazione degli eventi
- in media solo il 50% dei registrati poi partecipa veramente all'evento a distanza e si collega, mentre il drop out durante il webinar è in genere basso (sotto il 10%)
- per questo rischio e per l'implicita difficoltà nel seguire la formazione a distanza da parte del discente, i webinar non devono essere troppo lunghi: il massimo delle ore da prevedere è di 3
- il maggior impegno orario di partecipazione alla formazione a distanza è anche riconosciuto formalmente, in quanto sono previsti 1,5 crediti ECM ogni ora al posto di 1 credito/ora attribuito alla classica formazione residenziale.

LE NOVITÀ INTRODOTTE CON LA PANDEMIA DALLA COMMISSIONE NAZIONALE ECM

Agli operatori sanitari, lavoratori dipendenti o liberi professionisti, che abbiano continuato a svolgere la propria attività durante il periodo di emergenza, sarà comunque riconosciuto come assolto il debito formativo relativo al periodo di pandemia (in base alla Legge

6.6.2020 n. 41 art. 6 comma 2 ter) nella misura dei 50 crediti ECM previsti per il 2020 come quota parte del totale di 150 crediti previsti per il triennio 2020-2022.

Sempre in ragione della pandemia, altre novità sono state deliberate dalla Commissione Nazionale per la Formazione Continua, che, in data 4.2.2021, ha disposto:

- **Professionisti in quiescenza che svolgono l'attività saltuariamente:** l'esenzione dall'obbligo di maturare crediti formativi prevista dal Manuale sulla formazione continua del professionista sanitario, viene consentita al sanitario che dichiari di aver cessato l'attività per pensionamento e che consegua un reddito annuo per le prestazioni occasionali che non supera i 5000 euro annui. A questi professionisti viene concessa una riduzione del debito ECM di 2 crediti ogni 15 giorni di sospensione dell'attività lavorativa nell'ambito del triennio. In caso di ripresa dell'attività, riparte l'obbligo di acquisizione dei crediti per l'intero triennio formativo.
- **Personale sanitario dei sistemi di emergenza territoriale:** la Commissione, nell'esprimere il suo orientamento relativo alla "Formazione sul Campo" ed in particolare al suo svolgimento all'interno del contesto lavorativo del professionista, sottolinea come la formazione continua di questi operatori, "per evidenti motivi di mantenimento delle capacità operative" non può essere sospesa o rimandata. Pertanto il divieto di svolgimento di "convegni, congressi e altri eventi" statuito dal DPCM del 14 gennaio 2021, all'art.1, comma 10, lettera o) non può ad essa essere applicato.
- La Commissione nazionale ECM ha adottato il 23.09.2021 la delibera in materia di **dossier formativo** (DF individuale e DF di Gruppo). Si tratta di uno strumento che consente al singolo professionista di creare un'agenda formativa personalizzata in base al proprio fabbisogno e/o a quello di un gruppo di cui fa parte per favorire la crescita professionale propria e collettiva. In particolare, la delibera prevede la possibilità di costituire il dossier formativo in tutti e tre gli anni del triennio, ma di poterlo modificare una sola volta per ciascun anno del triennio di riferimento.

La nostra FNOMCeO ha ritenuto opportuno ripetere l'esperienza, già realizzata nel 2019, di costruire un Dossier formativo di Gruppo, relativo al triennio formativo in corso, nel quale ha inserito tutti gli iscritti, medici e odontoiatri.

La costruzione del suindicato dossier consente ad ogni medico e odontoiatra di acquisire immediatamente un bonus di 30 crediti formativi assegnati nel triennio 2020-2022; qualora il professionista, entro il 31 dicembre 2022, realizzasse almeno il 70% del proprio percorso formativo rispettando le tre aree prescelte, conseguirà gli ulteriori 20 crediti previsti, che saranno assegnati nel triennio successivo (2023-2025). (Comunicazione FNOMCeO n. 197 reperibile al link https://portale.fnomceo.it/archivio-comunicati-ordini/).

Vanno segnalate inoltre due novità non direttamente correlate con la pandemia:

- la Commissione nazionale per la formazione continua ha nel luglio 2020 stabilito di inserire tra le tematiche speciali di interesse nazionale la "Medicina di genere" prevedendo un incremento di 0,3 crediti/ora per gli eventi ECM che avranno per oggetto tale tematica.
- per chi non avesse completato il conseguimento dei crediti per i trienni 2014/2016 e 2017/2019 (B**OX 3**), il **recupero dei crediti** mancanti è consentito fino al 31 dicembre 2021 ed il relativo spostamento si può effettuare sul sito del CoGeAPS a cura del professionista (delibera del 10 giugno 2020).

BOX 3

COME VERIFICARE I CREDITI OTTENUTI

Per verificare i crediti ECM ottenuti, è necessario iscrivervi all'area privata del Co.Ge.A.P.S.

Secondo quanto stabilito dall'Accordo Stato Regioni del 5 Novembre 2009, il Co.Ge.A.P.S. è **"l'organismo nazionale deputato alla gestione delle anagrafiche nazionali e territoriali, dei crediti ECM attribuiti ai professionisti che fanno capo agli Ordini, Collegi nonché le rispettive Federazioni nazionali e Associazioni professionali, consentendo a questi le relative funzioni di certificazione delle attività formative svolte"**.

L'accesso ai propri dati può avvenire agevolmente utilizzando le credenziali SPID.

Sul sito dell'AGE.NA.S (https://ape.agenas.it/home.aspx) è possibile consultare esaustive FAQ su questi argomenti di nostro interesse: Crediti ottenuti all'estero, Dossier formativo, Autoformazione, Provenienza crediti… e molto altro.

PROSPETTIVE FUTURE

Naturalmente è in tutti noi la speranza che i danni ed i condizionamenti che la pandemia ha determinato possano essere presto solo più un triste ricordo. Nella formazione gli eventi correlati al COVID-19 hanno verosimilmente accelerato un processo di cambiamento che per questioni logistiche e di costi sarebbe comunque avvenuto. Anche nella definizione degli obiettivi formativi assistiamo a mutazioni legate alla necessità di acquisire nuove competenze che sono richieste ai professionisti della sanità. La sfida è ora ritornare a processi formativi, magari blended, misti, che consentano di massimizzare i vantaggi insiti nelle tecniche in presenza ed in quelle a distanza, correggendo gli aspetti negativi.

È soprattutto necessario che i sistemi di valutazione siano ritarati alla luce delle nuove tecniche didattiche utilizzate, in modo da riuscire a cogliere le ricadute professionali che la partecipazione agli eventi ECM è in grado di produrre ed in particolare il proficuo cambiamento che la formazione comporta nell'immediato e nel corso del tempo. Ciò è da sempre il punto critico di ogni evento formativo, ma l'accentuarsi delle distanze tra formatori e professionisti discenti corre il rischio di acuire questa criticità.

IL SISTEMA ECM

Facciamo chiarezza sugli organi istituzionali.

AGE.NA.S - Agenzia Nazionale per i Servizi Sanitari. Ha in carico la gestione amministrativa del programma di ECM ed il supporto alla Commissione Nazionale per la Formazione Continua

COMMISSIONE NAZIONALE - Dirige il sistema di accreditamento avvalendosi degli organi di supporto quali il Comitato di Garanzia e l'Osservatorio Nazionale.

COMITATO DI GARANZIA

a) vigila sull'indipendenza dei contenuti formativi degli eventi da interessi commerciali;

b) monitora i piani formativi e i singoli eventi formativi;

c) vigila sulla corretta applicazione della normativa E.C.M. in materia di sponsorizzazioni, pubblicità e conflitto di interesse anche attraverso verifiche in loco nelle sedi degli eventi formativi;

d) istruisce i procedimenti di verifica nei confronti dei provider;

e) elabora pareri e proposte alla Commissione nazionale sulle materie di propria competenza.

OSSERVATORIO NAZIONALE

a) vigila sulla qualità dei contenuti degli eventi formativi;

b) verifica la coerenza degli eventi realizzati con gli obiettivi formativi programmati;

c) relaziona alla Commissione nazionale per la formazione continua sui flussi di offerta e domanda formativa avvalendosi dell'Anagrafe nazionale;

d) rileva i dati costitutivi del report annuale nazionale sullo stato di attuazione del Programma nazionale E.C.M.;

e) promuove ricerche sui criteri e le modalità per l'avvio e lo sviluppo di nuove e più efficaci metodologie di valutazione dei percorsi formativi;

f) elabora pareri e proposte alla Commissione nazionale per la formazione continua sulle materie di propria competenza;

g) supporta le valutazioni di qualità delle attività formative compiute dai provider in relazione agli obiettivi nazionali e regionali di formazione.

COMITATO TECNICO REGIONI

Il Comitato Tecnico delle Regioni offre supporto alla Commissione nazionale nell'ambito dei lavori delle sezioni in cui si articola la Commissione stessa, nell'attività di armonizzazione del sistema nazionale e dei sistemi regionali e delle Province autonome di Trento e Bolzano

CO.GE.A.P.S.

Il Co.Ge.A.P.S. (Consorzio Gestione Anagrafica Professioni Sanitarie) è un organismo che riunisce le Federazioni Nazionali degli Ordini e dei Collegi e le Associazioni dei professionisti coinvolti nel progetto di Educazione Continua in Medicina.

Il Co.Ge.A.P.S. nasce per essere lo strumento attuativo della Convenzione stipulata con il Ministero della Salute che prevede la realizzazione di un progetto sperimentale per la gestione e certificazione dei crediti formativi ECM, l'istituzione di una anagrafe degli professionisti sanitari e l'allestimento di un servizio tecnico permanente di aggiornamento dedicato ai rapporti con gli enti pubblici.

REGIONI E PROVINCE

Alle Regioni è affidato il compito di promuovere sul proprio territorio il sistema per la formazione continua, mediante appropriate forme di partecipazione degli Ordini e dei Collegi professionali (per esempio consulte regionali per la formazione continua).

Sitografia

- DPCM 4 Marzo 2020 - https://www.gazzettaufficiale.it/eli/id/2020/03/04/20A01475/sg
- DPCM 8 Marzo 2020 - https://www.gazzettaufficiale.it/eli/id/2020/03/08/20A01522/sg (sospensione attività formative d'aula)
- AGE.NA.S. Agenzia Nazionale per i Servizi Sanitari Regionali - https://ape.agenas.it/Home.aspx
- Delibera della Commissione Nazionale per la Formazione Continua - Infezione da Coronavirus 2019-NCOV - https://ape.agenas.it/documenti/normativa/Delibera_Coronavirus_2019_nCoV_14_02_2020.pdf
- 17/06/2020 - Commissione Nazionale per la Formazione Continua - Delibera emergenza epidemiologica da Covid-19 - https://ape.agenas.it/documenti/Normativa/Delibera_emergenza_covid-19_10_06_2020.pdf

Lo stile dell'abuso. Violenza domestica e linguaggio

Roma, Treccani, 2021

Intervista all'autrice, Raffaella Scarpa
Docente di linguistica medica e clinica presso l'Università degli Studi di Torino.

Tra i tanti punti di vista dai quali si analizza il fenomeno della violenza domestica nessuno è stato più sottovalutato del linguaggio. Eppure, l'uso delle parole, la loro combinazione, lo "stile del discorso" costituiscono invece il mezzo fondamentale di cui l'abusante si avvale per ridurre e mantenere la donna in uno stato di soggezione e soccombenza. Oggi la violenza è un ampio contenitore mediatico e non solo. Ma è spesso difficile orientarsi per non rischiare di essere parziali e incompleti. Esiste una particolare forma di male subito che fa dell'assenza di ragione il suo principio costituente, e questo è insito nella violenza domestica.

Professoressa come nasce il percorso che ha portato a trattare un tema così discusso da un punto di vista nuovo, cioè la prospettiva linguistica?

La lingua degli abusanti, la forma che prendono le loro parole quando si rivolgono alla loro compagna in effetti non era mai stato oggetto di indagine. Occorre un orecchio ben addestrato – quello dei linguisti in genere lo è – per intercettare quelle piccole incrinature che caratterizzano il discorso maltrattante che invece appare assolutamente normale. Mi piace studiare i comportamenti linguistici "estremi" (la lingua del delirio, della follia, del fine-vita, della violenza ecc.) proprio per ciò che si nasconde sotto le parole. Ricordo una testimonianza, vado a memoria ma il senso è questo: "non capisco ancora adesso cosa nel suo modo di parlare mi facesse così paura, non c'era nulla di strano eppure mi paralizzavo".

Professoressa, sappiamo che per il grande pubblico la linguistica è molto connotata, spesso confusa con una disciplina che si occupa della correttezza grammaticale, della competenza lessicale o sintattica o della didattica delle lingue straniere. Possiamo fare un po' di chiarezza?

Certo, mi è capitato diverse volte di essere scambiata per una 'maestrina dalla penna rossa' o di una insegnante di lingue straniere. La linguistica è molte cose; la mia linguistica è un sapere che usa sonde di profondità per scoprire le latenze, il non detto, la forza ignota che struttura ciò che scriviamo e diciamo e che non è chiara, spesso, neppure a noi. Molti anni iniziai a studiare la lingua della psicosi presso il reparto di psichiatria dell'Amedeo di Savoia, quella fu una straordinaria occasione che mi costrinse a impegnarmi a comprendere quali verità nascondeva la lingua del delirio.

È stata proprio questa esperienza che mi ha dato la possibilità di esercitarmi al dissotteramento dei significati profondi del testo, per questa ragione la mia passione per la stilistica.

A questo proposito, lo stile non è un concetto semplice. Come lo si riconosce?

Lo stile non è certamente un concetto semplice, soprattutto quando non è applicato al testo letterario. Io ho rimodulato il concetto di analisi stilistica che, nella nostra tradizione, è un metodo applicato essenzialmente ai testi letterari, pensandolo per i testi non letterari. L'analisi linguistica è la mappatura del testo (sul piano grammaticale, testuale, retorico, logico-argomentativo) mentre l'analisi stilistica attribuisce un valore aggiunto, cioè individua uno stilema, ovvero quella figura linguistica che dice più del suo significato grammaticale: mette in relazione la struttura della lingua con l'istanza profonda che la genera, cioè mette in risonanza la matrice profonda del parlante e funziona proprio come una sorta di "macchina della verità". In estrema sintesi l'analisi stilistica lega il soggetto alla sua propria lingua in maniera stretta e incontrovertibile.

Nel caso della violenza domestica, soltanto i sensori acutissimi della stilistica potevano essere in grado di cogliere ciò che deve per agire sotto traccia e per non essere disinnescato.

Il testo è carico di testimonianze forti. Lei ha toccato biografie con garbo ma senza risparmiare le ferite, ma ribadisce sempre che ha filtrato il "troppo".

Questo lavoro di ricerca dura da circa 20 anni. Non in modo continuativo e dedicato. Ma diluito col tempo, diluendo anche l'ascolto di queste testimonianze. Questo tempo aiuta anche ad assimilarle. Io ho scelto di non appoggiarmi ad una rete istituzionale, ma ho cercato storie ad alta grado di autenticità. Volevo essere un interlocutore libero, svincolato da un ruolo codificato. Il numero dei casi non è infinito, ma la tipologia è molto ricca. E ho trovato persone - abusate e abusanti - che hanno messo a di-sposizione la loro storia e le loro parole, il libro l'hanno fatto loro, lo dico senza alcuna retorica.

Ho dovuto ovviamente tagliare molti dettagli per la protezione della privacy, ma an-che le parti più dure per rispetto al tollerabile. Non volevo perpetrare il gioco dell'abuso. Lo sappiamo e lo vediamo tutti i giorni sui media: insistenza su particolari, morbose descrizioni che col tempo rischiano di agevolare proprio il meccanismo stesso della violenza, anestetizzando progressivamente il senso del limite, del tollerabile.

A questo proposito Lei scrive nella dedica: "Dedicato a chi non sa riconoscere l'intollerabile"…

Non ai fragili, ma a chi non riconosce l'intollerabile. Questa differenza è importante. Non è un appello a chi è in condizione di fragilità, ma a chi non è – non riesce, non può – essere in ascolto di sé e ascoltare il mondo e la realtà dei fatti. Non è possibile che le campagne di comunicazione confondano i piani, rendendo ancora più fragili soggetti che non lo sono. Stiamo sbagliando a costruire un immaginario in cui se non appartieni ad una iconografia di donna o persona distrutta o umiliata, allora non rientri nel repertorio di immagini che riportano alla violenza domestica. L'ideologia vittimaria è oggi il primo travestimento delle ragioni dei forti.

Potere, violenza, linguaggio. Pensiamo alla relazione medico-paziente: pos-siamo riflettere su quando ci siamo detti - in modo traslato e rimodulato?

La relazione medico-paziente da sempre è la rappresentazione di un potere istituzionalizzato. In cui la soggezione del sottoposto (paziente) non è prodotta, ma è reale. Noi tutti sappiamo quanto le parole di un operatore sanitario riverberino, come delle onde sonore che appartengono ad un'altra lingua, con derive di significato infinito quando siamo in un contesto di assistenza, in una condizione di fragilità. A volte determinate espressioni generano un ottundimento, una sorta di dolore che non sappiamo da dove arriva. E si entra in una confusione protettiva. Ovviamente in questo contesto non si ha a che fare con l'abuso, ma comunque con una condizione di potere che può generare dolore e a volte una sorta di paralisi afasica.

Professoressa, come possiamo rilanciare la riflessione?

Possiamo dire che dobbiamo forse ripartire dalla definizione. E non sono sicura che la categoria di violenza sia adeguata per descrivere queste diverse condizioni di abuso. Spesso negli studi si attesta che gli atteggiamenti violenti sono riconoscibili. Ma nella violenza domestica non è così, soprattutto nei casi in cui la lesione non è fisica, o non soltanto fisica. È "lo stile dell'abuso" – che è essenzialmente una macchina linguistica di menzogna, manipolazione, assoggettamento e annichilimento – che crea le precondizioni per la violenza comunemente intesa.

DESTINO ETERNITÀ DOLORE

Di tutte le cose è necessario dire che è impossibile che non siano cioè è necessario affermare che tutte sono eterne.

Emanuele Severino

Corinna Albolino

Università Ca' Foscari di Venezia. Specializzata in scrittura autobiografica presso la Libera Università dell'Autobiografia di Anghiari (Arezzo).

"Capita. Capita da giovani, capita da vecchi, capita che suoni positivo… capita che sia negativo"

Questa è la vita, sembra dirci in un suo testo Gina Lagorio riferendosi al tumulto degli eventi felici o tragici che, con tutto il carico delle emozioni che li accompagnano, intessono il nastro del nostro vissuto imprimendone senso.

Felicità e dolore sono allora affezioni, sentimenti in risposta a qualcosa che ci accade e rinviano alla pienezza della vita stessa che ama manifestarsi nella fantasmagoria delle sue forme arrivando fino a toccare l'anima. Sono epifanie, manifestazioni attribuite di volta in volta al gioco del *Caso*, all'espiazione di una *Colpa*, a una *Causa* conoscibile o a un ineluttabile *Destino*.

In particolare, la questione si complica quando a stravolgerci la vita è improvvisamente il negativo, nella forma di quella tremenda malattia che nell'immaginario ha il potere di evocare spettri di morte. In riferimento a tali eventi, un rimando importante va a Freud, là dove teorizza e avvalora che Eros e Thanatos, Amore e Morte, sono i due principi che intrecciano e governano l'esistenza. Sono elementi costitutivi della vita stessa. Freud mutua dalla filosofia questi due concetti che affondano infatti le loro radici etimologiche nelle origini greco-giudaico-cristiane dell'Occidente. Di amore illo tempore tematizza già Platone che tratta nei termini di *divina mania*, esplicitando quella condizione di *follia*, di estraniamento che cattura l'anima allorché invasa e sconquassata da Eros, il dio della danza e dell'ebbrezza.

Più cogente è l'idea di morte in quel significato *in-audito* di annientamento, di andare nel nulla da parte di ogni essente che gli antichi Greci hanno elaborato nella notte dei tempi, se seguiamo l'interpretazione di Emanuele Severino, uno dei più insigni filosofi contemporanei. Per primi essi hanno pensato la radicalità dell'opposizione logica tra essere, esistere hic et nunc e l'assolutamente nulla di sé. L'ente, tutto ciò che esiste, è questa oscillazione tra l'essere e il nulla, vale a dire è il provenire dal nulla e l'andare nel nulla di sé. Con i Greci si inaugura allora l'Occidente come apertura e sviluppo di una storia nichilista in cui ogni ente è identificato nella sua essenza con il niente. A fronte del divenire inteso come evidenza massima, perché suffragata dalla nostra innegabile esperienza, un processo tragico in cui ogni essente vacilla tra l'essere e il non-essere, tutto il percorso della riflessione filosofica si impone come lo strenuo tentativo di salvare i fenomeni, ciò che appare, dall'abisso del nulla. È la ricerca di un principio, di un fondamento meta-fisico immutabile ed eterno che ci sottragga da questo orizzonte conferendo senso alla nostra esistenza. È infatti dinanzi allo svanire, dileguare delle cose e più ancora di fronte al nostro sparire, davanti a questa aleatorietà, instabilità di ogni cosa presente, che nasce la filosofia come interrogazione, insonne ricerca del significato dell'essere, del senso della vita. E come bene esplicita Platone nel Teeteto e ribadisce Aristotele nel primo libro della Metafisica, è la *meraviglia*, quel sentimento complesso suscitato dallo stupore, turbamento, smarrimento per il divenire del mondo, a spingere l'umanità a domandare, voler sapere, conoscere. Rispetto a questa spiegazione più edulcorata del termine, irrompe il pensiero di Severino che ne dà una valenza più potente, più tragica. *Thàuma* (meraviglia) è piuttosto il terrore, quel terrore che lascia attoniti, sbigottiti e dice di quel sentire che si carica di angoscia quando vediamo l'annientamento di tutto ciò che esiste. Nell'esperienza della morte che è sempre morte dell'altro/a, nella rapina di ciò che ci è più caro, proiettiamo l'anticipazione del nostro destino di mortali. È l'imprevedibilità degli accadimenti a gettarci nell'angoscia, il fatto che non possiamo cioè prevedere e dunque controllare ciò che ci capita. Spiazzante è l'inquietudine se si pensa poi che il sopraggiungente possa portare dolore, morte. Ma sempre la filosofia che nasce da questo sgomento si pone altresì come *consolatio, phàrmakon*, rimedio di sopravvivenza. La dimostrazione di un principio divino si fa quindi abbraccio eterno che trattiene dal dissolversi nel nulla. In questa originale interpretazione severiniana, la storia occidentale diventa un sorprendente scenario in cui questi assoluti, immutabili si avvicendano come apparati, strutture fondanti in grado di conferire valore alla realtà, alla nostra vita. Lungo questo percorso storico, afferma il filosofo, prima il *Divino* elaborato dagli antichi greci e immanente a tutte le cose, poi il *Dio cristiano* esito dell'incontro tra tradizione greca e cristiana, quindi la *Scienza moderna* suffragata dal trionfo della Ragione illuminista, oggi la *Tecnica*, sono le grandi torri edificate per placare l'angoscia prodotta da quel tragico destino di finitezza evocato dagli antichi Greci. Potenti costruzioni, armamentari di simboli, credenze, ideologie che di volta in volta hanno declinato la nostra vita strappandola all'assurdo, conferendole un significato. Ma nel tempo questi baluardi hanno mostrato *piedi di argilla*, perché rivelatisi incapaci di adempiere alla loro funzione consolante.

QUANDO IL DOLORE CI INCHIODA

È nella severità della malattia oncologica, nei momenti drammatici in cui sentiamo che ne va della nostra vita, nella vertigine in cui ogni senso sembra smarrirsi, che questi riferimenti rassicuranti chiamati a soccorrerci, rivelano la loro impotenza. Perché a differenza dell'uomo greco che disincantato sapeva guardare in faccia la morte, stracciarle tutte le maschere illusorie e accettare fino in fondo il limite della finitezza, noi abitatori dell'Occidente più avanzato, rimaniamo invece figli di una cultura cristiana che, congedandosi da un concetto di morte come componente naturale della vita, ne ha perso tutta la tragicità. La morte assume qui la valenza di colpa, una colpa esito dell'allontanamento da Dio. Un Dio che, seppure onnipotente, nelle situazioni più cruciali non sa trattenerci dalla caduta negli inferi e non sa nemmeno confortarci perché anch'egli stesso, tremante di paura di fronte al baratro del nulla, ha gridato ed invocato il Padre.

Nella società attuale poi, neppure sa metterci al riparo dall'angoscia la scienza medica alla quale abbiamo da tempo affidato il destino del nostro organismo, perché ha mostrato, attraverso ricerche rigorose, sofisticate strumentazioni tecnologiche, di poter rompere la catena della necessità del destino e intervenire sui grandi eventi della vita. Un sapere scientifico che ambisce, nella evoluzione del progresso, a regalarci l'immortalità, soddisfacendo la nostra tensione più intima di diventare simili a Dio. Ma quando il dolore ci inchioda e il mondo attorno a noi si spegne e tutta l'attenzione implode sul corpo, avremmo invece bisogno di risposte immediate, certe, fondate su granitiche evidenze senza eccezioni. Al contrario, la scienza non ci illumina ma ci confonde nella penombra della probabilità, parlando di statistica, di verità provvisorie esito dell'accordo temporaneo e prevalente tra i ricercatori. E progressivamente crolla così anche il conforto alimentato dalla potenza della *thékne*, l'eco di quel mitico fuoco strappato da Prometeo agli dei e donato agli uomini perché divenissero artefici del proprio destino.

Dunque rimaniamo mortali, preda del terrore della morte perché è l'ignoto che ci spaventa. Se l'evidenza di nascita, malattia, morte, così come sono da sempre creduti e sperimentati dall'umanità, non fossero altro che esito di una errata e sedimentata interpretazione culturale della realtà? Frutto di un erroneo modo di intendere il divenire che si è imposto lungo tutta la nostra storia? E se la morte, concepita da sempre come distruzione radicale dell'essere, fosse invece, alla luce di una nuova ma rigorosa elaborazione severiniana, solo lo scomparire momentaneo dell'ente da un orizzonte più ampio definito cerchio dell'apparire? E se poi questo ente riapparisse infinite volte perché la totalità dell'essere, come già teorizzava all'origine Parmenide, padre venerabile della filosofia, è uno *sfero* eterno e immutabile?

Centro Studi Terapie Naturali e Fisiche

A.M.I.A.R. – TORINO

www.agopuntura.to.it

SCUOLA DI PERFEZIONAMENTO IN AGOPUNTURA

Direttore: Dott.ssa Tiziana Pedrali

Coordinatore scientifico: dott. Giovanni Battista Allais **Coordinatore didattico: dott. Giuseppe Lupi**

La Scuola di Perfezionamento in Agopuntura C.S.T.N.F. con D.D. n° 288 del 3 maggio 2017 è stata **inserita nell'elenco regionale degli Istituti pubblici e privati accreditati per la formazione nelle Medicine non Convenzionali**, come previsto dalla DGR n° 19-4764 del 13/03/2017.
La Scuola, attiva dal 1978, che da dicembre inizierà il suo 44° anno di attività, **è abilitata,** quindi, a rilasciare ai medici diplomati un **attestato per l'iscrizione negli elenchi dei medici Esperti in Agopuntura depositati presso gli Ordini dei Medici e degli Odontoiatri di tutt'Italia,** avendo l'accreditamento valenza nazionale.
In virtù dell'accreditamento, gli iscritti avranno diritto all'**esonero dai** previsti **50 crediti ECM annuali.**
Il C.S.T.N.F. ha ottenuto il **Patrocinio dell'Ordine dei Medici e Odontoiatri** di Torino.
Il **programma** didattico sviluppa gli aspetti tradizionali e scientifici dell'Agopuntura attraverso un **corso triennale composto da 500 ore di lezioni teorico-pratiche.** Il monte-ore è composto da: 330 ore di lezioni teoriche frontali, 120 ore di didattica a distanza e 50 ore di pratica clinica in regime di tutoraggio presso **5 ambulatori pubblici convenzionati con il CSTNF per la didattica e la ricerca scientifica.**
Il CSTNF è convenzionato con **l'Università di Medicina Tradizionale Cinese di Nanchino** per l'organizzazione di Masters di pratica clinica, lo scambio di docenti e la ricerca scientifica. Dal 2019 ha iniziato la collaborazione con la **ZCMU (Zhejiang Chinese Medical University) di Hangzhou**.
Tutti i diplomati sono inseriti nel **Registro dei Medici Agopuntori F.I.S.A. (Federazione Italiana delle Società di Agopuntura)**, consultabile sull'app *MyAgopuntura.*
In qualità di **Provider ECM n° 820** il C.S.T.N.F. ha finora organizzato **222 edizioni** di eventi ECM.

SEGRETERIA C.S.T.N.F.: C.so Galileo Ferraris 164, 10134 TORINO
Tel. 373.7999648/011.3042857 (ore.900-13.00) - e-mail: info.cstnf@fastwebnet.it

LO SGUARDO DI SEVERINO

Un pensiero, quello di Severino, che va ascoltato, capito e interrogato. Un pensiero *in-audito* o visionario che sulle prime può scandalizzare o essere liquidato come ennesima rete consolatoria posta sul mare del mistero dell'essere. Pura follia per l'uomo di Chiesa che crede nella creazione dal nulla di tutte le cose ad opera di un Demiurgo quasi che gli enti originariamente fossero un niente e, a maggior ragione, per l'uomo di scienza che, rigettando ogni fede e necessità del destino, confida solo nella conoscenza e nel dominio delle cause degli eventi sopraggiungenti. Si tratta in realtà di una speculazione rigorosa, articolata in numerosi saggi ed in dialogo con i propri obiettori. Una rilettura di tutta la storia del pensiero occidentale che demolisce a colpi di stringenti argomentazioni e riduce a illusione quell'evidenza dell'esperienza che ci fa credere e affermare che quando una cosa, un ente, scompare definitivamente dal nostro campo di osservazione, muoia, vada nel nulla. L'esempio ormai paradigmatico riportato dal filosofo è quello della legna che bruciando pensiamo si annienti e diventi cenere. In realtà, noi assistiamo ad una sequenza di eventi eterni che compaiono e scompaiono: prima la legna, poi la legna che brucia ed infine la cenere. Dunque quello che noi dichiariamo essere l'evidenza massima del divenire non è che un abbaglio della nostra esperienza che ci fa dire che gli enti si trasformano continuamente diventando altro da sé. In realtà, la totalità dell'essere, fatta di tutte le sue singole determinazioni, è eterna e scorre nel nostro limitato campo visivo come i molti fotogrammi della pellicola di un film. Severino assegnando un diverso e nuovo significato al divenire in termini di progressivo comparire e scomparire degli eterni, offre una spiegazione razionale dell'impossibilità della morte, in grado di liberarci dall'angoscia di ritornare nel nulla.

MA È POSSIBILE ANDARE OLTRE L'ESPERIENZA PIÙ IMMEDIATA SENZA CADERE NELL'INGANNO?

Proprio questo è capitato ad Einstein elaborando la sua nota e tutt'ora accreditata teoria della relatività secondo cui, in opposizione alla fisica classica, lo spazio è curvo e non è un vuoto ma "energia-materiale" e il tempo scorre diversamente a diverse altezze. Uno schiaffo all'esperienza quotidiana che solo in seconda battuta è stata costretta a riconoscere il primato del pensiero di Einstein che si è affidato alla sola ragione.

Se questo radicale ribaltamento di ciò che appariva incontrovertibile è avvenuto nel pensiero scientifico, perché non potrebbe accadere lo stesso per la tesi di Severino?

Perché l'eternità non potrebbe essere il nostro vero destino?

Bibliografia Essenziale

Emanuele Severino, *Essenza del Nichilismo*, Adelphi 1981

Emanuele Severino, *Destino della Necessità*, Adelphi 1980

Emanuele Severino, *Testimoniando il Destino*, Adelphi 2019

Emanuele Severino, *Tautótēs*, Adelphi 1995

Umberto Galimberti, *Psiche e Techne*, Feltrinelli 1999

Salvatore Natoli, *La felicità di questa vita*, Mondadori 2000

Gina Lagorio, *Capita*, Garzanti 2008

Carlo Rovelli, *Relatività generale. Una semplice introduzione.* Adelphi 2021

CI SONO COSE A CUI NON SI È MAI DEL TUTTO PREPARATI. PER QUESTO CI SIAMO NOI.

ANAAO ASSOMED TI FORNISCE TUTTA L'ASSISTENZA E I SERVIZI NECESSARI A FRONTEGGIARE AL MEGLIO OGNI CIRCOSTANZA.

ISCRIVITI AD ANAAO ASSOMED: FINO AL 1 GENNAIO 2023 LA POLIZZA RC COLPA GRAVE È GRATUITA.

SCOPRI TUTTI I SERVIZI SU **WWW.ANAAO.IT**

MEDICAL INSURANCE BROKERS

ANAAO ASSOMED
ASSOCIAZIONE MEDICI DIRIGENTI

NUOVA TOYOTA YARIS CROSS HYBRID

VIENI A PROVARLA ANCHE SABATO E DOMENICA

ENERGIA IRRESISTIBILE

MOTORE HYBRID DYNAMIC FORCE® DA 116 CV

TRAZIONE ANTERIORE
OPPURE INTEGRALE INTELLIGENTE AWD-i

SISTEMI DI SICUREZZA ATTIVA
TOYOTA SAFETY SENSE 2.5* DI SERIE

E CON **WE**HYBRID, ENTRI IN UN MONDO DI VANTAGGI ESCLUSIVI

SPAZIO 4

LA TUA CONCESSIONARIA UFFICIALE TOYOTA.

VIA REISS ROMOLI, 93 **TORINO** - TEL. 011 2251711
NUOVA SEDE ALL'INTERNO DI SPAZIO LA CITTÀ DELL'AUTO
VIA BOTTICELLI, 82 **TORINO** - TEL. 011 24 66 211
CORSO SAVONA, 25 **MONCALIERI**
TEL. 011 64 09 356

Seguici su: **www.spazio4to.spaziogroup.com**

*I sistemi di sicurezza attiva del Toyota Safety Sense sono progettati per cercare di assistere il guidatore in talune situazioni di potenziale pericolo e non coprono tutte le variabili che possono intervenire in occasione della guida. La loro operatività e/o il loro funzionamento può essere difatti influenzato da fattori esterni, anche atmosferici. Per tale motivo vi invitiamo a leggere attentamente le indicazioni contenute nell'apposito Libretto di Istruzioni. I predetti sistemi non sono in grado di evitare i rischi di incidente né di sostituirsi al conducente ed è necessario che quest'ultimo mantenga il controllo del proprio veicolo in ogni momento, senza distrazioni. Dovete pertanto guidare la vostra Toyota prestando la dovuta massima attenzione perché Toyota Safety Sense potrà aiutarvi, ma sarete sempre e solo voi gli artefici principali della vostra sicurezza e di chi vi sta intorno. Messaggio pubblicitario con finalità promozionale. Maggiori informazioni su toyota.it. Immagine vettura indicativa. Valori massimi WLTP riferiti alla gamma Yaris Cross Hybrid: consumo combinato 5,1 l/100 km, emissioni CO_2 115 g/km, emissioni NOx 0,007 g/km (WLTP – Worldwide harmonized Light vehicles Test Procedure ai sensi del Regolamento UE 2017/1151).