Sotto attacco ospedali e device

Il rischio non si limita ai dati dei pazienti ma riguarda il funzionamento di strutture di cura e delle protesi

di **Agnese Codignola**

L'11 maggio 2017 il presidente Donald Trump ha emesso un ordine esecutivo rivolto a tutte le agenzie federali, affinché mettessero in atto misure per migliorare la sicurezza dei network federali e delle infrastrutture. Il 12 maggio 2017 WannaCry, il malware arrivato dalla Russia, ha infettato centinaia di server sensibili in tutto il mondo, Stati Uniti compresi, e ha colpito decine di ospedali e farmacie. Sempre negli Stati Uniti, nel 2014 un attacco aveva colpito 206 ospedali in 29 stati, violando i dati di 4,5 milioni di pazienti.

Sono solo alcuni tra gli esempi più recenti di "incidenti" che, secondo uno studio pubblicato nel settembre scorso da esperti di diritto, bioetica e salute pubblica di Harvard sugli Annals of Internal Medicine, sono stati più di 2mila, tra il 2009 e il 2016: troppi, per continuare a trattare la questione come se fossero eventi isolati. Da qui l'iniziativa di Trump. In febbraio, è arrivato un altro segnale: l'American College of Cardiology ha reso note le sue linee guida per prevenire gli attacchi ai dispositivi quali pacemaker, defibrillatori impiantabili e altri, a oggi mai verificatisi, ma relativamente semplici da portare a termine. La cybersecurity non riguarda dunque solo la protezione dei dati personali, ma anche il funzionamento degli ospedali e quello delle protesi, oggi iperconnesse, e quindi attaccabili.

Dati sensibili

L'azienda di Cambridge (Boston) Foundation Medicine prende i campioni di sangue o di tessuto di chi ha un tumore e in poche ore analizza lo stato di oltre 350 geni, per capire a quale tipo di farmaco (o sperimentazione) è meglio indirizzare il malato. Attiva dal 2009, ha nei suoi database il dna di quasi 200mila pazienti: un patrimonio inestimabile. I dati sono del-

l'azienda, che li utilizza anche per studi non strettamente relativi al singolo paziente, per esempio per verificare quanto una certa mutazione è frequente. E magari per cedere (dietro lauto compenso) quanto scoperto ad aziende come la Loxo, Connecticut, fondata nel 2013 per trovare farmaci antitumorali in base ai difetti genetici.

C'è quindi una questione che va ben oltre quella, già tutelata da quasi tutte le legislazioni, relativa alla possibilità che una certa persona venga discriminata perché, per esempio, è portatrice del gene di Angelina Jolie, il Brca, e quindi esposta a un significativo rischio di cancro. C'è uno scambio che a volte è commercio e che non è sempre trasparente in tutti i passaggi. Oltre a ciò, secondo diversi esperti, il possesso delle informazioni biologiche sta uccidendo la ricerca indipendente, perché le agenzie statali faticano a immagazzinare i dati e quando collaborano con le aziende devono assicurare la cessione dei dati, fatto che impedisce valutazioni successive o diverse da quelle stabilite dall'azienda. Con tanti saluti alla libertà di ricerca. Anche per questo la Fda ha obbligato Foundation Medicine a cedere una parte dei suoi dati relativa a bambini malati o a tumori rari, ma è evidente che si tratta di un provvedimento tampone.

Il rischio negli ospedali

La giornata di un ricoverato è scandita da esami e terapie, coordinati dai sistemi centralizzati. Ma, come hanno evidenziato i cardiologi americani, ogni atto ospedaliero è un potenziale sito di attacco, perché le macchine potrebbero non funzionare a dovere, i dati essere modificati, le terapie colpevolmente sbagliate e così via. Come se ne esce? Secondo molti esperti curando al massimo la sicurezza fino dalla progettazione, perché intervenire a valle, magari quando il danno è fatto, è molto complicato e a volte impossibile. È necessario adottare misure sistemiche, come ha ribadito Dhanunjaya Lakkireddy, coordinatore del rapporto dei cardiologi: «Bisogna prevedere sempre, negli staff, personale con un'elevata specializzazione informatica e approntare sempre circuiti alternativi tanto per l'immagazzinamento dei dati quanto per il funzionamento degli strumenti, e poi finanziare monitoraggi continui, per identificare le eventuali criticità prima possibile».

Dispositivi personali

Milioni di persone ospitano nel proprio corpo un device - pacemaker, defibrillatori impiantabili, pompe insuliniche, gli elettrodi cerebrali profondi e altro ancora - che costituisce un potenziale punto d'attacco informatico. Per questo la Fda ha specifiche linee guida sia pre che post marketing, e per questo i cardiologi americani hanno deciso di fornire istruzioni. La richiesta, forte, va a ai produttori. E non solo. Scrive Lakkireddy: «Sono loro che si devono occupare fino dalla progettazione della protezione dei dispositivi, per esempio con sistemi di alimentazione di riserva specifici. Ma tutti devono fare ogni sforzo per la sicurezza e le autorità sanitarie, se necessario, devono introdurre standard e comportamenti obbligatori».

PAZIENTI

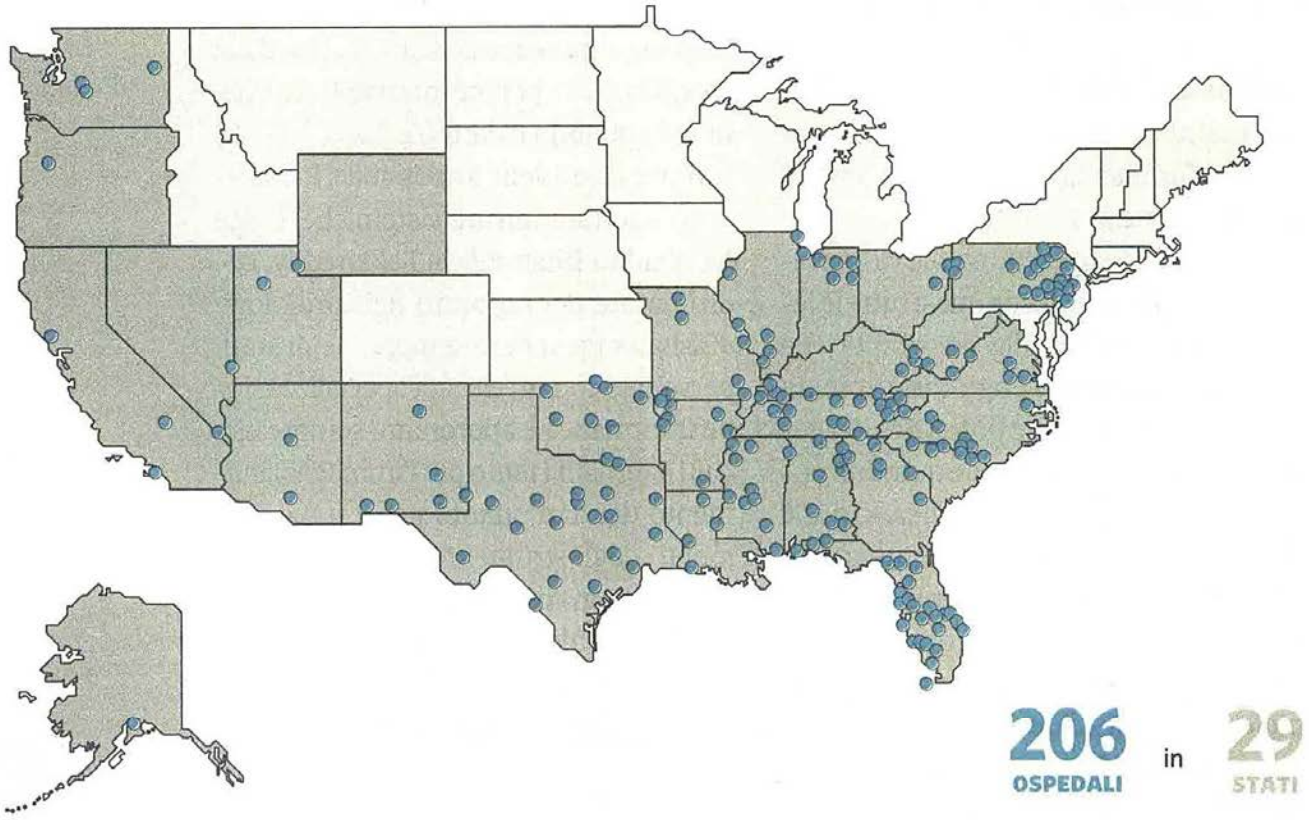
Cosa rischiano i pazienti?

—

I pazienti che rischiano di più sono quelli che hanno un device come pacemaker, defibrillatore impiantabile, pompa insulinica o elettrodi cerebrali perché sono un potenziale punto di attacco informatico

Gli hacker contro gli ospedali

L'attacco informatico del 2014 ha colpito 206 ospedali in 29 stati americani



Il caso italiano

In Italia la situazione ricalca quella europea e occidentale: esistono normative abbastanza efficienti, che tuttavia faticano a tenere il passo con la realtà. Spiega Laura Liguori, socia dello Studio Portolano Cavallo ed esperta di privacy: «Il trattamento dei dati sanitari ricade nel codice sulla privacy, che prevede anche casi specifici. La normativa italiana dovrà però essere adattata al regolamento europeo». Quando poi i dati e le informazioni, ovvero anche i campioni biologici, servono per la ricerca scientifica, la normativa italiana prevede altre tutele, come spiega Elisa Stefanini associata di Portolano Cavallo ed esperta di *life sciences*: «Occorre l'autorizzazione dell'Aifa e quella dei comitati etici, ed è quindi necessario soddisfare ulteriori condizioni, che aumentano la sicurezza».

Anche se non sempre se ne ha la percezione, tra i vantaggi di una sanità pubblica e universalistica c'è anche la tranquillità di sapere che le informazioni sulla propria salute possono essere impiegate per studi clinici o di base, ma tali studi devono essere approvati anche per quanto riguarda il trattamento di dati.

© RIPRODUZIONE RISERVATA