Il labile confine tra riservatezza ed esposizione

La vulnerabilità dei big data senza regole sulla privacy.
La necessità di un cambio di paradigma in una prospettiva di ricerca sociale

È innegabile che l'uso dei big data offra potenzialmente opportunità enormi anche per il settore sanitario e che stiano rivoluzionando il nostro modo di essere cittadini e pazienti. Flussi sempre maggiori di dati permettono di definire trend e tendenze, intercettare i bisogni dei cittadini, anticipare eventuali problemi nell'ambito della sanità pubblica, per esempio di carattere epidemiologico, per non parlare dei conseguenti vantaggi in termini di costi. L'aggettivo "big" si applica, infatti, al concetto di informazione in tre direzioni: dal punto di vista del *volume* di dati che si possono raccogliere (quantità), dell'*alta variabilità* di queste informazioni (cioè dalla provenienza contemporanea da più fonti) e, infine, dalla *velocità* con cui i dati possono essere raccolti, condivisi e interpretati.

Tuttavia, *big* è anche il divario fra le emergenti opportunità che questo paradigma porta con sé e la nostra capacità di far fronte ai problemi che esso ci pone, per primi quelli riguardanti la sicurezza e la privacy del titolare dei dati, che rimane sempre l'individuo. È importante precisare che privacy e sicurezza non sono sinonimi: la sicurezza è essenziale per garantire la privacy. Stiamo vivendo in un mondo a due velocità, dove la "gara" fra le tecnologie pensate per garantire la sicurezza dei sistemi informatici in termini di privacy e l'attività di hacker e truffatori assomiglia a quella fra Achille e la tartaruga. Per non parlare dei problemi strutturali intrinsechi all'utilizzo di sistemi informatici per lo stoccaggio e il trattamento dei nostri dati, per esempio quelli che scegliamo più o meno consapevolmente di condividere attraverso app e device.

Intrusioni pericolose

Gli interessi che ruotano intorno alle informazioni medico-sanitarie sono enormi. Lo studio "Privacy and security in the era of digital health: what should translational researchers know and do about it?" pubblicato nel marzo del 2016 – a firma fra gli altri di Eric Topol (autore nel 2012 del best seller "The creative destruction of Medicine") – esamina molto bene i due principali problemi posti dall'utilizzo dei big data in sanità dal punto di vista della privacy: l'hacking da un lato e le frodi dall'altro. Nel 2015 l'hacking è stata la prima causa di violazioni negli Stati Uniti e nel 2014 l'healthcare è stato il settore che ha visto il maggior aumento di attacchi, e solo dal 2013 al 2014 l'ambito sanitario ha visto un incremento del 21,7% dei furti di identità. Le conseguenze economiche di tutto questo non sono affatto secondarie, dal momento che nel 2015 il danno economico è stato maggiore del 125% rispetto a cinque anni prima. Sempre più frequenti anche le frodi, come i furti di identità per ottenere prescrizioni di farmaci e i tentativi riusciti di phishing tramite email, per ingannare gli utenti convincendoli a fornire dati personali, password e via dicendo, fingendosi un'organizzazione affidabile. Secondo quanto riportavano Topol e colleghi, quasi un utente su quattro apre questo tipo di email, offrendo di fatto il fianco ai malintenzionati.

Il risultato è che il processo di implementazione di una e-health autenticamente basata sull'uso dei big data è ancora un miraggio e la barriera principale è appunto la sicurezza, la corazza troppo fragile su cui i sistemi sanitari possono fare affidamento per garantire la privacy dei cittadini. Di fatto i problemi aperti dall'utilizzo dei big data sono ben lungi dall'essere risolti, così come siamo lontani dal poter parlare di un'implementazione sicura dei sistemi di e-health. Non è un caso, infatti, che l'ultimo rapporto sull'argomento pubblicato dall'Ufficio europeo dell'Organizzazione mondiale della sanità (Oms) nel 2015 si intitoli "From innovation to implementation. E-health in the Who European Region": l'innovazione c'è, per l'implementazione vi è ancora parecchio lavoro da fare, e la principale barriera per la messa in pratica di sistemi di e-health è proprio la minaccia dal punto di vista della privacy dei dati. I risultati messi in luce dall'Oms sono netti: sebbene l'80% dei paesi europei possegga una legislazione per la protezione della nostra riservatezza, solo il 13% possiede una strategia per regolare l'uso dei big data in sanità e, ancora meno, il 9% si è dotato di policy per vigilare sull'uso dei dati sanitari da parte di privati. Inoltre, solo il 26% dei paesi rispondenti al sondaggio afferma di avere attivi sistemi di vigilanza sui sistemi mobile per garantire la sicurezza e la qualità nel trattamento dei dati e un paese su due non ha una legislazione precipua per permettere agli individui l'accesso ai propri dati nel fascicolo sanitario elettronico o una legislazione che consenta al paziente di decidere con chi condividere ogni singola partizione di dati del proprio fascicolo.

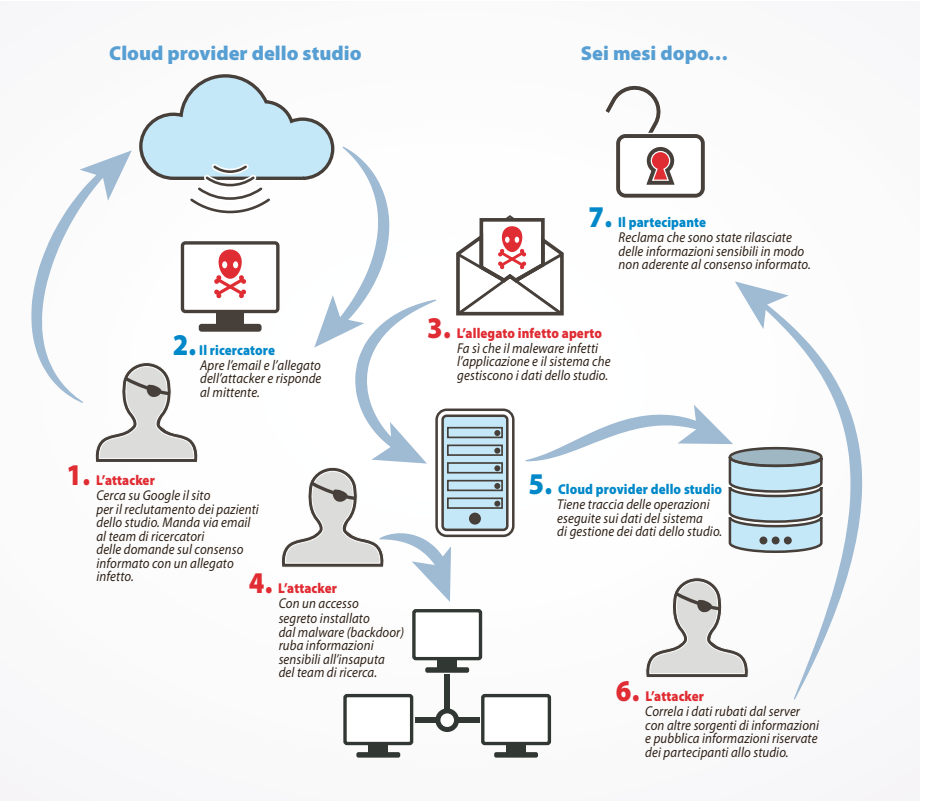
Seguendo la classificazione dell'Enisa (Agenzia europea per la sicurezza delle reti e dell'informazione), i principali problemi per la privacy sono:

1. la perdita di controllo e trasparenza da parte del sistema,
2. la questione della riusabilità del dato,
3. i rischi che emergono per la privacy dalla possibilità di incrociare i dati ottenendo nuove informazioni (a chi appartiene a questo punto questa nuova classe di informazioni?),
4. i rischi legati alle attività di profiling e decision making sulla base dell'analisi dei big data.

a p.30 ⟶

Attacchi alla sicurezza nelle rete

Come gli hacker attaccano i dati sensibili della ricerca traslazionale.



Fonte. Filkins BL, et al. Am J Transl Res 2016; 8:1560-80.

→ *da p.29*

Flussi di dati fuori controllo

È necessario, tuttavia, fare delle distinzioni fra quelli che sono i problemi di privacy dei sistemi di e-health realizzati dalle strutture sanitarie, come il già citato fascicolo sanitario elettronico, la cartella clinica elettronica, la ricetta elettronica, la tessera sanitaria e via dicendo, e i flussi di dati personali che costantemente i privati cittadini regalano alle diverse compagnie (per la maggior parte private) tramite le app presenti su smartphone e tablet, o durante l'utilizzo di software online e social media. Questo ultimo canale è oggi estremamente vulnerabile, eterogeneo, privo di regole e quindi di un'adeguata vigilanza. In soldoni, sebbene i servizi come il fascicolo sanitario elettronico non possano dirsi immuni da pericoli, come hackeraggi e frodi, essi sono comunque imbrigliati all'interno di una fitta rete di regole – a maglie più o meno strette a seconda del paese – che codificano in maniera chiara diritti e doveri dei titolari del trattamento dei nostri dati sanitari. Vengono fissate, per esempio, delle misure minime per la protezione del titolare dei dati, dei criteri di cifratura, la tracciabilità delle operazioni effettuate e dei criteri per garantire che chi sottoscrive un contratto per la condivisione dei propri dati online lo possa fare in maniera libera, specifica e informata.

Tutto questo non deve essere per legge in alcun modo garantito invece dai produttori privati di app e software, con il risultato che molto spesso l'utente non sa esattamente che cosa sta scaricando sul suo smartphone, e dove e in che modo sono trattati i suoi dati sanitari. Claire Porter sulle pagine de *The Guardian*, in un articolo intitolato "Little privacy in the age of big data", pone la questione in questi termini: "Is volunteering our personal data simply the price we pay for free services?" (questa condivisione volontaria dei nostri dati personali è forse semplicemente il prezzo che paghiamo per avere servizi gratuiti?). La questione è estremamente delicata perché ci coinvolge molto più da vicino di quanto pensiamo. La maggior parte delle app che noi tutti scarichiamo quotidianamente non ha dovuto soddisfare alcun criterio di valutazione né sostenere alcun esame che ne provasse l'effettiva validità e, soprattutto, non è soggetta ad alcuna regola che la obblighi a garantire la nostra privacy o a fornire informazioni precise sul prodotto che stiamo acquistando.

Vi è poi il problema geografico, non secondario in termini legislativi: dove e come sono conservati fisicamente i miei dati? Chi può accedervi? E in caso di controversia, dovuta per esempio a un furto, sotto quale giurisdizione ci troviamo? Viviamo inoltre in un profondo paradosso, quello secondo cui è punibile il produttore di una app che dichiara di utilizzare i dati sanitari dei cittadini in un certo modo e poi non lo fa, ma non colui che non dichiara anticipatamente nulla a proposito del possibile utilizzo dei dati che raccoglie.

> *Le politiche sulla privacy dei venditori non possono essere considerate accessibili e trasparenti se le persone non sono in grado di valutarle e interpretarle correttamente.*
>
> — Health insurance portability and accountability act

La logica attuale è la seguente: deve essere cura del cittadino, del paziente, dell'utente informarsi: una volta che accetta di utilizzare una app se ne assume tutta la responsabilità. Alla fine a fare la differenza è il grado di interesse del singolo a informarsi, e non si tratta di un'eccezione ma, a quanto pare, della regola. Un'ottima sintesi su questo è stata recentemente pubblicata dal Department of health and human services americano dal titolo "Examining oversight of the privacy & security of health data collected by entities not regulated by Hipaa". Secondo gli esperti oggi la maggior parte delle entità che collezionano dati negli Stati Uniti (qui non si fa riferimento solamente alle app) non è regolata dall'Hipaa (Health insurance potability and accountability act), che dal 1996 regolamenta la privacy dei dati e le disposizioni di sicurezza per la tutela delle informazioni sanitarie. E non solo: i cittadini americani sarebbero oggi troppo poco e male informati sulle sorti dei propri dati sensibili che raccolgono tramite le entità che utilizzano, come le app, e non sempre essi hanno facile accesso ai propri stessi dati.

Sono cinque in particolare le differenze che intercorrono fra un'entità coperta da Hipaa e una che non lo è (in termini tecnici, *non covered entity*): garantire l'accesso ai propri dati come un diritto; regolamentare il riuso dei dati da parte di terze parti; garantire misure standard di sicurezza; utilizzare una terminologia chiara sulle questioni di privacy all'interno delle informative che gli utenti devono sottoscrivere prima di scaricare il prodotto; e, infine, definire l'uso corretto e quello scorretto dell'informazione dal punto di vista della riservatezza.

Il mondo del mercato privato, senza regolamentazioni ferree in merito alla privacy, ci espone dunque potenzialmente a molte più vulnerabilità rispetto a quello dei sistemi sanitari, ma i due ambiti sono destinati a intersecarsi. Cosa accade per esempio quando sono i medici stessi a utilizzare una app qualsiasi per gestire i nostri dati sanitari?

Un cambio di paradigma

In questo scenario così estremamente caotico, è necessario quindi – chiosa l'Enisa – un cambiamento di paradigma, non più basato sulla dicotomia "big data *versus* privacy", bensì sul binomio "big data *with* privacy". Slogan a parte, il concetto è quello di integrare le politiche per garantire la sicurezza del trattamento dei dati sanitari a qualsiasi livello nelle modalità in cui pensiamo all'uso dei big data, per uscire finalmente da questo scenario in cui a fare la differenza per un cittadino informato sui destinatari dei dati sanitari che sta per condividere sia solamente il suo grado di interesse su queste questioni e la voglia di leggere le informative punto per punto chiedendo spiegazioni dove qualcosa non è chiaro.

Il punto è che non è facile decidere come legiferare. Su questo aspetto si è espresso nel maggio 2014 anche l'Ufficio del Presidente degli Stati Uniti per la scienza e la tecnologia, proponendo in un documento dal titolo "Big data and privacy: a technological perspective" alcune raccomandazioni per la creazione di nuovi regolamenti. L'idea è quella di non concepire la lotta per la tutela della privacy come se quella fra Achille e la tartaruga fosse una mera sfida tecnologica: la cartina di tornasole rimangono le effettive applicazioni pratiche di queste tecnologie, il loro uso. Privacy – chiosano gli esperti – non significa solo anonimizzare, né mantenere un segreto. La via indicata dalla Casa Bianca è quindi quella di concentrare la ricerca e i relativi finanziamenti su tecnologie che diano segnali tangibili di aiutare a proteggere la privacy all'interno dei meccanismi sociali che influenzano i comportamenti e la vita privata delle persone. Per questo serve puntare su un'adeguata formazione dei cittadini e assumere la prospettiva di una ricerca sociale. I big data sono anzitutto una scienza sociale.

[Pagine a cura di **Cristina Da Rold**]

Le cinque raccomandazioni della Casa Bianca

1. L'attenzione della politica dovrebbe essere focalizzata più sull'uso dei big data e meno sulla loro raccolta e analisi.

2. Le politiche e le regolamentazioni ad ogni livello governativo non dovrebbero includere particolari soluzioni tecnologiche, ma dovrebbero essere formulate in termini di risultati da raggiungere.

3. Con il coordinamento e il sostegno dell'Office of science and technology policy (Ospt) della Casa Bianca, le agenzie del Networking and information technology research and development program dovrebbero rafforzare la ricerca statunitense nell'ambito delle tecnologie collegate alla privacy e in quelle importanti aree delle scienze sociali che formano/caratterizzano il successo dell'applicazione stessa di queste tecnologie.

4. L'Ospt della Casa Bianca insieme alle istituzioni dell'istruzione e società professionali idonee dovrebbe incoraggiare le possibilità di formazione e training in ambito di protezione della privacy, inclusi i percorsi di carriera professionale.

5. Gli Stati Uniti dovrebbero fare da guida sia in campo internazionale sia nazionale adottando politiche che incentivino l'uso di tecnologie pratiche per la protezione delle privacy già oggi esistenti.

Fonte. Executive Office of the President, President's Council of Advisors on Science and Technology. Office of the president president's council of advisors on science and technology Report to the President "Big data and privacy: a technological perspective executive". Washington, maggio 2014.