DigitCult | Scientific Journal on Digital Cultures

Il rapporto costo/beneficio dalla pratica medica alla tutela dei dati personali

Alessandro Vercelli
Department of Neuroscience
Neuroscience Institute Cavalieri Ottolenghi
Regione Gonzole 10, Orbassano (TO), Italy

Abstract

Il mondo interconnesso e l'Internet delle cose sollevano diverse preoccupazioni sulla nostra privacy e sulla conservazione dei dati personali. L'enorme aumento della capacità di memorizzare dati (big data) e la possibilità di analizzare questi dati in tempi brevi, grazie ai recenti sviluppi dell'intelligenza artificiale come machine e deep learning costituiscono insieme una grande opportunità e una minaccia per l'individuo. Le differenze culturali nelle diverse nazioni, qui discusse, hanno generato approcci diversi alla questione. Ovviamente i big data hanno un incredibile valore economico e le aziende private e gli enti governativi hanno un forte interesse ad avere accesso ai dati, sotto molti punti di vista.
La recente pandemia dovuta alla SARS COV-2 ha costretto i governi ad agire per limitarne la diffusione e, anche di conseguenza alle preoccupazioni relative alla propria salute, le persone hanno accettato un accesso da moderato a esteso ai propri dati privati. Numerose app per il tracciamento dei contatti sono state sviluppate nei diversi paesi, con vari livelli di intrusione anche a seconda delle specifiche sensibilità culturali. Nella Comunità Europea è stato raggiunto un equilibrio accettabile tra diritti alla privacy e diritto alla salute, anche grazie al recente GDPR entrato in azione nel 2018.

The Cost/Benefit Relationship from Medical Practice to Data Protection

The connected world and the internet of things raise several concerns about our privacy and the storage of personal data. The enormous increase in the capability to store data (big data); the possibility to analyse these data in a short time, thanks to the recent developments of artificial intelligence such as machine and deep learning, represent both a great opportunity and a threat for the individual. Cultural differences in the different nations, here discussed, have generated different approaches to the question. Of course, big data have an incredible economical value, and private companies and governmental entities have a strong interest in having access to them, from many points of view.
The recent pandemics due to SARS COV-2 have forced the government to take action to limit the spread of the pandemics, and, even consequently to the concerns relative to own's health, people have accepted from moderate to extended access to their private data. Several apps for contact tracing have been developed in the different countries, with different levels of intrusion also depending on specific cultural sensibilities. In the European Community an acceptable balance between privacy rights and the right to health has been reached, also thanks to the recent GDPR into action from 2018.

Published 21 August 2020

Correspondence should be addressed to Alessandro Vercelli, NICO, Regione Gonzole 10, Orbassano (TO), Italy. Email: alessandro.vercelli@unito.it

DigitCult, Scientific Journal on Digital Cultures is an academic journal of international scope, peer-reviewed and open access, aiming to value international research and to present current debate on digital culture, technological innovation and social change. ISSN: 2531-5994. URL: http://www.digitcult.it

 doi:10.4399/97888255361642

Introduzione

In Minority Report (libro pubblicato nel 1956), da cui è stato tratto nel 2002 un famoso film di Steven Spielberg, Philip K. Dick narra la storia di una squadra di polizia costituita da tre mutanti capaci di prevedere e così impedire crimini del futuro prima che vengano commessi. In tempi più moderni, le città di Chicago (Illinois) e di Manchester (New Hampshire) utilizzano nella vita reale tecniche di analisi dei dati (distribuzione dei crimini, degli arresti, telecamere, fino a previsioni del tempo) per predire dove si potrebbero verificare potenziali problemi per la sicurezza e per identificare le condizioni per eventi criminogeni. Ciò permette una precisa dislocazione delle forze di polizia e una efficace azione di prevenzione. In Cina, telecamere sorvegliano il comportamento dei cittadini, effettuano il riconoscimento facciale e assegnano dei "voti" ai singoli, che così vengono classificati acquisendo il diritto a diversi gradi di libertà…

Se dal punto di vista della società queste tecniche presentano degli evidenti vantaggi, dal punto di vista del singolo individuo possono comportare restrizioni alla libertà prima ancora di aver compiuto un evento criminoso, o comunque cambiamenti significativi delle proprie abitudini (sapendolo, eviterò determinate aree, non frequenterò più determinati amici…).

La faccenda dei dati Facebook-Cambridge Analytica è stata uno dei maggiori scandali politici avvenuti nel 2018. Cambridge Analytica aveva raccolto i dati personali di milioni di account Facebook senza il loro consenso e li aveva usati per scopi di propaganda politica. Lo scandalo ha sicuramente rappresentato un momento fondamentale nella comprensione pubblica della importanza dei dati personali.

La salute e i dati personali

Negli ultimi anni i dati personali hanno assunto una enorme rilevanza economica, politica e sociale. La possibilità di raccogliere dati biometrici, sanitari e comportamentali dei singoli individui, di conservarli in quantità finora inimmaginabili in spazi ristretti e di analizzarli in tempi molto rapidi, non solo a scopo descrittivo ma anche predittivo, grazie alle tecniche di intelligenza artificiale come machine e deep learning rappresenta un nuovo strumento conoscitivo e interpretativo del mondo (Soriano-Valdez et al. 2020). Esso può essere utilizzato a livello di singoli individui, di gruppi e di intere società.

Come tutte le nuove tecnologie anche la raccolta e l'analisi di grandi quantità di dati (big data, caratterizzati dalle tre V: volumi – grandi quantità, velocità – rapidità di accesso e analisi, e varietà – eterogeneità dei dati tra gli individui e i tipi di dati) personali è un Giano bifronte. Se da un lato le loro potenzialità possono essere molto positive per il miglioramento delle condizioni del singolo e della società, il loro uso potrebbe costituire una intrusione nella privacy dell'individuo con conseguenze molto pericolose per la sua libertà e per i suoi diritti, di ogni genere.

Di chi sono i dati personali?

I dati personali, quindi, hanno un enorme valore economico e la loro gestione rappresenta un bene (eventualmente un cespite) di cui è necessario conoscere il proprietario. Negli Usa al centro del sistema vi sono l'autonomia dei privati e la libertà individuale, e l'approccio è di tipo autoregolamentante, utilitaristico (cioè i dati appartengono a chi li usa) oltre che settoriale (il settore medico, per esempio), laddove la privacy è tutelata solo nell'ambito delle pratiche commerciali, tramite l'equilibrio del mercato. Le imprese, che regolamentano la privacy inserendo clausole nei loro termini di servizio, hanno interesse a proteggere la privacy perché se sono troppo aggressive rischiano di perdere clienti. Inoltre, le cause collettive (class action) rappresentano un forte deterrente alle pratiche commerciali scorrette. Quindi, negli Usa la tutela della privacy è attribuita principalmente alla Commissione per il Commercio Federale (FTC, Federal Trade Commission), per la quale tale tutela è un'estensione della tutela del consumatore e della legittimità delle pratiche commerciali.

L'Europa ha, invece, un approccio generalista (la privacy è tutelata indipendentemente dal settore di applicazione) e centralizzato, e la tutela dei dati personali è un diritto fondamentale dell'individuo.

L'approccio americano è sicuramente più efficace e adattabile alle mutazioni tecnologiche, ma in compenso finisce per far diventare la privacy un bene economico da poter scambiare all'interno di un ampio mercato dei dati personali, così facendo passare l'aspetto individuale in secondo piano. Inoltre, l'approccio settoriale determina una moltiplicazione delle norme che complica l'effettiva capacità del cittadino di comprendere i suoi effettivi diritti.

Nel 2016 la Comunità Europea ha adottato un regolamento per la protezione dei dati personali che è entrato in vigore il 25 maggio del 2018. Lo scopo è quello di identificare delle regole per il mercato digitale che costituiscano una "impalcatura" armonica e semplificata per un governo moderno della protezione dei dati. Il principio fondamentale è quello di mettere gli individui nelle condizioni di mantenere il controllo dei propri dati personali. Fondamentale in primis è la definizione di dati personali e di dati sensibili: per esempio i dati sulla salute e i dati genetici.

I principi fondamentali del trattamento dei dati devono essere una loro elaborazione corretta e legale, con la limitazione ben precisa degli scopi di utilizzo, la riduzione al minimo necessario della quantità dei dati raccolti, le regole per un ulteriore elaborazione successiva, la definizione precisa del loro tempo di conservazione, la standardizzazione del loro livello di accuratezza e l'individuazione di chi ne è responsabile. I soggetti da cui i dati vengono raccolti hanno il diritto a una chiara e precisa informazione (anche dal punto di vista linguistico), di accedere ai propri dati e di esprimere la contrarietà, di portabilità e di essere informati di eventuali violazioni della privacy dei dati.

Nei paesi asiatici (quindi non solo la Cina) i dati personali assumono un valore prioritario per la società, per cui l'individuo e le sue libertà passano in secondo piano rispetto al bene comune. Quindi il proprietario dei dati personali in questi paesi è la società o più esplicitamente lo Stato.

Problemi etici

Il panorama in evoluzione dei big data sul tema salute pone nuove domande su concetti etici, alcuni familiari (come privacy, riservatezza e consenso informato), altri di nuovo riscontro (Price and Cohen 2019). Una review sistematica recente (Kallman et al. 2019) ha introdotto alcuni temi importanti tra le linee guida dei principi e delle norme che regolano la condivisione dei dati personali sul tema della ricerca nel campo della salute: vantaggi e valore per la società; distribuzione di rischi, benefici e oneri; rispetto per individui e gruppi; e la fiducia e l'impegno del pubblico. In particolare, in questa review si pone l'accento sulla deidentificazione dei dati, per il rispetto della privacy.

Fondamentali, per ogni tipo di raccolta, gestione e analisi dei dati personali sono la presenza di comitati etici, che verifichino il rispetto di regole condivise, e la trasparenza, che permetta all'individuo di conoscere i propri diritti, doveri e le conseguenze della condivisione dei propri dati personali. Il consenso informato singolo per ogni uso può essere poco pratico.

Dubbi sulla privacy sorgono prima nella raccolta e poi nell'uso dei dati. Le fonti di dati possono essere svariate: files elettronici sulla salute (cartelle cliniche), assicurazioni, strumenti IoT (per esempio un semplice global positioning system, "GPS"), social media.

Importante è valutare quali sono i rischi di raccogliere, condividere e pubblicare i dati dei singoli sulla localizzazione. Bisogna valutare cosa di questi dati è alienabile e cosa può succedere ai singoli in caso di reidentificazione (Goldenholz et al. 2018). Fondamentale è la figura di chi custodisce i dati. Chi sarebbe interessato e sarebbe capace di risalire al singolo a cui appartengono i dati? Chi li vuole raccogliere deve avere strategie adeguate da metter in atto per ridurre i rischi. In ultima analisi è necessario valutare un bilancio tra raccolta e uso dei dati per la salute del singolo.

Una visione unitaria mondiale

In quanto detto sinora emerge l'importanza delle diversità culturali e del pluralismo a livello nazionale e mondiale: si pensi ai diversi modelli americano, europeo, asiatico. E' però essenziale, per condividere i dati e trarne giovamento su scala planetaria, non mettere in discussione la dignità umana, i diritti umani e le libertà fondamentali (UNESCO Universal Declaration of Bioethics and Human Rights in 2005, art. 12). La dichiarazione dell'UNESCO del 2005 mette l'accento sui diritti dell'individuo. Anche se questo principio è stato tacciato di imperialismo morale della bioetica occidentale, bisogna constatare che le culture evolvono, complici anche internet e i social media e quindi è possibile che tra le diverse culture i principi sulla privacy e sulla gestione

 doi:10.4399/97888255361642

dei dati personali possano avvicinarsi, anche per ragioni economiche (per esempio, chi non si uniforma alla legislazione europea non può operare economicamente in Europa…).

Le app di tracciamento personale e la loro minaccia alla privacy

In questo periodo, complice il rischio del contagio dovuto alla pandemia SARS-CoV-2, diversi Stati hanno sviluppato delle app che permettono di tracciare i movimenti dei singoli, e quindi i loro contatti (contact tracing) che in un secondo tempo potrebbero sviluppare la patologia. Si tratta in realtà di una evoluzione di app già in uso per vari scopi. Per esempio, la possibilità di incontrare amici di FB nelle vicinanze può rivestire una utilità sociale. Può anche però favorire la proliferazione di offerte pubblicitarie per il singolo, il tracciamento degli incontri del singolo (quindi anche di attività che non vorremmo fossero di dominio pubblico) e monitorare continuamente il singolo e i suoi comportamenti.

Il rischio delle app di contact tracing dipende dalla vulnerabilità (e dai dati cui ha accesso) dell'app e del sistema di contact tracing. Se la app ha accesso a dati sensibili (salute, geolocalizzazione) e se utilizza tecnologie di rete wireless (WiFi, bluetooth) per la trasmissione di dati o il tracciamento, queste rendono il sistema vulnerabile, perché costituiscono porte di accesso ai nostri smartphone e quindi ai nostri dati sensibili. D'altro canto, molte delle app, soprattutto nel mondo occidentale, permettono di valutare il rischio di contrarre il virus, per aver incontrato o anche solo incrociato un malato, così da mettere sull'avviso il singolo sui rischi che corre e la società sulla necessità di isolarlo fino a che rappresenta un rischio per la salute degli altri.

Nel mondo occidentale molte di queste app sono state costruite in modo da lasciare al singolo la decisione di condividere i propri dati con il resto della popolazione, mantenendo la propria privacy. Ovviamente esiste la possibilità di una violazione della privacy, sia da parte dei gestori delle app, sia da parte di entità terze. Si tratta di una eventualità che in assoluto, nemmeno nelle app migliori, non può essere esclusa al 100%. Alcune delle app introdotte nel mondo occidentale cercano di anonimizzare il più possibile i dati, proteggendo i proprietari dello smartphone dalla sua identificazione, e di lasciare al singolo la decisione su quali provvedimenti prendere in caso di possibile contatto con un malato. In altri continenti, le app sono molto più intrusive e prendono letteralmente possesso dello smartphone raccogliendone tutti i dati utili allo scopo di tracciare le attività dell'individuo.

Non discuto qui dei dettagli tecnici, di cui non sono un esperto, ma la aderenza di queste app ai massimi standard di sicurezza è messa in discussione da diversi esperti del settore, complice anche la fretta con cui queste app sono state introdotte in uso. La app Immuni, sviluppata da una startup italiana e consigliata dalla stessa OMS, pur con qualche critica da parte degli esperti del settore (per ragioni ignote è mancata una precisa risposta alle richieste specifiche di dettagli), ha ricevuto una molto positiva valutazione da parte del MIT per quanto riguarda gli standard di sicurezza. La app tedesca è stata testata anche dalla associazione degli hacker, con una valutazione molto positiva. Recentemente Google e Apple hanno reso possibile alle app di diverse nazioni di "parlarsi", per cui un turista tedesco in Italia è in grado di incrociare i suoi dati con quelli di Immuni.

Ciononostante la app Immuni al momento stenta a sfondare (al momento in cui scrivo registra tra i 2 e i 4 milioni di download), per diverse ragioni: in primis, per uno scarso supporto politico e una ridotta pubblicizzazione nei media; poi per il fatto che gli smartphone di vecchia generazione (in Italia ancora molto presenti) e i cellulari Huawei (molto in uso in Italia) non sono compatibili perché la app sfrutta i sistemi Google e Apple. Infine, la difficoltà in Italia di eseguire test per il COVID-19 in tempi rapidi e il conseguente rischio di un lungo autoisolamento qualora fossimo a conoscenza di esser stati in contatto con un malato hanno sicuramente costituito un freno alla sua installazione.

Conclusioni

Per quanto riguarda la nostra società occidentale e italiana, la speranza di non condividere i nostri dati personali è una battaglia di retroguardia probabilmente già persa in partenza. Andando al supermercato le nostre preferenze e i nostri desideri vengono continuamente indagati, e nel momento in cui accettiamo una "tessera fedeltà" vendiamo tutte le informazioni sui nostri bisogni e desideri in cambio di uno sconto sul conto finale. Quando cerchiamo al computer un biglietto

aereo o un hotel in cui soggiornare, o qualsiasi bene, automaticamente le nostre richieste vengono registrate e nelle settimane a venire ci vengono proposte delle offerte che possono essere utili. Le nostre televisioni sono diventate smart, cioè sono collegate ad internet: questo fa sì che i dati sulle nostre preferenze nei programmi (ma anche sugli spot pubblicitari e sui tempi in cui li seguiamo a seconda del prodotto pubblicizzato) vengano continuamente registrati e analizzati. Le assicurazioni offrono degli sconti nel caso accettiamo di installare un geolocalizzatore sulla nostra auto: è ovvio che ogni nostro movimento verrà tracciato (e quindi anche ogni nostra infrazione al codice della strada, anche se non viene comunicata alle autorità), ma d'altro canto se avremo un incidente d'auto sarà più facile ricostruirne le dinamiche, se l'auto verrà rubata sarà possibile localizzarla, così come non avremo più il problema di ricordarci dove l'abbiamo parcheggiata.

In tutti questi esempi cediamo parte dei nostri dati personali, e della nostra privacy, in cambio di qualche vantaggio. Tutto sta a valutare il rapporto tra i rischi in cui noi incorriamo e i benefici che ne abbiamo. Il diritto alla protezione dei dati non è un diritto assoluto e va bilanciato con quello alla salute: nessuno prevale ed esiste un bilanciamento, una legge interna di proporzionalità per cui viene ceduto solo per il contrasto della pandemia, senza effettuare una profilazione, e su base temporanea, subordinata allo stato di emergenza.

Soprattutto nella società occidentale, esistono dei cosiddetti garanti e delle istituzioni che disciplinano e regolamentano questi scambi e che proteggono gli individui. Si tratta di una lotta continua che può essere condotta solo a livello di società e di autorità garanti, possibilmente sovranazionali, cui il singolo può partecipare grazie a una piena presa di coscienza e di responsabilizzazione. D'altro canto, la rinuncia a una parte della propria privacy, a fronte di norme chiare e condivise, può rappresentare non solo un atto interessato, quando riguarda la propria salute, ma anche un atto di generosità verso i concittadini, per preservare la salute degli altri.

La pandemia da SARS-CoV-2 ha posto le nazioni e i continenti di fronte alle proprie debolezze strutturali e culturali. Nei paesi in cui l'individuo si integra in una società collettiva, che rappresenta il bene primario, la sua privacy e la sua libertà costituiscono un bene forse parzialmente alienabile in virtù dell'interesse collettivo, sempre con il consenso informato del singolo. Dove prevale l'individualismo, sia per identità culturale della popolazione sia per l'orientamento politico dei suoi dirigenti, il diritto alla libertà individuale assume un valore assoluto rispetto altri diritti, come quello alla salute, che riguardano anche gli altri. La comunità europea e la sua cultura hanno raggiunto un equilibrio, per quanto faticoso da mettere in atto, tra gli interessi dell'individuo e quelli della società e la sua recente legislazione sulla privacy ne è una pietra miliare. Questa legislazione regola anche gli aspetti più economici e il rapporto con le multinazionali, e andrà adeguata mano a mano alle sfide e agli attacchi che queste possono portare ai dati personali.

References

Dick, Philip K. *The Minority Report*. New York: Fantastic Universe, 1956.

Kalkman, S., M. Mostert, C. Gerlinger, J.J.M. van Delden, and G.J.M.W. van Thiel. "Responsible Data Sharing in International Health Research: a Systematic Review of Principles and Norms." *BMC Med Ethics* 20 (2019): 21. doi:10.1186/s12910-019-0359-9.

Price, W. Nicholson, and I. Glenn Cohen. "Privacy in the Age of Medical Big Data." *Nat Med* 25.1 (2019): 37-43. doi: 10.1038/s41591-018-0272-7.

Goldenholz, D.M., S.R. Goldenholz, K.B. Krishnamurthy, J. Halamka, B. Karp, M. Tyburski, D. Wendler, R. Moss, K.L. Preston, and W. Theodore. "Using Mobile Location Data in Biomedical Research while Preserving Privacy." *J Am Med Inform Assoc* 25 (2018): 1402-1406. doi: 10.1093/jamia/ocy071.

Unione Europea. "Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016." Gazzetta ufficiale dell'Unione europea 4/5/2016 L. 119/1.

Soriano-Valdez, D., I. Pelaez-Ballestas, A. Manrique de Lara, and A. Gastelum-Strozzi. "The Basics of Data, Big Data, and Machine Learning in Clinical Practice." *Clin Rheumatol* 2020 Jun 5. doi: 10.1007/s10067-020-05196-z.

UNESCO. *Universal Declaration of Bioethics and Human Rights 2005*. Available at https://en.unesco.org/themes/ethics-science-and-technology/bioethics-and-human-rights

Acknowledgements

The author is grateful to C. Cracco, F. Di Cunto e F. Rioli for critical reading of the manuscript.