La nuova civiltà nell'era dei dati Controllo, tracciamento e sicurezza

Ogni attività sulla Rete lascia tracce e informazioni degli utenti. I device perennemente connessi implicano rischi per la privacy. Regole e trasparenza per gestire la società della sorveglianza

di Giorgio Merli*

Come già sappiamo, oggi ci sono già ben 4,5 miliardi di persone connesse attraverso Internet e, entro il 2030, ci saranno 75 miliardi di dispositivi IoT (Internet of Things) connessi o connettibili, che immetteranno in Rete dati che ci riguardano. Si tratta di informazioni provenienti dalle nostre case (contatori di energia, elettrodomestici, ecc.), dalle nostre auto (Gps, scatole nere, ecc.), dai nostri smartphone (dall'uso delle App per geolocalizzazione, ecc.), dalle nostre attività su Internet (compreso quanto si concede via accettazione dei *cookie* per poter accedere ai siti che ci interessano), dalle nostre fruizioni di servizi nelle città *smart*.
Ciò significa che nessuno di noi può dire di avere ancora una privacy.
La fioritura di una varietà di App di *contact tracing* tese a contrastare la pandemia di covid ha acceso numerose discussioni sia sulla loro efficacia sia sui problemi di tutela della privacy, con particolare riferimento ai dati sanitari delle persone e alle loro frequentazioni.
Senza entrare nel merito dell'efficacia delle soluzioni adottate (logiche di monitoraggio e tecnologie utilizzate), esse hanno fatto prendere atto a tutti che di fatto siamo già in una logica da Grande Fratello che ci osserva continuamente e come vuole.

Lo scopo degli identificativi

Inutili i tentativi di minimizzare tale realtà, che è ben nota ai competenti e ora anche a un pubblico più vasto, visti i recenti avvenimenti di sanzioni a società telefoniche e grazie ai numerosi servizi giornalistici che stanno affrontando il tema (come il docufilm *Social dilemma* di Netflix).
Occorre essere consapevoli che l'utilizzo di un'App costituisce di per sé l'apertura di una porta di accesso ai nostri dati: infatti i sistemi operativi dei nostri smartphone mettono a disposizione una serie di

* *Consulente di multinazionali e Governi, Docente in università in Italia e all'estero*

Application program interface (Api) per permettere alle stesse App di utilizzare le diverse funzionalità offerte dal dispositivo (quali Gps, fotocamera, ecc). Attraverso le Api è possibile accedere a diversi identificatori del device, i quali permettono di risalire al suo proprietario.
Non a caso l'ID del nostro smartphone si chiama Identity for advertiser (Idfa) nei sistemi IoS-Apple e Android advertising ID (AaID) nei sistemi Android. Come dire che la finalità dei dati identificativi è dunque ben chiara: sono nati proprio per realizzare pubblicità mirate e personalizzate sulla base del monitoraggio dei nostri comportamenti e interessi, debitamente interpretati da algoritmi *ad hoc*.
Esistono anche altri identificativi che vengono utilizzati da molteplici stakeholder e Applicazioni. Analizzandone in dettaglio alcuni sarà facile capire come i *big player* della tecnologia riescano facilmente a risalire al proprietario del dispositivo e alle sue abitudini di vita semplicemente incrociando questi ID con i dati di posizione e quelli di accesso alla Rete Internet.
Il più importante è l'International mobile equipment identity (Imei), che è l'identificativo unico di ogni smartphone. Esso rimane invariato anche se l'Applicazione viene reinstallata o se il dispositivo è ripristinato alle impostazioni di fabbrica.
Si tratta di un ID hardware che rende possibili alcuni processi, quali la verifica della garanzia del prodotto acquistato, la registrazione dello stesso nel database del produttore, la localizzazione e il blocco del terminale in caso di furto o smarrimento per proteggere i dati personali, l'installazione di aggiornamenti.
Ci sono poi l'indirizzo Macwlan (l'identificativo che ogni dispositivo collegabile a una Rete Internet possiede) e quello di bluetooth (anch'esso unico, utilizzato per esempio dall'App Immuni).
Poiché l'Imei è legato alla Sim, possiamo essere certi che nessuno di noi ha dati anonimizzati, in quanto ciò è impossibile fisicamente. Tra l'altro l'acronimo Sim sta per Subscriber identity module, intendendo nei fatti che la nostra *smart card* è legata ai dati anagrafici che dobbiamo fornire all'operatore telefonico quando sottoscriviamo un nuovo contratto.
Del resto, senza questo legame non si saprebbe a chi far pagare il traffico consumato. E dal momento che le Sim sono tracciate da stazioni radio gestite dalle aziende Telecom, queste hanno in ogni istante i nostri dati di posizione, indissolubilmente legati alla nostra identità.
Tali informazioni sono in teoria riservate, ma sono facilmente vendute – legalmente o no – a chi ne può essere interessato (si pensi alle recenti sanzioni comminate ad alcuni operatori telefonici e, nello specifico, dirette a qualche loro dipendente indagato per furto e vendita di dati personali).

L'assenza di anonimato

È quindi velleitario il volerci garantire che i nostri dati siano anonimizzati. Come minimo dobbiamo fidarci di chi li ha in gestione in sistemi comunque 'hackerabili' e/o accessibili dai loro dipendenti.
Con questa realtà, che in effetti ci regala numerosi vantaggi operativi sia a livello business sia di vita privata, occorre prendere atto dei numerosi rischi connessi alla mancanza di anonimato.
È per questo motivo che sono state attivate regole e leggi che tentano di limitare tali rischi. Prime fra tutte quelle della Comunità europea, note come Gdpr (General data protection regulation) e diventate un riferimento mondiale.
Quelle preparate ora in California (culla di buona parte delle Applicazioni che ci hanno introdotto nel mondo dei dati) sono in effetti molto simili. Ovviamente occorre auspicare che gli standard mondiali si allineino. Sarebbe altrimenti difficile riuscire a tenere in un qualche modo sotto controllo fenomeni come quelli delle criptovalute, e comunque dei social, se potranno avvalersi di punti di entrata più 'tolleranti'.
Si pensi a quanto sta succedendo in questi giorni sul tema della liceità di certi comportamenti su Facebook e Twitter.
Si pensi, anche, al previsto massiccio monitoraggio e utilizzo dei dati riguardanti la salute che ci aspetterà nei prossimi anni (processo accelerato dalla pandemia di covid-19). Oppure ai diversi possibili utilizzi dei dati personali che si potranno fare a seconda delle politiche e dei modelli di riferimento (come ha fatto la Cina per tenere sotto controllo la pandemia e come fa tuttora, usando anche il riconoscimento facciale, per tenere sotto controllo quanto può interessare all'Amministrazione pubblica, alle forze dell'ordine e ai servizi di sicurezza). Proprio l'occasione del covid-19 ci ha fatto capire che fine

BOZZA

può fare la privacy nel caso di 'urgenti' problemi di salute e/o di sicurezza in ambienti socio-politici accentrati e direttivi.
Possiamo comunque già capire come molti nostri dati personali siano già di fatto, più o meno ufficialmente, nelle mani degli operatori Internet, dell'ecommerce, delle Amministrazioni pubbliche, dei Servizi segreti e degli hacker interessati (per proprio conto o per chi lo richiede).
Purtroppo possiamo anche già intuire come essi possano finire nelle mani della criminalità per usi diretti e indiretti più o meno leciti e sicuramente per quelli completamente illeciti che si consumano nel mondo del Deep e del Dark Internet, dove si va dal commercio di armi a quello che più ci preoccupa come persone, cioè del commercio di organi umani. Pensiamo infatti a come potrebbe vivere e quali timori potrebbe avere una persona con una configurazione sanguigna rara da trovare, una volta che i suoi dati fossero accessibili in rete. Potrebbe, per esempio, diventare un bersaglio molto importante per un qualche trapianto d'organo, in una qualche parte del mondo, in una qualche clinica specializzata e non troppo ufficiale. Specialmente in questo caso, ma comunque anche per motivi molto più banali, il fatto che qualcuno possa liberamente accedere alle nostre informazioni, senza peraltro che ne veniamo a conoscenza, deve costituire motivo di forte preoccupazione.

La disponibilità dei dati in tempo reale

Tutto ciò, però, non deve farci dubitare di Internet e di tutte le opportunità e facilità di vita che ci offre, ma sicuramente ci può spingere a trovare il modo di limitarne i pericoli (che, dobbiamo prenderne atto, non saranno mai comunque totalmente nulli). Occorre dunque accettare il fatto che le infrastrutture IT e di telecomunicazioni odierne non permettono l'anonimizzazione dei dati e che, contemporaneamente, non si può più adottare un approccio integralista per la tutela della privacy (anche perché è impossibile nella nuova logica dei social globali). Ci possono essere momenti di parziale ravvedimento nella troppa leggerezza nel rendere visibili dati e fatti personali (come accaduto nel mese di settembre 2020, quando una significativa percentuale di utenti ha abbandonato Facebook e Instagram a fronte di allarmi in tal senso), ma il trend di aumento dell'uso di Internet sarà irreversibile (magari con l'avvento di nuovi social diversamente caratterizzati).
La nuova economia digitale infatti si basa e si baserà sempre più sulla disponibilità in tempo reale delle nostre informazioni per permettere il funzionamento della nuova realtà con i loro Smart service.
Alcune fruizioni di servizi e alcuni adempimenti amministrativi e sociali non si possono già più fare in altro modo se non per via digitale (e la pandemia ne ha accelerato il corso).
Il vero valore positivo dei dati sta proprio nella loro possibilità di condivisone per acquisti, adempimenti, fruizione ed erogazione di servizi, sviluppo e utilizzo della conoscenza. Gli aspetti negativi risiedono nel loro possibile utilizzo incontrollato, illegale, fraudolento e criminale.
Un utilizzo positivo è anche quello della possibilità di un'analisi intelligente dei dati per i più disparati scopi, dall'intelligence contro il terrorismo alla ricerca di nuovi farmaci, dalla robotizzazione di processi di business alla gestione del rischio, dallo sviluppo di nuovi prodotti all'erogazione di servizi personalizzati, dalla gestione intelligente della mobilità alla fruizione dei servizi delle Smart city, ecc.
Purtroppo però anche in questi casi esiste la già diffusa negatività del loro utilizzo illegale che avviene a nostra insaputa.

Democrazia digitale e Intelligenza Artificiale

Un ulteriore utilizzo, che può essere contemporaneamente positivo e negativo, è quello della trasparenza dei dati nei confronti della Pubblica amministrazione. A tal riguardo il capitolo più importante è probabilmente quello che riguarda la digitalizzazione per il funzionamento della democrazia.
Il tema della democrazia digitale è infatti all'ordine del giorno in ambiente europeo e non solo. È già in elevato stato realizzativo in Paesi dove la democrazia è 'gestita dall'alto'. Si pensi alla realtà cinese dove tutto è controllato e gestito digitalmente (ovviamente in *top-down*), contemplando tutti i processi di rapporto con la Pubblica amministrazione e gestione in tempo reale di controlli, sanzioni e diritti umani. Oppure ai "crediti sociali" (una sorta di patente a punti) usati come criterio per il diritto di fruizione dei servizi della comunità, dell'accesso alla finanza, all'educazione, ecc. Ben diversa l'accezione dei Paesi democratici europei, dove democrazia

BOZZA

digitale significa possibilità ci contribuzione alla gestione della cosa pubblica in *bottom-up*. Si vedano a tal riguardo Applicazioni come quelle realizzate a Barcellona, dove i cittadini possono partecipare alle decisioni sugli investimenti pubblici.
Un altro tema importante è quello della diffusione dell'utilizzo dell'Intelligenza Artificiale (AI) applicata all'analisi dei dati personali o comunque dei comportamenti delle persone, in modo più o meno aggregato. Fino a quando se ne considerano le applicazioni per la robotizzazione dei processi (non solo produttivi, ma anche nei processi bancari, assicurativi, legali, della mobilità, ecc.), la situazione e le considerazioni sono simili a quelle già fatte per i dati immessi in Rete attraverso gli smartphone e i dispositivi IoT.
Ben diverse, invece, sono le implicazioni quando si parla di AI applicata nel mondo dei Servizi segreti, della politica, delle ricerche delle case farmaceutiche e di tutte le aziende interessate a studiare segnali deboli e riservati del mercato e delle persone anche attraverso i social e altre informazioni e attività personali digitalizzate (si pensi, per esempio, ai nostri dati sanitari archiviati presso la struttura sanitaria).
In tal caso il Grande Fratello si trasforma in un qualcosa che studia in profondo i nostri comportamenti e sentimenti e tenta di condizionarci o usarci per qualche interesse specifico (si pensi a come cercano di indirizzare i nostri acquisti, ai tentativi di influenzare le votazioni e alle *fake news* immesse ad arte su Internet).

Data ownership e controllo dei dati

Prendendo atto di tutto ciò e non immaginando grandi possibilità di reversibilità, come già anticipato, occorre almeno garantire a noi cittadini la massima possibilità di controllo di utilizzo dei dati. Avendo anche capito che è impossibile anonimizzarli a livello di geolocalizzazione e su altri aspetti, non rimane che auspicare la promozione e la realizzazione di sistemi che aumentino la possibilità di controllo, conoscenza e possibilmente di gestione (*ownership*) da parte delle persone, dei cittadini e dei clienti delle aziende.
Si tratta, quindi, di creare strutture più trasparenti e sicure (anche l'evoluzione delle tecnologie di cybersecurity avranno un ruolo importante) all'interno delle quali le persone possano condividere e tenere sotto controllo quei dati che decidono di mettere a disposizione della comunità e delle aziende.
Ciò significa che occorre mettere gli individui nelle condizioni di avere visibilità e controllo sulle terze parti che accedono e utilizzano i loro dati (dopo aver concesso le autorizzazioni del caso). Solo in questo modo si potrà recuperare la fiducia dei cittadini nelle istituzioni e dei clienti nelle aziende con cui

hanno rapporti. Prendere atto dello *status quo* – così come descritto finora – serve a creare quella consapevolezza necessaria a sviluppare nuovi strumenti tecnologici che rimettano il controllo dei dati in mano ai loro possessori (cittadini e clienti).
Si potrebbe in questo modo superare il concetto di Data privacy – pur sempre fondamentale, ma adeguato a specifici contesti – e iniziare a parlare di Data ownership, ovvero di controllo unilaterale sull'accesso ai propri dati, così come previsto dalla Gdpr e dalla strategia sui dati della Commissione europea per il 2020.
Occorre dunque realizzare infrastrutture e piattaforme che possano operare su Internet garantendo tale *ownership*.
Per poterlo fare esistono due prerequisiti da soddisfare: volerlo fare e saper implementare la tecnologia necessaria. Per quanto riguarda quest'ultimo aspetto si potrebbe già farlo, ma ci sono forti resistenze a riguardo da parte di chi ha grandi interessi nel poter gestire liberamente i nostri dati personali (primi fra tutti i 'potenti' di Internet, dei social e dell'ecommerce).
Sicuramente in tal senso spingono invece ora le regole che le comunità politiche e sociali hanno configurato e cercano di imporre.

Il ruolo delle Blockchain

Se il focus dell'ultima decade è stato quello di cercare di risolvere il problema della Data privacy, l'obiettivo dei prossimi anni sarà probabilmente quello della ricerca di soluzioni tecnologiche che consentano di applicare tali regole.
Un ruolo importante lo giocheranno probabilmente le Blockchain, che sono di fatto una sintesi di regole e tecnologia.
Queste consentiranno infatti ai cittadini e ai clienti di controllare l'accesso ai propri dati, aumentando in modo significativo la loro fiducia e disponibilità a collaborare (anche per rendere le città un posto migliore in cui vivere). Esse, inoltre, garantiranno

BOZZA

l'affidabilità del dato consentendo a larghe comunità con interessi simili di avere informazioni e contratti regolarmente 'registrati' e certi (non a caso le Blockchain vengono spiegate col concetto di "notariato diffuso"). È su tale logica, come ben sappiamo, che si basano le cosiddette criptovalute che, fra non molto, saranno chiamate semplicemente *digital currency*, in quanto diventeranno un modo normale per la gestione delle transazioni di business.

Ma come può essere strutturata una soluzione tecnologica che implementi la Data ownership?

Le Gdpr gettano le basi legali per il riconoscimento della proprietà del dato, ma questo non è ancora sufficiente. Trattandosi di un contesto digitale, la proprietà deve essere riconosciuta anche dal punto di vista sostanziale, ovvero a livello tecnologico.

Questo significa che occorre adottare un sistema decentralizzato per la gestione della condivisone dei dati.

Ancora oggi è il proprietario dell'infrastruttura tecnica, tipicamente un Data broker-market place ad avere il controllo sui dati che la attraversano, potendo così garantire solo trasparenza, ma non il controllo sulla condivisione con terze parti.

È necessaria, invece, un'infrastruttura tecnica dove sia l'origine del flusso di dati ad averne il controllo, ovvero il Data owner.

Esistono già possibili soluzioni a riguardo. La più efficace è a mio avviso quella brevettata negli Usa da Ecosteer (startup italiana con sede a Bolzano): essa propone un *overlay network* per la gestione della condivisione dei flussi di dati, garantendo ai loro proprietari il pieno controllo sull'accesso di terze parti (i Data user).

Si tratta di uno strumento software basato su Smart contract gestiti in Blockchain e su una End-to-end encryption (oggetto del loro brevetto). Con tale struttura i Data owner possono concedere e revocare unilateralmente l'accesso ai loro dati, automatizzando così il Consent management previsto dalla Gdpr.

È proprio lo Smart contract a creare la relazione diretta tra Data owner e Data user e a fissare il valore del dato in *token*, cioè crediti spendibili con gli stakeholder coinvolti (una sorta di punti fedeltà, quali quelli già utilizzati da carte di credito, supermercati, ecc.). È così possibile avere anche un meccanismo di ricompensa per la condivisone dei dati.

Fondamentale è la fiducia degli utenti

Il controllo e la remunerazione per il loro utilizzo (chi ha interesse a usare i nostri dati ci deve ricompensare in un qualche modo) in un sistema decentralizzato (cioè non gestito nei contenuti da *broker* e *owner* di un *market place*) sono alla base della fiducia ottenibile dai cittadini.

Tale fiducia è necessaria per promuovere la loro partecipazione digitale ai business di cui sono di fatto clienti (è quasi una 'democrazia nel business'). Come sostenuto recentemente da Antonello Soro (Presidente dell'autorità garante della privacy) e come ben spiegato da Shoshana Zuboff, accademica americana, nel suo libro *Il capitalismo della sorveglianza*, stiamo correndo il rischio di scivolare verso una 'società della sorveglianza', una nuova forma di organizzazione nella quale la raccolta di dati da parte di aziende private, e talvolta di Stati, è tale da limitare pesantemente la nostra libertà.

Solo l'attivazione di regole e meccanismi che possano garantire trasparenza, controllo e *ownership* può garantire una limitazione degli aspetti negativi, enfatizzando quelli positivi. I problemi di privacy e di sfruttamento economico dei dati che si stanno evidenziando ci danno l'opportunità di prendere atto di come la tecnologia sia stata finora disegnata e gestita in modo non del tutto etico e di porvi rimedio, reindirizzandola opportunamente.

BOZZA