UNITELMA SAPIENZA

InterLex FORUM20 LA CITTADINANZA DIGITALE

LA CITTADINANZA DIGITALE

La profilazione dei cittadini digitali, la minaccia più grave nell'era dei Big Data

Manlio Cammarata – 8 settembre 2017

Che significa “Big Data”?

Con l’espressione “Big Data” si indica un vasto campo di applicazione delle tecnologie informatiche, basato su:

- Grandi basi di dati, acquisite generalmente con sistemi automatici attraverso l’analisi di altre basi di dati, log, cookie, social media, scansione di messaggi email e altri strumenti di cattura, spesso occulti.
- Elaborazione dei dati attraverso sistemi di “intelligenza artificiale” (AI) dedicati ai diversi settori.
- Sfruttamento dei risultati delle elaborazioni a fini economici, o di ricerca scientifica pura o applicata, e vendita di dati strutturati per determinati impieghi.
- Per quanto riguarda le persone (non solo fisiche), la creazione di “profili” utilizzabili a fini sociali, commerciali ed eventualmente politici.

L’utilità dei Big Data

In alcuni campi i Big Data consentono progressi che non sarebbero possibili con altri mezzi.

Per esempio, nella ricerca medica, lo studio delle malattie, e quindi la creazione di nuovi farmaci o di nuovi protocolli terapeutici, sono il frutto di ricerche su vastissimi campioni di popolazione.

In particolare, la ricerca epidemiologica su vasta scala permette di prevedere (e di controllare) la diffusione di gravi malattie, oltre che di mettere a punto nuovi farmaci.

Nel campo del marketing, i Big Data indicano le tendenze di acquisto dei consumatori e permettono sia la creazione di nuovi prodotti sia la loro commercializzazione con azioni mirate.

Consentono, soprattutto, di agire sul singolo consumatore e di fornirgli comunicazioni personalizzate che influenzano le sue scelte.

Questo significa che limitano la sua libertà di scegliere.

Chi sono i padroni dei Big Data?

I Big Data richiedono grandi investimenti e, come presupposto, un controllo esteso dei sistemi di comunicazione. Imponenti strutture di ricerca e sviluppo creano e aggiornano continuamente gli strumenti di ''intelligenza artificiale'' indispensabili per la raccolta e l'elaborazione delle masse di dati.

Sono quindi poche le organizzazioni che possono disporre di strutture di Big Data. Di solito si indicano come le ''sei sorelle'', ricordando le ''sette sorelle'' del petrolio nel secolo scorso:

Google, Yahoo, Apple, Amazon, Facebook, Microsoft.

Qualcuno aggiunge la cinese AliBaba, portando così a sette il numero degli Over The Top (OTT), i grandi padroni mondiali dei dati, i ''petrolieri'' del terzo millennio.

(Come OTT si indicano spesso anche i grandi operatori delle TLC)

“Tanto non ho niente da nascondere”

È la risposta di chi viene informato sui rischi che corre ogni volta che usa il telefonino o invia un’email senza curarsi di proteggere (per quanto possibile) i propri dati.

Davvero non hai niente da nascondere?

Per questo hai un account di posta elettronica con Gmail?

Forse non sai che quando apri un account Gmail acconsenti a un trattamento dei tuoi dati che comporta almeno:

- la mappa di tutti i tuoi contatti, compresa la frequenza con la quale comunichi con ciascuno di loro;

- la lettura (da un sistema automatico) del contenuto delle email, con l’estrazione di informazioni sul tuo stato di salute, delle tue opinioni politiche, dei tuoi acquisti online… fino a dettagli come le misure delle tue scarpe o di altri indumenti.

Ti sta bene? Sono fatti tuoi. Ma…

Il problema è che sono anche fatti miei

Google non raccoglie e tratta solo i tuoi dati, quando scrivi a qualcuno, ma anche quelli di chi ti scrive. Quando ti mando una email con informazioni sul mio conto (esempio banale: dove e per quanti giorni sono stato in vacanza), il sistema tratta questo dato e lo può vendere a qualche tour operator o a qualche organizzazione del marketing del turismo. Insomma, mi ruba il dato e se lo rivende.

Questo è un problema che dovrebbe essere seriamente preso in considerazione, anche se è difficile risolverlo sul piano tecnico e giuridico. In effetti, allo stato attuale della normativa (GDPR), non ho la possibilità di negare il consenso al trattamento da parte di un soggetto con il quale non ho alcun rapporto, che non mi rende nessuna informativa, che è difficile (se non impossibile) da controllare per le autorità alle quali è affidato questo compito.

Ma non basta...

Dal telefonino al televisore *smart*

I nostri dati personali, anche quelli che crediamo restino confinati nel nostro ambito familiare sono spesso raccolti nell'ambito dei Big Data. Spesso non sappiamo neanche bene da chi, e a chi vengono venduti.

La raccolta più diffusa e pervasiva avviene attraverso gli smartphone.

Ogni volta che ci serviamo di una app, questa è autorizzata a leggere praticamente tutto il contenuto dell'apparecchio, email comprese.
Il telefonino racconta tutto di noi, in particolare dove siamo e dove andiamo, oltre ai nomi delle persone con cui siamo in contatto.

Un'altra fonte di informazioni è costituita dagli apparecchi domestici intelligenti (smart), sempre collegati a un *cloud* e che, per di più, sono intrinsecamente insicuri e quindi esposti ad attacchi e furti di dati.

Ti piace l'idea che il tuo televisore veda, senta e trasmetta a qualcuno tutto quello che fai e che dici, anche quando credi di averlo spento?

La legalità dei trattamenti è spesso discutibile

Per la normativa ‘’in fase di dismissione’’ (Codice privacy, direttiva 45/96) molti trattamenti sono legittimi solo all’apparenza, in particolare per quanto riguarda i cookie, ormai presenti su quasi la totalità dei siti. Infatti essi vengono depositati ancora prima che l’interessato veda l’informativa, spesso non ha la possibilità di negare il consenso e, in primo luogo, l’informativa stessa non indica il vero fine della raccolta dei dati.

Nessuno indica l’uso a fini di profilazione. Invece si scrivono formule generiche e fuorvianti come ‘’ per migliorare la tua esperienza di navigazione’’, e simili, che appaiono più o meno inoffensive.

Inoltre i dati raccolti, che vengono qualificati come ‘’anonimi’’, spesso non lo sono, poiché esistono procedure efficaci per ‘’de-anonimizzare’’ i dati.

Tutto questo nell’inerzia delle autorità competenti.

Con i nuovi regolamenti UE cambierà qualcosa?

Il Regolamento generale sulla protezione dei dati (GRDP), in vigore dal 24 maggio 2016 e ''applicabile'' dal 24 maggio 2018, sotto molti aspetti sembra più efficace delle norme introdotte a partire dalla direttiva 95/46. Tuttavia restano diversi punti critici.

Tutto il settore delle telecomunicazioni e dei servizi internet sarà oggetto di un altro regolamento (cosiddetto *e-privacy*), ancora in fase di discussione (anche se dovrebbe essere applicabile dal 24 maggio 2018, insieme al Regolamento generale).

Nella proposta del Regolamento *e-privacy* ci sono disposizioni che sembrano (relativamente) efficaci per limitare lo strapotere degli OTT nei trattamenti dei dati personali.

Per questo è oggetto di attacchi da parte delle lobby degli stessi OTT, attacchi che rischiano non solo di renderlo meno efficace, ma anche di ritardarne l'applicazione, con conseguenze negative per i titolari, a causa della vigenza contemporanea di norme vecchie e nuove.