

Analisi. «Datificati» fin dalla nascita. Una minaccia per la libertà

Claudia La Via mercoledì 24 febbraio 2021

I rischi di una società in cui in Rete si costruiscono e si vendono le identità dei cittadini



Dalle app per la gravidanza ai dispositivi che controllano lo stato di salute, fino alla didattica a distanza: così il commercio dei profili digitali alimenta le disuguaglianze - Archivio Avvenire

I browser per navigare sul web, le app sul telefono, i social network, ma anche le visite mediche, i pagamenti elettronici, e ora persino la scuola e l'università. Sono sempre più numerose le nostre attività che generano dati capaci di parlare di noi. Siamo tutti cittadini "datificati". Sottoposti cioè a quella "datificazione" entrata nella Treccani tra i neologismi del 2019 e definita come «il processo tecnologico che trasforma vari aspetti della vita sociale o della vita individuale in dati, che vengono successivamente trasformati in informazioni dotate di nuove forme di valore anche economico». I nostri figli, le nostre famiglie, le nostre vite: tutto viene trasformato in dati, che vengono condivisi e venduti come "materie prime" su cui guadagnare anche senza il nostro esplicito – o almeno del tutto consapevole – consenso.

Essere datificati è inquietante. È sgradevole la sensazione che si prova quando, dopo avere abbozzato un controllo di massima, ci si accorge di quante siano le informazioni sul nostro vissuto che comunque abbiamo messo e continuiamo a mettere a disposizione di aziende private. Grazie alle decine di "Termini e condizioni" che

abbiamo accettato senza leggere o perché non avevamo scelta, abbiamo offerto a queste aziende la possibilità di usare le nostre informazioni personali per costruirci attorno delle “identità uniche digitali” da vendere ai famigerati “soggetti terzi”: investitori pubblicitari (nel migliore dei casi), compagnie assicurative, banche o potenziali datori di lavoro (negli scenari più minacciosi). Per chi si è avventurato nella lettura delle oltre seicento pagine del «Capitalismo della sorveglianza» di Shoshana Zuboff, psicologa e filosofa di Harvard, non è un mistero che le compagnie tech della Silicon Valley stiano già oggi sfruttando le nostre informazioni personali anche per predire e condizionare i nostri comportamenti.

In molti casi i dati dei figli che affidiamo ai social o alle applicazioni possono essere ceduti a terzi e questo può intrappolare i bambini in stereotipi capaci di condizionare le loro vite future

Lo scenario di un mondo in cui Big Tech guadagna controllando la quotidianità delle persone si fa ancora più spaventoso se pensiamo ai nostri figli. I bambini nati negli ultimi anni sono «la prima generazione di cittadini ad essere datificati ancora prima di nascere» racconta Veronica Barassi in «child | data | citizen», libro appena pubblicato da MIT Press, la casa editrice del Massachusetts Institute of Technology, che riassume un progetto di ricerca antropologica sul precario stato di salute della privacy dei minori in Occidente. Ne emerge una realtà allarmante su come i dati personali raccolti influenzano le nostre vite. A partire dai bambini, che sono profilati ancora prima di esistere. Come? Nel momento in cui una donna cerca su internet informazioni riguardanti una gravidanza ancora solo da progettare, ad esempio, il motore di ricerca inizia a raccogliere i primi dati sul bambino che verrà. Le app per tracciare la gravidanza collezionano informazioni sui progressi dell'embrione fino alla nascita. Le ricerche dei genitori sul web e le informazioni sul figlio che renderanno pubbliche nel tempo sui social network contribuiranno a costruirgli un “primo livello” di profilazione. Gli assistenti vocali che sempre più persone si mettono in casa, poi, ascoltano quello che si dice in famiglia e raccolgono a loro volta informazioni preziose per definire l'identità di genitori e figli.

La creazione di questo enorme database prosegue negli asili e nelle scuole, dove inizia la profilazione “professionale” della persona. Strumenti come il registro scolastico elettronico o le piattaforme per seguire le lezioni a distanza e fare i compiti possono raccogliere un'enormità di dati su rendimento scolastico e abitudini di apprendimento dei singoli alunni. In alcuni casi questi dati possono essere ceduti a terzi. «Questo rischia di intrappolare i bambini in stereotipi che possono condizionare le loro vite e avere un impatto sulle loro opportunità future», sottolinea Barassi. Ma si pensi anche ai dispositivi indossabili dai bambini e che registrano ore di sonno, battito cardiaco, numero di passi, attività fisica...

È facile intuire, ma difficile comprendere a pieno che cosa possono fare Google, Facebook, Apple, Amazon e gli altri giganti digitali con questi gigabyte di informazioni sulle nostre vite e sulle nostre famiglie. «Queste aziende sono in grado di aggregare un'enormità di dati e informazioni apparentemente scollegate tra loro e reperite dai contesti più disparati come salute, scuola, attività in Rete e social network e creare un'identità digitale unica riconducibile a un individuo preciso, identificabile tramite nome, cognome e indirizzo», spiega Barassi. Rifiutare di concedere i dati non è sempre possibile, ad esempio non si può rinunciare alla didattica digitale o alle piattaforme per accedere a prestazioni sanitarie. In Europa la General Data Protection Regulation (GDPR) è una delle norme più stringenti in materia di protezione dei dati personali. Eppure, nota Barassi, ha «un approccio individuale, incapace quindi di proteggere i bambini da intercettazioni ambientali e da informazioni condivise da terzi, ma anche da profilazioni effettuate sulla base delle scelte e dei valori dei propri genitori».

La Commissione Ue lavora a un nuovo Data Governance Act al fine di aumentare il controllo sul tracciamento

Che la situazione sia preoccupante lo conferma il fatto che lo scorso novembre la Commissione europea ha avviato i lavori per un nuovo Data Governance Act al fine di aumentare il controllo sul trattamento dei dati in tutti gli Stati membri. Le leggi però non azzerano le minacce. Perché ci sono aziende che ignorano le regole e perché a volte la protezione dei dati personali degli utenti non è abbastanza sicura. Barassi cita ad esempio un report del 2018 che mostra come i “broker” specializzati nei dati legati alla formazione negli Stati Uniti operano senza regole vendendo alle aziende liste di studenti con dettagli identificativi che li profilano secondo etnia, religione, affluenza scolastica e stili di vita. In «child | data | citizen» ci sono tante immagini di quello che succede in una società data driven. La mamma che ha perso il bambino alla fine della gravidanza e ora online è tormentata dai banner di pubblicità di prodotti per neonati. L'americano benestante che ha visto ridursi il fido della carta di credito perché fa spesso la spesa in un supermercato frequentato da gente più povera. Le aziende che vendono agli uffici del personale il profilo digitale dei candidati a un posto di lavoro.

La grande minaccia di Big Data è quella di una società dove la disuguaglianza è inesorabile, perché le persone sono condannate ad essere quello che ha deciso per loro un algoritmo segreto in base ai dati che è riuscito a raccogliere. «La profilazione che viene costruita a partire dal tracciamento delle nostre vite rischia di avere un impatto sui nostri diritti e sulle nostre scelte future», nota Barassi. Un minaccia resa ancora più ingiusta dal fatto che gli algoritmi possono sbagliare: «Una società che si affida ai dati per compiere anche scelte politiche non contempla il fatto che gli algoritmi esagerano nella semplificazione della realtà e possono trascurare informazioni che gli utenti non rendono pubbliche. Che cosa possiamo fare quando ci accorgiamo che il racconto che gli algoritmi hanno costruito su di noi è falso e pieno di pregiudizi?». La risposta non può che essere politica e deve coinvolgere i governi, le aziende e i cittadini: «Dobbiamo

unire le forze per iniziare ad immaginare modelli istituzionali e di business che affrontino la questione della fallacia degli algoritmi: dobbiamo iniziare a lottare per il diritto alla giustizia dei dati».

© RIPRODUZIONE RISERVATA

ISCRIVITI ALLA NEWSLETTER DI AVVENIRE: IL MEGLIO DELLA SETTIMANA

(<https://www.avvenire.it/Account/Registernewsletter?sectionUrl=newsletter&nc=02>)