La nostra identità digitale alimenta un mercato invisibile. Serve a fare spot mirati, ricerche ma anche a manipolarci.

Tempo fa, gli spettatori di Beyoncé hanno ricevuto un regalo inatteso: al suo concerto ad Anversa, in Belgio, potevano prendere gratis una lattina di Pepsi da un distributore. Bastava accedere a Facebook da un monitor e cliccare un "*like*". Un fatto eccezionale? No: siamo bersagliati ogni giorno di offerte in cambio dell'iscrizione a newsletter, siti, carte fedeltà. In quell'occasione, però, i dati personali erano ripagati subito, e con un bene tangibile.
Ma quanto valgono i nostri dati? Ben più di una bibita in lattina. Basta fare un calcolo: nel 2016, Facebook era valutata 350 miliardi di dollari, grazie ai dati del suo miliardo e 650 milioni di utenti; dunque ciascuno di loro rende oltre 212 dollari. Se si aggiunge quanto fruttiamo a Google, Microsoft, Apple, Amazon, un utente di Internet vale in media, per la pubblicità, 1.200 dollari l'anno. Che alimentano, dice la rivista *Forbes*, un mercato di 130,1 miliardi di dollari: come il Pil dell'Ungheria.

BISCOTTI AVVELENATI. I nostri profili, infatti, servono alla pubblicità: hai cercato sul Web un volo per Parigi? Su tutti i siti che visiterai appariranno banner di hotel parigini. È il sogno di ogni venditore: arrivare subito ai clienti interessati. Ma perché dovremmo preoccuparci se Google sa dove andremo? Perché in realtà questa grande quantità di dati (*big data*) non serve solo al marketing: quando usiamo un'app o la carta di credito, lasciamo briciole di informazioni su di noi, i "biscotti" (*cookie*, file che registrano le nostre azioni sul Web). Con questi biscotti nutriamo un esercito invisibile. E, avverte il saggista Craig Lambert nel libro *Lavoro ombra* (Baldini & Castoldi), «potete star certi che, presto o tardi, quell'esercito troverà qualcosa da fare». Quei dati, infatti, arrivano a società poco note e potenti, le quali, incrociando, comprando e vendendo informazioni, assemblano dossier su di noi. I nostri acquisti, ma anche i viaggi, i gusti sessuali, le preferenze ▶

I PADRONI DEI DATI

IL NUOVO PETROLIO. Il lungo viaggio dei dati digitali: alimentano ricerche, pubblicità, campagne mirate e... servizi segreti. Perciò sono fonte di ricchezza.

COSA SANNO DI NOI

DATI PERSONALI: nome, email, telefono.

DATI SOCIO-DEMOGRAFICI*: età, sesso, città di residenza, fascia di reddito, occupazione, dimensione del nucleo familiare.

DATI COMPORTAMENTALI*: ricerche effettuate, siti visitati (acquisti, viaggi, frequenza di navigazione), posizione geografica.

DATI SENSIBILI:** malattie, orientamento politico, religioso o sessuale, dati biometrici.

**dati anonimi, non riconducibili a una singola persona.*
***dati che dovrebbero essere trattati in modo separato e in forma riservata.*

CHE FINE FANNO LE INFORMAZIONI

RISULTATI PERSONALIZZATI
I risultati delle ricerche (su motori di ricerca e social network) cambiano da un utente all'altro a seconda delle sue attività passate e della sua posizione geografica.

RISULTATI SPONSORIZZATI
Quando si inserisce una parola in un motore di ricerca, fra i risultati appaiono annunci sponsorizzati: alcuni inserzionisti hanno pagato per apparire quando qualcuno digita determinate parole (per esempio, scarpe da tennis).

PUBBLICITÀ DIRETTA
Quando si visualizza o si clicca su un banner pubblicitario, il browser registra un cookie (coè un file con i dati identificativi e di navigazione): così l'inserzionista sa quante persone hanno visto l'annuncio e quanto deve pagare al sito che lo ospita.

REMARKETING
Quando si naviga su un sito di e-commerce (Amazon), il browser registra la ricerca fatta (es: tostapane), anche se non si acquista nulla. Quando il navigatore andrà su altri siti (che ospitano inserzioni di Amazon), apparirà un banner sui tostapane di Amazon.

VIGILANZA E MONITORAGGIO
Particolari software sono in grado di riconoscere una persona (o almeno la sua presenza, il sesso e l'età), localizzandola in un punto preciso.

PUBBLICITÀ PROGRAMMATICA
Quando si naviga su un portale Web, i cookie arrivano a varie concessionarie di pubblicità digitale. A seconda del tipo di utente (uomo o donna, giovane o anziano, aquirente di musica o di vestiti, etc.), le concessionarie contattano gli inserzionisti interessati a raggiungere quella categoria di utenti. È un'asta in tempo reale, e si svolge in modo automatico in millesimi di secondo: chi aveva offerto di più avrà il proprio banner sul portale.

INFORMAZIONI SENSIBILI
Queste informazioni non sono pubblicamente accessibili, ma possono essere usate da governi e istituzioni.

MARKETING DIRETTO
L'utente riceve telefonate, email e posta cartacea da società che vendono beni o servizi. O da candidati politici.

STUDI STATISTICI
I comportamenti degli utenti vengono studiati per capire le tendenze generali in ogni campo: dalle abitudini di acquisto al rischio di incendi, fino alla diffusione delle malattie o al funzionamento di auto, aerei, impianti.

CHI LE USA

SOCIETÀ E RICERCATORI
- Produttori di beni/servizi.
- Società di consulenza, marketing e sondaggi.
- Università ed enti di ricerca
- Società informatiche.

DATA BROKER
Sono società specializzate nell'aggregare informazioni sulle persone: possono comprarle (da società finanziarie, telefoniche, di ricerca) o raccoglierle sul Web. Poi studiano i dati e li vendono sul mercato. I dati sono aggregati in grandi segmenti (per esempio, maschi fra 18 e 30 anni) e poi rivenduti a società interessate a raggiungere quel segmento per fare pubblicità mirata.

GOVERNI
- Istituzioni.
- Servizi segreti.

CRIMINALI
- Hacker: per rubare soldi, password, informazioni, indirizzi email.

COME VENGONO ESTRATTE

COMPUTER
I nostri dati di navigazione (ricerche, email, acquisti) sono raccolti dai portali nei cookies, file che poi vengono archiviati nei loro database.

SMARTPHONE E ALTRI DISPOSITIVI
Grazie a sensori, antenne, app registrano i nostri comportamenti. Possono essere presenti anche in auto, braccialetti, elettrodomestici intelligenti...

ISCRIZIONI A CONCORSI, SERVIZI, RACCOLTE PUNTI

CARTE FEDELTÀ DI NEGOZI E SUPERMERCATI

VIDEOCAMERE, DRONI, SATELLITI

ALTRI SERVIZI
Conti correnti e carte di credito, linea telefonica, linea elettrica, assicurazioni, viaggi, partecipazioni a fiere, noleggio di auto.

SERVIZI PUBBLICI
Anagrafe, ospedali, fisco, casellario giudiziario, catasto, scuole.

Xinhua / Eyevine/Contrasto

ARCHIVIO DI ACQUISTI. Il centro dati di Alibaba, il più grande sito di vendita online al mondo, a Zhangbei (Cina).

Siamo tutti schedati in categorie, ma non sappiamo in quali e con quali criteri

politiche. E queste informazioni sono usate per catalogarci: 40enne milanese, single; vedova 60enne romana ecc. Tutte variabili usate per influenzarci: possono migliorare le cure mediche, ma anche limitare la libertà politica, finanziaria e lavorativa. Insomma, possono diventare biscotti avvelenati.

Com'è possibile? Basta ricordare la storia di Amazon, che ha reso il suo fondatore, Jeff Bezos, l'uomo più ricco al mondo. All'inizio, i redattori di Amazon – che allora vendeva solo libri – riunivano gli acquirenti in categorie (appassionati di cucina o di gialli), per inviare proposte su misura. Poi si sono accorti che, invece delle persone, era meglio paragonare i prodotti: chi comprava un giallo di Camilleri acquistava anche un racconto di Pennac. Amazon aveva scoperto la potenza della "correlazione": non so perché l'acquisto di A sia legato a quello di B; ma se c'è uno, è probabile ci sia pure l'altro. E posso fare previsioni. Così Bezos licenziò i redattori, affidandosi agli algoritmi. Oggi 1/3 delle sue vendite arriva dal sistema automatico di raccomandazione.

Però i dati non servono solo ai venditori, ricorda Viktor Mayer-Schönberger sul suo libro *Big data* (Garzanti). Incrociando quelli presenti negli archivi delle imposte, nel casellario giudiziario, e nell'ufficio di igiene, il Comune di New York ha identificato in modo preciso gli edifici a rischio di incendio: oggi il 70% delle ispezioni individua (su 900mila alloggi) le case da sgomberare, contro il 13% del passato. E Carolyn McGregor, dell'Ontario Institute of Technology (in Canada), ha creato un software che registra 1.260 parametri al secondo (battito cardiaco, temperatura, pressione...) nei neonati prematuri: segnala un'infezione 24 ore prima che appaiano i sintomi. I big data, insomma, possono salvare molte vite.

GRAVIDANZA. Accanto agli straordinari benefici, però, urge evidenziare i rischi, spesso invisibili. I dati, ad esempio, possono svelare i nostri segreti più intimi: l'ha scoperto Target, una catena di supermarket. Studiando gli acquisti delle clienti, aveva identificato 20 prodotti (integratori, lozioni e altri) legati alla gravidanza: un dato cruciale, visto che un figlio cambia le abitudini d'acquisto. Così, quando una donna comprava quei prodotti, le inviavano offerte mirate. Un giorno, però, un cliente del Minnesota chiamò inferocito il direttore d'un negozio: alla figlia liceale erano arrivati sconti per bebè. «Volete convincerla a restare ▶

DAL 2018 PRIVACY PIÙ TUTELATA

MULTE. Il Far West della privacy ha i mesi contati: il 25 maggio 2018 entrerà in vigore il nuovo regolamento europeo sulla protezione dei dati (Gdpr), e sarà più facile essere tutelati sul Web. I siti dovranno dire, in modo chiaro ed esplicito (basta paginate in legalese), quali informazioni raccolgono, e per quali scopi. E dovranno chiedere il consenso per ciascuno di questi usi. Gli utenti potranno chiedere di cancellare i propri dati in modo altrettanto facile. Pene esemplari per chi trasgredisce: sanzioni fino a 20 milioni di euro o al 4% del fatturato globale annuo. Nelle aziende digitali è istituita la figura del Data protection officer, un esperto di diritto e di tecnologia che dovrà vigilare sul rispetto delle norme e la tutela dei dati. Basterà?

TRAFFICO DIGITALE. Giacarta (Indonesia). I cellulari dicono dove siamo: segnalano gli ingorghi e consentono spot localizzati.

Reuters/Contrasto

I politici possono diffondere idee populiste in modo mirato. E senza controllo

incinta?», ha detto. Ma poi ha richiamato per scusarsi: sua figlia era davvero incinta. Target l'aveva saputo prima di lui.
I "biscotti" digitali, inoltre, come ha scoperto Amnesty international, possono essere raccolti per usi inquietanti: la segregazione etnica e religiosa. Dopo i proclami di Donald Trump contro gli immigrati musulmani, Amnesty ha verificato se si potessero identificare quelli residenti negli Usa. Ha trovato una società, la ExactData.com, che offriva una lista di 1,8 milioni di musulmani per 138mila dollari: 7 centesimi a persona. Non era l'unica: da decenni, ben prima del Web, decine di società, i *data broker*, raccolgono dati su chiunque. E ci catalogano, vendendo i dati al miglior offerente. Compresi i servizi segreti. Uno dei più grandi data broker, Axciom, ha classificato 500 milioni di persone nel mondo: nel 2001 rivelò di avere nel suo database 11 dei 19 autori dell'attentato alle Torri gemelle.

CANCELLATEMI! Queste società agiscono in un vuoto legislativo dove ogni abuso è possibile. Nel 2011, uno studente di legge austriaco, Maximilian Schrems, chiese a Facebook i propri dati: ha ricevuto 1.222 pagine con gli ultimi 3 anni della sua vita, comprese le informazioni che lui aveva cancellato. Eppure Facebook diceva di conservare solo gli ultimi 3 mesi di navigazione. Schrems ha fatto causa, e solo nel 2015 la Ue ha dato una stretta alle regole sulla privacy per gli europei.
Eppure, siamo arrivati a questo punto per nostra volontà, scrive il sociologo Zygmunt Bauman in *Sesto potere* (Laterza). «L'anonimato è morto, ma l'abbiamo ucciso noi: lo riteniamo un prezzo ragionevole da pagare in cambio delle meraviglie che ci offrono (app, motori di ricerca, siti di notizie). Siamo tutti controllati, ma anche controllori: coi social network vediamo cosa fanno gli altri».
E oltre ai rischi per la privacy, questi Grandi Fratelli hi-tech creano un altro pericolo: possono sbagliare. «Chi profila centinaia di milioni di persone con migliaia di fonti diverse farà molti errori», sottolinea Cathy O' Neil, ex analista di Wall Street. «E rischia di distruggere la vita delle persone: se una banca ti ha bollato come mutuatario ad alto rischio, il mondo ti tratterà come un parassita che non paga i debiti, anche se non è così». Oltre agli errori c'è il problema dei "dati vicarianti": se un dato manca, lo si sostituisce con altri, approssimativi o inadeguati: «Oggi, per valutare un candidato, metà delle aziende controlla il suo indice di affidabilità creditizia. Un indice comodo, ma non rivela competenza o serietà sul lavoro», dice O' Neil. E lo stesso accade con le assicurazioni, che valutano quanto far pagare ai clienti basandosi sulle loro ricerche su Google.
Infine, ci sono «società senza scrupoli che cercano disperati e ignoranti per spillare loro soldi. Un algoritmo errato o malevolo moltiplica le iniquità su vasta scala». Perciò O' Neil ha ribattezzato gli algoritmi *Armi di distruzione matematica*, titolo del suo nuovo libro (Bompiani).

ABUSI. Gli scenari più inquietanti sono in politica. Uno dei segreti del successo di Trump, per esempio, è un data broker, Cambridge Analytica. I suoi analisti hanno profilato gli elettori, per poi mostrare a ognuno slogan differenziati sul Web: alle donne promettevano supporti alle famiglie; ai disoccupati, posti di lavoro. Ma le campagne politiche personalizzate si prestano ad abusi: possono prendere di mira elettori poco istruiti, emarginati, poveri, per bombardarli con campagne che agitano spauracchi strumentali, come la sicurezza, dice Zeynep Tufekci, sociologa all'University of North Carolina. E nascondono gli annunci populisti a elettori che ne sarebbero indignati. Così le *fake news* si diffondono: nel 2015, il 43% dei repubblicani credeva che Obama fosse musulmano. «Chi fa marketing politico», avverte O' Neil, «ha un dossier su tutti noi, ma nasconde cosa dice ai nostri amici: così non possiamo capire perché hanno idee sbagliate. Questo ci impedisce di verificare le notizie e unire le forze, minando la democrazia».
Un allarme, questo, condiviso in Italia da Antonello Soro, garante della privacy: «C'è una grande asimmetria di potere fra noi e chi possiede i dati. Un numero esiguo di aziende ha conoscenze gigantesche e ha tutti i mezzi per influenzarci. Hanno un potere che si affianca, fin quasi a sopraffarla, all'autorità dello Stato».

CHE FARE? Per Mayer-Schönberger, le soluzioni sono: 1) trasparenza: le società devono mostrare i propri dati e gli algoritmi con cui sono raccolti; 2) certificazione: i criteri d'elaborazione dei dati devono essere certificati da un algoritmista imparziale, iscritto in un albo; 3) confutabilità: le società devono indicare come correggere i dati.
«Abbiamo il diritto di sapere come siamo classificati e, in caso di errori, di correggerli», conclude Massimo Marchiori, docente di informatica all'Università di Padova. «La tecnologia c'è, manca la volontà: gli interessi in gioco sono enormi. Gli algoritmi sono scatole nere piene di segreti aziendali ferocemente custoditi. Se tutti potessero accedervi, molte società sarebbero sommerse da reclami, e dovrebbero rinunciare al business. Ma se non interveniamo pagheremo un prezzo molto più alto di una bibita in lattina».

Vito Tartamella