Il dato è mio ma non lo gestisco io

Le informazioni che la Rete "ascolta" dicono tutto di noi anche se non sappiamo bene a chi. Eppure in Europa la legislazione sulla privacy è avanzata e spesso siamo noi («Accetto. Accetto. Accetto») a elargire con leggerezza il consenso

DI **ELENA MONTOBBIO**

È tutta una questione di bite e byte. Un apparecchio per i denti e l'unità di misura della memoria di computer e smartphone. Cosa li lega? La mia osteopata. Da anni soffro di mal di schiena e per provare a prevenire alcuni disturbi mi è stato consigliato di prendere in considerazione un bite e di guardare online i diversi modelli disponibili. Detto fatto. Meno di 24 ore dopo il mio cellulare squilla; la chiamata arriva da Albenga, Liguria. Al telefono una gentile signora dall'accento straniero mi propone servizi dentali in cliniche private dell'Albania. Pensano a tutto loro, viaggio e soggiorno inclusi. Stupita della tempestività chiedo come abbia fatto a reperire il mio numero di telefono: «Tramite alcuni banner presenti su siti che lei ha visitato», ammette candidamente. Rifiuto le offerte di trasferta e provo a richiamare il numero – nessuno risponde – lo cerco su internet e corrisponde a quello di un negozio di Savona che vende motori per barche.

Come è possibile? La domanda è stata posta ad Andrea Ciappesoni, Dpo (Data Protection Officer) ed esperto di Cybersecurity, che da settembre 2019 ha lanciato il sito *bugfixing.it* per aiutare aziende e privati a mettere in sicurezza i propri sistemi e la mole di dati che trattano. Il tutto in conformità con le nuove regole europee previste dal GDPR (General Data Protection Regulation) entrato in vigore in tutti gli Stati dell'Unione europea dal maggio 2018. «Sicuramente», ha spiegato Ciappesoni, «visitando un sito di bite hai dato il consenso ad alcuni cookies di profilazione dell'utente; hanno poi incrociato i tuoi dati personali con account mail o Google e sono arrivati ad avere il cellulare. Il numero di telefono di Albenga invece è virtuale, non esiste davvero».

Ciappesoni, che ama definire il suo team di BugFixing "hackers etici" – esperti di cybersecurity e ingegneri che studiano gli hackers e le tecniche che utilizzano per attaccare siti, aziende e devices – racconta come ormai i dati siano il «nuovo petrolio». Vale per i dati e ancora di più per i metadati, secondo Edward Snowden, il genio dell'informatica del North Carolina ora esule in Russia per aver denunciato le società di intelligence made in Usa di aver violato la Costituzione e la privacy dei cittadini americani.

Le informazioni che generiamo possono svelare tutto di noi. Cosa ci piace, cosa guardiamo, con chi parliamo, dove abbiamo dormito e a che ora ci siamo svegliati. E tutte queste informazioni hanno un valore economico. Perché possono orientare le scelte commerciali e politiche con algoritmi in grado di fare analisi predittive e pilotare il voto. Per Google, Amazon, Facebook, e alcune società di marketing la raccolta di dati (tranne per alcune eccezioni svelate anche da Snowden) avviene alla luce del sole e tramite il nostro consenso autorizzato ("Accetto, Accetto, Continua, Accetto" digitiamo tutti i giorni quando navighiamo in Rete), ma le principali compravendite avvengono nel deep web, la patria degli hacker e degli scambi illeciti. «Si va da pochi centesimi a parecchie migliaia di euro. Oggi sono spesso i dati sanitari posseduti dagli ospedali a essere rubati, oppure si possono trovare liste di password per violare siti internet o account privati», continua il fondatore di BugFixing. Perché come lui stesso ammette, la sicurezza totale non esiste. Tutti i sistemi sono "bucabili", è solo questione di tempo. Un serio attacco lanciato per trovare una password ci mette qualche secondo per identificarne una composta da sei cifre (un milione di possibilità) e solo qualche ora se abbiamo aggiunto anche il nome di una persona. Proteggersi vuol dire quindi creare sistemi di allerta, sentinelle che monitorano il confine dei sistemi, usare la crittografia per far diventare i dati illeggibili e rendere la vita degli hacker (quelli veri che per un'ora di lavoro possono chiedere centinaia di migliaia di euro) più complessa.

Con l'entrata in vigore del GDPR, però, è diventato un obbligo per le aziende lavorare sulla sicurezza per proteggere la privacy degli utenti. Ma la nuova legge europea, spiega ancora Ciappesoni, «è spesso vista dagli imprenditori come l'ennesimo fardello burocratico e molte volte ci si riduce ad aggiornare l'informativa o poco più, trascurando che il GDPR è l'unica normativa che punisce per «insufficienti misure di sicurezza» (art. 32) con multe fino a un massimo di 20 milioni di euro o al 4 per cento del fatturato globale in caso di multinazionali». Marriott International Inc è stata sanzionata dal garante britannico per 110 milioni di euro a seguito di un incidente informatico notificato nel novembre 2018 che ha esposto a rischi i dati personali di circa 339 milioni di ospiti; British Airways per 223 milioni dopo che il sito web della compagnia è stato hackerato e il traffico deviato verso un sito fraudolento che ha raccolto i dettagli di circa 500mila clienti.

A livello globale l'Europa ha cercato di fare un balzo in avanti per la difesa della privacy e delle libertà personali vietando, tra le altre cose, il trasferimento dei dati dei suoi cittadini fuori dal Vecchio Continente a eccezione di quei Paesi che hanno un regolamento simile al nostro (una decina in tutto). Oltre a tutta l'Africa, nella lista mancano Stati Uniti, Cina e Russia reputati dal garante europeo come Paesi che non trattano i dati personali con la dovuta sicurezza. Ma allora Amazon, Google, Alexa, Facebook e LinkedIn che tutti i giorni accumulano dati su dati di ciascuno di noi? Per loro esiste il Privacy Shield, una sorta di scudo per la salvaguardia delle nostre informazioni personali, un elenco pubblico di tutte quelle società americane che hanno aderito ad alcune condizioni inderogabili per l'Europa per poter aver accesso ai dati dei suoi cittadini o di chiunque transiti sul nostro territorio.

La raccomandazione (elementare ma non scontata) è quella di leggere tutte le voci che comportano il nostro consenso. Non ci può essere un automatismo nel nostro assenso, ogni passaggio demanda alla società che gestisce il servizio un nostro diritto. Ogni volta che accettiamo di esporre i nostri dati «stiamo firmando un vero e proprio contratto», mette in guardia Ciappesoni, un accordo scritto che il Garante fa firmare ai cittadini europei perché reputa che le informazioni che vengono raccolte siano sensibili e meritino un'autorizzazione informata e ragionata. Ma quante persone leggono davvero le pagine e pagine di condizioni di uso di Alexa dove c'è scritto nero su bianco che i dati vengono registrati su un Cloud per profilare meglio l'utente, che la società può modificare a sua discrezione qualsiasi termine del contratto pubblicando le nuove condizioni sul sito di Amazon e che per disabilitare la registrazione delle nostre conversazioni bisogna seguire una procedura? E chi si mette in casa un frigorifero in grado di sapere cosa mangiamo, darci consigli sulle ricette e ordinare la spesa con un comando vocale, sa a quale azienda privata sta vendendo i dati sui suoi usi e consumi? E chi è il proprietario dei server su cui questi dati sono salvati?

Snowden, che difficilmente potrà camminare ancora sul suolo americano senza finire in un carcere federale per tradimento, ha le idee chiare al riguardo, come scrive in *Errore di sistema*: «Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire. O che la libertà di stampa non ci interessa perché non ci piace leggere». Peccato che ormai quello che diciamo, cosa leggiamo e chi siamo è già salvato in un archivio dentro un bunker da qualche parte nel mondo... ■

Nella fotografia, un uomo riflesso nel monitor mentre partecipa a un allenamento presso Cybergym, un centro di addestramento alla "guerra informatica" gestito dalla Israel Electric Corporation, a Hadera, una città sulla costa tra Tel Aviv e Haifa.

Contrasto