Altro che privacy, ecco come un compratore di dati scopre la vostra identità

Due ricercatori hanno comprato dei pacchetti di "dati di navigazione in forma anonima" per dimostrare quanto è facile risalire alle informazioni degli utenti

Tre milioni di cittadini tedeschi con la **cronologia web spifferata**potenzialmente ai quattro venti: sono solo la punta di un iceberg che la ricerca compiuta dal giornalista Svea Eckert e dal data scientist Andreas Dewes vuole descrivere al resto del mondo nel corso della conferenza Def Con di Las Vegas dedicata al mondo dell'hacking, per dimostrare quanto **le nostre identità siano facilmente tracciabili** in Rete.
La coppia si è finta un'agenzia di marketing in cerca di grandi pacchetti di dati di navigazione in forma anonima, da fornire in pasto ai propri algoritmi di intelligenza artificiale per educarli a tracciare profili di consumatori quantomeno attendibili. Tanto le è bastato per riuscire a

rivolgersi con successo a un data broker, un soggetto specializzato nell'acquisizione e nella rivendita di questi pacchetti di dati, dal quale **ha acquisito un database di tre miliardi di url** visitati nell'ultimo mese dai già citati tre milioni di utenti.
Le cronologie sono state vendute prive delle informazioni personali dei loro proprietari, ma questo non ha impedito a Eckert e Dewes di dimostrare la loro tesi: una volta in possesso di una mole del genere di dati, per quanto siano stati resi anonimi, diventa facile **incrociarli per risalire a chi li ha generati**. Mettere insieme tutti gli indirizzi visitati da uno stesso dispositivo dipinge infatti un quadro piuttosto completo non solo sulle abitudini dell'individuo che lo possiede, ma ne rivela potenzialmente anche nome e cognome.
Chiunque visiti la propria pagina su Twitter Analytics ad esempio si ritrova il proprio nome utente direttamente nell'indirizzo internet, e quindi nella cronologia; per svelare l'identità di altri può bastare incrociare la pagina web del cinema di zona visitato più spesso insieme al sito di home banking, al meteo e ai profili Facebook più sbirciati. Sono operazioni che non possono (ancora) essere svolte del tutto in automatico, ma che **in alcuni casi possono rivelarsi fruttifere**: il duo in questo modo ha raccontato di aver potuto ricostruire le preferenze di un giudice in fatto di video a luci rosse e di essere risalito alle prescrizioni mediche di un parlamentare.
Per rimanere al sicuro da simili raccolte indiscriminate di dati dovrebbe essere sufficiente **fare attenzione ai plugin installati sul proprio browser**. Il database acquisito da Eckert e Dewes è stato infatti compilato a partire da una serie di strumenti del genere, uno dei quali – ironicamente – si chiama Web of Trust e offre protezione e anonimato nella navigazione Internet. Il plugin in questione è gratuito e, come molti altri della categoria, per mantenersi in attività **vende proprio questo genere di informazioni** al miglior offerente; i suoi tentativi di rendere anonime le cronologie acquisite però lasciano evidentemente a desiderare.