Il lato nell’ombra delle politiche di Apple

- Giovanna Branca, 13.11.2021

Big Tech e sorveglianza. Gabriele Ientile di Privacy Network spiega l’ambivalenza della compagnia fondata da Steve Jobs nella raccolta dei dati degli utenti

Una legge federale sulla privacy che sia significativa e completa dovrebbe puntare non solo a consentire ai consumatori il controllo dei propri dati, ma anche a gettare una luce su coloro che trafficano con i loro dati dietro le quinte». Così scriveva il Ceo di Apple Tim Cook sul *Time* nel 2019, perorando la causa di una legge sulla privacy che regoli il mondo big tech. E in questa direzione sembra essersi mossa la compagnia fondata da Steve Jobs nel corso degli anni, per esempio nell’ultimo aggiornamento di iOS (il 15) che ha introdotto nuovi strumenti *privacy friendly*. Apple però è il Giano bifronte dei dati e dalla sorveglianza: se da un lato celebra pubblicamente una politica di protezione degli utenti, è anche uno dei più grandi “raccoglitori” di dati, anche sensibili, del mondo high tech. Ne abbiamo parlato con il responsabile legale di Privacy Network, Gabriele Ientile.

La quantità di dati che Apple raccoglie sugli utenti è sconfinata.
Il solo fatto di avere un dispositivo orientato alla privacy – ed è vero che Apple lo è più di Android – non basta: bisogna stare attenti alle app che si installano, individuare sempre quali sono quelle che raccolgono meno dati. E su questo va detto che con iOS 15 Apple ha fatto un buon lavoro: per la prima volta gli utenti hanno la possibilità di disabilitare il tracciamento per molte app e sono stati introdotti i *privacy label*, delle etichette che sullo store indicano, per ogni app, quali dati raccoglie e a quale fine (Privacy Network sul proprio sito ha una guida essenziale, *Privacy kit*, dove vengono indicati alcuni software consigliati, *ndr*). Ma in fondo Apple si comporta esattamente come ogni altra big tech, il cui mantra è quello di raccogliere dati. Non è necessario sapere per cosa serviranno nellimmediato, solo averne il più possibile. Non a caso si paragonano i dati al petrolio: accumularne in gran quantità, il più possibile eterogenei e dettagliati può essere sempre utile per un’azienda che si muove nell’economia digitale. Per sviluppare nuove tecnologie come per attività lesive della privacy: le informazioni personali possono essere sfruttate per l’advertising, su cui si basa il grosso dell’economia di Facebook e Google.

Apple però si è sempre posta, all’esterno, come una compagnia che protegge la privacy degli utenti.
Apple ha trovato nella privacy un modo per perseguire i propri obiettivi, o meglio un unico obiettivo – quello di ogni azienda: il profitto. La tutela della privacy è legata al suo modello di business, che a differenza di quello di Facebook e Google – che ruota intorno all’advertising è incentrato principalmente sullo sviluppo di dispositivi. Apple ha capito che ha tutto da guadagnare se migliora le impostazioni della privacy, e limita la quantità di dati che le sue concorrenti riescono a raccogliere. Ne beneficia sotto due profili: una diminuzione degli introiti pubblicitari di Facebook e un aumento dei propri – perché anche Apple seppure in un contesto più piccolo vende pubblicità: sullo store, sull’app di notizie e quella musicale. La seconda ragione per cui lo fa è che si rivolge a una nicchia: vende moltissimi dispositivi ma è un marchio di lusso, ed è stato studiato che a essere disposta a spendere per la privacy è la fascia più ricca della popolazione. Da un lato così si fa pubblicità con il suo utente tipo, e al tempo stesso limita le sue concorrenti e migliora le proprie attività di advertising.

Raccoglie però anche dati sensibili come quelli biometrici, e nel corso degli anni ha contribuito a normalizzare la loro raccolta.
Nel *Capitalismo della sorveglianza* Shoshana Zuboff illustra come questa normalizzazione sia una

pratica consolidata all'interno delle aziende big tech: introdurre una tecnologia che all'inizio suscita clamore per la sua invasività, poi smorzare i toni, fare un passo indietro e aspettare qualche mese per lanciare effettivamente le funzioni in questione quando ormai la notizia è stata assimilata. Apple raccoglie una quantità spaventosa di dati biometrici: il riconoscimento facciale, l'impronta digitale Quello di uno smartphone è un ambito limitato ma nel momento in cui noi non sappiamo dove finiscono i dati di un dispositivo potrebbe accadere qualunque cosa, specialmente ora che si parla di un loro utilizzo per installare telecamere a riconoscimento facciale, come in Italia stanno pensando di fare a Udine e a Como. Il solo fatto che questi dati esistano è pericoloso. Inoltre la vendita di advertising mirato spesso è collegata alla ricostruzione della personalità emotiva, come è avvenuto nel caso di Cambridge Analytica che utilizzava il modello delle 5 personalità per ricostruire le tendenze delle persone e mostrare loro la pubblicità più adatta. Apple vende tantissimi servizi che possono permettere di ricostruire la personalità degli utenti, non solo i dati biometrici ma anche quelli sulla salute, il sonno, il battito cardiaco, i nostri interessi Un altro elemento che sottolinea la sua incongruenza rispetto alla privacy è il diverso trattamento di utenti e dipendenti: a molti di loro è stato impedito di cancellare gli hard disk dei propri computer, e non è garantita la separazione tra informazioni lavorative e quelle personali. Altra questione molto importante sono gli utenti in Cina, dove Apple non è attenta alla privacy come in Europa e negli Usa. Ai data center dove sono conservati i dati degli utenti cinesi, secondo alcune accuse, possono avere accesso alcuni funzionari governativi. Non sappiamo quanto sia vero, ma è senz'altro coerente con il fatto che l'azienda ha bisogno di sfruttare il lavoro a basso costo in Cina e questo potrebbe essere il prezzo da pagare.

Il processo di normalizzazione del capitalismo della sorveglianza potrebbe venire applicato anche a un nuovo strumento sviluppato da Apple, che ne ha per ora sospeso la distribuzione dopo le polemiche che ha suscitato: quello per individuare contenuti pedopornografici fra le foto degli utenti.

L'intercettazione delle immagini è stata introdotta da un regolamento europeo, che per la prima volta ha permesso alle aziende di effettuare dei controlli per verificare se circolino sulle loro piattaforme materiali pedopornografici. La foto viene sottoposta a quella che viene chiamata funzione di hashing, che consente di confrontare le immagini con un database di immagini pedopornografiche. Con questo sistema, sia Ue che Apple ritengono di poter individuare i contenuti illegali proteggendo la privacy degli utenti. Ma verrebbe comunque inaugurato uno strumento che, usato diversamente, potrebbe rappresentare un sistema di sorveglianza – il cui potenziale di controllo è illimitato. E non risolverà il problema: rischia di togliere all'utente comune la protezione della crittografia end to end, la più sicura nel campo delle telecomunicazioni, mentre il criminale ci metterà pochissimo a spostarsi su un altro sistema, come il protocollo Onion (quello usato sul Dark Web, *ndr*), che gli consenta di nascondersi. E cè anche un problema etico: per far funzionare l'algoritmo l'enorme database di materiale pedopornografico viene convertito principalmente da personale sottopagato, in India e nel sud est asiatico, che passa ore e ore a visualizzare queste immagini con enormi ripercussioni psicologiche.