Comportiamoci bene che il «piccolo fratello» ci spia

di Andrea Granelli

Foaddabiri, ingegnere di Twitter, ha recentemente condiviso sul social network uno screenshot della Privacy Dashboard di WhatsApp dove vengono normalmente elencati gli accessi a microfono e fotocamera. Dabiri mostra che l'app di WhatsApp installata sul suo smartphone ha effettuato numerosi accessi al microfono durante le ore notturne (quando dormiva e quindi non poteva usare il servizio di messaggistica).

Il Ceo di Twitter Elon Musk ha ovviamente cavalcato subito la notizia, affermando che "non ci si può fidare di WhatsApp". Per Meta si tratta di un bug di visualizzazione di Android, ma intanto Musk sfrutta l'occasione per attaccare la piattaforma. E in difesa di Menlo Park si unisce Yann LeCun, una delle figure più autorevoli dell'intelligenza artificiale moderna.

Il tema è purtroppo annoso ed è noto da tempo. Per pescare a caso nella infinita casistica – anche molto articolata per le molte e differenti specifiche – possiamo ad esempio richiamare il caso di alcune foto intime di una ragazza 'rubate' addirittura da Roomba e finite sui social, in un gruppo Facebook, dove mostrano scene di vita domestica, appunto anche intime. Tra queste quelle di una ragazza, in bagno, in maglietta viola e con i pantaloncini abbassati. Risulta che le foto siano state inviate dall'azienda produttrice – iRobot – a una startup che si occupa di intelligenza artificiale (Scale AI). Sono stati proprio i lavoratori di questa azienda a condividere le foto su Facebook. I fatti risalgono all'autunno 2020 in Venezuela, ma sono usciti su media di massa a fine dicembre del 2022.

iRobot, recentemente acquistata da Amazon, si giustifica dicendo che il Roomba "fotografo" è un J7, un modello «di sviluppo» con modifiche hardware e software non presenti nei prodotti di consumo destinati all'acquisto.

Quello che mi interessa sottolineare non sono tanto le possibili implicazioni giuridiche o le eventuali responsabilità, quanto piuttosto la direzione verso cui si stanno muovendo i produttori di tecnologie, che incominciano a introdurre sistemi di osservazione e ascolto in oggetti non considerati "digitali" e parte della vita domestica di tutti i giorni.

Le motivazioni possono essere legittime: ad esempio – nel caso di Roomba – osservare meglio la casa e la sua configurazione per migliorare l'efficacia della pulizia. Sta di fatto che è sempre più probabile che gli oggetti che ci circondano e ci accompagnano nella nostra vita saranno sempre più capaci di osservarci e di ascoltarci, senza che necessariamente noi li autorizziamo a farlo.

Questo problema non verrà facilmente risolto nel breve, anche perché è molto difficile determinare quando accade veramente. Ma le potenzialità ci sono tutte e ciò alimenta i pensieri paranoici e complottisti.

Credo allora che l'approccio più corretto che gli utenti possano avere sia non solo chiedere alla legge il massimo della tutela – lo darei per scontato – ma anche utilizzare due ulteriori accorgimenti: Innanzitutto l'analisi di queste macchine "intelligenti" per capire se ci sono aree di potenziale criticità; sulla rete stanno ad esempio diffondendosi luoghi dove vengono segnalate le eventuali criticità. Questa attività di "disinfestazione digitale" che oramai vediamo come norma nei film di spionaggio è particolarmente importante quando parliamo di temi sensibili che non devono essere condivisi. Dall'altra parte bisognerà abituarsi a una maggiore trasparenza della nostra vita privata, riducendo al minimo i comportamenti di cui ci si potrebbe vergognare. Dobbiamo ricordarci che le nostre tracce digitali stanno proliferando, impronte relative a ciò che facciamo sulla Rete: non solo visitare un sito ma anche commentare in un certo modo, chiedere una certa cosa o manifestare una certa preferenza. Molte di queste tracce non sono accidentali ma dipendono dalla nostra insipienza, in quanto spesso ne autorizziamo la raccolta e l'analisi. Quanti di noi, infatti, leggono i contratti che accettiamo nel momento in cui sottoscriviamo una app gratuita? Oppure quanti ne comprendono tutte le possibili implicazioni?

D'altra parte, l'uso strumentale delle informazioni personali non è una novità digitale. Il rischio della manipolazione si è manifestato da quando l'uomo ha iniziato a comunicare. Come non ricordare una celebre massima attribuita al Cardinal de Richelieu: "Che mi si diano due righe scritte dalla mano dell'uomo più onesto, e ci troverò di che farlo impiccare". Questi comportamenti prudenziali sono particolarmente necessari anche perché una delle problematicità del mondo digitale è che l'innovazione non solo corre molto veloce, ma genera continuamente nuove opportunità il cui impatto – sia positivo che negativo – si capisce solo successivamente, quanto iniziano a diffondersi ed emergono le pratiche d'uso.

Per sua natura, quindi, è una legislazione ex post; il che significa che, anche nel caso ideale in cui la legislazione tuteli nel modo corretto, c'è sempre un intervallo temporale non trascurabile in cui non vi può essere copertura normativa.

photocredit: tashatuvango (stock.adobe.com)