R.it | Sicurezza

Cosa rischiamo se si supera il confine della privacy

Viviamo già nell'età dell'oro della sorveglianza. Andare oltre sarebbe un colpo mortale alla sicurezza di tutti

di JUAN CARLOS DE MARTIN

Stampa

19 febbraio 2016

I due killer di San Bernardino (ansa)

DOPO mesi di confronti riservati, lo scontro tra il governo americano e i giganti digitali è diventato pubblico, anzi, plateale. Apple ha, infatti, rifiutato di eseguire l'ordine di un giudice federale riguardante l'accesso all'iPhone di uno dei due attentatori di San Bernardino. I dati dell'iPhone, infatti, sono "oscurati" da tecnologie crittografiche che, senza l'aiuto di Apple, l'Fbi non è in grado di penetrare.

La decisione di Apple - spiegata online da una lettera di Tim Cook - ha trovato il consenso degli amministratori delegati di Google e di WhatsApp, oltre che delle associazioni a tutela dei diritti civili come l'Aclu e la Electronic Frontier Foundation.

Cosa sta capitando?

È fuori di dubbio che grazie alla crittografia - una tecnologia ormai utilizzabile da chiunque - è possibile rendere dati (per esempio i file di un computer) o comunicazioni (per esempio uno scambio in chat) inaccessibili a terzi. Questo fatto ha spinto esponenti delle forze dell'ordine a parlare - fin dall'inizio degli anni '90 - del rischio di una "discesa nell'oscurità" di potenziali malfattori. Rischio di cui si è tornati a parlare con insistenza in questi ultimi due anni, dopo che alcune aziende, tra cui proprio Apple, reagendo alle rivelazioni di Edward Snowden, hanno cominciato a inserire nei loro prodotti tecniche crittografiche molto avanzate.

Ha ragione l'Fbi? Apple e altre aziende stanno irresponsabilmente dotando potenziali assassini, mafiosi e terroristi di strumenti inaccessibili alla giustizia?

No, secondo un gruppo di esperti della Harvard University le cose non stanno così. Nel rapporto pubblicato a inizio mese e significativamente intitolato: "Non facciamoci prendere dal panico " ("Don't Panic") gli esperti americani (tra cui esponenti di altissimo livello delle agenzie di sicurezza Usa) sottolineano, infatti, che è opportuno considerare la situazione nel suo complesso e non solo lo specifico fatto che alcune comunicazioni possono essere rese impenetrabili dalla crittografia.

E la situazione nel suo complesso - già oggi, ma ancor più in futuro - è più convincentemente descrivibile come un'età dell'oro della sorveglianza più che l'età della "discesa nell'oscurità".

I motivi principali sono quattro.

Il primo è che oggi, a differenza di 25 anni fa, quando è cominciato questo dibattito, ciascuno di noi indossa un dispositivo di tracciamento in tempo reale della propria posizione, noto anche come telefono cellulare. Ne sono derivati enormi benefici per le forze dell'ordine.

Il secondo motivo è che anche se il contenuto di una comunicazione è inaccessibile a causa della crittografia, le informazioni su chi sta chiamando chi, in quale momento e da quale luogo - i cosiddetti metadati - sono invece generalmente accessibili, aiutando molto il contrasto di attività illecite. Il terzo motivo a sostegno della tesi che viviamo nell'età dell'oro della sorveglianza è che oggi su ciascuno di noi esistono innumerevoli database digitali - dai dati dei social network a quelli finanziari, dalle email agli Sms - che, messi insieme, forniscono un quadro estremamente dettagliato della nostra vita.

Il quarto motivo è che la comunicazione può anche essere crittografata, ma se si riesce ad accedere, con un apposito software di sorveglianza o con una tradizionale intercettazione ambientale (entrambe regolate per legge e approvate da un giudice), allo smartphone o al computer che trasmette o riceve i dati, il gioco è fatto: basta registrare le attività della tastiera (o del microfono, altoparlante, schermo).

Di contro, l'indebolimento della crittografia, come implicito nella richiesta dell'Fbi a Apple o come esplicitamente previsto dalle iniziative di alcuni governi, come quello inglese, sferrerebbe un colpo mortale alla sicurezza di tutti. Come dice, infatti, il noto esperto di sicurezza Bruce Schneier, non è tecnicamente possibile progettare un sistema di sicurezza che funziona solo per persone con una certa cittadinanza o con una determinata moralità: una volta indebolita la crittografia per favorire l'accesso al nostro governo, anche altri governi - magari assai meno democratici del nostro - potranno prima o poi entrare dalla stessa porta, per non parlare di criminali e altri malintenzionati.

Non facciamoci, dunque, prendere dal panico: l'oscurità non sta calando.

Ci saranno, questo sì, angoli più o meno bui. Ma le risorse per gettare fasci potenti di luce non sono mai state così ampie. Così ampie, anzi, da porre il problema - soprattutto con la diffusione della internet delle cose - di come preservare i benefici della rivoluzione digitale senza una pericolosa e generalizzata riduzione della nostra privacy.

Divisione Stampa Nazionale — Gruppo Editoriale L'Espresso Spa - P.Iva 00906801006 — Società soggetta all'attività di direzione e coordinamento di CIR SpA