

UE, tutte le chat saranno esaminate in cerca di pedopornografia



Meno di un anno fa, [Apple](#) annunciò che avrebbe inserito nei propri prodotti una funzionalità che, analizzando i contenuti dei dispositivi e confrontandoli con materiale pedopornografico noto ([CSAM, Child Sexual Abuse Material](#)), avrebbe dovuto consentire l'individuazione di quanti fanno traffico di questo genere di contenuti.

Subito si levarono le voci di quanti, pur condividendo il fine dichiarato da Apple, non potevano fare a meno di rilevare come in questo modo un'azienda privata ottenesse il diritto di curiosare all'interno dei dispositivi degli utenti, violando sistematicamente la privacy e, naturalmente, esponendo chiunque al rischio di diventare un "falso positivo".

La reazione fu talmente decisa che Apple tornò sui propri

passi, e la cosa sembrò finire lì. Invece, l'idea deve essere piaciuta molto alla Commissione Europea, che ha avanzato una nuova proposta di regolamentazione comunitaria che riprende e rende ancora più invasiva la sorveglianza immaginata da Apple.

La [proposta](#) contiene tutta una serie di obblighi per i «*fornitori di servizi online*» e in particolare per quanti gestiscono i servizi di comunicazione e messaggistica, quali WhatsApp, Telegram, Signal e via di seguito.

In base alla proposta, dovrà essere condotta una scansione continua dei messaggi scambiati dagli utenti alla ricerca non soltanto di materiale pedopornografico noto – e quindi rilevato perché confrontato con un database esistente – ma anche di contenuti che gli algoritmi di [machine learning](#) potrebbero considerare come tale.

Anche il contenuto dei messaggi di testo sarà analizzato: l'[algoritmo](#) dovrà valutare se, in ogni conversazione, esistano per esempio gli estremi per un caso di adescamento di minore.

Se i riscontri saranno positivi, il sistema automatico avviserà le autorità della nazione in cui si trova l'utente sospettato, le quali potranno a quel punto emanare un «*ordine di individuazione*», che dovrà essere – spiega la Commissione – «*mirato e specifico*» per violare il meno possibile la privacy dei cittadini dell'Unione.

Nonostante le rassicurazioni, molti esperti di questioni legate a riservatezza e sorveglianza sono già in allarme: «*È una vergognosa legge di [sorveglianza](#) indegna di una qualsiasi libera democrazia*» [ha commentato](#) Jan Penfrat, di EDRI (European Digital Rights).

Il professore di crittografia Matthew Green ha rincarato la dose, [affermando](#): «*Questo documento è la cosa più spaventosa che abbia mai visto. Propone un nuovo sistema di sorveglianza di massa che leggerà i messaggi di testo privati, non per rilevare CSAM, ma per individuare l'"adescamento"*».

Uno dei problemi della proposta – rileva Ella Jakubowska, di EDRi – è che gli ordini di cui parla la Commissione *possono* essere mirati, ma non c'è alcun obbligo in merito. *«Lascia completamente spalancata la porta che conduce a una sorveglianza molto più generale».*

Non dovrebbe nemmeno essere necessario spiegare come tutto ciò comporti inoltre la fine della [crittografia](#) end-to-end, non vietandola ma vanificandola: ed è facile prevedere che ciò accadrebbe a cascata in tutto il mondo, non soltanto nell'Unione Europea.

«Non esiste alcun modo per fare ciò che la proposta della UE vuol fare senza consentire ai governi di leggere ed esaminare i messaggi degli utenti su vastissima scala» spiega Joe Mullin, della Electronic Frontier Foundation. *«Se diventasse legge, questa proposta sarebbe un disastro per la privacy non soltanto nella UE, ma in tutto il mondo».*

È ancora Ella Jakubowska, infine, a sottolineare un ulteriore pericolo, che già era stato rilevato quand'era Apple a voler esaminare il contenuto di [iPhone](#) e [iPad](#): quello, già citato, dei falsi positivi.

Allora, il pericolo poteva quantomeno considerarsi ridotto poiché il confronto delle immagini e dei video scovati sui dispositivi avveniva con materiale che sicuramente era definibile come pedopornografico. Nel caso della proposta della UE, invece, il giudizio spetta alla IA.

«Già c'è stato un sollevamento quando Apple suggeriva qualcosa di simile per trovare gli CSAM noti» spiega Jakubowska. *«Se adesso aggiungiamo ambiguità e situazioni che dipendono dal contesto, in cui gli strumenti basati sulla IA sono notoriamente inaffidabili, le sfide diventano molto più grandi. Basta vedere quanto sono imprecisi i [filtri](#) antispam. Sono in circolazione da 20 anni, ma quanti ancora si trovano dello spam nelle caselle di posta e si vedono classificare*

come posta indesiderata email legittime? Già questo mostra tutti i limiti della tecnologia».

«L'intera proposta si basa su qualcosa di infattibile, se non proprio impossibile, dal punto di vista tecnico» conclude l'esperta di EDRI. E non si riesce a nascondere il sospetto che una motivazione nobile – la lotta alla pedopornografia – venga usata come grimaldello per far passare una sorveglianza pervasiva con ben altri scopi.