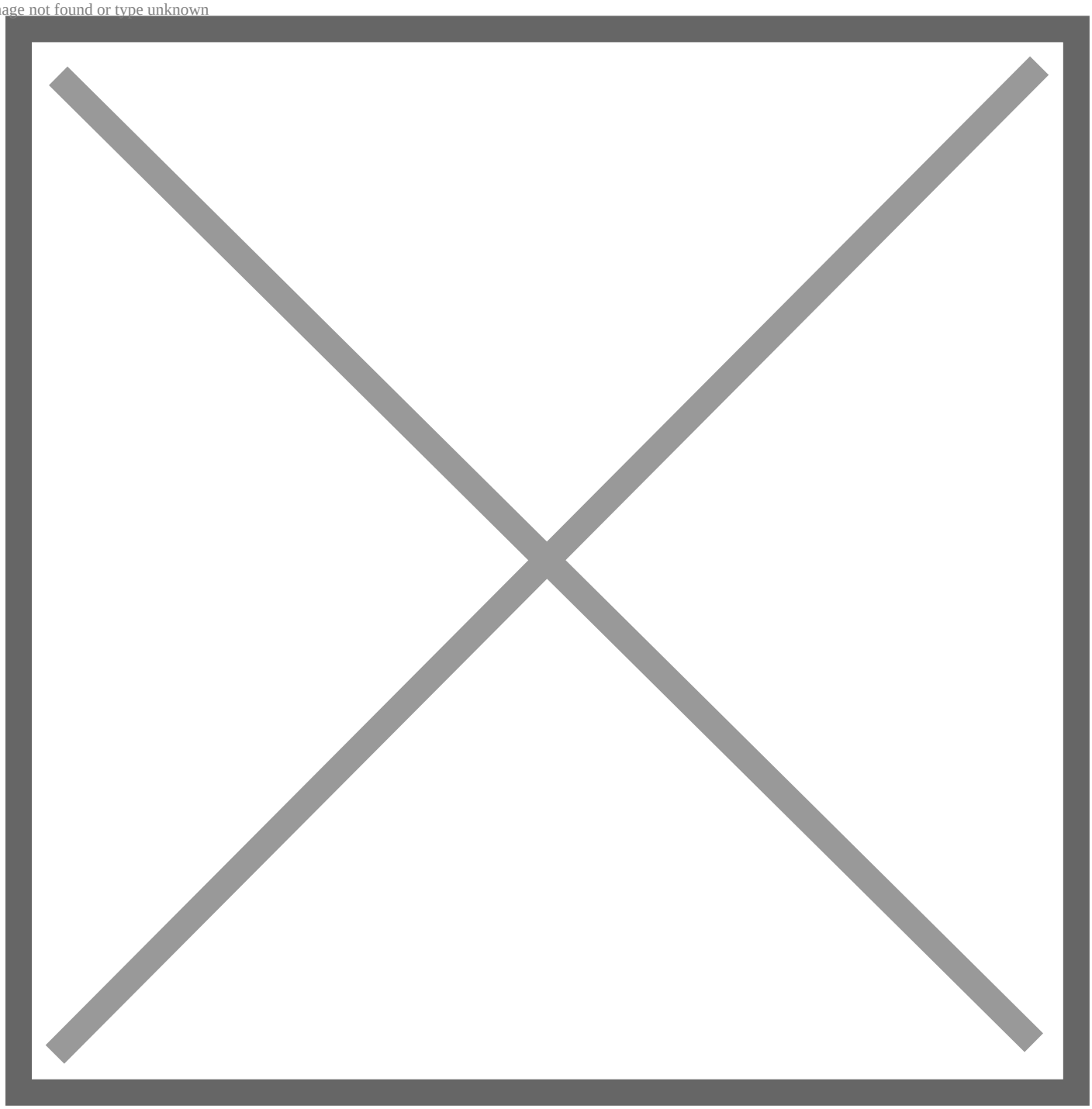
Image not found or type unknown



TECNOLOGIA E DIRITTI

Londra: Starmer vuole i dati degli utenti. Apple resiste (giustamente)

ECONOMIA 15_02_2025

Tim Cook (ad di Apple) al 10 Downing Street (La presse)

Daniele Ciacci

Image not found or type unknown

Il governo britannico ha recentemente avanzato una richiesta senza precedenti ad Apple: accedere ai dati crittografati degli utenti nel cloud attraverso l'Investigatory Powers Act (IPA). Questa mossa solleva serie preoccupazioni sulla privacy digitale e sulla sicurezza dei dati, posizionando il Regno Unito in una zona grigia tra l'approccio che la società americana ha adottato in merito: uno più garantista negli Stati Uniti, uno più invasivo in Cina.

La richiesta si concentra sul servizio Advanced Data Protection (ADP) di Apple, che utilizza la crittografia end-to-end, rendendo i dati accessibili solo al proprietario dell'account. Alcuni esperti di cybersecurity, tra cui il Professor Alan Woodward dell'Università del Surrey, hanno espresso forte preoccupazione per l’iniziativa del Regno Unito. Il motivo è molto semplice: creare una "backdoor" per il governo significa inevitabilmente creare una vulnerabilità sfruttabile da attori malintenzionati.

Lisa Forte, esperta di cybersecurity dell'azienda Red Goat, evidenzia un paradosso fondamentale: i criminali e i terroristi, obiettivo dichiarato di questa iniziativa, semplicemente si sposteranno su altre piattaforme e su diverse tecniche, lasciando i cittadini rispettosi della legge privi della loro privacy. È come installare una porta di servizio in un edificio blindato: una volta creata, diventa un punto debole potenzialmente sfruttabile da chiunque ne scopra l'esistenza.

Il confronto internazionale è illuminante. Gli Stati Uniti hanno ripetutamente tentato di forzare Apple a sbloccare dispositivi in casi specifici, come nel 2016 dopo una sparatoria di massa a Dallas e nel 2020 per un caso simile. In entrambe le occasioni, Apple ha resistito con fermezza, considerando la privacy un diritto fondamentale non negoziabile. L'FBI ha dovuto trovare metodi alternativi per accedere ai dispositivi specifici, preservando l'integrità generale del sistema di sicurezza.

All'estremo opposto troviamo la Cina, dove il controllo governativo sui dati degli utenti è prassi consolidata. Le aziende tecnologiche operanti nel paese sono obbligate a fornire accesso ai dati su richiesta, creando un precedente pericoloso che il Regno Unito sembra ora voler seguire, seppur in forma più limitata, anche in Europa.

La posizione di Apple è stata finora inequivocabile: la società ha dichiarato che preferirebbe ritirare i servizi di crittografia dal mercato britannico piuttosto che compromettere la sicurezza dei suoi utenti. Tuttavia, l'IPA si applica a livello mondiale a qualsiasi azienda tech con presenza nel mercato britannico, rendendo questa soluzione potenzialmente inefficace.

Privacy International ha definito questa mossa un "attacco senza precedenti" ai dati privati degli individui, avvertendo che potrebbe incoraggiare regimi repressivi a fare richieste simili. La questione va oltre la semplice privacy: riguarda il delicato equilibrio tra sicurezza nazionale e diritti individuali nell'era digitale.

Il dilemma è complesso: mentre alcune organizzazioni sottolineano il ruolo della crittografia nel facilitare abusi sui minori, gli esperti di sicurezza informatica avvertono che indebolire la crittografia non fermerà i criminali, ma esporrà milioni di utenti comuni a rischi significativi.

La sfida lanciata dal Regno Unito ad Apple rappresenta un momento cruciale nella storia della privacy digitale. Se il governo dovesse prevalere, potrebbe creare un precedente pericoloso, aprendo la strada a richieste simili anche da parte di altri paesi. La questione non è se le backdoor verranno scoperte e sfruttate da attori

malintenzionati, ma quando ciò accadrà, mettendo a rischio la sicurezza digitale di milioni di persone.