

“ L'intervista **Alessandro Del Ninno**

«La legge Usa non è chiara interverrà la Corte suprema»

ROMA Avvocato Alessandro Del Ninno, lei si occupa tutti i giorni di tutela della privacy e tecnologie informatiche, ci spiega cosa accade negli Stati Uniti e perché la Apple si rifiuta di collaborare alle indagini?

«Questo caso torna su un punto particolarmente attuale. Già nell'agosto dello scorso anno una interessante lettera al New York Times del procuratore capo di Manhattan, quello di Parigi, del capo della polizia di Londra e del capo della Corte suprema spagnola, sollevava il caso dicendo che l'utilizzo della crittografia sta ostacolando le indagini in generale e quelle sul terrorismo in particolare. In realtà qui ci troviamo in un caso ancora più specifico. Il giudice qui non chiede solo di esibire i dati, ma di costruire un nuovo software, di modificare il firmware del cellulare in questione in modo che la Fbi possa fare tentativi illimitati di immettere la giusta password e aprire il cellulare, bypassando la cancellazione automatica al decimo tentativo». **Perché Apple si oppone?**

«Prima di tutto l'azienda ha comunicato che questo software al

momento non esiste, la Apple non ce l'ha. Da settembre 2014, l'azienda ha adottato per tutti i nuovi prodotti una crittografia full disk, per garantire la totale privacy e totale controllo dei propri dati attraverso una tecnologia che neanche il produttore può bypassare e lo stesso farà Android. Apple teme che dopo questo ordine di creare un software per aprire questo cellulare di una generazione leggermente precedente, si chieda di modificare anche i nuovi prodotti, lasciando una cosiddetta backdoor agli investigatori per accedere ai dati».

Non potrebbero semplicemente aprire questo cellulare così importante?

«No, perché neanche loro hanno la password, quando l'utente la sceglie nemmeno il produttore può conoscerla».

Il danno alle indagini però c'è. In tempi di terrorismo internazionale è davvero giusto tutelare la privacy a qualunque costo?

«Dal punto di vista filosofico, è una questione di scelte. E' vero che le indagini possono essere danneggiate, ma è altrettanto ve-

ro che in alcuni casi, come dimostra la vicenda Snowden, l'uso massiccio di dati personali ha dato indubbiamente un messaggio sbagliato. Dal punto di vista legale, mancano legislazioni specifiche. Gli stati di New York e della California hanno proposto una legge che imponga alle aziende di costruire software che in alcuni casi consentano agli investigatori di accedere ai dati. A livello federale, c'è invece una nuova norma in senso opposto. Anche in Euro-



pa non c'è una normativa precisa su questo punto. Un conto è l'esibizione di qualcosa che un'azienda ha, come nel caso di intercettazioni e tabulati, un conto è obbligare l'azienda a creare un software per accedere ai dati».

Quindi in Italia e in Europa ci sarebbe stato lo stesso problema?

«Probabilmente sì, l'obbligo di "facere" come si dice, al momento non è previsto e secondo me sancirlo significherebbe aprire un fronte pericoloso».

Non si rischia di rendere i terroristi o criminali tecnologicamente più attrezzati degli investigatori?

«Il rischio di danneggiare le indagini esiste, anche se teniamo conto che la crittografia è stata a sua volta introdotta per tutelare gli utenti da alcune forme di delinquenza, come il furto di dati o identità. Molto probabilmente a questo punto dovrà intervenire la corte suprema per dirimere il caso».

Sara Menafra

© RIPRODUZIONE RISERVATA

**L'AVVOCATO ESPERTO
DI DATI SENSIBILI
E TECNOLOGIE:
ANCHE IN EUROPA
NON C'È NORMATIVA
IN PROPOSITO**