

Seguici

<https://www.facebook.com/RaiEconomia><https://twitter.com/#!/RaiEconomia>

ECONOMIA

[\(/default.aspx\)](#)

Fotogallery Economia

() ()



Allarme Smog: le 10 città più inquinate al ...



Angela Merkel è la persona dell'anno 2015 ...



I più potenti del mondo secondo Forbes. In ...



Ecommerce in Italia: € ricerca "Let ...

[Tecnologia \(/categorie/tecnologia/1167/1/default.aspx\)](#)

Ti potrebbero interessare

anche...

Sicurezza vs privacy: il caso di San

Bernardino

Mi piace 4

G+1 0

2

<http://www.addthis.com/bookmark.php?v=250&pubid={ra-52a19f7c5da3aa52}>

Apple in cifre: vendite iPhone +35%

Al terzo trimestre

fiscale gli utili di Apple sono arrivati a 10,7 miliardi di ...

<http://www.economia.rai.it/articoli/apple-in-cifre-vendite-iphone-35/30835/default.aspx>

Arriva il nuovo iPhone6

Il 19 settembre l'iPhone 6 e l'iPhone 6 Plus arriveranno in nove Paesi (Usa, Francia, ...

<http://www.economia.rai.it/articoli/arriva-il-nuovo-iphone6/25516/default.aspx>

Cosa ci dicono i numeri di Apple e Facebook

Apple e Facebook hanno diffuso i dati sul bilancio trimestrale. Le due società, ...

<http://www.economia.rai.it/articoli/cosa-ci-dicono-i-neri-di-apple-e-facebook/24733/default.aspx>

SUL PORTALE DI ARTE & DESIGN

<http://www.arte.rai.it>

Steve Jobs

Steve Jobs, padre indiscusso della tecnologia attuale, la sua storia ha conquistato ...

<http://www.arte.rai.it/articoli/steve->

Nell'ultimo mese è stato molto acceso il dibattito sulla vicenda che ha visto contrapposti la Apple e l'Fbi, Cupertino si è opposta alla decisione del giudice federale Sheri Pym di forzare il codice criptato dell'iPhone5 dell'attentatore di San Bernardino, Syed Farook. La vicenda si basa sul fatto che uno dei pilastri del sistema di sicurezza iPhone è che dopo 10 tentativi di accesso al telefono con un Pin errato, tutti i dati contenuti al suo interno vengono automaticamente cancellati. L'intento è chiaro: impedire a chiunque d'impadronirsi con fini illeciti dei dati sensibili di uno smartphone prodotto dalla società di Cupertino. Per questo l'Fbi ha chiesto ad Apple di creare un sistema operativo ad hoc da installare sull'iPhone dell'attentatore per potere avere accesso al dispositivo, illimitatamente. Il tutto è avvenuto facendo appello al **All Writs Act, legge risalente al 1789**, che offre ai tribunali il potere di chiedere aiuto a terzi per i procedimenti giudiziari.

L'amministratore delegato di Apple Tim Cook, ha scritto una lettera (di cui trovate la traduzione integrale in basso), il 16 febbraio rivolta ai propri consumatori, nella quale, pur schierandosi contro ogni forma di terrorismo e mettendosi a disposizione dell'Fbi, si è rifiutata di creare il software richiesto, con la motivazione che se finisse nelle mani sbagliate potrebbe potenzialmente sbloccare ogni iPhone del pianeta, compromettere la sicurezza dei dati personali di tutti gli acquirenti del pianeta, minare l'immagine dell'azienda.

Al fianco di Tim Cook si sono schierati anche l'ad di Google Sundar Pichai e con lui si è mosso con un tweet anche il Ceo di WhatsApp, Jan Koum. L'appoggio a Apple è arrivato anche da Mark Zuckerberg di Facebook, che ha diffuso una dichiarazione: "Continueremo a combattere aggressivamente contro le richieste alle società di indebolire la sicurezza dei loro sistemi". E dal ceo di Twitter, Jack Dorsey. Nel dibattito è intervenuto anche **Andrus Ansip, commissario Ue per il digital single market** che, schierandosi con Apple, ha allargato la questione a settori come l'e-banking e l'e-voting: "Chi si fiderebbe del voto online se sapesse che da una 'porta di servizio' si possono manipolare i risultati delle elezioni? Non deve esserci contraddizione tra la protezione della privacy e la sicurezza dei cittadini".

La lettera di Tim Cook (<http://www.apple.com/customer-letter/>)

Il governo degli Stati Uniti ha chiesto ad Apple di fare un passo senza precedenti, un passo che a nostro avviso mette a rischio la sicurezza dei nostri utenti. Noi ci siamo opposti a questa ingiunzione, poiché avrebbe ripercussioni molto più estese rispetto al caso giudiziario in oggetto. Questi avvenimenti esigono l'avvio di un dibattito pubblico e noi vogliamo che i nostri clienti e tutti i cittadini del nostro paese capiscano a fondo che cosa è esattamente in gioco.

La necessità della cifratura

Gli smartphone, a cominciare dall'iPhone, sono diventati una parte essenziale e irrinunciabile della nostra vita. Gli utenti li utilizzano

[jobs/21939/default.aspx](http://www.economia.rai.it/articoli/sicurezza-il-caso-di-san-bernardino/32629/default.aspx))

SUL PORTALE DI **MEDIA**

(<http://www.media.rai.it>)



Steve Jobs

Steve Jobs, padre indiscusso della tecnologia attuale, la sua storia ha conquistato ...

(<http://www.media.rai.it/articoli/steve-jobs/21939/default.aspx>)

Foto del giorno

Video del giorno

Più visti



([/articoli/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx](http://www.economia.rai.it/articoli/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx))

Sicurezza vs privacy: il caso di San Bernardino ([/articoli/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx](http://www.economia.rai.it/articoli/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx))

Nell'ultimo mese è stato molto acceso il dibattito sulla vicenda che ha visto contrapposti la Apple e l'Fbi, Cupertino si è opposta alla decisione del giudice federale Sheri Pym di forzare il codice criptato dell'iPhone5 dell'attentatore di San Bernardino, Syed Farook. La vicenda si basa sul fatto che uno dei pilastri del sistema di sicurezza iPhone è che dopo 10 tentativi di accesso al telefono ...

Recenti

per immagazzinare una quantità enorme di informazioni personali, dalle nostre conversazioni private a foto, musica, annotazioni, agenda e contatti, dati riguardanti le nostre finanze e la nostra salute, persino dove siamo stati e dove andremo. Tutti questi dati devono essere protetti da hacker e criminali che mirano ad avere accesso ai nostri dati per impossessarsene e servirsene a nostra insaputa e senza il nostro consenso.

I clienti contano sul fatto che Apple e altre aziende tecnologiche facciano tutto il possibile per tutelare i dati personali, e noi della Apple ci siamo impegnati fino in fondo a proteggere queste informazioni. Mettere a repentaglio la sicurezza delle nostre informazioni personali equivale a mettere a rischio la nostra stessa sicurezza. Ecco perché la cifratura è un aspetto cruciale del nostro mestiere. Per molti anni, abbiamo utilizzato il criptaggio per proteggere i dati personali dei nostri clienti, perché siamo convinti che questo sia l'unico modo per garantire la sicurezza di tali informazioni. Abbiamo deciso persino di **immagazzinare questi dati fuori dalla nostra stessa capacità di accesso**, perché crediamo che il contenuto del vostro iPhone non ci riguarda minimamente.

Il caso di San Bernardino

Come tutti i cittadini di questo paese, anche noi siamo rimasti sconvolti dal barbaro attentato di San Bernardino, lo scorso dicembre. Lamentiamo anche noi la perdita di vite umane e reclamiamo giustizia per tutte le vittime. **Nei giorni successivi al massacro, l'FBI ha chiesto il nostro aiuto, e noi abbiamo lavorato giorno e notte per contribuire agli sforzi dello stato per risolvere questo caso agghiacciante.** Non abbiamo nessuna simpatia per i terroristi. Quando l'FBI ci ha chiesto di consegnare i dati in nostro possesso, li abbiamo forniti. Apple ha onorato i mandati di comparizione e di perquisizione, anche nel caso di San Bernardino. Abbiamo inoltre messo a disposizione dell'FBI i nostri ingegneri per fornire assistenza, e abbiamo dato il nostro contributo alle varie ipotesi investigative al vaglio degli inquirenti. Nutriamo il massimo rispetto per i professionisti dell'FBI e siamo convinti della bontà delle loro intenzioni.

Fino ad oggi, abbiamo fatto tutto quanto è stato in nostro potere di fare, entro i limiti della legge. Oggi però il governo americano ci ha chiesto qualcosa che noi non abbiamo, qualcosa che secondo noi presenta un rischio elevatissimo: ci hanno chiesto di installare una porta di servizio al nostro iPhone, la cosiddetta backdoor. Per scendere nei particolari, l'FBI ci chiede una nuova versione del sistema operativo dell'iPhone per aggirare alcune importanti funzioni di sicurezza, per installarla sull'iPhone che è stato recuperato nel corso delle indagini. Nelle mani sbagliate, questo software – che ancora non esiste oggi – avrebbe la capacità di sbloccare qualunque iPhone capitato tra le mani di qualcuno. L'FBI usa parole diverse per definire questo strumento, ma la realtà è questa: creare una versione di iOS capace di aggirare le funzioni di sicurezza in questo modo equivale a installare una porta di accesso secondaria. E mentre il governo sostiene che il suo utilizzo sarebbe limitato a quest'unico caso, non abbiamo alcun modo per garantire tale controllo.

La minaccia alla sicurezza dei dati



(/articoli/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx)

Sicurezza vs privacy: il caso di San Bernardino

Nell'ultimo mese è stato molto acceso il dibattito sulla vicenda che ha visto ...



Bce: abbassa tutti i tassi, QE sale a 80 miliardi

(/articoli/bce-abbassa-tutti-i-tassi-qe-sale-a-80-miliardi/32612/default.aspx)

Per rispondere ad un quadro macroeconomico dell'eurozona in visibile peggioramento, ...



Guardia di Finanza: ecco i dati del Rapporto annuale

2015

(/articoli/guardia-di-finanza-ecco-i-dati-del-rapporto-annuale-2015/32600/default.aspx)

Tutelare l'economia legale e le imprese rispettose delle regole, garantendo allo ...



Al posto tuo: così web e robot ci stanno rubando il

lavoro

(/articoli/al-posto-tuo-cosi-web-e-robot-ci-stanno-rubando-il-lavoro/32598/default.aspx)

Le macchine hanno sempre rimpiazzato gli uomini. Prima però lo facevano nei compiti ...



L'economia globale dal 1980 al 2015, in un video

(/articoli/leconomia-globale-dal-1980-al-2015-in-un-video/32584/default.aspx)

La liberalizzazione economica, la globalizzazione e l'aumento della multinazionali ...

Alcuni sostengono che creare una porta di servizio per un unico iPhone rappresenta una soluzione semplice e ben delimitata. Ma chi afferma questo ignora sia le basi della sicurezza digitale che le possibili conseguenze di ciò che il governo ci chiede. Nel mondo digitalizzato di oggi, la “chiave” di un sistema di criptaggio è quell’informazione che sblocca i dati, e la sua sicurezza dipende dalle protezioni da cui è stata circondata. **Una volta resa nota questa informazione, o non appena viene rivelato il modo per aggirare il codice, il criptaggio potrà essere annullato da chiunque sia in possesso di quelle conoscenze.**

Il governo assicura che tale strumento verrebbe utilizzato un’unica volta, su un unico iPhone. Ma non è vero. **Una volta creata, la tecnica potrebbe essere riprodotta in modo illimitato**, su un numero infinito di supporti. Nel mondo reale, sarebbe l’equivalente di un passe-partout, o chiave primaria, capace di aprire centinaia di migliaia di serrature – dalle banche ai ristoranti, dai negozi alle case private. Nessuno può accettare una simile ipotesi. Il governo chiede ad Apple di violare i telefoni dei nostri stessi utenti e di annullare decenni di innovazioni nel campo della sicurezza a protezione dei nostri clienti – tra cui decine di milioni di cittadini americani – dagli attacchi di sofisticati hacker e di cyber criminali. Gli stessi ingegneri che hanno inserito nell’iPhone potenti sistemi di criptaggio per proteggere i nostri utenti sarebbero costretti, paradossalmente, a indebolire quelle protezioni e a mettere a rischio la loro sicurezza. **Nella nostra storia non esiste precedente di un’azienda americana alla quale venga chiesto di esporre i suoi clienti al pericolo di attacchi informatici.** Per anni, i crittologi e gli esperti di sicurezza nazionale ci hanno ammonito dei pericoli in agguato per le falle nei sistemi di criptaggio. Acconsentire alla richiesta del governo significherebbe danneggiare unicamente i cittadini rispettosi della legge che fanno affidamento sulla Apple per la protezione dei loro dati. Hacker e criminali continueranno a criptare, utilizzando gli strumenti a loro disposizione.

Un precedente pericoloso

Anziché seguire l’iter legislativo tramite il Congresso, l’FBI propone di appellarsi all’**All Writs Act del 1789** per giustificare l’espansione del suo raggio di azione. Il governo ci chiede di annullare funzioni di sicurezza e aggiungerne di nuove al sistema operativo, consentendo di inserire un codice elettronicamente. Questo consentirebbe di “forzare” l’accesso ai dati di un iPhone, tramite la selezione di migliaia o milioni di combinazioni alla velocità di un moderno computer. Le possibili conseguenze della richiesta del governo americano sono spaventose. Se il governo può ricorrere all’All Writs Act per sbloccare il vostro iPhone, allora potrà intrufolarsi negli smartphone di chiunque per catturare i loro dati. Il governo potrebbe estendere questa violazione della privacy e costringere Apple a creare un software di sorveglianza per intercettare i vostri messaggi, carpire i vostri dati sanitari o finanziari, scoprire dove vi trovate, e persino catturare suoni e immagini a vostra insaputa.

La nostra opposizione agli ordini del governo non è stata una scelta alla leggera. **Noi abbiamo il dovere di far sentire la nostra voce davanti a quello che consideriamo uno**

sconfinamento dei poteri da parte del governo americano. Se impugnamo le richieste dell'FBI, lo facciamo con il massimo rispetto per la democrazia americana e per amore del nostro paese. Noi crediamo fermamente che è negli interessi di tutti fare un passo indietro e riflettere sulle possibili ripercussioni. Seppur convinti della bontà delle intenzioni dell'FBI, riteniamo sbagliato che il governo ci imponga di creare una backdoor nei nostri prodotti mobile, perché temiamo giustamente che tale richiesta vada a minacciare quelle stesse libertà che il nostro governo ha il compito e il dovere di proteggere.

Alessandro del Ninno - avvocato e professore universitario - esercita a Roma come Of Counsel dello Studio legale Tonucci & Partners. E' specializzato nei settori Information & Communication Technology, Data Protection, Proprietà Intellettuale e Industriale, Telecomunicazioni e Diritto dei Consumatori. <http://www.alessandrodelninno.it/>
(<http://www.alessandrodelninno.it/>)

Tags

[apple \(/cerca.aspx?s=apple\)](#)[fbi \(/cerca.aspx?s=fbi\)](#)[iphone \(/cerca.aspx?s=iphone\)](#)[privacy \(/cerca.aspx?s=privacy\)](#)[san bernardino \(/cerca.aspx?s=san bernardino\)](#)[tecnologia \(/cerca.aspx?s=tecnologia\)](#)[tim cook \(/cerca.aspx?s=tim cook\)](#)

Condividi questo articolo

[Mi piace](#)

4

[G+1](#)

0

2

(<http://www.addthis.com/bookmark.php?v=250&pubid={ra-52a19f7c5da3aa52}>)

Inserisci il codice nel tuo articolo

```
<iframe width="630" height="500" src="http://www.economia.rai.it/embed/sicurezza-vs-privacy-il-caso-di-san-bernardino/32629/default.aspx"
```

Ultimi Tweets

Tweet di @RaiEconomia



Rai Economia
@RaiEconomia

#Sicurezza vs #privacy: il caso di #SanBernardino ow.ly/ZqFgl #Apple #FBI #timcook #iPhone



[Incorpora](#)

[Visualizza su Twitter](#)

Attività recenti



Rai Economia

Mi piace questa Pagina 4,7t

Di' che ti piace prima di tutti i tuoi amici



Rai Economia

37 minuti fa

Sicurezza vs privacy: il caso di San Bernardino

[Avv. Alessandro del Ninno](#)

Tag Cloud

[pensioni \(/cerca.aspx?s=pensioni\)](#)

[disoccupazione \(/cerca.aspx?s=disoccupazione\)](#)

[lavoro \(/cerca.aspx?s=lavoro\)](#)

[economia \(/cerca.aspx?s=economia\)](#)

[Renzi \(/cerca.aspx?s=Renzi\)](#)

[Draghi \(/cerca.aspx?s=Draghi\)](#)

[Bce \(/cerca.aspx?s=Bce\)](#)

Social Media



(<http://www.economia.rai.it/rss.aspx>)

RSS
Subscribe



(<https://twitter.com>)

[/#!/RaiEconomia](#)

Followers



(<https://www.facebook.com>)

[/RaiEconomia](#)

4.734
Fans



(<https://plus.google.com>)

[/112282616066052204167/posts?rel=author](#)

NaN
Fans

(<http://www.teche.rai.it/>)

IN COLLABORAZIONE CON



Rai Economia

Direttore: Silvia Calandrelli

Rai Storia (<http://www.raistoria.rai.it/>) | Rai Scuola (<http://www.raiscuola.rai.it/>) | Rai Letteratura (<http://www.letteratura.rai.it/>) |
Rai Arte (<http://www.arte.rai.it/>) | Rai Filosofia (<http://www.filosofia.rai.it/>) | Rai Media (<http://www.media.rai.it/>) |
Rai Economia (<http://www.economia.rai.it/>) | Rai Scienze (<http://www.scienze.rai.it/>) | Rai Italiano (<http://www.italiano.rai.it/>) |
Grande Guerra (<http://www.grandeguerra.rai.it/>) | Rai 5 (<http://www.rai5.rai.it/>)



Rai - Radiotelevisione Italiana Spa
Sede legale: Viale Mazzini, 14 - 00195 Roma
Cap. Soc. Euro 242.518.100,00 interamente versato
Ufficio del Registro delle Imprese di Roma
© RAI 2015 - tutti i diritti riservati. P.Iva 06382641006

Privacy policy (<http://www.rai.it/dl/rai/text/ContentItem-5a0d5bc3-9f0e-4f6b-8b65-13dd14385123.html>) | [Cookie policy](#)
(<https://www.iubenda.com/privacy-policy/844946/cookie-policy>) | Società trasparente (<http://www.rai.it/societatrasparente>)

Engineered by Rai Digital