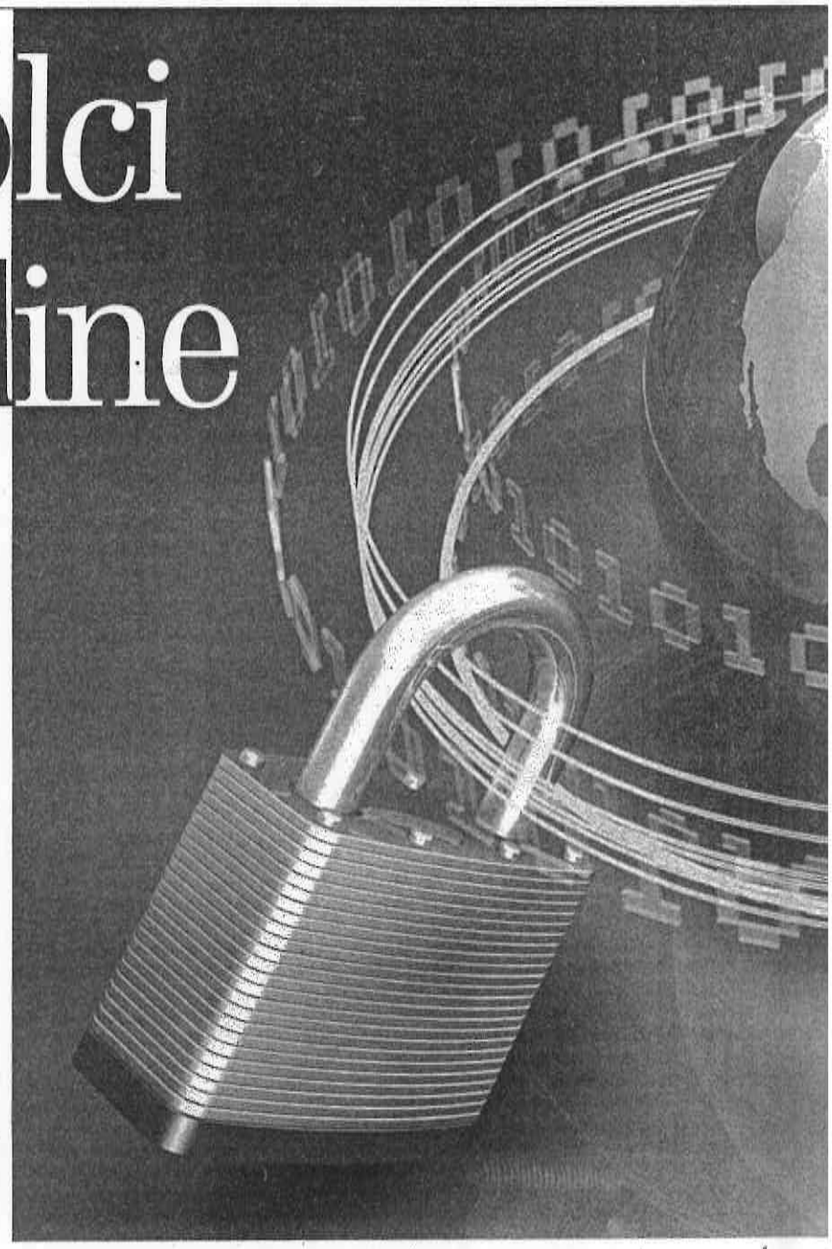
CODICI APERTI

Le tecnologie dolci del controllo on line



Daniele Pizio

«Per Apple, la vostra fiducia è tutto». Firmato Tim Cook. È quanto sostenuto dal Ceo di Cupertino in una lettera apparsa il 17 settembre sull'homepage della mela morsicata, contestualmente al rilascio di iOS 8 e all'aggiornamento delle *policy* aziendali in fatto di privacy. A pochi giorni dalla presentazione di iPhone 6, il successore di Steve Jobs si è lanciato in un'operazione trasparenza con cui ha inteso ribadire l'impegno della compagnia nello sviluppo di tecnologie privacy oriented.

IOS 8, l'ultima versione del sistema operativo montato dai «melafonini», presenta infatti una serie di nuove funzionalità concepite appositamente per garantire una maggior sicurezza alle comunicazioni e ai dati personali dell'utente. Un esempio è l'introduzione della *full disk encryption*: una sorta di cassaforte virtuale che protegge le informazioni archiviate all'interno di un iPhone e che può essere aperta solo dal proprietario del dispositivo con una password da lui impostata. Un sistema di cifratura blindato, che la stessa Apple non potrebbe scardinare, nemmeno di fronte ad eventuali richieste di collaborazione da parte di forze di polizia e agenzie di *law enforcement* impegnate in indagini penali.

Apple e Google hanno annunciato che i loro prodotti e servizi saranno rispettosi della privacy. Un proposito in palese contraddizione con il modello di business delle due major della Rete. Lo sostengono giuristi, mediattivisti e esperti in sicurezza informatica. Sullo sfondo l'amara realtà del diritto alla riservatezza ormai ridotto a merce pregiata

Un diffuso scetticismo

Non passa neppure un giorno e Google, principale concorrente di Cupertino nel mercato degli smartphone, annuncia che non sarà da meno. Dalla prossima versione di Android (nome in codice *L*) «la cifratura verrà abilitata automaticamente - ha dichiarato il portoavoce Niki Christoff -. I nostri clienti non dovranno neppure pensare a come attivarla».

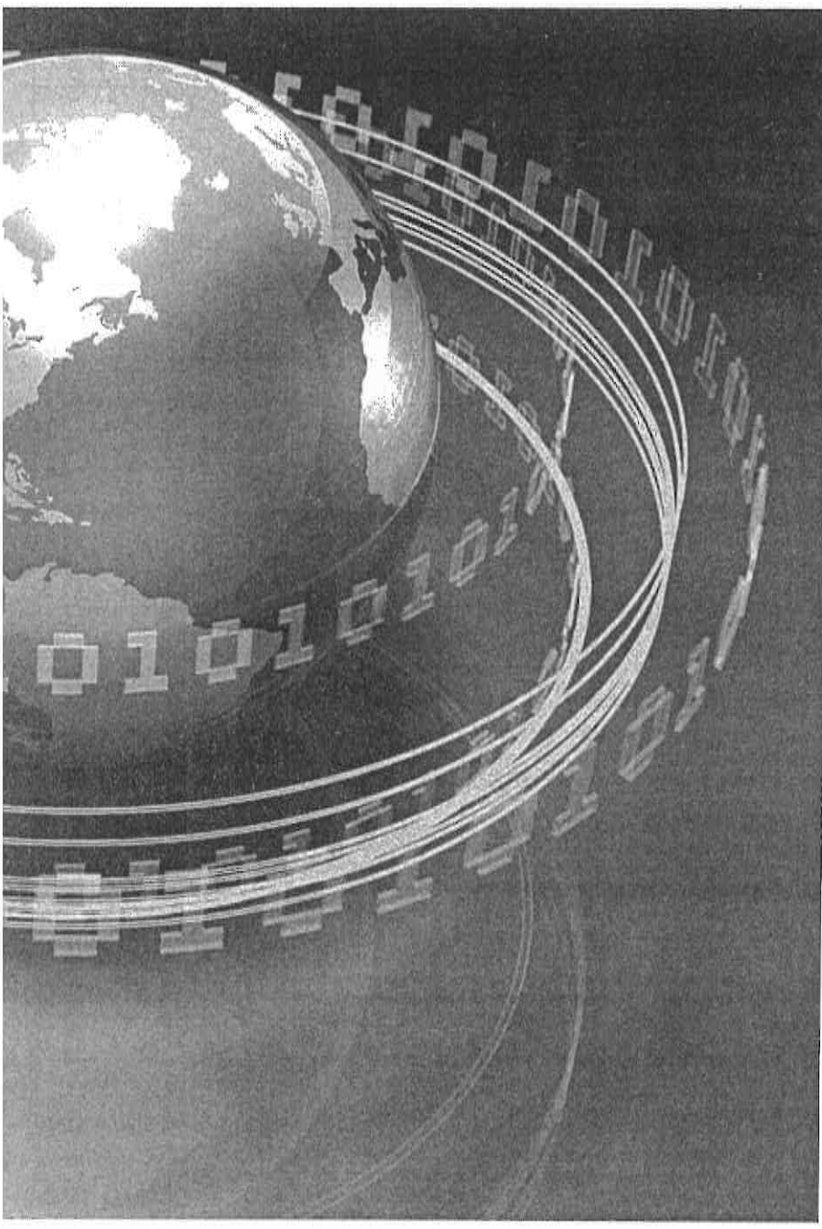
Nonostante le promesse sbandierate a mezzo stampa da Christoff e le solenni dichiarazioni di intenti fatte da Cook, lo scetticismo serpeggia tra gli addetti ai lavori. «Non vedo che interesse dovrebbe avere Google a rendere i suoi servizi *privacy enabling* - sostiene Claudio Nex Guarnieri, esperto di sicurezza informatica e attivista per i diritti digitali -. È contro il suo modello economico». Una larga fetta degli introiti di Big G deriva infatti dalla vendita di pubblicità personalizzate, ritagliate a misura d'utente, grazie a un costante monitoraggio delle sue attività on-line. E per quanto riguarda Apple? Il giudizio di «Nex» non cambia di molto. Sebbene il ricercatore ammetta che «i miglioramenti introdotti da iOS 8 siano interessanti», queste sono tutt'altro che una panacea ai mali del tecno controllo dilagante. Milioni di persone utilizzano infatti in maniera assolutamente inconsapevole servizi come iCloud, un software che replica in modo automatico sui server di Cupertino fotografie, filmati, rubriche e messaggi di testo contenuti nelle memorie di iPhone e iPad. «Apple può accedere a quei dati in qualsiasi momento e per qualsiasi motivo. E per quanto mi riguarda - conclude Guarnieri - resta un partner del progetto Prism».

Il declino del Silicon Valley Consensus

Nutrono perplessità simili anche i mediattivisti di Av.A.Na (acronimo di *Avviso Ai Naviganti*), storico Hacklab del centro sociale Forte Prenestino di Roma. «Rispediamo l'invito di Cook al mittente. Perché mai dovremmo fidarci?». Gli hacker capitolini in particolare puntano il dito contro la chiusura dei sistemi operativi targati Apple e Google: «per definizione un sistema sicuro deve essere analizzabile». In altre parole, il suo codice sorgente deve essere disponibile allo scrutinio di quegli sviluppatori intenzionati a revisionarlo per scovarvi eventuali malfunzionamenti o vulnerabilità. Ios non soddisfa questa condizione, Android solo parzialmente.

C'è poi un altro problema: l'hardware, ovvero le componenti fisiche del cellulare, che gli smanettoni del Forte definiscono «un colabrodo». Già, perché «la rete telefonica non solo fornisce un tracciamento dettagliato degli spostamenti e delle relazioni di ogni individuo, ma i circuiti collegarvisi sono in grado di scavalcare ogni precauzione adoperata dal sistema operativo». Fantascienza? Niente affatto. Si tratta di un'ipotesi già verificata a febbraio dai ricercatori della *Free Software Foundation*.

Che il *Silicon Valley Consensus* sia colato a picco dopo il Datagate non è un mistero. Proprio quest'estate un rapporto presentato dal *New America Foundation's Open Technology Institute* aveva evidenziato come la fine della privacy individuale fosse solo una delle conseguenze della sorveglianza di massa. Altrettanto significativa risulta-



va essere la perdita di credibilità dell'industria tecnologica statunitense. Un danno d'immagine con ricadute direttamente economiche, dato che «per Google ed Apple la fiducia degli utenti è un bene da preservare - spiegano gli hacker di Av.A.Na. - Non dimentichiamoci che queste aziende traggono profitto dalle nostre comunicazioni, dai dati che immettiamo sulle loro piattaforme. Se smettiamo di farlo perché la loro reputazione crolla, alla lunga anche i loro bilanci potrebbero fare la stessa fine. Un utente spensierato invece comunica di più. E quindi produce di più».

Un escamotage cosmetico

E in questo senso, oltre alle rivelazioni di Edward Snowden, non sembra aver giovato neppure il cosiddetto scandalo *Fappening*. Il 31 agosto centinaia di foto esplicite sono state indebitamente sottratte dagli account iCloud di vip e personaggi del mondo dello spettacolo per poi essere riversate in rete. Tra le vittime anche la modella Kate Upton e l'attrice Jennifer Lawrence: celebrità internazionali a cui basta un tweet per influenzare i gusti e le preferenze commerciali di milioni di consumatori.

Adeguatamente contestualizzata, la «svolta» di Mountain View e Cupertino sembra quindi più un escamotage cosmetico che un effettivo tentativo di rafforzare la privacy dei propri utenti: una strategia di marketing dispiegata per tranquillizzare i clienti e allineare il brand aziendale ai timori di un pubblico globale, turbato dallo stillicidio quotidiano di notizie che testimonia la progressiva dissoluzione di ogni sfera d'intimità.

Nel solco tracciato da un bisogno di riservatezza sempre più diffuso e palpabile, si fa strada poco alla volta un nuovo trend economico. Giorno dopo giorno prende piede un vero e proprio mercato della privacy, chiamato a fare le veci di quegli strumenti giuridici tradizionali dimostratisi inadeguati a difendere l'individuo dallo sguardo pervasivo dell'occhio elettronico.

Non si contano più ormai le app per smartphone, vendute con la promessa di tutelare le comunicazioni degli utenti da orecchie indiscrete; impazzano i *blackphone* (telefonini spacciati come dispositivi a prova di intercettazione); nascono addirittura iniziative di *crowdfunding* per finanziare capi di abbigliamento fatti con tessuti in grado di schermare tablet e cellulari.

Che tali prodotti siano soluzioni efficaci conta fino a un certo punto: il loro valore risiede piuttosto negli immaginari che sono in grado di veicolare. La lotta al Grande Fratello diventa un business e può essere intrapresa semplicemente acquistando un gadget su Ebay. «Da questo punto di vista - affermano gli hacker di Av.A.Na - la privacy sta ormai diventando una moda». Google ed Apple l'hanno capito bene. «Queste multinazionali, insieme ai loro prodotti, vendono un sistema fideistico di valori da loro stabilito. Come se fosse un software, lo aggiornano ogni volta che lanciano sul mercato un nuovo sistema operativo o un nuovo telefono». Il risultato, concludono, è che «l'autonomia dell'individuo si riduce ad una scelta acritica tra prodotti».

La corsa alla crittografia

Ma la guerra commerciale tra Apple e Google è anche spia di profonde mutazioni che stanno investendo le fondamenta giuridiche del concetto di sicurezza. «In passato questa veniva considerata prioritaria rispetto alla privacy - spiega l'avvocato Fulvio Sarzana, esperto di diritto dell'informazione -. Si trattava di una nozione di tipo collettivo e la sua formulazione era una prerogativa delle istituzioni statali». Dopo il Datagate sono però intervenute trasformazioni di tipo tecnologico e normativo che hanno messo in discussione la validità di tale assunto. La corsa alla crittografia nell'industria tecnologica, la sua adozione da parte di milioni di persone, l'acuirsi della crisi di legittimità degli attori politici tradizionali; tutti elementi che indicano come l'idea di sicurezza vada sempre più declinandosi su un piano individuale. Essa non è più codificata dal legislatore, ma erogata sotto forma di servizio da un'impresa privata cui viene corrisposto un compenso economico. Stesso discorso vale per la privacy. «Pensiamo a quanto accade intorno al tema del diritto all'oblio - dice il giurista -. Anche in quel caso Google svolge un ruolo monopolistico: è solo lui a stabilire come e quando concederlo». Lo spostamento di competenze da entità statali a sovrastatali si fa completo, «così come si sposta anche la questione della tutela individuale del cittadino: oggi è necessario capire come difendersi dagli abusi di potere delle grandi corporation, oltre che da quelli dello Stato». Perso il monopolio di privacy, perso anche quello della sicurezza, al vecchio Leviatano, sostiene Sarzana, «non rimane che quello della repressione».