

Il Datagate mette a rischio crittografia e libertà

Con la scusa di proteggere la privacy nascono servizi "a prova di NSA". Inutili e pericolosi provocheranno l'effetto opposto.



Un effetto collaterale del Datagate è lo sfruttamento spregiudicato dell'isteria da "violazione della privacy" per vendere posta elettronica e accesso alla rete protetti da sistemi crittografici. A parte alcune evidenti eccezioni (transazioni commerciali, dati sanitari, informazioni giudiziarie) si tratta di servizi inutili, privi di reale efficacia e, soprattutto, pericolosi per l'individuo e la collettività.

Sono inutili, perché rendono più complicato usare il PC e introducono ulteriori potenziali problemi nel funzionamento quotidiano. La conseguenza è che dopo un po' verranno abbandonati, magari maledicendo il giorno in cui si è scelto di utilizzarli. Provate a cercare informazioni sulle difficoltà create dall'utilizzo di file system cifrati (largamente disponibili per i maggiori sistemi operativi). Scoprirete che diventa paradossalmente indispensabile tenere una copia "in chiaro" dei dati perché il rischio di non accedere più alle informazioni perché è stata smarrita la password o perché un certo software non è supportato dall'upgrade del sistema operativo è troppo elevato.

Sono privi di reale efficacia se usati su larga scala perché per essere sicuri di essere sicuri, dovreste, ogni volta, fare boot da cd con un sistema operativo live, evitare accuratamente di scrivere informazioni su disco prima di avere cifrato il file, memorizzare permanentemente le informazioni solo su *storage* a sua volta cifrato assicurandovi, infine, che nella RAM o altrove non rimangano tracce di quanto avete scritto. Alternative non ce ne sono: la messa in sicurezza delle informazioni è binaria. O la si applica oppure no perché qualsiasi processo meno rigoroso la rende inefficace. E' evidente che il flusso di lavoro necessario per garantire una protezione efficace ai file generati, custoditi e inviati tramite il proprio computer è talmente complesso da non essere sostenibile nell'attività di routine e dunque buon senso vorrebbe

che attività così complesse coinvolgano un insieme limitato di dati.

Inoltre, utilizzando prodotti commerciali a codice chiuso non c'è nessuna reale garanzia di sicurezza perché la realtà del mercato del software dimostra chiaramente che troppo spesso il codice compilato nasconde una quantità inaccettabile di bug ed errori di programmazione. Sono pericolosi perché alimentano una distorta cultura della privacy che porterà, ancora una volta, paradossalmente, se non all'eliminazione, quantomeno alla forte compressione di questo diritto. Come scriveva Clifford Stoll in *High Tech Heretic* pubblicato nel 2000 ben pochi messaggi hanno bisogno della protezione di sistemi crittografici moderni ... la maggior parte della posta elettronica e dei messaggi elettronici è così pedestre che nessuno sprecherebbe una settimana a decifrarli. Ciò nonostante, oggi va di moda includere nei messaggi che si immettono in rete la firma di una chiave pubblica PGP. Questa sigla fa sembrare importante il traffico: qualcuno mi manda un messaggio con un sigillo attaccato. In altri termini, con buona pace di quelli che cercano di "esistere" vivendo perennemente connessi a Facebook, la nostra vita è straordinariamente poco interessante per governi e autorità, mentre lo è moltissimo per aziende e profilatori commerciali. Cioè gli stessi soggetti che, oggi, si lamentano dell'intrusione governativa nei "propri" - notate il virgolettato - dati. In altri termini, le imprese che cifrano il traffico, proteggono il loro business ed evitano le cause fatte dagli utenti. Non sono certo la EFF o Privacy International, nel senso che si "preoccupano" della privacy solo nella misura in cui questo è funzionale al loro business.

Infine, l'utilizzo indiscriminato di crittografia per ogni dove - così come iniziano a proporre gli inefabili "venditori di insicurezza" - farà sì che al primo caso (anche finto) di impossibilità di

arrestare pedofili e terroristi, le aziende "sicure" verranno accusate di favorire i delinquenti. E allora annunceranno "accordi garantisti" con le forze di polizia per l'accesso ai dati in loro possesso, mentre politici e (certi) giuristi - magari per tacitare la piazza volgare e ignorante - invocheranno la messa fuorilegge della crittografia o il suo utilizzo "controllato". Il pendolo, che grazie al Datagate si era spostato verso l'estremizzazione della tutela della privacy, comincia - anzi ri-comincia - a oscillare pericolosamente verso l'estremo opposto.

E la storia ricomincia. Sì, ricomincia, perché il Datagate non è altro se non la versione aggiornata del Clipper Chip (1993) e prima ancora di *Echelon* (1988, ricordate?). Ma, soprattutto, il Datagate è l'erede diretto di Herbert Osborn Yardley, fondatore della *Black Chambers*, l'antenata della NSA. Nel 1920 la scoperta di cosa facesse esattamente questa struttura provocò la reazione sdegnata dell'allora presidente americano, Hoover, che nel tagliarle i fondi dichiarò: *I gentiluomini non leggono la posta altrui!* Evidentemente, però, il presidente Hoover e i suoi successori cambiarono idea, oppure definirono in modo diverso il concetto di "gentiluomo" così da essere moralmente giustificati quando davano ordine di "intromettersi" nella vita privata di quelli che non rientravano nella "categoria".

Seguendo questa linea di ragionamento si potrebbe concludere, allora, che hanno ragione i governi a fare quello che fanno. Se i network di intercettazione globale esistono da decenni e nessun cittadino è stato deportato in Alaska o "suicidato" allora, tutto sommato, vuol dire che "possiamo fidarci". Il ragionamento è suggestivo, ma sbagliato. I governi sono fatti di persone, le persone cambiano e, soprattutto, si comportano secondo le proprie convinzioni morali - sulla base del *do the right thing* - piuttosto che secondo la legge. Quindi è semplicemente stupido pensare che i grandi poteri smetteranno di raccogliere informazioni su chiunque o che una qualche legge possa impedire a chi ha le risorse per farlo di ficcanasare nella vita privata di qualcun altro.

L'unico modo per conservare un segreto è non dirlo a nessuno. D'altra parte, come scriveva nel XVII secolo François de La Rochefoucauld, come possiamo pretendere che qualcuno protegga i nostri segreti, se noi stessi non siamo stati in grado di farlo?