Lettori: n.d.
Diffusione: n.d.
nòva 24
Dir. Resp.: Roberto Napoletano
07-LUG-2013
da pag. 9

Internet a mandata doppia

Con il datagate c'è chi propone la crittografia di massa. Una strada percorribile ma solo mettendo a rischio l'economia del web

Sala: «L'elevata qualità dei servizi è possibile solo grazie all'elaborazione-dati»

di **Alessandro Longo**

Forse non ci resta che confidare nella crittografia di massa per proteggere i nostri dati, ergo la nostra libertà, dagli spioni. Governi o multinazionali. Tecnicamente è possibile, praticamente no perché distruggerebbe i fondamenti di internet così come la conosciamo. Questo almeno per ora. Ma fra qualche anno arriverà una nuova forma di crittografia, "omomorfa", in grado di proteggere i dati lasciandoli al tempo stesso utilizzabili per i servizi.

È il senso di un dibattito che sta crescendo tra gli esperti, a fronte dello scandalo *datagate*. Il noto giornalista Jeff Jarvis l'ha detto con un articolo sul *Guardian*: solo l'avvento della crittografia di massa su tutti i dati personale può salvare la nostra privacy. Le norme infatti si stanno dimostrando obsolete o comunque aggirabili. La stessa Europa, avanguardia mondiale per la privacy, sta avendo grosse difficoltà ad aggiornare la direttiva Data Privacy, risalente al 1995. Ce la dovrebbe fare nel 2014, ma è ancora da vedere se sarà poi in grado di fare rispettare la normativa da governi e multinazionali stranieri (già non ci riesce con le attuali leggi, come ha fatto il giurista Stefano Rodotà commentando il *datagate*).

Le norme invecchiano perché la tecnologia evolve. È grazie al suo sviluppo che le intercettazioni di massa sono possibili. Per due motivi. Primo, perché con la diffusione del digitale le nostre vite lasciano tracce (dati) archiviabili, copiabili e analizzabili dalle macchine. Secondo, perché evolvono gli strumenti hardware (storage, potenza di calcolo) e software (analytics), anche via cloud, che consentono tutto questo. Allora, se le norme sono deboli, dalla tecnologia può arrivare la soluzione così come è arrivato il problema. In pieno spirito internet, l'antidoto al proprio stesso male. Crittografia di massa, quindi, che in teoria può avvenire in due modi: con l'adozione di software da parte degli utenti o con la scelta di provider internet e produttori di browser di integrare la crittografia su tutti i dati. «Passare a una diffusione a tappeto della crittografia in ogni possibile tratta di internet è fattibile, di costo limitato e impedirebbe le intercettazioni a tappeto», dice Massimiliano Sala, direttore del laboratorio di Crittografia all'università di Trento. «Ci potrebbero essere rallentamenti nel traffico, ridotti però grazie all'uso di Hardware security module (che generano le chiavi) di fascia alta. Il problema è che la crittografia di massa metterebbe in ginocchia l'economia di internet», aggiunge. «L'elevatissima qualità dei servizi a cui siamo abituati, la geolocalizzazione ad esempio, è possibile solo grazie alle elaborazioni fatte dai gestori dei servizi, che hanno addirittura inventato dei nuovi algoritmi (big data) proprio per riuscire a gestire e incrociare la mole enorme delle informazioni in loro possesso». «Avere il proprio conto cifrato sul server della banca lo rende inutile: come fa la banca a sommare i soldi in arrivo da un bonifico se non sa quanti soldi avete? Dovrebbe ogni volta mandarvi un avviso di scaricare un file, che decifrate a casa e poi rimandate indietro», continua Sala.

Idem per la pubblicità online, che vive della possibilità di personalizzare il messaggio grazie all'uso dei nostri dati personali. A maggio un gruppo di editori tedeschi ha lanciato l'allarme sui conti perché troppi lettori bloccavano la pubblicità con sistemi come AdBlock. Chi vive di pubblicità online da tempo osteggia i sistemi Do Not Track che, integrati nei browser, consentono di non farsi tracciare dai network. Figuriamoci che possono pensare della crittografia di massa.

«Non credo che vedremo una crittografia di massa. Non è chiaro se gli utenti la supporteranno e l'industria digitale si opporrebbe strenuamente», conferma Karin Von Abrams, analista di eMarketer.

In molti studi sulla privacy online (di Accenture, Microsoft e, in Italia, dell'Università di Salerno) si evince che gli utenti sono sì preoccupati per la riservatezza dei propri dati online, eppure fanno poco per proteggerli. Forse la questione è che mancano ancora due cose: la consapevolezza dell'importanza della privacy e strumenti semplici per difenderla. Entrambi però possono crescere, «è un possibile effetto positivo dello scandalo *datagate*», dice Rodotà. «La sola via d'uscita è la crittografia omomorfa, che renderebbe possibile l'elaborazione di dati cifrati senza aprirli. Purtroppo questi algoritmi sono ancora troppo pesanti e ci vorranno dieci anni ancora per la maturità», dice Sala.

«Lo Stato non potrà mai vietare la crittografia, anche se la Francia ci ha tentato negli anni '80. Perché non si può vietare lo studio della matematica», aggiunge An-

data stampa 32° Anniversario

drea Monti, noto avvocato esperto di questi temi.

Sembra una via almeno da tentare. «Il mondo deve dotarsi di un sistema di diritti forte su internet e una tecnologia che lo garantisca (inclusi i sistemi di crittografia). Altrimenti internet perderà il suo potenziale enorme di democrazia possibile», chiosa Giuseppe Iacono, fondatore di Stati Generali dell'Innovazione.

© RIPRODUZIONE RISERVATA