Di Marco Maglio
Lunedì 16 Luglio 2007 10:10

Mentre la stampa di questi giorni, riprendendo l'allarme lanciato dal Garante per la protezione dei dati personali, presenta al Paese la privacy come una vera "emergenza nazionale", io vado controtendenza e cerco sicurezza nella tecnologia. Penso che, al di là degli allarmismi, bisognerebbe partire dalla realtà per cercare di governarla. Per capirlo basta leggere quello che scriveva oltre dieci anni fa Phil Zimmermann, l'inventore del sistema di criptazione dei dati più popolare del mondo: il PGP (acronimo di Pretty Good Privacy). Mi sembra una lettura illuminante che vale molto di più di mille analisi approfondite per spiegare quali siano i reali termini del problema e quale sia il modo pratico e concreto per affrontarlo."È personale. È privato. E sono solo affari tuoi. Potresti dover pianificare una campagna elettorale, voler discutere delle tue tasse, o avere una relazione segreta. Oppure potresti stare facendo qualcosa che non dovrebbe essere illegale, ma che lo è. Comunque sia, non vuoi che la tua posta elettronica (E-mail) o i tuoi documenti segreti siano letti da nessun altro. Non c'è niente di male nel difendere la tua privacy. La privacy è importante tanto quanto la Costituzione.Forse credi che le tue E-mail sono così sicure che la cifratura non è necessaria. Se sei davvero un cittadino rispettoso della legge senza niente da nascondere, perché non scrivi le tue lettere sulle cartoline postali? Perché non ti sottoponi ad un test della droga se te lo chiedono? Perché richiedi un mandato se la polizia vuole cercare in casa tua? Stai cercando di nascondere qualcosa? Devi essere un sovversivo o un spacciatore se nascondi la tua posta dentro a delle buste. O forse un pazzo paranoide. I cittadini che rispettano la legge hanno bisogno di cifrare le loro E-mail? Cosa succederebbe se i cittadini rispettosi della legge dovessero usare cartoline per mandarsi la corrispondenza? Se qualcuno provasse a rivendicare la propria privacy mettendo le proprie lettere in una busta, sarebbe un sospettato. Forse le autorità aprirebbero le sue lettere per vedere cosa sta nascondendo. Fortunatamente, non viviamo in un mondo come questo, dal momento che tutti proteggono la maggior parte delle proprie lettere con buste. Così nessuno che utilizzi buste normalmente è sospettato. La sicurezza viene dai numeri. Nello stesso modo, sarebbe bello se tutti cifrassero di routine le proprie E-mail, innocenti o non, così

che nessuno che cifrasse le proprie E-mail private fosse sospettato. Pensa a questa come ad una forma di solidarietà.Oggi, se il Governo vuole violare la privacy di normali cittadini, deve spendere un certo ammontare di tempo e denaro per intercettare, aprire, leggere le lettere e ascoltare trascrizioni di intercettazioni telefoniche. Questo tipo di monitoraggio è costoso e non pratico su larga scala. È fatto solo in casi particolari quando ne vale la pena.Sempre più spesso le nostre comunicazioni private viaggiano attraverso canali elettronici. La posta elettronica sta gradualmente rimpiazzando la posta tradizionale. I messaggi E-mail sono incredibilmente facili da intercettare ed esaminare per parole chiave di particolare interesse. Questo può essere fatto facilmente su larga scala, automaticamente per tutti i messaggi senza che nessuno se ne accorga. I cablogrammi internazionali sono già esaminati in questo modo su grande scala dalla NSA (National Security Agency, n.d.T).Stiamo andando verso un futuro dove le nazioni saranno interconnesse con reti di dati in fibre ottiche ad alta velocità, collegando insieme tutti i nostri computer sempre più ubiquitari. Le E-mail saranno la normalità per tutti, non la novità che sono oggi. Il Governo proteggerà le nostre E-mail con protocolli di cifratura da lui stabiliti. Probabilmente la maggior parte delle persone glielo consentirà. Ma forse alcune persone preferiranno utilizzare le proprie misure protettive.Il documento del Senato 266, un documento anticrimine del 1991, ha nascosto nel suo interno una disposizione sconvolgente. Se questo documento non ancora legale diventasse realmente legge, forzerebbe i produttori dei dispositivi di sicurezza ad inserire delle speciali porte di accesso nei loro prodotti, così che il Governo possa leggere i messaggi cifrati di chiunque. È scritto:"È raccomandato dal Congresso che i fornitori di servizi di comunicazione elettronici e i produttori di dispositivi di comunicazione elettronici debbano assicurare che i sistemi di comunicazione permettano al Governo di ottenere i contenuti in chiaro di voce, dati e altre comunicazioni quando propriamente autorizzato dalla legge"Questo provvedimento è stato respinto dopo una severa protesta dei cittadini e gruppi industriali. Nel 1992, la proposta della intercettazione della "Digital Telephony" del FBI e stata introdotta al Congresso. Richiederebbe a tutti i produttori del dispositivi di comunicazione di costruire speciali porte di intercettazione che permettano al FBI di intercettare remotamente tutte le forme di comunicazione elettronica dagli uffici del FBI. Sebbene non ha mai attirato nessun sostenitore nel Congresso nel 1992 per via della opposizione dei cittadini, è stato riproposto nel 1994.Ancora più allarmante è l'ardita iniziativa politica della Casa Bianca sulla cifrazione, sviluppata dalla NSA dall'inizio dell'amministrazione Bush, e rivelato il 16 Aprile 1993. Il nocciolo di questa iniziativa è un dispositivo di cifratura costruito dal Governo, chiamato Clipper chip, contenete un nuovo algoritmo di cifratura segreto della NSA. Il governo sta incoraggiando le industrie private ad inserirlo dentro a tutti i prodotti di comunicazione sicura, come telefoni sicuri, FAX sicuri, e così via. AT&T sta inserendo Clipper nei suoi prodotti vocali sicuri. Ecco il punto: al momento della fabbricazione, ogni chip Clipper sarà associato ad una chiave univoca della quale il governo si farà un copia, per custodirla come garanzia. Niente di cui preoccuparsi, il Governo promette che userà queste chiavi per intercettare il traffico solo se debitamente autorizzato dalla legge. Purtroppo però, per rendere il chip Clipper completamente effettivo, il successivo passo logico sarebbe dichiarare fuorilegge ogni altra forma di crittografia.Se la privacy diviene fuorilegge, solo i fuorilegge avranno la privacy. I servizi segreti hanno accesso a buone tecniche crittografiche. Così come i grandi trafficanti di droga e di armi. Così come industrie del settore difesa, compagnie petrolifere o altri colossi finanziari. Ma la gente comune e le organizzazioni politiche nascenti non hanno mai avuto accesso a tecnologie crittografiche a chiave pubblica di livello militare. Non fino ad ora. PGP permette alla gente avere la loro privacy a portata di mano. C'è un bisogno sociale crescente di questo. Ecco

perché l'ho scritto."Che ne dite? Io ora ho capito perchè ho bisogno di PGP. Torneremo sul tema prossimamente. Stay tuned!