

La sicurezza dei nostri dati personali è in pericolo ogni volta che ci colleghiamo a Internet. Scopriamo quali sono le minacce e cosa possiamo fare per eliminarle o quantomeno minimizzarle.

● Di Dario Orlandi

DIFENDERE LA

PRIVACY



ACRY

ONLINE

Una parte sempre più consistente del lavoro, del tempo libero e dello studio si basa sugli strumenti offerti da Internet; le opportunità di comunicazione, conoscenza e intrattenimento sono quasi infinite, tanto che pochissimi oggi sarebbero disposti a rinunciarvi. Ma ogni volta che visitiamo una pagina Web, leggiamo una mail o acquistiamo un oggetto o un servizio,



sveliamo qualcosa di noi. L'accumulo di queste informazioni permette di tracciare profili molto precisi sui gusti, gli interessi e perfino i problemi (economici, di salute e così via) di ogni navigatore; informazioni preziose, che fanno gola a molti e vengono comprate e vendute ogni giorno. Nelle prossime pagine analizzeremo i rischi principali per la privacy e la sicurezza personale che si corrono online, e cercheremo di individuare gli strumenti e i comportamenti più adatti per minimizzarli.

Vi siete mai chiesti come sia possibile che un sito Web proponga proprio le pubblicità di un prodotto che vi serve, oppure come Amazon sembri leggersi nel pensiero quando invia la newsletter settimanale con gli sconti e le offerte speciali? Questo (e altro) accade perché molte informazioni su di voi non sono più private, e vengono utilizzate per proporvi le pubblicità o i prodotti a cui potreste essere più interessati. La gestione dei dati personali nell'era digitale è un argomento complesso e multiforme. Coinvolge molti attori diversi e varie problematiche, tanto che è difficile fornirne un quadro esauriente. Inoltre, le minacce e i rischi cambiano continuamente, così come mutevoli sono i servizi e le tecnologie che trattano le informazioni sensibili dei navigatori.

INTERNET E LA PRIVACY

Quando si analizzano i comportamenti online, ci si rende conto di come le azioni e gli atteggiamenti siano molto diversi rispetto a quelli tenuti nella vita reale. Fin dalla sua nascita, Internet è stata percepita da molti come una sorta di porto franco, dove le regole comuni non erano in vigore e dove gli utenti erano protetti dall'anonimato. In realtà, invece, è vero l'esatto opposto. Chi naviga sul Web, accede ai social network o semplicemente utilizza un telefono cellulare lascia moltissime tracce, piccoli brandelli di informazione che hanno poco valore e poco interesse se presi singolarmente, ma che invece possono svelare moltissimo se accumulati nel corso del tempo e analizzati in maniera sistematica. Le problematiche relative alla privacy e all'anonimato in Rete sono molte, e di varia natura: la prima, probabilmente la più importante, riguarda la protezione delle informazioni personali, in particolare di quelle sensibili. Ad essa si lega il tema del tracciamento dei comportamenti online: chi avesse accesso alle ricerche effettuate e alla cronologia delle pagine visitate, potrebbe ricavare moltissime informazioni sul

conto di un navigatore: progetti, interessi, stato di salute, opinioni politiche e molto altro ancora. Nella maggior parte dei casi i singoli dati non sono decisivi, a meno che non si riesca a catturare esattamente una particolare informazione (l'acquisto di un farmaco, l'inserimento di un commento in un forum e via di questo passo). L'analisi dei comportamenti online non è quasi mai svolta da persone che controllano il traffico e segnalano eventuali attività sospette, come accade per esempio con le tradizionali intercettazioni telefoniche; è affidata invece ad algoritmi capaci di macinare un'enorme mole di dati, per ricavare informazioni significative e tendenze consolidate.

NAVIGATORI ACCERCHIATI

Chi utilizza un computer, uno smartphone o un tablet per accedere a Internet si trova sostanzialmente accerchiato. Innanzi tutto, esiste il pericolo che le informazioni memorizzate sul dispositivo locale vengano salvate e poi recuperate da remoto; questo è il comportamento di molti malware e spyware, che infestano i computer fin dagli albori dell'informatica di massa. Cambiano naturalmente le tecniche utilizzate e le falle sfruttate per intrufolarsi nei computer, ma il comportamento è quasi sempre lo stesso; i

→ HTTPS

Https (*HyperText Transfer Protocol Secure*) è un protocollo comunemente utilizzato per accedere con una connessione sicura a un server Web. La cifratura dei dati viene gestita dal protocollo Ssl/Tls, che viene applicato automaticamente (sui server che lo supportano) quando viene usato <https://> come prefisso dell'Url della pagina, al posto del tradizionale <http://>.

GOOGLE PUÒ INVADERE POTENZIALMENTE LA PRIVACY DEI SUOI UTENTI?

Secondo Eric Schmidt, presidente del consiglio di amministrazione, non è un grosso problema:

“se non hai nulla da nascondere, non hai nulla da temere”.



malware si rendono invisibili e difficili da eliminare, dopodiché cercano di accedere alle informazioni più sensibili e le trasmettono ai server di comando e controllo remoti. Ma la minaccia non è rappresentata soltanto dai tradizionali malware; chi ha accesso agli apparati di smistamento del traffico della rete locale, per esempio, può facilmente controllare tutto quello che entra ed esce da ciascun computer connesso. In altre parole, l'amministratore della rete locale potrebbe accedere a molte informazioni sensibili.

Una rete locale potrebbe nascondere altre insidie, specialmente se è pubblica (per esempio quelle degli esercizi commerciali o degli aeroporti) o se qualcuno ha modo di introdursi, come può capitare quando è disponibile un accesso Wi-Fi non adeguatamente protetto.

Se le connessioni sono cifrate (per esempio tramite il protocollo **https**) l'impresa diventa molto più ardua, ma esistono varie tecniche pensate per ingannare chi pensa di essere al sicuro, e magari non presta troppa

attenzione alle informazioni mostrate dal browser. Un hacker potrebbe, per esempio, tentare di reindirizzare automaticamente le connessioni https verso le pagine http in chiaro, oppure proporre al client un certificato contraffatto e instaurare una connessione sicura, ma con un server diverso da quello atteso.

CHI CERCA I NOSTRI DATI?

I dati personali sono un bene prezioso che viene comprato e venduto in un mercato molto ricco. Uno degli attori in questo mercato è certamente la criminalità informatica: i dati sensibili sono venduti da chi li raccoglie, con mezzi quasi sempre illeciti, e acquistati da chi invece vuole utilizzarli per i suoi scopi. Carte di credito, indirizzi di posta elettronica, o numeri dell'assistenza sanitaria (negli Stati Uniti e in altri Paesi che li utilizzano come strumenti di riconoscimento) sono prede ambite e ben pagate.

Varie agenzie di sicurezza, governative e private, vogliono poi conoscere

tutto il possibile su ogni navigatore. Le informazioni private sono utili non solo per la prevenzione dei crimini, ma anche per l'erogazione di servizi, o comunque per compilare un profilo completo di un utente. Le assicurazioni, per esempio, sono molto interessate a conoscere i dettagli della cartella clinica di un potenziale cliente; i dati sensibili possono tornare utili agli istituti di credito, quando devono decidere se concedere un prestito o un fido, così come ai partner commerciali, prima di siglare un contratto di fornitura. Ma le informazioni private sono preziose anche per altri scopi. Alcune società sono cresciute fino a diventare giganti nel settore IT semplicemente in virtù delle informazioni possedute sui loro utenti.

Uno dei casi più eclatanti, ma certamente non l'unico, è quello di Facebook, che alla fine dello scorso anno ha superato i 200 miliardi di dollari di capitalizzazione. Il principale asset di Facebook è l'archivio di informazioni sui suoi utenti, e la possibilità di raggiungerli con messaggi (tipicamente pubblicitari) mirati.

Spesso chi si preoccupa per le violazioni della privacy è bollato come paranoico, e i fautori della sorveglianza di massa in nome della sicurezza utilizzano un'argomentazione piuttosto comune, ripresa in varie forme nel corso del tempo: “se non hai nulla da nascondere, non hai nulla da temere”. L'ha fatta propria persino Eric Schmidt, presidente del consiglio di amministrazione di Google, che qualche anno fa ha affermato, replicando a chi si lamentava delle possibili invasioni della privacy degli utenti da parte di Google “... se hai qualcosa che non vuoi che nessuno sappia, forse non dovresti farla del tutto...”. Come ha risposto sul suo blog il celebre crittologo ed

Più di 800 milioni di persone utilizzano Facebook ogni giorno. La rete sociale creata da Mark Zuckerberg è di fatto un immenso database di informazioni personali.

informazioni condivise

 TRACKING

Tracking methods that work in your browser. A combination of these can produce "zombie cookies" that are intentionally difficult to delete. Bellow is the result of saving an unique string "l80hr6homl" using various techniques.

HTTP Cookies	Yes	180hrs6homi
Flash Cookies	Yes	180hrs6homi
HTTP ETags	Yes	180hrs6homi
Web cache	Yes *	zdhrrww7x2f
window.name Caching	Yes	180hrs6homi
IE userData	No	-
HTML5 Cached PNGs	Yes *	zdhrrww7x2f
HTML5 Session Storage	Yes	180hrs6homi
HTML5 Global Storage	No	-
HTML5 Local Storage	Yes	180hrs6homi
HTML5 Database Storage	Yes	180hrs6homi
Silverlight Storage	No	-

* Works but saved string is not updating properly.

BROWSER FEATURES

Configuration information may be used by Web sites to create a unique fingerprint of your browser.

Panoptick

How Unique — and Trackable — Is Your Browser?

Your browser fingerprint appears to be unique among the 4,999,105 tested so far

Currently, we estimate that your browser has a fingerprint that conveys at least 22.25 bits of identifying information.

The measurements we used to obtain this result are listed below. You can read more about our methodology, statistical results, and some defenses against fingerprinting in [this article](#).

Help us increase our sample size:

Browser Characteristics	bits of identifying information	one in x browsers have this value	value
User Agent	15.08	34716.01	Mozilla/5.0 (Windows NT 6.2; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.94 Safari/537.36
HTTP_Accept-Header	20.67	1666368.33	text/html,*/*; q=0.8,application/javascript;q=0.6,application/xml;q=0.2

esperto di sicurezza Bruce Schneier “... la privacy ci protegge dagli abusi di chi ha il potere ... [ed è] una necessità umana di base ... Troppi caratterizzano il dibattito come una scelta tra sicurezza e privacy. La vera scelta è tra privacy e controllo. La sorveglianza di massa è la definizione stessa di uno stato di polizia, ed è per questo che dovremmo difendere la privacy anche quando non abbiamo nulla da nascondere”.

ATTENZIONE AL BROWSER

È il programma più utilizzato in quasi tutti i computer e nei dispositivi mobile, e la porta d'accesso principale a Internet: il browser è lo strumento che espone più informazioni sugli utenti, e dev'essere utilizzato con cautela. Le molte tecnologie accumulate nel corso del tempo hanno trasformato un semplice visualizzatore di documenti html in un ambiente programmabile ricchissimo di funzioni, ma anche incredibilmente complesso.

I browser moderni possono eseguire vere e proprie applicazioni, anche molto evolute; per ottenere questo livello di potenza, è necessario un ambiente molto flessibile. Alcune informazioni sugli utenti sono inviate direttamente nell'header della richiesta `http`: ogni volta che il browser si collega con un server remoto, infatti,

invia un pacchetto di dati in cui sono contenute anche alcune informazioni sulle funzioni disponibili e sulla configurazione. Naturalmente, la prima informazione inviata è l'indirizzo IP, necessario al server per sapere dove inviare il pacchetto di risposta. Ma l'IP, in realtà, non è particolarmente rilevante se si utilizza una connessione consumer.

Quasi tutti i provider, infatti, utilizzano IP dinamici, ossia assegnano un indirizzo selezionato a caso in un pool ogni volta che un utente si collega. Un indirizzo IP, quindi, non identifica quasi mai un utente in modo univoco. I provider hanno tutte le informazioni necessarie per risalire all'utente, se si conosce l'indirizzo IP, la data e l'ora della connessione; ma, come abbiamo già accennato, queste informazioni sono di solito protette e vengono comunicate soltanto dietro richiesta dell'autorità giudiziaria. Ma, purtroppo, ci sono molti altri metodi per identificare univocamente gli utenti: insieme all'indirizzo IP del computer, infatti, il browser invia moltissime altre informazioni, utili al server per restituire i dati più pertinenti e utili.

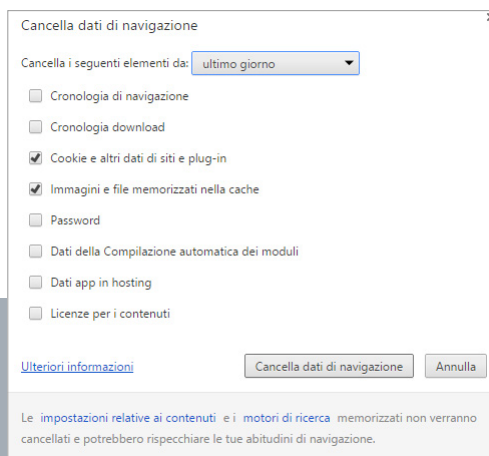
Per fare un esempio banale, il browser comunica la lingua del sistema operativo installato, e il server può così rispondere direttamente con la pagina tradotta nell'idioma dell'utente. I problemi iniziano quando la quantità di informazioni cresce troppo: il browser, infatti, comunica il suo nome e versione, il sistema operativo, la risoluzione dello schermo, la presenza di plug-in e tecnologie specifiche (Flash, Java, Silverlight e così via), l'elenco completo dei font installati e molto altro ancora. Per avere un'idea dei dati inviati dal browser, ed eventualmente per testare l'efficacia dei sistemi di mascheramento, si può visitare l'indirizzo www.stayinvisible.com, che analizza le informazioni ricevute e compila un report facile da consultare.

Tutte queste informazioni sono potenzialmente utili al server per restituire contenuti rilevanti e ottimizzati (per esempio pagine più compatte e leggere se ci si collega da un dispositivo mobile), ma la loro quantità le rende pericolose: i dati sono così tanti che la loro combinazione può permettere un'identificazione univoca dell'utente e del computer. Per verificare questo

*Il browser Web
è lo strumento che espone
più informazioni sugli utenti,
quindi va utilizzato
con particolare cautela.*



Tutti i principali browser offrono una modalità di navigazione privata; la pagina iniziale di Chrome sottolinea però che il nome può trarre in inganno: questa funzione infatti non rende anonima la navigazione, né la protegge in alcun modo.



Tutti i principali browser utilizzano una scorciatoia comune per raggiungere la funzione di eliminazione dei cookie: basta premere Ctrl+Maiusc+Canc.

aspetto si può visitare il sito <https://panopticklick.eff.org>, realizzato dalla Electronic Frontier Foundation (Eff); nel nostro caso, la combinazione di informazioni è risultata unica tra i quasi 5.000.000 di configurazioni analizzate, e oltre 22 bit di informazioni permettevano di individuare univocamente il nostro browser. È la cosiddetta browser fingerprint (impronta digitale del browser), che secondo le analisi di Eff è in grado di identificare oltre 8 utenti su 10.

BISCOTTI INDIGESTI

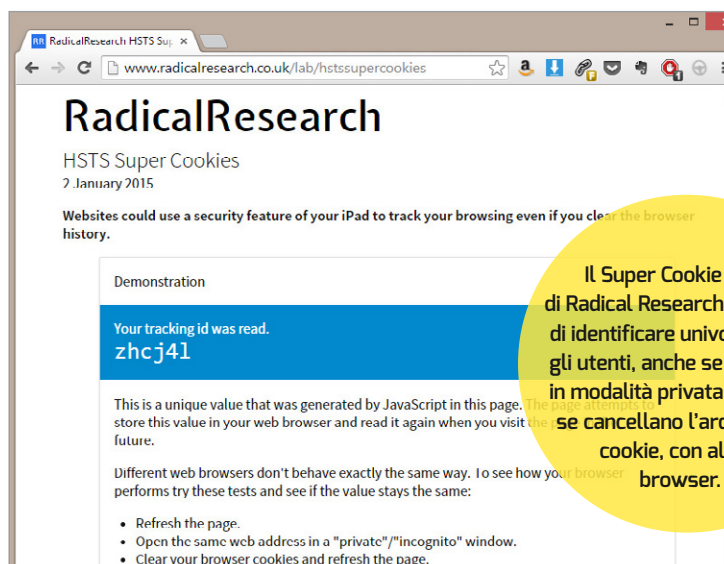
Un'altra tecnologia che ha importanti ripercussioni sul fronte della privacy è quella dei cosiddetti cookie (letteralmente biscotti), piccole quantità di dati che i server possono salvare sul computer, attraverso il browser.

I server remoti possono sfruttarli per memorizzare in locale preferenze di navigazione e informazioni sull'utente; l'esempio più noto è quello dei sistemi di riconoscimento automatico, per evitare di ripetere il login ogni volta che ci si collega a un sito visitato di frequente.

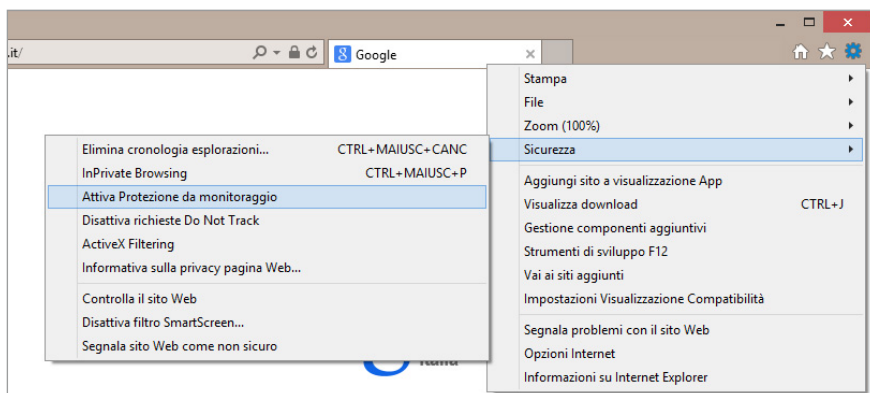
Anche i cookie, quindi, sono stati pensati per un uso totalmente lecito, e in molti casi si rivelano preziosi; ma si prestano anche a molti abusi. In un primo tempo, erano leggibili da parte di qualsiasi server, e si poteva facilmente risalire ai siti visitati. Questa enorme falla è stata rapidamente turata: oggi ciascun sito può accedere soltanto ai dati salvati dallo stesso dominio. Ma, come vedremo, esistono molti metodi per aggirare questo blocco, specialmente da parte dei grandi fornitori di servizi.

Insieme alla cronologia, i cookie sono il bersaglio principale delle funzioni di "navigazione anonima", offerte da tutti i principali browser. Ogni produttore ha scelto una denominazione diversa, ma le funzioni sono sostanzialmente le stesse: quando si apre una finestra di navigazione anonima, le pagine visitate non vengono aggiunte alla cronologia del browser, e i cookie vengono eliminati automaticamente alla fine della sessione.

Questi accorgimenti permettono di nascondere le tracce più evidenti della navigazione (per esempio se state cercando un regalo – o un nuovo lavoro – e non volete insospettire gli altri utenti del Pc), ma le connessioni non hanno nulla di privato, né di anonimo. La denominazione di queste funzioni è anzi pericolosa, poiché potrebbe trarre in inganno gli utenti



Il Super Cookie HSTS di Radical Research permette di identificare univocamente gli utenti, anche se navigano in modalità privata e perfino se cancellano l'archivio dei cookie, con alcuni browser.



Internet Explorer espone la funzione do-not-track, che aggiunge agli header http un flag per segnalare ai server remoti la volontà di non essere tracciati.

meno esperti e spingerli a trascurare le normali cautele. In realtà, basta aprire una sessione di navigazione privata e visitare nuovamente i siti segnalati in precedenza (www.stayinvisible.com e <https://panopticlick.eff.org>) per notare immediatamente che nulla è cambiato sul fronte della tracciabilità: come segnala Chrome nella pagina iniziale della modalità *Incognito*, “se navighi in incognito, la tua navigazione non viene nascosta al tuo datore di lavoro, al provider di servizi Internet o ai siti Web che visiti”.

I cookie tradizionali sono una tecnologia consolidata, e la maggioranza degli utenti ha imparato a gestirla in modo efficace. Inoltre, gli sviluppatori dei browser hanno corretto i principali rischi per la sicurezza, e continuano a lavorare per risolvere eventuali problemi che dovessero emergere. Uno dei più recenti è il cosiddetto Super Cookie HSTS, una tecnica che sfrutta una nuova funzione di sicurezza per individuare univocamente gli utenti. Il bersaglio è la funzione *HTTP Strict Transport Security*, che ironicamente è stata pensata proprio per migliorare la sicurezza delle comunicazioni.

I siti Web possono utilizzare questa tecnologia per assicurarsi che l'utente si connetta utilizzando soltanto il protocollo https; aggiungono all'header della risposta un flag che segnala al browser la necessità di passare automaticamente dalla connessione in chiaro a quella protetta. Gli esperti di sicurezza di Radical-Research (www.radicalresearch.co.uk) hanno sfruttato questo comportamento

per creare un super cookie capace di identificare univocamente gli utenti: è sufficiente analizzare il flag HSTS di un numero sufficiente di siti Web (nell'implementazione di esempio ne hanno usati 32) per generare un numero identificativo univoco, capace di rendere individuabile un utente.

La gestione di queste informazioni è particolarmente problematica: i super cookie, infatti, sono trasparenti alla navigazione privata, e in alcuni casi (per esempio in Safari) non possono neppure essere eliminati, poiché il browser non permette di cancellare i flag HSTS. Chrome e Firefox eliminano invece le informazioni quando si cancellano i cookie, e Firefox non consente più (dalla versione 34.0.5) di recuperare i dati quando si naviga in modalità privata. Internet Explorer, infine, non supporta la tecnologia HSTS, ed è attualmente immune da questo exploit; le prossime versioni del browser Microsoft, però, dovrebbero includerla, e quindi potrebbero risultare vulnerabili.

Le tecniche di tracciamento degli utenti di Internet sono numerosissime e si evolvono di continuo.

NON SEGUIRMI, GRAZIE

Come abbiamo visto, le tecniche di tracciamento degli utenti sono moltissime, e si evolvono continuamente. Gli sviluppatori dei browser sono impegnati a correggere eventuali falle, e a cercare nuovi compromessi tra l'usabilità e la sicurezza. I responsabili dello sviluppo di Chrome, per esempio, hanno dibattuto a lungo sulle contromisure da prendere per mitigare l'impatto del Super Cookie HSTS, e delle molte altre tecniche di fingerprinting passivo (ovvero di analisi delle informazioni fornite dal browser); attualmente, la policy è quella di non intervenire su ogni potenziale fonte di informazioni, per non vanificare gli scopi iniziali (e legittimi) delle tecnologie coinvolte. Naturalmente, gli sviluppatori correggono i difetti e le distorsioni più evidenti, e per questo è importante mantenere il browser sempre aggiornato: per default, Chrome si aggiorna automaticamente in background, senza neppure chiedere il consenso dell'utente.

Un approccio diverso al problema del tracciamento è quello proposto dalla tecnologia Do-not-track: si tratta, semplicemente, di un flag aggiunto alle richieste http, in cui il browser segnala la volontà da parte dell'utente di non essere tracciato.

Non implementa nessun espediente tecnico per evitare il tracciamento, ma dichiara in modo esplicito (e legalmente vincolante) il suo rifiuto. Il flag do-not-track sposta la questione su un altro piano: chi dovesse comunque analizzare le preferenze dell'utente compirebbe una violazione volontaria, e si troverebbe in una posizione difficile da difendere qualora fosse chiamato a risponderne in giudizio. In alcuni Paesi, come per esempio gli Stati Uniti, le cause collettive sono un forte deterrente alle



pratiche commerciali scorrette, e questa soluzione potrebbe garantire una certa efficacia, in particolare nei confronti delle aziende che attirano l'attenzione dell'opinione pubblica.

PRIVACY E SERVIZI ONLINE

Alcuni fornitori di servizi si trovano in una posizione particolarmente vantaggiosa, e accumulano un'enorme quantità di informazioni sui loro utenti. È il caso, per esempio, di Google, che secondo gli ultimi dati di NetMarketShare elabora oltre il 62% di tutte le ricerche effettuate a livello mondiale.

La seconda posizione, con il 18,9%, è occupata dal servizio cinese Baidu, mentre tutti gli altri servizi si spartiscono il restante 18,6%. Google ha quindi accesso a moltissime informazioni, e può profilare i suoi utenti, registrati oppure no. Conosce nei dettagli cosa hanno cercato, quali pagine hanno poi visitato, e molto altro ancora.

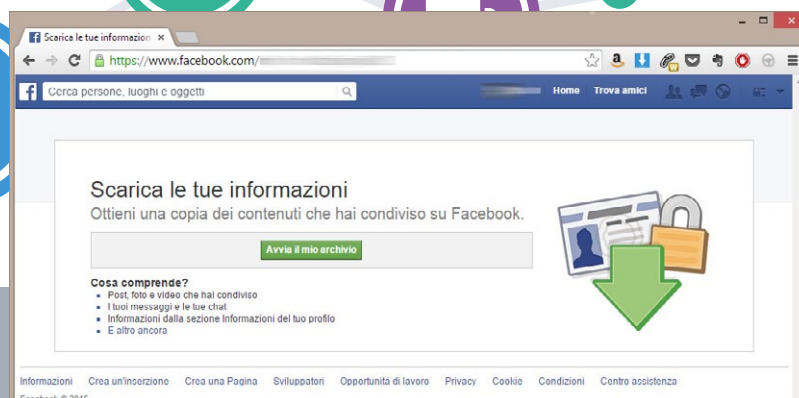
Chi utilizza il servizio di posta elettronica Gmail permette agli algoritmi di Google di analizzare anche la

corrispondenza, e offre quindi un'immagine di sé ancora più nitida. Si potrebbe pensare che basti effettuare il logout dall'account Google per evitare l'associazione tra utente e ricerche effettuate (o pagine visitate), ma non è così semplice: Google, per esempio, salva comunque in locale dei cookie per tenere traccia delle ricerche svolte e dei siti visitati. Spesso, questa profilazione "anonima" avviene senza che l'utente se ne renda conto, e senza nessun feedback visibile, anche se non si passa dai server di Google. Per esempio, è sufficiente che un sito Web utilizzi il servizio gratuito di analisi del traffico Google Analytics, oppure integri i banner pubblicitari di Google

AdSense, per far sì che l'azienda di Mountain View possa registrare la visita. Questi comportamenti spiegano, almeno in parte, perché Google abbia convenienza a offrire tanti servizi di alta qualità in modo gratuito. Quando un utente effettua il login al proprio account Google, il suo profilo può essere immediatamente completato con i dati raccolti quando non era collegato all'account: dato che i cookie in questione erano stati impostati dagli stessi domini, possono essere letti senza alcun problema. Per evitare di essere tracciati, bisognerebbe svuotare l'archivio dei cookie prima di effettuare il login con i servizi di Google; è una soluzione poco pratica ma (come vedremo) esistono software che possono aiutare a semplificare e automatizzare la procedura.

I SOCIAL NETWORK

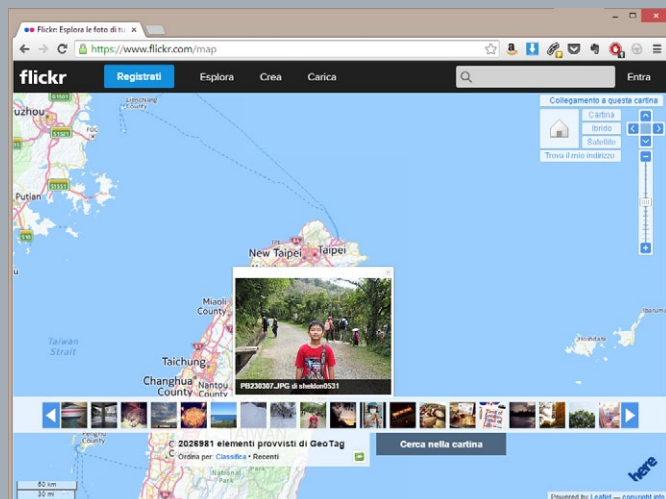
Il tracciamento tramite cookie è comune per tutti i servizi che riescono a ottenere un'ampia diffusione e possono raccogliere informazioni sui loro utenti: Facebook, per esempio, può associare un utente a tutte le pagine visitate in cui sia presente un pulsante *Mi piace*. Anche in questo caso, effettuare il logout prima di navigare non mette al riparo dal tracciamento, a meno che non si svuoti anche l'archivio dei cookie. La maggioranza degli utenti, comunque, non solo non cancella i cookie, ma non si preoccupa neppure di effettuare il logout; anzi, è in qualche modo invitata a restare sempre connessa, ad esempio per sfruttare le funzioni di autenticazione verso siti di terze parti, indubbiamente comode, oppure i servizi di messaggistica in tempo



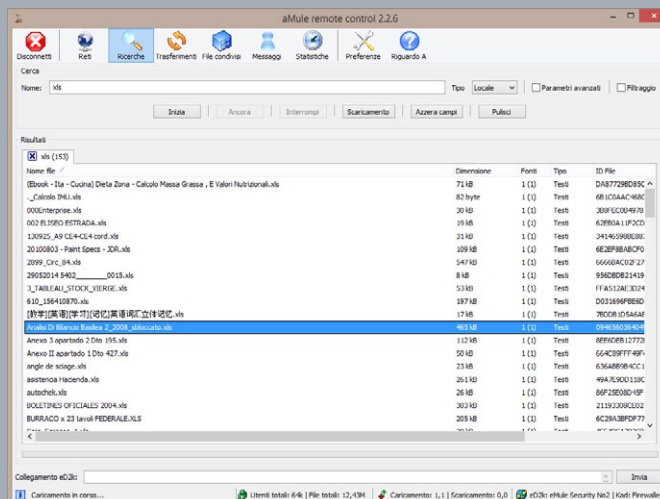
Se si scarica e analizza l'archivio dei contenuti condivisi su Facebook ci si può rendere conto di quanti dati personali rimangono memorizzati in questo social network.



Google Analytics è uno strumento gratuito preziosissimo per valutare l'andamento del traffico verso un sito Web; Google raccoglie però anche molte informazioni sui navigatori.



Alcuni servizi di condivisione delle foto supportano il geotagging, ma non tutti i sono consci dei pericoli per la privacy legati a questa funzione.



Basta un po' di distrazione o un errore di configurazione per condividere involontariamente sulle reti peer to peer documenti privati.

reale. Ma oltre ad analizzare le abitudini di navigazione, i social network contengono un'enorme massa di informazioni private, spesso molto più significative e sensibili. Reti di relazioni, opinioni politiche, orientamento sessuale e perfino informazioni mediche vengono spesso condivise con una scarsissima attenzione alle implicazioni e alle possibili conseguenze.

Chi si occupa di selezione del personale, per esempio, verifica spesso le informazioni pubblicate su Facebook dai candidati; e lo scrupolo dei singoli può essere vanificato dalla scarsa attenzione di qualche amico, anche a causa di una selva di impostazioni e opzioni dedicate alla privacy che rendono difficile avere il completo controllo sulle informazioni rese pubbliche.

Molto interessante, a questo proposito, è l'analisi svolta da Matt McKeon, che ha visualizzato graficamente i cambiamenti interscisi nelle impostazioni di default di Facebook nei primi cinque anni di vita (<http://mattmckeon.com/facebook-privacy>). Il secondo quinquennio non ha visto inversioni di tendenza, e anzi le opzioni relative alla privacy continuano a cambiare.

Spesso non ci si rende conto di quante informazioni siano presenti su Facebook: per avere uno sguardo d'insieme basta raggiungere la homepage del servizio, completare eventualmente il login, fare clic sull'icona a forma di

freccia verso il basso (in alto a destra nella barra degli strumenti della pagina) e selezionare *Impostazioni* nel menu a discesa. Nella sezione *Generali*, in fondo alla pagina, si trova il link *Scarica una copia dei tuoi dati di Facebook*; aprendolo si raggiunge una pagina che permette di creare una copia di tutte le informazioni memorizzate. Basta fare clic su *Avvia il mio archivio* e inserire nuovamente la password di autenticazione.

OLTRE IL BROWSER

Fino a questo punto abbiamo analizzato principalmente i rischi che riguardano la navigazione e l'uso dei servizi online, ma i pericoli sono molti di più. Per esempio, i post su Facebook, i check-in di

Attenti ai post
Chi cerca personale spesso verifica i profili Facebook dei candidati.

Foursquare (ora Swarm) e i tweet contengono spesso informazioni sulla posizione geografica, che potrebbero finire nelle mani sbagliate. Questo vale, a maggior ragione, per i minori: grazie alle analisi delle informazioni condivise sui social network si può sapere che scuola frequentano, dove si trovano in un determinato momento, vederne le foto e molto altro ancora. Whatsapp, invece, mostra per default l'ultimo accesso: è difficile sostenere di essere andati a letto presto, se si stava usando lo smartphone a notte fonda.

A volte i pericoli sono molto più subdoli: molte App fotografiche per smartphone e tablet, per esempio, includono

le coordinate geografiche tra i metadati memorizzati nei file d'immagine. Chi analizzasse queste informazioni potrebbe riuscire a risalire all'indirizzo dell'abitazione privata, e a molte altre informazioni sugli spostamenti e sui luoghi frequentati. Molti siti Web e social network, da Ebay a Facebook, eliminano le informazioni Exif dalle immagini pubblicate, ma esistono molti altri modi per distribuire o condividere le fotografie digitali.

Anche la posta elettronica ha i suoi problemi: molte comunicazioni, infatti, transitano ancora in chiaro, e possono essere intercettate e lette con estrema facilità. Alcuni servizi, come per esempio il già citato Gmail di Google, analizzano la corrispondenza con algoritmi automatici, al fine di proporre messaggi pubblicitari più rilevanti. Ma la diffusione di Gmail è tale che l'analisi della corrispondenza si estende anche a chi non utilizza il servizio: è quello che ha potuto constatare l'attivista Benjamin Mako Hill, dopo aver



analizzato lo storico della sua corrispondenza negli ultimi 10 anni (ne abbiamo parlato in dettaglio nell'editoriale software del numero di settembre 2014 di *PC Professionale*); il 57% dei messaggi a cui ha risposto provenivano da account Gmail. Di conseguenza, Google ha comunque potuto analizzare più di metà della sua corrispondenza.

Le ultime considerazioni riguardano i sistemi di condivisione peer to peer: i network principali sono tenuti costantemente sotto controllo, non soltanto per individuare e perseguire chi dovesse condividere programmi e contenuti coperti da copyright, ma anche per analizzare la diffusione di documenti e informazioni. Nonostante le tecniche di offuscamento e gli altri artifici messi in campo dagli sviluppatori dei sistemi peer to peer, è fin troppo semplice recuperare informazioni su ciascun utente.

Finché si usa Bittorrent per scaricare velocemente l'ultima versione di una distribuzione Linux non c'è nulla da temere, ma spesso la configurazione di questi software porta a condividere molto più di quanto si voglia: per esempio, molti utenti indicano la stessa cartella di destinazione per i download dalle reti peer to peer e dal Web. Questa impostazione ha come conseguenza che tutti i file scaricati saranno condivisi nella rete p2p; finché si tratta di file comuni (l'installer di un freeware, o i driver per la scheda video) i rischi sono contenuti, ma è fin troppo semplice dimenticarsi dei pericoli e lasciare nella cartella di download anche immagini o documenti personali. Basta collegarsi a un servizio peer to peer che integri un motore di ricerca (per esempio la rete eDonkey) ed effettuare qualche ricerca inconsueta (per esempio cercare i file con estensione Xls, oppure i documenti di Word con la stringa *clienti*) per rendersi conto di come non sempre siano condivisi soltanto file musicali, film e videogiochi.



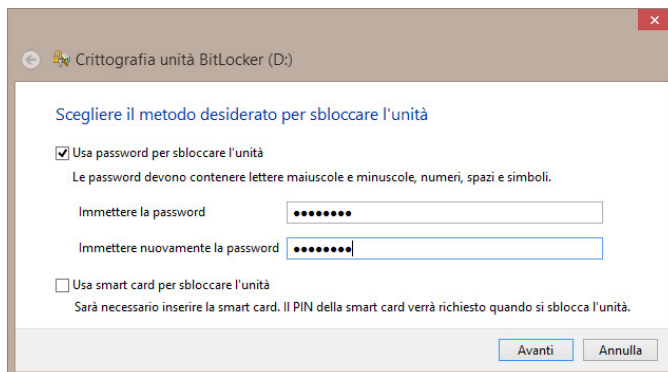
COME PROTEGGERE LA NOSTRA PRIVACY

La lettura delle pagine precedenti potrebbe preoccupare, ed è giusto che sia così: i rischi legati alle violazioni della privacy sono moltissimi e spesso sottovalutati. Il primo passo per ridurre l'esposizione è proprio quello di prendere coscienza del livello di rischio a cui i normali utenti di Internet sono esposti, e valutare quindi ogni azione in modo più consapevole e informato. La risposta, infatti, non può essere cancellarsi da tutti i servizi e spegnere il computer, anche perché le informazioni già raccolte spesso non possono essere eliminate. Invece, è essenziale conoscere tutte le implicazioni e agire di conseguenza: i rischi più gravi, infatti, sono quelli corsi in maniera inconsapevole, utilizzando strumenti e servizi senza conoscerli realmente.

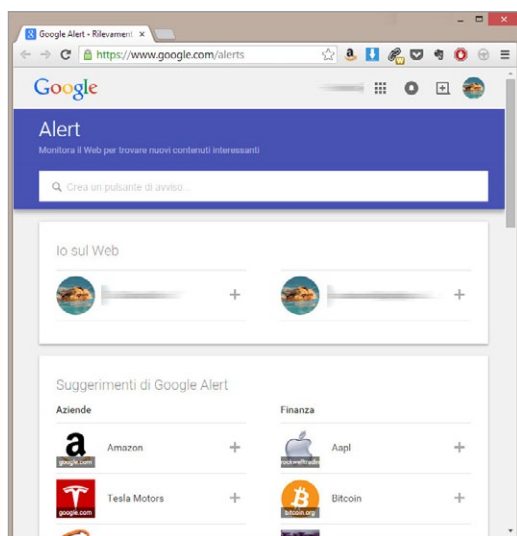
Per quanto riguarda la difesa dagli hacker, le contromisure da adottare

sono quelle tradizionali: scegliere un antivirus e un firewall efficaci, mantenerli sempre aggiornati, scaricare e applicare tempestivamente gli update ai software e al sistema operativo. Inoltre è opportuno evitare comportamenti a rischio, come l'installazione di software di provenienza illegale, la navigazione su siti poco raccomandabili o l'avvio di allegati ai messaggi di posta elettronica. Nonostante tutte queste precauzioni, il rischio non è completamente azzerato: può sempre capitare un malware non riconosciuto dall'antivirus, o un attacco che renda pericoloso un sito con contenuti altrimenti leciti.

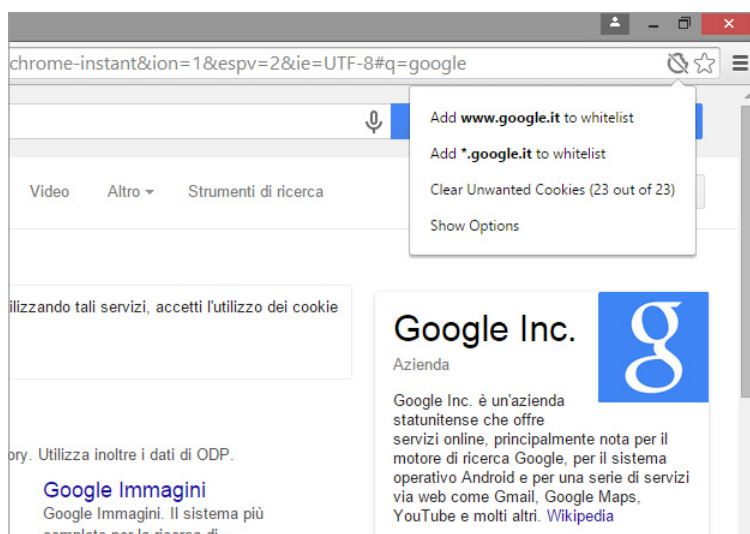
Proteggersi dalle agenzie governative e dai servizi di intelligence è molto più complicato; Edward Snowden, l'analista che ha svelato il sistema controllo di massa messo in campo dall'Nsa, suggerisce di criptare l'hardware e



BitLocker è una funzione integrata nelle versioni professionali di Windows fin dai tempi di Vista; permette di criptare interi dischi e partizioni per proteggerne i contenuti.



Impostando un Google Alert relativo al proprio nome, o ad altri dati personali, spesso si possono individuare tempestivamente eventuali violazioni della privacy.



L'estensione Vanilla Cookie Manager migliora e completa le funzioni native di Chrome – non proprio sofisticatissime – per la gestione dei cookie. È molto facile accedervi, grazie all'icona aggiunta alla barra dell'indirizzo.

le comunicazioni in rete. Questo non è sempre possibile, specialmente se si utilizzano i servizi tradizionali di Internet, ma verificare la sicurezza dei canali di comunicazione e agire con circospezione è di certo una buona abitudine. Per proteggere il contenuto del computer si possono creare volumi cifrati; la soluzione più semplice è Bitlocker, uno strumento di Windows disponibile fin dai tempi di Windows Vista, per lo meno nelle versioni del sistema operativo dedicate ai professionisti.

Utilizzarlo è davvero molto semplice: basta aprire Esplora file, fare clic destro sull'unità da proteggere (Bitlocker lavora a livello di unità logica, cioè protegge un intero disco o partizione), selezionare *Attiva Bitlocker* e seguire le istruzioni della procedura guidata per impostare il sistema o i sistemi di sblocco (password, smart card, chiavetta Usb) e poi cifrare i dati. Se il computer integra un Tpm (trusted platform module, un circuito integrato che contiene chiavi crittografiche) si può attivare addirittura la cifratura del disco di sistema.

Da Windows 7 in poi, Bitlocker può proteggere anche le unità removibili: è assolutamente consigliabile proteggere le chiavette Usb e i dischi esterni in cui si pensa di memorizzare informazioni private, perché le loro piccole dimensioni e l'uso in mobilità rendono queste memorie di massa molto più soggette allo smarrimento e al furto.

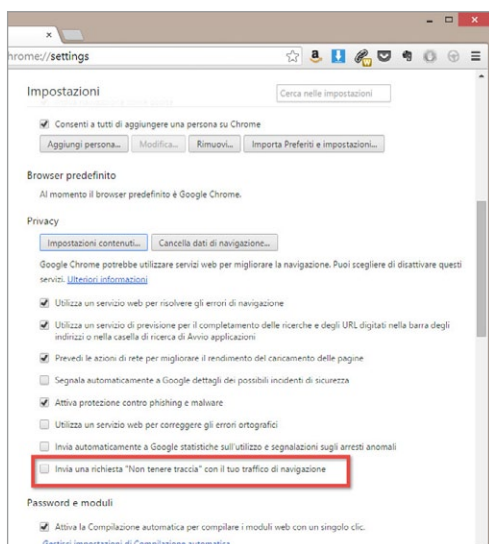
NAVIGAZIONE PIÙ PROTETTA

Per verificare quali nostre informazioni personali siano disponibili sul Web, e per essere informati tempestivamente di potenziali nuovi problemi, si può utilizzare il servizio Google Alert, che tiene sotto controllo l'archivio di pagine Web di Google e segnala le novità che corrispondono a uno specifico argomento. Basta visitare il sito www.google.com/alerts e attivare gli allarmi relativi al proprio nome, o a informazioni specifiche (per esempio l'indirizzo email privato) per individuare rapidamente possibili problemi. Nella sezione *Io sul Web* si possono

trovare alcuni alert preimpostati per individuare le informazioni personali, naturalmente solo dopo il login con il proprio account Google.

Nelle pagine precedenti abbiamo illustrato alcune tecniche utilizzate per tracciare i comportamenti di navigazione degli utenti; per migliorare il livello di protezione, è opportuno innanzitutto effettuare il logout quando si conclude una sessione di navigazione, specialmente se si utilizzano servizi delicati, come l'home banking o la posta elettronica. Inoltre, è utile cancellare l'archivio dei cookie; pochi sanno che quasi tutti i browser offrono una scorciatoia da tastiera





L'opzione che abilita il flag do-not-track in Chrome è inserita tra le impostazioni avanzate, e richiede un certo impegno per essere scovata.

comune per raggiungere velocemente la gestione dei cookie: basta premere **Ctrl+Maiusc+Canc** e poi selezionare la funzione di cancellazione, diversa per ogni browser. Chrome, per esempio, mostra il pulsante *Cancella dati di navigazione*.

Si può inoltre attivare l'opzione do-not-track, per richiedere di non essere tracciati; la sequenza esatta dipende dal browser utilizzato: in Chrome, per esempio, bisogna aprire la pagina di configurazione (basta fare clic sul pulsante in alto a destra nella toolbar e selezionare *Impostazioni* nel menu a discesa), poi fare clic sul collegamento *Mostra impostazioni avanzate* in fondo alla pagina e spuntare la voce *Invi una richiesta "Non tenere traccia" con il tuo traffico di navigazione* nella sezione *Privacy*. Internet Explorer rende l'accesso a questa opzione ancora più semplice: basta fare clic sul pulsante a forma di ruota dentata, in alto a destra, e selezionare *Sicurezza/Attiva Protezione da monitoraggio*. In Firefox, infine, bisogna richiamare il menu principale (premendo il tasto **Alt**), poi selezionare *Strumenti/Opzioni*, raggiungere

la scheda *Privacy* e spuntare la voce *Richiedi ai siti di non effettuare alcun tracciamento*. Come abbiamo già spiegato, però, questa impostazione non garantisce che la richiesta dell'utente venga effettivamente esaudita.

Oltre alle funzioni integrate nel browser, ci sono molti altri strumenti che possono aiutare nella gestione dei cookie e delle altre impostazioni di navigazione: tra i tool di terze parti segnaliamo CCleaner, disponibile gratuitamente all'indirizzo www.piriform.com/ccleaner. Da qualche tempo il produttore ha realizzato anche un'edizione a pagamento (CCleaner Pro),

ma quella gratuita è più che sufficiente per gestire i dati di navigazione. Il vantaggio di utilizzare un tool di terze parti è l'indipendenza dal particolare browser utilizzato: CCleaner, infatti, può agire contemporaneamente su tutti i browser. Per semplificare l'installazione si può visitare la pagina www.piriform.com/ccleaner/builds e scaricare il Basic Installer, privo di toolbar e altri componenti inutili. La funzione *Ricerca cookie intelligente* propone un compromesso tra comodità e sicurezza: in questa modalità, infatti, CCleaner cerca di individuare i dati relativi al login ai servizi Web, e li esclude dalle operazioni di pulizia. Questa impostazione è certamente pratica, ma potrebbe vanificare la pulizia, se l'intento invece è proprio quello di eliminare tutti i riferimenti a servizi specifici. Le impostazioni di Internet Explorer sono nella scheda *Windows* della sezione *Pulizia*, mentre gli eventuali altri browser sono elencati nella scheda *Applicazioni*. Usare CCleaner è semplicissimo: dopo aver selezionato quali tipologie di elementi cancellare, basta fare clic su *Analizza* per ottenere un report sulle informazioni trovate, oppure *Avvia pulizia* per eliminarle. Esistono anche molte estensioni dedicate alla gestione dei cookie, per tutti i principali browser. Chi usa Firefox, per esempio, può scaricare *Self-Destructing*

Cookies per automatizzare l'eliminazione delle informazioni memorizzate in locale dai server remoti: tiene traccia dei dati aggiunti da ogni sessione, e li cancella appena l'utente chiude la relativa scheda nel browser. Le opzioni permettono di modificarne il comportamento: per esempio, si può creare una whitelist di cookie accettati, oppure si può evitare che l'estensione mostri avvisi popup dopo aver completato la pulizia. Gli utenti di Chrome, invece, possono scaricare *Vanilla Cookie Manager*: le sue funzioni sono leggermente diverse, ma anche questa estensione include strumenti di pulizia e una whitelist.

Rimozione intelligente

Tool come CCleaner permettono di eliminare i cookie indesiderati

Tra le estensioni per Firefox vale la pena di segnalare anche *Taco (Targeted Advertising Cookie Opt-out)*, un tool pensato per fermare le più conosciute tecniche di tracciamento e irrobustire il comportamento del browser, per evitare che i server remoti possano sfruttarne le debolezze per ottenere informazioni sui comportamenti di navigazione. Può essere utile tenere sotto controllo anche l'esecuzione di codice Javascript; alcune delle tecniche che abbiamo illustrato (per esempio il Super Cookie HSTS) sono basate su uno script eseguito in locale. Per controllare l'esecuzione di script locali si possono utilizzare estensioni come *NoScript* per Firefox o *Scriptsafe* per Chrome; purtroppo, però i siti Web moderni si basano pesantemente sull'esecuzione di codice lato client, e bloccando Javascript si rendono inutilizzabili moltissimi servizi. Entrambe le estensioni consentono di impostare eccezioni, per garantire il funzionamento dei siti più importanti.

SERVIZI WEB E SOCIAL NETWORK

Come abbiamo già accennato, molti servizi raccolgono informazioni sugli utenti (con oppure senza la loro collaborazione) e spesso li rendono accessibili con troppa liberalità. Nel caso di Google, qualche impostazione può limitarne la curiosità: per esempio, si può visitare la pagina www.google.com/ads/preferences e fare clic sui due collegamenti *Disattiva gli annunci basati sugli interessi su Google* e *Disattiva gli annunci Google basati sugli interessi*

Esistono estensioni per vari browser che semplificano l'eliminazione dei cookie indesiderati; ottima è Self-Destructing Cookies per Firefox.



i certificati Ssl e ne valuta l'affidabilità. Un altro passo utile per evitare la profilazione è non utilizzare i servizi di ricerca di Google. Un'alternativa pensata proprio per proteggere la privacy dei navigatori è DuckDuckGo (<https://duckduckgo.com>), di cui abbiamo già parlato in passato. I pulsanti presenti nella zona inferiore della pagina home permettono di aggiungerlo ai motori di ricerca integrati nel browser e di impostarlo come pagina iniziale.

Ma per proteggere l'identità e navigare in modo anonimo non basta controllare ed eliminare i cookie: in alcuni casi, è necessario oppure utile mascherare l'indirizzo IP di provenienza, per evitare la censura, rendere anonima la connessione o semplicemente per accedere a informazioni altrimenti non raggiungibili.

Per ottenere questo livello di protezione si possono utilizzare sistemi proxy e Vpn: queste tecnologie utilizzano uno o più server per triangolare tutto il traffico, in ingresso e in uscita, per nascondere la reale posizione del client. Il meccanismo è molto semplice, per lo meno dal punto di vista teorico: il client invia i pacchetti a un server remoto, che a sua volta li smista verso le destinazioni finali, senza aggiungere dettagli sulla loro reale provenienza. Quando riceve le risposte le instrada poi verso il client (tramite un canale sicuro), completando la comunicazione. In questo modo si possono superare molti blocchi alla navigazione (anche se in alcuni casi i filtri lavorano a

livello di Dns), e fingere di trovarsi in un'altra parte del mondo: scegliendo un proxy statunitense, per esempio, si può accedere a servizi come Hulu o Netflix. Naturalmente, un proxy non garantisce la privacy da solo: si è ancora vulnerabili a tutte le tecniche di tracciamento, ed è opportuno associare questa tecnologia a un browser o ad applicazioni che limitino l'invio di informazioni private. Inoltre, l'anonimato è garantito soltanto se i gestori del servizio sono affidabili: i loro server, infatti, conoscono le reali sorgenti e destinazioni di tutti i pacchetti di dati in transito.

Proxy e Vpn sono tecnologie nate per altri scopi, ma molto utili per migliorare la privacy e garantire un certo livello di anonimato; la prima in realtà è stata pensata per interporre un filtro tra la rete locale e Internet, vagliando i protocolli e le applicazioni che possono comunicare con l'esterno.

Viene usata spesso in ambito aziendale, per bloccare l'uso di software non autorizzati o per limitare l'accesso ad alcuni siti Web. La Vpn (Virtual Private Network) è un canale di comunicazione sicuro, instaurato tra due host attraverso Internet. Una Vpn permette di collegarsi a un computer o a una rete remota e comunicare come se ci si trovasse all'interno della stessa Lan; di per sé stessa, quindi, questa tecnologia non garantisce l'anonimato. Le Vpn pensate per la privacy, però, instaurano un canale di comunicazione cifrato verso un server remoto, e poi utilizzano quest'ultimo come punto d'appoggio

“

Le Vpn e i proxy server sono stati sviluppati per altri scopi, ma sono molto utili anche per la protezione della privacy.

COME FUNZIONA LA RETE TOR



Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



Download Tor

- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android.

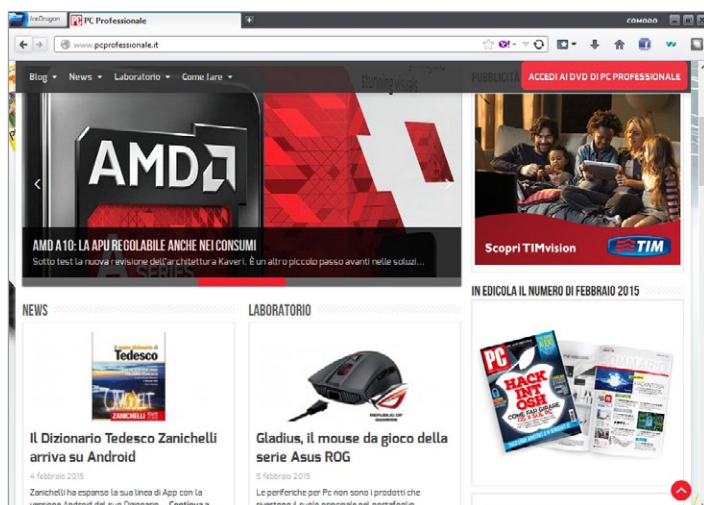
What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state

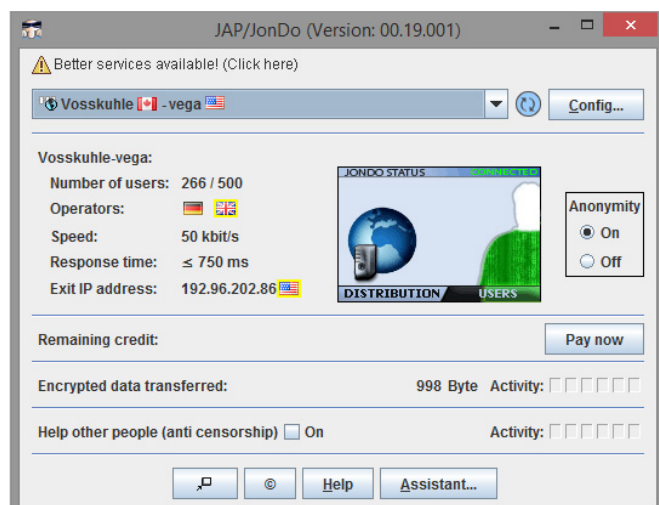
Why Anonymity Matters

Tor protects you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites

Tor è certamente la tecnologia di anonimizzazione più conosciuta e utilizzata; è basata su un complesso sistema di indirizzamento dei pacchetti, che rende molto difficile e dispendioso il tracciamento. Come molte tecnologie relative alle comunicazioni, è stato originariamente sviluppato con fini militari; nello specifico, dai laboratori di ricerca della Marina Militare statunitense (US Navy). Tor protegge contro l'analisi del traffico, ossia le tecniche che non hanno per oggetto i dati contenuti nei pacchetti trasmessi e ricevuti. Può sembrare un rischio minore, ma non lo è: correlando un utente con l'accesso a un sito specifico, in un determinato istante, si può scoprire molto su di lui. Per esempio, se un dissidente avvia una sessione di chat con un giornalista dall'altra parte del mondo, potrebbe correre gravi rischi anche se non si conosce il contenuto esatto della conversazione. Invece di utilizzare il normale sistema di routing dei pacchetti Tcp, che individua la strada più breve tra due host e permette di conoscere tutta la strada percorsa da ogni pacchetto, Tor realizza un percorso protetto e volutamente tortuoso. Ciascun nodo (relay) della rete conosce soltanto la posizione del nodo precedente (da cui riceve i dati) e di quello successivo (a cui invia il pacchetto), grazie all'uso di un sistema di cifratura a chiave doppia che permette di inserire nel pacchetto informazioni leggibili soltanto da ciascuno dei nodi coinvolti. Questo rende la rete resistente anche alla compromissione di alcuni nodi. Una volta creato il percorso protetto, questo rimane utilizzabile per 10 minuti, dopodiché il client ne negozia automaticamente uno nuovo. Una volta stabilito il collegamento, si può utilizzare qualsiasi protocollo basato su Tcp, e ogni applicazione che utilizzi la tecnologia di proxy Socks.



IceDragon è un browser derivato da Firefox; implementa una varietà di strumenti e ottimizzazioni in grado di rendere la navigazione più sicura.



Il servizio JonDo maschera l'indirizzo e la provenienza geografica degli utenti e consente persino di usare più server proxy in cascata.

per inviare e ricevere i pacchetti di dati, mascherando la posizione e l'indirizzo del client. Le offerte disponibili in questo settore sono molte, ma non tutte sono gratuite: per far transitare il traffico di molti utenti attraverso uno o più server serve un'infrastruttura di rete costosa e molta banda. Se si vuole ottenere una velocità di comunicazione accettabile è spesso necessario passare

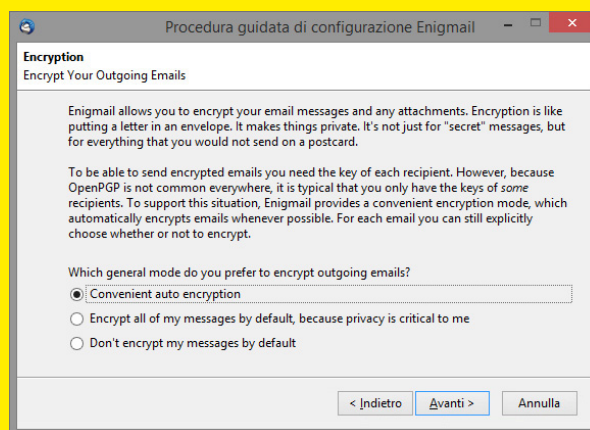
agli abbonamenti premium. In molti casi, i servizi offrono un accesso gratuito, limitato nella velocità o nel numero di "punti d'uscita" su Internet, mentre l'abbonamento a pagamento garantisce un servizio più ricco e performante. Un client proxy assai interessante è JonDonym, che utilizza più server in cascata per migliorare l'anonimità anche nei confronti degli stessi operatori

del servizio. Il servizio è raggiungibile all'indirizzo <https://anonymous-proxy-servers.net>, e offre vari strumenti perconfigurati: il proxy tool JonDo, disponibile per moltissime piattaforme software (compreso Android), e il browser JonDoFox, derivato da Firefox e già pronto per navigare in modo protetto. L'accesso gratuito ha alcune limitazioni: lavora solo sulle

INSTALLARE ENIGMAIL IN THUNDERBIRD

Uno dei maggiori pregi del client di posta di Mozilla è l'architettura espandibile, che consente di aumentare la dotazione di funzioni di default. Una delle aggiunte più interessanti riguarda la protezione delle comunicazioni, con un sistema di cifratura a chiave doppia. Questa tecnologia permette di proteggere un messaggio cifrandolo con la chiave privata del mittente e quella pubblica del destinatario, per garantire sia la provenienza sia la protezione del contenuto. Uno dei sistemi di cifratura a doppia chiave più conosciuti e diffusi è Pgp, che nell'implementazione aperta GnuPG è la base dell'estensione Enigmail. Vediamo come installarla, configurarla e utilizzarla.

Avviate Thunderbird e richiamate il menu principale premendo il tasto **Alt**, poi selezionate *Strumenti/Componenti aggiuntivi* per aprire la pagina di gestione delle estensioni. Digitate *Enigmail* nel campo di ricerca in alto a destra e fate clic sul pulsante *Installa* a fianco del risultato giusto (di solito è il primo dell'elenco). Una volta conclusi il download e l'installazione, fate clic sul collegamento *Riavvia adesso* per completare il setup. Si aprirà automaticamente la procedura



Enigmail individua i destinatari di cui conosce la chiave pubblica, e cifra automaticamente i messaggi a loro diretti.

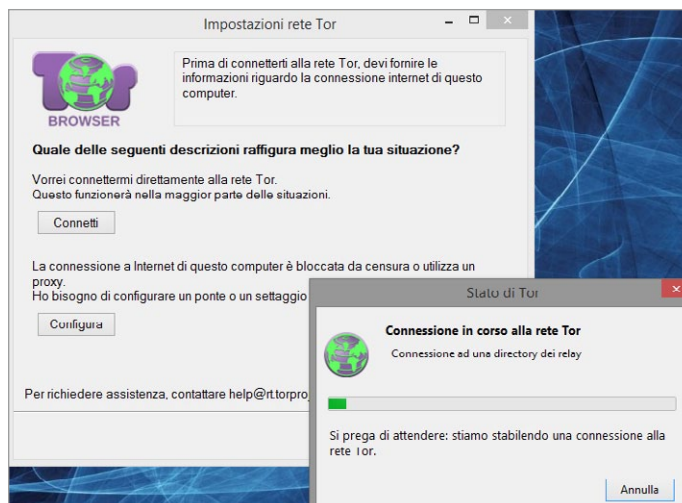
guidata di configurazione di Enigmail; fate clic su *Avanti* per iniziare a configurare l'estensione. Il primo passo è installare GnuPG, oppure indicare la cartella in cui si trova se è già presente nel sistema. Fate clic su *Installa* per avviare il download e poi l'installazione di questo componente. L'installer di GnuPG mostrerà una tradizionale procedura guidata, in italiano. Le impostazioni di default sono perfette per l'uso

comunicazioni http e https, ha un limite di 2 Mbyte per l'upload di file e una velocità media di circa 30/50 kbit/s. Tra i servizi Vpn segnaliamo il veterano CyberGhost VPN (www.cyberghostvpn.com/en), sul mercato da moltissimi anni (la versione gratuita ha qualche limitazione sul fronte della velocità); molto ricco, ma piuttosto costoso, è VyprVPN di GoldenFrog (www.goldenfrog.com/vyprvpn), uno dei pochi servizi a offrire un server d'uscita in Italia.

Un discorso più approfondito merita Private Internet Access (www.privateinternetaccess.com) un servizio di livello professionale, che offre un'eccellente protezione, sia dal punto di vista tecnico sia da quello legale. La sua offerta è molto ricca e comprende molti punti d'uscita su Internet, in varie parti del mondo (sfortunatamente non ancora in Italia). Supporta anche sistemi di pagamento anonimi, come Bitcoin e varie carte prepagate.

RETI ANONIMIZZANTI

Oltre alle reti private virtuali e agli anonimizzatori, esistono alcune tecnologie pensate per sovrapporre un nuovo protocollo di comunicazione ai tradizionali standard di rete; sono i sistemi



di routing anonimo decentralizzato: reti delocalizzate che spesso utilizzano complessi sistemi di distribuzione dei pacchetti peer to peer per rendere non rintracciabili i flussi di dati. Il più noto e diffuso è Tor, acronimo di *The Onion Network* (la rete a cipolla). Per accedere alla rete Tor basta scaricare un piccolo software dal sito www.torproject.org. Esistono anche pacchetti completi che includono anche un browser preconfigurato: il suo nome è Tor Browser ed è scaricabile dallo stesso sito Web. Nella

pagina di download sono indicati alcuni suggerimenti per garantire l'anonimato: in particolare, gli sviluppatori consigliano di non installare plug-in di terze parti (il browser è basato su Firefox, e in teoria è compatibile con le estensioni per il browser Mozilla), ed evitare l'uso dei client Bittorrent, poiché spesso ignorano le impostazioni del proxy e vanificano l'anonimizzazione (oltre ad appesantire la rete). Tor introduce un forte livello di anonimato nel trasporto dei pacchetti, ma questo

Tor è la rete anonimizzante più diffusa e conosciuta; protegge le comunicazioni verso qualsiasi host Internet e permette di raggiungere pagine e servizi nascosti, altrimenti inaccessibili.

con Enigmail, e non è necessario modificare nulla. Dopo aver completato l'installazione di GnuPG tornate alla procedura guidata di Enigmail e fate clic su *Avanti*; il passo successivo permette di decidere quali messaggi cifrare automaticamente. L'impostazione più efficace è probabilmente *Auto encryption*, che cifra automaticamente solo i messaggi verso i destinatari di cui si conosce la chiave pubblica. Un clic su *Avanti* porta al passo successivo, in cui bisogna decidere se firmare i messaggi in uscita oppure no: la firma digitale non protegge il contenuto del messaggio, ma ne assicura la provenienza. Fate clic su *Avanti* per raggiungere un ulteriore passaggio, in cui potete decidere se modificare alcune impostazioni di default di Thunderbird per garantire un funzionamento migliore con Enigmail. La pagina successiva permette di generare oppure di importare le chiavi pubbliche e private: se non ne avete mai creata una selezionate la prima opzione e fate clic su *Avanti*, poi inserite e confermate una frase segreta di protezione di almeno 8 caratteri.

La procedura guidata mostrerà un riassunto delle scelte fatte; fate clic su *Avanti* per applicarle e generare la coppia di chiavi. Una volta completato questo passaggio, Enigmail propone di generare anche un certificato di revoca per la chiave, utile per invalidarla automaticamente in caso di furto, smarrimento o

compromissione. Salvate il certificato in un luogo sicuro (per esempio su una chiavetta Usb cifrata) e completate la procedura. A questo punto, Enigmail è pronta per essere usata; se avete mantenuto le impostazioni di default, tutti i messaggi inviati saranno automaticamente firmati, e si potrà creare un messaggio criptato per comunicare con chiunque abbia una coppia di chiavi Pgp. Le chiavi pubbliche possono essere facilmente scambiate come file o come porzioni di testo: per inviare la vostra chiave selezionate *Enigmail/Gestione chiavi* nel menu principale, fate clic destro sulla chiave e selezionate una delle voci di esportazione disponibili: per esempio *Copia chiavi pubbliche negli appunti*, oppure *Invia chiavi pubbliche via email*.

Le chiavi possono anche essere pubblicate su un server, che svolge la funzione di directory degli utenti. Sempre dalla finestra di gestione delle chiavi, potete anche effettuare ricerche negli archivi online: selezionate *Server/Ricerca chiavi* e inserite il nome dell'utente da individuare. Creare un messaggio cifrato è semplicissimo: aprite la finestra di composizione e utilizzate le funzioni offerte dal menu a discesa richiamabile con un clic sul pulsante *Enigmail*. Ancor più semplice è decifrare un messaggio ricevuto: basta selezionarlo e fare clic sul pulsante *Decifra*, nella toolbar principale di Thunderbird.

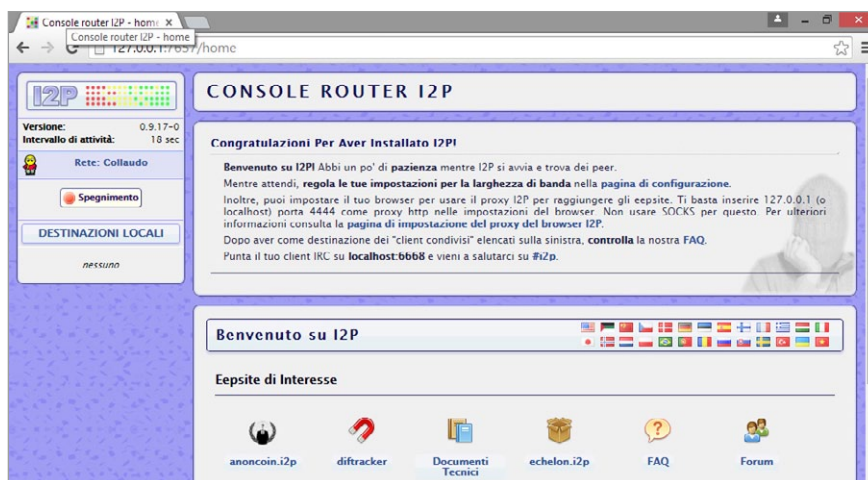
non è sufficiente per garantire una totale sicurezza. Esistono vari studi che hanno supposto la creazione di sistemi autonomi per analizzare i punti d'ingresso e di uscita della rete; con analisi di tipo statistico sul traffico in transito, si potrebbero associare i pacchetti in ingresso a quelli in uscita e rendere vana la protezione, ma i costi e le difficoltà di implementazione sarebbero enormi.

Molto più realistici sono i rischi legati a bug nell'infrastruttura della rete, o nei software utilizzati per la comunicazione. Abbiamo già accennato ai problemi del protocollo Bittorrent, ma anche alcune vecchie versioni di Firefox sono state attaccate con successo. Il bug Heartbleed, individuato nella libreria crittografica OpenSSL, ha reso violabili le chiavi private di molti relay; per precauzione, nel mese di aprile 2014 sono stati spenti oltre 580 nodi, poi le chiavi sono state rinnovate dopo l'aggiornamento del software operativo.

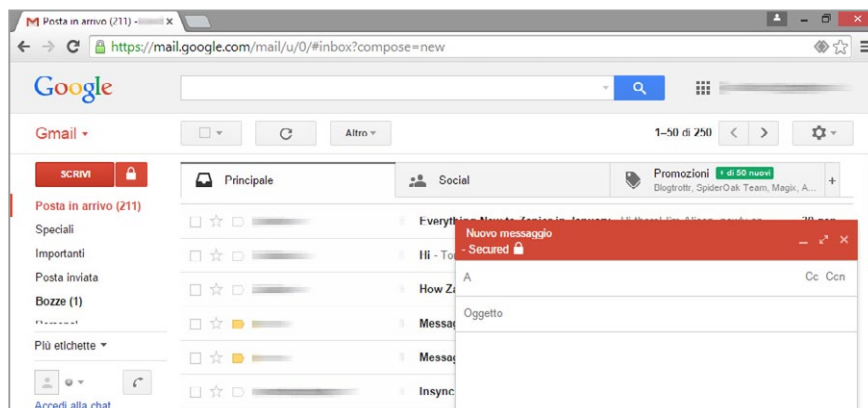
Oltre ad anonimizzare le connessioni Internet tradizionali, la rete Tor (e, come vedremo, anche altre reti di questo genere) permette di creare servizi raggiungibili solo dall'interno della rete, come per esempio server http, ftp o chat. È il cosiddetto deep Web, dove si può trovare davvero di tutto: dai siti dedicati al confronto sulle libertà digitali e alla controinformazione proveniente da Paesi con regimi totalitari, a portali di commercio elettronico legati alle droghe o alle armi da fuoco.

PEER TO PEER E POSTA ELETTRONICA

Come abbiamo già accennato, Tor non è l'unica rete anonima: altre tecnologie di questo genere sono i2p (The Invisible Internet Project, <https://geti2p.net/it>) e RetroShare (<http://retroshare.sourceforge.net>). Entrambe offrono client molto più ricchi rispetto al semplice browser, con scambio e condivisione di file, comunicazione in tempo reale (via chat o addirittura tramite voce e video), invio e ricezione di messaggi simili alle email e molto altro ancora. Le reti peer to peer di tipo tradizionale,



I2p è una rete peer to peer che permette ai suoi membri di comunicare in modo sicuro, pubblicare informazioni, ricevere e inviare messaggi e molto altro ancora.



L'estensione Secure Mail for Gmail aggiunge alla Web mail di Google un'opzione per inviare messaggi cifrati, che il destinatario potrà aprire solo se conosce la password.

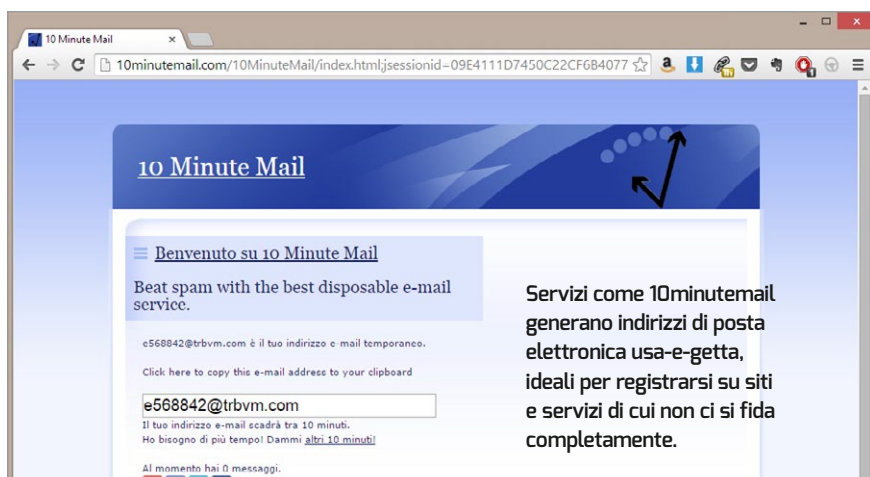
dedicate allo scambio dei file, devono essere invece utilizzate con molta attenzione, perché spesso non offrono una grande robustezza e sono tenute sotto stretta sorveglianza.

La navigazione e lo scambio di file non sono certo le uniche opportunità offerte da Internet: i servizi disponibili in rete sono numerosissimi, e quasi tutti rappresentano un rischio potenziale

per la nostra privacy. Come abbiamo già accennato, le reti anonime come i2p e Retroshare integrano anche molti altri strumenti di comunicazione, tra cui client di posta, blog e forum, comunicazione in tempo reale e file sharing. Ma in molti casi, si vuole semplicemente proteggere l'account di posta elettronica dall'attacco degli spammer, oppure assicurare la riservatezza della



“I servizi offerti da Internet sono numerosissimi e quasi tutti rappresentano un rischio potenziale per la nostra privacy.”



corrispondenza. Esistono semplici servizi per generare indirizzi email usa-e-getta, da sfruttare ad esempio per registrarsi su un sito di cui non ci si fida completamente. Ottimo, e molto conosciuto, è www.10minutemail.com, che crea immediatamente un indirizzo con una vita di soli 10 minuti. Molti servizi di Web mail, come Outlook.com o Yahoo Mail, permettono di creare alias per evitare di rendere pubblico l'indirizzo principale: in Outlook.com, per esempio, basta fare clic sul nome utente in alto a sinistra, selezionare *Impostazioni account/Panoramica*, fare clic su *Aggiungi o modifica alias* e infine su *Aggiungi alias*.

Esistono anche strumenti per cifrare il contenuto delle comunicazioni, e renderle leggibili soltanto dal legittimo destinatario. Sono strumenti molto

maturi, disponibili da decenni; però non hanno mai preso piede tra l'utenza consumer. Ed è un peccato, perché sono piuttosto semplici da usare e possono essere approcciati anche dagli utenti meno esperti. Ottima per esempio è l'estensione Enigmmail per Thunderbird, a cui abbiamo dedicato un box. Gli utenti di Outlook, invece, possono installare OutlookPrivacyPlugin (<https://github.com/dejavusecurity/OutlookPrivacyPlugin>), che richiede però lo scaricamento di alcuni strumenti di terze parti, come Gpg4win e il framework .NET 4.5. La procedura di installazione è comunque spiegata nel dettaglio nella pagina del prodotto.

Chi è ormai abituato alle funzioni di Gmail, può sfruttare alcune estensioni per implementare la cifratura dei messaggi anche nel servizio di Google.

Un esempio è *Secure Mail for Gmail*, una semplice estensione per Chrome capace di cifrare un messaggio con una password, che dev'essere conosciuta anche dal destinatario. Molto più sofisticata e potente, ma anche complessa da utilizzare, è MailVelo (www.mailvelope.com), un'estensione per Chrome e Firefox che implementa un sistema OpenPGP completo ed è compatibile con Gmail, Yahoo Mail e Outlook.com.

Anche se si usano servizi di posta elettronica via Web non bisogna necessariamente rinunciare alla privacy, e consentire che i messaggi vengano analizzati da un sistema automatico. Esistono infatti servizi che offrono caselle private, sicure e senza pubblicità; naturalmente, però, non si tratta di prodotti gratuiti. Hushmail (www.hushmail.com), per esempio, ricorda da vicino l'interfaccia di Gmail, ma non mostra nessun banner e memorizza tutte le informazioni in forma criptata. Si può creare un account gratuito, che ha un limite di capienza di 25 Mbyte e richiede almeno un accesso ogni tre settimane, oppure acquistare un piano a pagamento a partire da 34,99 Dollari Usa all'anno. Più ricco e complesso è MyKolab, un servizio di Web mail professionale che integra anche funzioni di gestione di contatti, condivisione dei file, calendario, note, impegni e molto altro ancora. I prezzi partono da circa 4,30 euro al mese per il solo servizio di posta elettronica e 2 Gbyte di spazio di memorizzazione. •

