

Silenzio, il cellulare ti spia Se il telefonino diventa nemico

Sistemi anti-truffe, chip anti-pedofilia: nobili motivazioni ma l'attacco alla privacy è garantito. "Alcuni programmi trasformano il cellulare in un delatore dei nostri comportamenti..." Usato dai regimi per localizzare i dissidenti. Ma anche dai genitori per controllare i figli

di RICCARDO STAGLIANO

PARAFRASANDO un vecchio slogan, viene da dire: il telefono, la tua voce, e le orecchie di qualcun altro. L'internazionale dell'intercettazione è un'idra trasversale, dall'Iran all'Australia, passando per il Vecchio Continente. A Teheran spiano i sostenitori di Moussavi, li individuano, li bastonano e li mandano in galera. A Sydney i genitori ansiosi monitorano a distanza i cellulari dei figli e se scoprono qualcosa che non li convince li spediscono a letto senza cena. Esiti diversi, modalità simili.

Il buco da cui entrano questi minacciosi spifferi per la nostra privacy (e libertà) è lo stesso. Ce lo portiamo in tasca. È l'apparecchio elettronico più amato dagli italiani. E il suo manuale di istruzioni, per nuovi modelli sempre più complessi, è una delle poche pubblicazioni a rialzare la media nazionale in fatto di statistiche di lettura. Sua maestà il telefonino.

La repressione post-elettorale nella Repubblica Islamica ha ravvivato il dibattito. Qualcuno se l'è presa con Nokia Siemens, la joint venture finnico-tedesca che l'anno scorso ha venduto alla Tci, l'operatore persiano, la tecnologia che permette di "entrare" nelle chiamate. La stessa a disposizione dei governi, previa autorizzazione del magistrato, di tutti i paesi dell'Unione Europea. Su internet, dove gli entusiasmi prendono fuoco come legna secca, c'è chi ha proposto di boicottare il marchio.

"È dura stabilire se il problema sia l'ignoranza o l'ipocrisia" ha ironizzato il blog tecnologico di Business Week, riferendosi alla richiesta di due senatori Usa di smettere di fornire tecnologia ai regimi autoritari. Perché il sistema è identico a quello usato negli Stati Uniti. La differenza è che lì, extraordinary renditions escluse, c'è una procedura democratica che evita gli abusi.

Archiviata quindi la polemica sull'uso a fin di bene (intercettare i terroristi) o malevolo (conculcare il dissenso politico) della tecnologia, restano molti interrogativi sulle potenzialità spionaggistiche dell'ormai irrinunciabile mezzo di comunicazione. Le dotazioni sempre più sofisticate, il fatto ad esempio che il chip Gps, per il posizionamento satellitare, sia ormai standard in quasi tutti i nuovi modelli, apre scenari distopici. Ogni telefonino, mandando in continuazione segnali ai satelliti, consentirà triangolazioni sempre più precise per localizzare geograficamente il suo possessore. Comodo quando ci avviseranno via sms che stiamo passando davanti a un negozio che fa una vendita promozionale. Scocciante se avete detto che eravate da tutt'altra parte e moglie o marito entrano in possesso dei dati sbugiardanti.

Il servizio in Gran Bretagna esiste da qualche tempo e si chiama FollowUs. In teoria il possessore

del telefono "tracciato" deve essere consenziente. In pratica se un altro se ne impadronisce, in una decina di minuti fa in tempo a registrare la sua sim, ricevere il primo degli sms che avvertono che siete sotto osservazione e disattivare la notifica dei messaggi successivi.

Risultato: chi prende in mano l'apparecchio di lì in poi non ne sa niente. Mentre allo spione basta entrare nel sito, pagare una ventina di euro e cominciare a seguire su una mappa interattiva gli spostamenti della preda. A partire da agosto i genitori australiani potranno usare MyMobileWatchdog, un software sviluppato originariamente per la polizia americana. Molto semplice, molto inquietante. Il funzionamento è analogo a quello appena spiegato. E con una dozzina di dollari al mese, collegandosi a un sito, papà o mamma potranno vedere il registro delle chiamate, leggere gli sms e guardare le foto scattate. Il sito statunitense capitalizza, a caratteri di scatola, la minaccia del "sexting", i messaggi a sfondo erotico mandati da adulti che si spacciano da coetanei. E tuttavia l'intervento a gamba tesa nella corrispondenza elettronica dei ragazzi è innegabile.

Se non bastasse, a partire dal 2010, l'arsenale del potenziale spione si arricchirà di una nuova arma. Da quella data tutti i telefoni Ericsson, ma con ogni probabilità non solo quelli, saranno dotati di un nuovo chip Rfid (Radio frequency identification), le cosiddette "etichette intelligenti" che si trovano tanto nei vestiti quanto nei rasoi da supermercato. Nel microcircuito saranno immagazzinate le generalità del titolare e altre informazioni identificative. Tra i tanti possibili usi, le società emittitrici di carte di credito sembrano le più interessate. Se il titolare si trova in un altro posto rispetto a dove avviene la transazione, è probabile che la carta sia finita nelle mani sbagliate. E il sistema, mettendo a confronto la localizzazione del telefonino con quella dello strumento di credito, darà in automatico l'allarme. È ovvio che si tratta di un servizio per l'utente.

Ma se, come prevede un recente studio commissionato da Microsoft, la pubblicità via cellulare diverrà il 5-10 per cento di quella totale da qui a cinque anni, è chiaro che questo passo avanti nella tracciabilità significherà un passo indietro nella quotidiana pace dei sensi digitali. In Giappone, l'unico altro paese al mondo che ci batte quanto a penetrazione di apparecchi portatili, il gestore Softbank d'intesa con il settore pubblico sta per lanciare un esperimento di politica sanitaria via telefonino. L'idea è di monitorare, attraverso i dati Gps trasmessi dai cellulari, i bambini delle scuole. E lo scopo, in caso di epidemia, è riuscire a risalire attraverso i tabulati dei giorni precedenti con chi gli infettati sono venuti in contatto. Ancora una volta, controllo per il bene della collettività. Ma quando i dati sono sui server diventano, per definizione, violabili.

Lo sa bene Guido Cometto, amministratore delegato della torinese Caspertech, tra le capofila dei criptofonini nostrani. "Invece di usare il normale canale "voce" noi facciamo transitare la chiamata su quello "dati" e lo cifriamo. È l'operatore telefonico, non i privati, ad essere tenuto a offrire una comunicazione in chiaro alla magistratura. Che se non riesce a disporre l'intercettazione può chiedere di disabilitare la linea". Non si scopre niente di cosa i sospetti criminali si stavano dicendo, ma tant'è. "D'altronde non è vietato connettersi in modalità cifrata al proprio conto corrente online, e si tratta sempre di dati".

I problemi rimangono, anzi aumenteranno. Il garante della privacy Francesco Pizzetti ne parlerà oggi nella sua relazione annuale al Parlamento: "Da tempo abbiamo verificato l'esistenza in commercio e anche su Internet di programmi che, una volta installati, consentono di localizzare costantemente l'apparecchio, rubarne i dati in esso contenuti e talvolta di ascoltare le conversazioni e leggere gli sms. In alcuni casi sono sistemi che possono avere usi "buoni", come consentire di rimanere in contatto durante un'escursione. Più spesso, però, no. L'uso di questi sistemi spia è e resta illecito e può dar luogo a gravi responsabilità penali". Programmi, dice, che "possono trasformare il cellulare in un delatore costante dei nostri comportamenti e quindi un nostro nemico".

E vista la quantità di informazioni intime, dall'agenda ai contatti, dalle foto alle dichiarazioni d'amore in 160 caratteri che gli confidiamo, la metamorfosi fa più paura di quella di Gregor Samsa.
(2 luglio 2009)

La url di questa pagina è <http://www.repubblica.it/2009/07/sezioni/tecnologia/privacy-telefoni/privacy-telefoni/privacy-telefoni.html?ref=hpspr1>

Abbonati a Repubblica a questo indirizzo
http://www.servizioclienti.repubblica.it/index.php?page=abbonamenti_page