

E vissero a lungo CRIPTATI e CONTENTI

POLITICI E VALLETTE,
ATTORI E BANCHIERI,
INDUSTRIALI E
CALCIATORI
FANNO LA FILA
PER DOTARSI
DI UN CELLULARE
CHE NESSUNO,
NEANCHE LA POLIZIA,
POSSA INTERCETTARE

di Mario Rossi

CONTRO LE INTERCETTAZIONI SI È SCATENATA LA

C'è un minimo comune denominatore che accompagna scandali e inchieste che, a ondate ricorrenti, si abbattono sul mondo del calcio, su quello dello spettacolo o su quello della finanza. Il filo rosso che li attraversa sono telefonini e intercettazioni, legali o illegali, che poi riempiono i faldoni delle Procure e le pagine dei giornali, finendo con il mettere in piazza anche i fatti più privati dei personaggi coinvolti. Fatti privati che, il più delle volte, non hanno alcuna attinenza con le inchieste in corso.

Siamo, insomma, un popolo di sorvegliati speciali: 33mila gli italiani con il telefono sotto controllo, secondo i dati forniti dal Ministero dell'Interno ed elaborati da Eurispes e 100 mila le intercettazioni legali effettuate ogni anno. Alle quali occorre aggiungere quelle illegali, ordinate da privati a investigatori senza scrupoli per te-

nere sotto controllo il calciatore che si sospetta incapace di seguire la disciplina del club, la moglie che si sospetta troppo compiacente con l'amico di famiglia (o il marito troppo affettuoso con la segretaria), la ditta concorrente che sta terminando una delicata ricerca o sta trattando un contratto internazionale.

LO SMARTPHONE DIVENTA INVIOLEBILE

E allora? Allora succede che si è scatenata la corsa al telefonino sicuro, a quello che nessuno, nemmeno la polizia è in grado di intercettare.

Ma esistono questi telefonini? Esistono, eccome! E cominciano anche ad essere alla portata di tutti. Sono telefonini (smartphone, per la precisione) sui quali viene montato un software in grado di filtrare le parole e trasformarle in pacchetti di dati incomprensibili a tutti,



CORSA ALLA CONQUISTA DEI TELEFONI INVIOLABILI

tranne che al cellulare gemello in mano alla persona con la quale si vuole chiacchierare indisturbati.

Alessandro Peroglio, direttore commerciale di Casper-tech, l'azienda torinese che produce Cryptech, il criptofonino (di cui parliamo a pag. 43) che oggi va per la maggiore, nomi non ne fa, ma conferma la corsa all'acquisto.

LA SICUREZZA NON È EGUALE PER TUTTI

"È successo - dice - che la gente ha capito quanto sia facile intercettare un cellulare. Non solo legalmente, ma soprattutto illegalmente. E corre ai ripari". Manager, professionisti, banchieri, politici (di ogni schieramento, abbiamo scoperto), giornalisti, e poi giù giù fino ai calciatori, alle stelle dello spettacolo (veline e tronie comprese), ai faccendieri e a chi si muove sul filo del codice penale fanno la fila per mettersi in tasca un

telefonino che li metta al sicuro da orecchie indiscrete. Ma questi apparecchi sono davvero sicuri? "Non tutti sono allo stesso livello - ammette PierPaolo Poli, di Speeka, che ha in listino tre diverse soluzioni (come diciamo a pag. 44) - ma non è detto che tutti abbiano bisogno dello stesso livello di sicurezza".

Resta il fatto che, come sottolinea Alessandro Peroglio, un buon sistema di sicurezza è davvero inviolabile anche per le forze di polizia che hanno un solo sistema per impedire questo tipo di comunicazione: far bloccare i telefoni dai gestori intervenendo sul codice IMEI. Non sapranno mai quali informazioni sono passate, ma almeno non ne passeranno di nuove.

Nelle pagine che seguono vi diamo una panoramica sui sistemi anti intercettazioni oggi a disposizione e vi diciamo anche quanto costano.

L'ENIGMA DI ALBERTI

Dice la leggenda che già Licurgo, tremila anni fa, avesse inventato un suo personale



sistema di cifratura, ma è Erodoto il primo testimone dell'importanza della crittografia in guerra. Racconta infatti di un nobile persiano che per far giungere ad Aristagora, tiranno di Mileto, delle istruzioni segrete, fece rasare il cranio di uno schiavo, vi fece tatuare le informazioni e poi inviò lo schiavo quando gli ricrebbero i capelli.

La prima macchina cifratrice di cui si abbia notizia fu inventata da un italiano nel XV secolo, Leon Battista Alberti. 500 anni più tardi, nel 1918, un tedesco brevettò una macchina, la famosa Enigma, che si basava sullo stesso principio ideato da Alberti.

Ed Enigma fu la protagonista delle grandi guerre del secolo scorso e solo la tenacia e la bravura del matematico inglese Alan Turing (inventore del primo calcolatore elettronico) riuscì a decifrare i crittogrammi di Enigma. Il che permise agli alleati di sconfiggere definitivamente la Germania di Hitler.



GLI "ABUSIVI"

 Sono assolutamente illegali, ma in realtà in rete si trovano diversi marchingegni e accrocchi più o meno artigianali con i quali lo spione "fai da te" può mettere

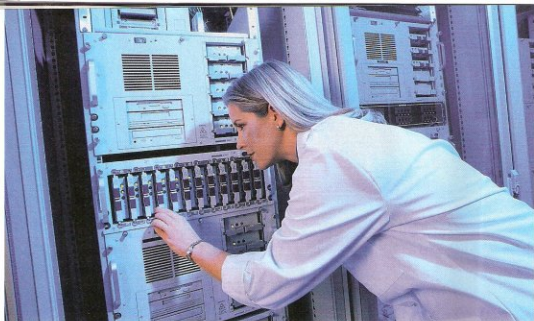
sotto controllo il coniuge, i figli, l'impiegato che si sospetta poco fedele o il concorrente. Si tratta di regola di microspie ambientali nascoste dentro un cavo o una spina telefonica e capaci di trasmettere fino a 700 metri di distanza voci e rumori capte all'interno di una stanza. Ma il rischio peggiore è quello di trovarsi fra le mani (magari come regalo di Natale e di compleanno) un cellulare nuovo che, in realtà, nasconde al suo interno un chip che



ritrasmette a un determinato numero di cellulare ogni telefonata fatta o ricevuta. E in questo caso oltre al danno c'è anche la beffa: le telefonate ritrasmesse vengono addebitate allo spiatto!



ritrasmette a un determinato numero di cellulare ogni telefonata fatta o ricevuta. E in questo caso oltre al danno c'è anche la beffa: le telefonate ritrasmesse vengono addebitate allo spiatto!



QUANDO IL "GRANDE ORECCHIO" DIVENTA LEGALE

Solo l'Autorità giudiziaria può ordinare di mettere sotto controllo una linea telefonica (fissa o mobile), quando presume che su quella linea transitino comunicazioni legate a ipotesi di reato. Le intercettazioni si realizzano usando una linea definita Res (Receiver End System) affittata dalla Pro-

cura presso il gestore telefonico. La linea collega la rete telefonica cui fa capo l'utenza da sorvegliare alla sala intercettazioni dove ci sono i server che archiviano tutto il traffico telefonico che parte o arriva a quell'utenza.

Quando il telefonino sotto controllo viene acceso, segnala immediatamente, attraverso i numeri IMEI e IMSI (i codici del telefonino e della SIM) e una triangolazione con le antenne della rete, la propria posizione.

Appena il telefono viene usato per una telefonata, il server registra in modo automatico tutta la conversazione. Se al suo proprietario viene assegnato un determinato codice di pericolo, la telefonata viene ascoltata in tempo reale da un agente che trasmette immediatamente il testo al giudice che conduce le indagini.

Le altre telefonate vengono archiviate su CD e quindi sabbinate per essere comunque a disposizione del giudice e della sua inchiesta.

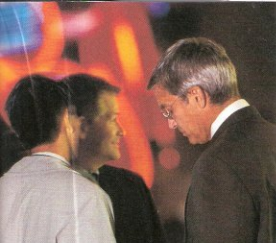


IL MITO DI ECHELON NON COLPISCE I CELLULARI?

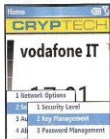
Echelon, la gigantesca rete di stazioni di intercettazione che gli Usa e gli alleati hanno messo in piedi subito dopo il secondo conflitto mondiale, continua a far parlare di sé. Da grande fratello che tutto scruta e tutto annota, il suo mito è stato sgretolato e ridotto a quello di banale spia commerciale. Questo è almeno il risultato di una inchiesta commissionata dal Parlamento Europeo a un giornalista investigativo inglese. Duncan Campbell affermava nel 1988 (ma da allora la tecnologia è radicalmente cambiata) che "non sono ancora disponibili strumenti automatici di riconoscimento di una specifica parola nell'ambito di una telefonata". In realtà pare che il vero problema di Echelon

sia la difficoltà di intercettare i cellulari dalle stazioni sintonizzate su Intelsat, il sistema su cui si appoggia Echelon, il quale oggi si limiterebbe a intercettare le comunicazioni fra i grandi gruppi europei per favorire le industrie Usa. A patto che i gruppi europei non usino i telefoni anti intercettazione di cui si parla in queste pagine.

 Perché in questo caso anche il mitico Echelon non riesce a intercettare altro che una serie di rumori indistinti.



Dr JEKYLL E Mr HYDE



Il criptofonino di CasperTech funziona come un normalissimo telefono e permette qualsiasi chiamata. Diventa inviolabile quando si decide di attivare il Cryptech con l'altra metà della coppia



Il tipo di chiamata (in chiaro o criptata) dipende dal tasto che si preme una volta digitato il numero. Se è criptata, appare l'avviso che avverte dell'attivazione del protocollo Diffie-Hellman



Il sistema costa 1.650 euro ai quali occorre aggiungere il prezzo del cellulare prescelto e l'IVA. 300 euro costa invece il software per criptare gli SMS, che va installato a parte

CRYPTTECH, L'INVOLABILE

"L'algoritmo AES 256 è alla base dei moderni sistemi di cifratura; è a disposizione di chiunque lo voglia usare e in effetti viene impiegato quasi da tutti (anche se taluni si sono fermati al più debole AES 128). Ma quello che gli altri non hanno è il protocollo Diffie-Hellman a 2.048 bit interfacciato al nostro sistema di chiavi simmetriche". A spiegare come funziona il sistema brevettato da CasperTech sui suoi cellulari è Pavel Ivanov, direttore tecnico della società nata nel 2003 nell'ambito dell'incubatore del Politecnico di Torino. "I nostri criptofonini - continua - sono smartphone con sistema operativo Windows Mobile sui quali installiamo il sistema di cifratura, compilato per ogni singolo apparecchio".

Le telefonate sono assolutamente protette in quanto avvengono tra una coppia di criptofonini che condividono una serie di chiavi di riconoscimento. Non solo: a ogni telefonata tra i due cellulari il sistema genera una chiave di cifratura diversa che nemmeno la CasperTech riesce a prevedere. La voce viene trasformata in dati, che vengono organizzati in pacchetti e spediti all'interlocutore attraverso il canale CSD. All'altro capo i pacchetti vengono rimessi in ordine, decifrat e ritrasformati in voce. Il tutto in meno di un secondo, tanto che conversando non ci si accorge del ritardo, anche perché il traffico si svolge in full duplex e non c'è il fastidioso effetto satellite.

ASSICURATO A VITA

Gli smartphone utilizzati da CasperTech come i Qtek e gli HTC che assicurano un ottimo funzionamento. Ma, sottolinea il direttore commerciale Alessandro Peroglio, "siamo in grado di installare il sistema anche su altri smartphone Windows Mobile, purché il processore abbia i requisiti necessari, che sono, sostanzialmente, una velocità di almeno 200 MHz".

I cellulari vengono venduti (il distributore in Italia è Emotion) almeno in coppia (le aziende in realtà ne acquistano lotti interi per creare vere e proprie reti inviolabili) e il sistema viene acquistato a vita. Questo significa che è possibile a un certo punto cambiare cellulare e far traslocare il sistema dal vecchio al nuovo. E in caso di furto il sistema diventa inutilizzabile e il ladro non riesce nemmeno ad arrivare a leggere la rubrica. Dati salvi, dunque, e inviolabili.



Gli HTC S620 (a sinistra) e S310. Soprattutto il primo è prediletto dagli uomini d'affari, grazie alla tastiera estesa che lo rende adatto alla gestione della posta elettronica



Il Qtek 8500 è il modello preferito dai personaggi dello spettacolo e dai mondo femminile. Elegante e supersottile piace anche a una parte del mondo politico

L'SMS SI AUTODISTRUGGE

CasperTech non ha pensato solo alla voce, ma anche ai messaggi di testo. SmsCrypto lavora con lo stesso algoritmo usato per rendere indecifrabile la voce. Si compone il testo e poi lo si invia. L'SMS (che non ha limiti di lunghezza) viene filtrato dall'algoritmo, reso illeggibile e trasmesso al destinatario che, per decifrarlo, deve avere la stessa applicazione e inserire una password concordata in precedenza. Una volta letto, il messaggio si autodistrugge senza lasciare alcuna traccia.



Il Siemens S35 elaborato da tedeschi Rohde & Schwarz. Il telefono è molto robusto ma il prezzo (6.000 euro ad apparecchio) lo pone a un livello difficilmente accessibile per un privato



Ecco come si presenta il display di uno smartphone con schermo touchscreen con il sistema di Secure GSM. A fianco il quadro comandi per la gestione avanzata dell'audio e del microfono

LA SICUREZZA SI COMPRA ANCHE ON-LINE

Se il criptofonino di CasperTech (che abbiamo provato) ci ha fatto un'ottima impressione per facilità d'uso e qualità della trasmissione, non possiamo ignorare che in commercio ci sono altri sistemi di cifratura delle telefonate. Un secondo sistema che abbiamo provato è infatti il Secure GSM distribuito in Italia da Speeka. Si tratta di un software (una versione demo la si può addirittura scaricare da Internet) che viene fornito con una chiave seriale valida per una coppia di cellulari al costo di 250 euro per telefono. Si installa con facilità su uno smartphone dotato di Windows Mobile e il suo utilizzo è sufficientemente intuitivo, una volta attivata la trasmissione CSD.

I suoi limiti sono che non esiste il modulo per cifrare gli SMS e funziona solo fra cellulari e non fra cellulare e linea fissa. In più noi abbiamo riscontrato qualche problema di audio a seconda del modello di smartphone sul quale lo abbiamo di volta in volta installato.

La stessa Speeka, in compenso, distribuisce altri sistemi di cifratura: si tratta di Enigma, un cellulare (da 1.900 euro) con il software preinstallato. Si tratta di un dual-band di produzione coreana con una chiave di cifratura a

128 bit (quasi tutti gli altri ormai viaggiano a 256 bit) e che in Italia ha un suo mercato. Più costoso (ma apprezzato da governi e ambasciate) l'altro cellulare di Speeka; si tratta di un vecchio Siemens S45 (anno di produzione il 2001) nel quale i tedeschi di Rohde & Schwarz hanno montato un sistema proprietario, un cryptochip. Anche qui la chiave di cifratura è a 128 bit e costa ben 6.000 euro ad apparecchio.

I SISTEMI CIFRATI PER SYMBIAN

Si è parlato di smartphone con Windows Mobile. E gli smartphone con Symbian (i Nokia, i Sony Ericsson e qualche Samsung)? Ci sono tre software: il russo GLK che non cripta SMS e telefonate a rete fissa e che, funzionando come half duplex, trasforma il cellulare in un walkie talkie. Costa sui 1.000 euro. Poi c'è un software anglo-tedesco, il Babilon NG. Lo abbiamo visto al CeBIT di Hannover, ma nemmeno i suoi dimostratori quella mattina sono riusciti a farlo funzionare. Infine dalla Slovacchia giunge notizia di un sistema Silentel: un'applicazione divisa tra hardware e software ancora allo stadio di prototipo.

COME GLI USA PER 50 ANNI HANNO SPIATO IL MONDO

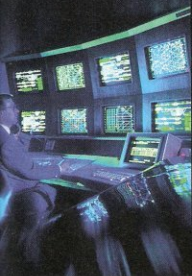
C'è chi cripta e chi decripta. E c'è anche chi fa il doppio gioco: vende sistemi di cifratura a governi e grandi aziende e vende le chiavi per decifrare quei messaggi a un altro governo, o meglio - a un servizio segreto legato a quel governo. Lo scandalo è venuto alla luce nel 1992, ma è tornato d'attualità qualche anno fa. Protagonisti la Crypto AG, società svizzera che aveva legato la sua reputazione alla sua neutralità, il BND, Bundesnachrichtendienst, vale a dire il servizio segreto tedesco, e la NSA, National Security Agency, l'agenzia americana per la sicurezza nazionale.

Il merito di aver scoperto la tresca va ai servizi segreti iraniani. In sostanza pare che la Crypto per mezzo secolo avesse fornito i ser-

vizi di cifratura ai governi di mezzo mondo (compreso il Vaticano), consegnando algoritmi e chiavi di cifratura che venivano passate anche al governo americano che era quindi in grado di leggere i messaggi cifrati con la stessa facilità con cui la mattina leggiamo il giornale. Secondo una fonte, in alcuni casi gli algoritmi e le chiavi di cifratura sarebbero stati addirittura manipolati, prima della consegna, anche dal BND tedesco. Dal 1993 a oggi ci sono state inchieste, processi e patteggiamenti condotti in gran segreto, ma quasi nulla di ufficiale è trapelato. Vale il detto secondo il quale i panni sporchi si lavano in famiglia. E non c'è miglior famiglia di quella dei servizi segreti.



Enigma, il cellulare coreano di Speeka: il sistema funziona con due SIM, una proprietaria e l'altra personale del cliente





DALLA SVEZIA CON BLUETOOTH

Anche gli svedesi della Sectra stanno lavorando a un loro sistema di cifratura che pare verrà a costare 4.800 euro. Si tratta di un generatore di chiavi esterno. Per il suo uso sarà indispensabile un collegamento Bluetooth.



MODULO SNAPCELL

Arriva da Israele lo Snapcell (in Italia è distribuito da CTE). Si tratta di un modulo scrambler del costo di 900 euro e realizzato per i cellulari Sony Ericsson. È una soluzione piuttosto invasiva (il modulo esterno si nota parecchio, come i vecchi moduli fotografici) che, inoltre, costringe all'uso di un auricolare.

LE PROPOSTE SU INTERNET

Per capire quanto sia delicato il problema della segretezza delle comunicazioni, basta cercare un po' in Internet e si scoprono decine di aziende che propongono sistemi "esclusivi" e "strabilianti". Ci sono i francesi di ERcom che propongono un SecPhone (secret phone) che però non si è ancora visto sul mercato; ci sono i tedeschi di Securestar con il loro PhoneCrypt, un software da 400 euro pubblicizzato come di grado militare, ma che pare sia di difficilissima installazione. Poi ci sono gli svizzeri di CTS-Swiss con un vecchissimo cellulare venduto a 4.000 euro e con un algoritmo proprietario. E non potevano mancare i russi e gli americani. I primi propongono un Signal-com, software certificato da Mosca (certamente non il miglior biglietto da visita per l'Occidente); gli americani di ELS Technologies pubblicizzano invece un loro software di cui viene reso noto soltanto il prezzo (1.200 euro circa). Un po' poco per fidarsi appieno.

nel PROSSIMO NUMERO in PROVA



- ▶ HTC S710
- ▶ Motorola MOTORIZR Z8

... e altre sorprese

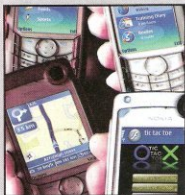


SPECIALE Mobile Navigation

Tutti i navigatori per smartphone e PND che vi guideranno sulle strade delle vacanze
Novità, prezzi e funzioni

TUTORIAL: PROGRAMMI

Quali software acquistare e come utilizzarli. Una guida ai programmi più utili, spiegati passo per passo, schermata per schermata.



LISTINO HI-TECH: smartphone, palmari, software di navigazione, PND e stampanti

in **EDICOLA** a **GIUGNO**