

SMARTPHONE

MAGAZINE

CELLULARI | PALMARI | NAVIGATORI | SOFTWARE E GIOCHI



**INTERGETTAZIONI
COME DIFENDERSI**

**Qualcuno
è in ascolto**



NAVIGATORI GPS

- ▶ TomTom Go 910
- ▶ Navman ICN750
- ▶ Mio C210
- ▶ Route66 Mobile 7 WMS



in REGALO
**UN ESCLUSIVO ACCESSORIO
PER IL VOSTRO CELLULARE**

AGOSTO/SETTEMBRE 2006 € 3,90
Periodico bimestrale - Anno 2 - n° 4

IL MONDO IN TASCA



Come archiviare
musica, foto,
video, appunti,
vocali, testi
e presentazioni
in 4 grammi
di memoria

LAB TEST

- ▶ Samsung i320N ▶ il più sottile al mondo
- ▶ Sony Ericsson P990i ▶ foto e business
- ▶ Nokia E61 ▶ l'e-mail sempre in tasca
- ▶ HTC MTeoR ▶ on-line alla velocità dell'UMTS



IMPARIAMO A...



Configurare
e utilizzare
la connessione
Wi-Fi del nostro
smartphone

IN ANTEPRIMA

- HTC TyTN ● BlackBerry 8707v
- i-mate PDA-N ● Sony Ericsson M600
- Fujitsu-Siemens LOOX T830

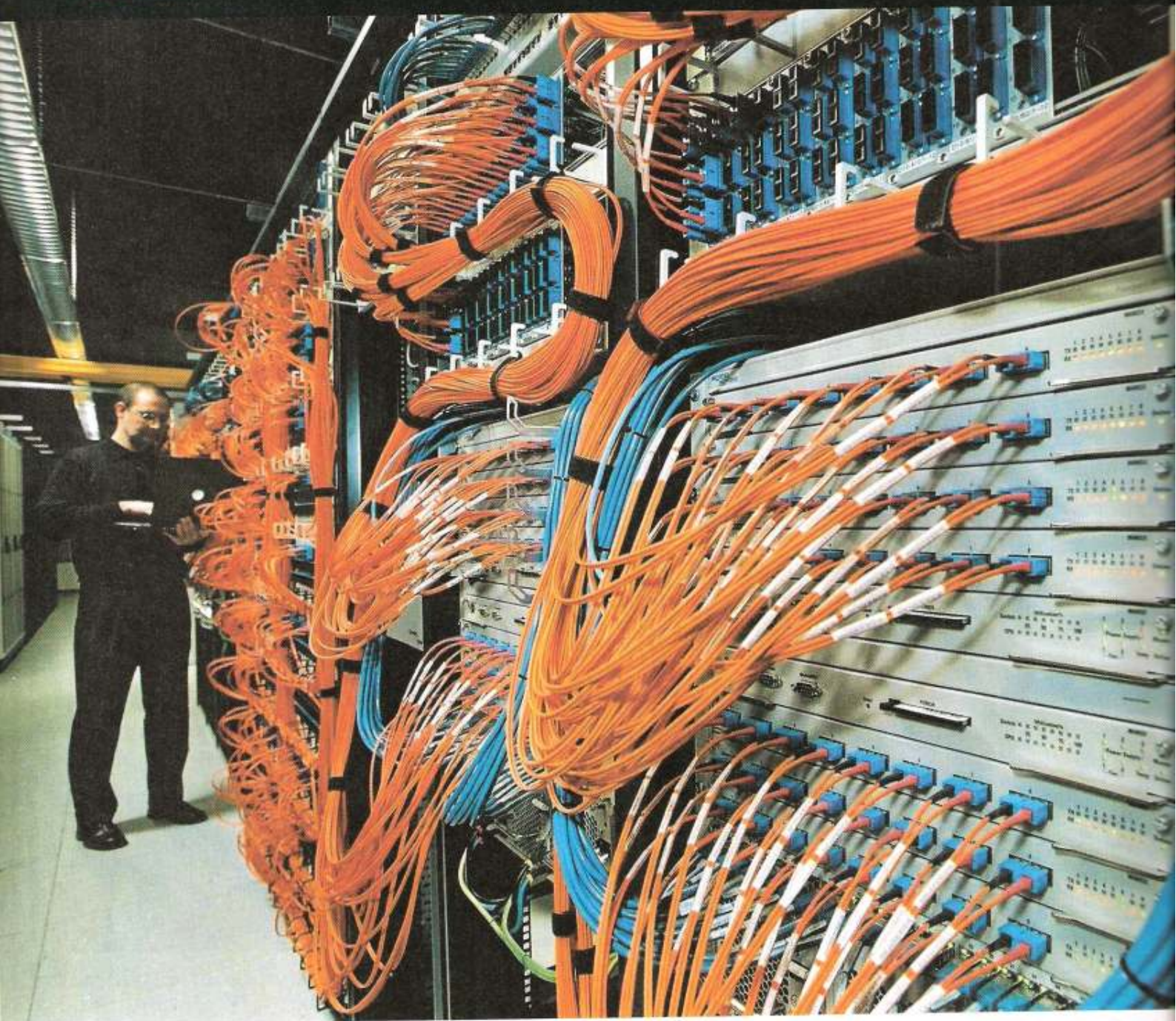


ATTUALITÀ
Dagli studi Tv
al cellulare.
Tutti i segreti
della Mobile Tv



ATTUALITÀ ■ intercettazioni telefoniche

I CELLULARI SPIA E I SEGRETI PER PROTEGGERE LE NOSTRE TELEFONATE



QUELLA DELLE INTERCETTAZIONI
STA DIVENTANDO UNA VERA
E PROPRIA SINDROME.
VI SPIEGHIAMO QUALI SONO
I VERI RISCHI E LE PRECAUZIONI
EVENTUALMENTE DA PRENDERE

di Christian Boscolo

**QUALCUNO
è in ASCOLTO**

Basta sfogliare qualche quotidiano uscito negli ultimi mesi per rendersi conto di quanto sia attuale il problema delle intercettazioni telefoniche. Lo scandalo di "Calciopoli", le recenti vicissitudini del principe Vittorio Emanuele di Savoia e i cosiddetti "furbetti del quartierino" sono balzati agli onori della cronaca proprio a causa di questa nuova tecnica investigativa usata dagli inquirenti. In questo caso però parliamo di intercettazioni perfettamente legali, regolarmente autorizzate dalla magistratura su richiesta del Pubblico Ministero. Gli inquirenti si sono limitati a richiedere i dati all'operatore GSM interessato, che dispone in tempo reale di tutte le informazioni sensibili, come l'intestatario dell'utenza, i numeri dei chiamanti e dei chiamati, inclusa la possibilità di localizzare la posizione del cellulare acceso. Tutto in regola dunque e senza l'ausilio di nessuna diavoleria tecnologica. Ma è davvero impossibile intercettare la conversazione di un abbonato senza rivolgersi all'operatore telefonico?

FILOSOFIA ZEN PER CELLULARE

Il proliferare dei telefoni spia ha dato il via ad una vera e propria guerra di marketing per la leadership in questo settore. Tra i messaggi pubblicitari più azzeccati e divertenti, abbiamo trovato un breve estratto del manuale di Sun Tzu, famosissimo stratega cinese e autore di un saggio sull'arte della guerra:

- **Conoscendo il vostro nemico e voi stessi in cento battaglie non perderete mai**
- **Quando non conoscete il nemico ma conoscete voi stessi avrete la stessa possibilità di vincere o perdere**
- **Se non conoscete né il vostro nemico, né voi stessi sicuramente perderete tutte le battaglie.**

LA RETE GSM

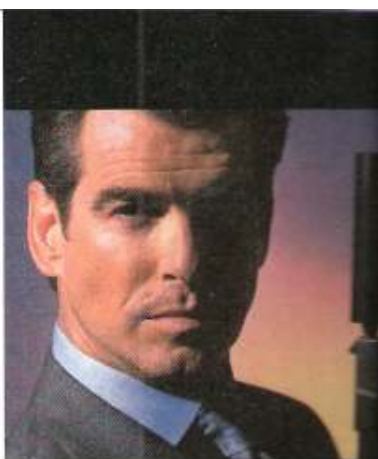
Il Global System for Mobile Communications (GSM) è attualmente lo standard di telefonia mobile più diffuso del mondo. Si stima che più di 2 miliardi di persone in 200 Paesi usino questo tipo di telefoni cellulari. Uno dei motivi che ha maggiormente contribuito alla diffusione di questo standard è stata la possibilità da parte degli utenti di accedere a tutta una serie di nuovi servizi a costi molto contenuti. Tutte le chiamate effettuate tramite telefono GSM sono "criptate", ovvero protette da un algoritmo che trasforma il segnale voce e impedisce di ascoltare una conversazione tramite un normale ricevitore.

Al momento gli algoritmi di protezione più diffusi sono l'A5/1 e l'A5/2. Il primo garantisce il maggior livello di protezione ed è utilizzato prevalentemente in Europa, mentre il secondo, nonostante sia utilizzato in molti altri Paesi, offre un livello di sicurezza più basso. Entrambi si sono però rivelati vulnerabili, tanto che sono stati previsti automatismi di cambio dell'algoritmo in caso di necessità. Nel 2002 il gruppo SAGE (Security Algorithms Group of Experts) dell'ETSI (European Telecommunications Standards Institute) aveva sviluppato un nuovo algoritmo denominato A5/3 e considerato da molti a prova di intrusione. Questo nuovo codice di protezione è però rimasto nel cassetto dei suoi inventori. I principali gestori di telefonia mondiale hanno infatti giudicato i costi per applicarlo ai loro servizi di telefonia troppo alti.

Anche se sembra spento, il cellulare spia può essere attivato a distanza e da quel momento si trasforma in un microfono indiscreto

BADA A QUEL CHE DICI...

Tra i metodi di intercettazione indiretta il più semplice e a buon mercato è quello di utilizzare un telefono spia. Ne esistono ormai a centinaia e sono facilmente reperibili su Internet digitando le parole: telefono + spia. Il sito www.endoacustica.com propone diversi modelli, quasi tutti marchiati Nokia. Del tutto simili ai normali telefoni in commercio, questi apparecchi sono in grado di trasformarsi in piccoli microfoni ambientali, con un raggio di ascolto di circa 5 metri. I più sofisticati sono anche in grado di fornire informazioni sui numeri chiamati, i messaggi ricevuti e addirittura di localizzare il telefono.



UNO 007 SENZA LICENZA DI UCCIDERE

La mania del telefonino non è una prerogativa esclusivamente italiana. Anche i palestinesi hanno sviluppato una spiccata dipendenza per i cellulari e i servizi di sicurezza israeliani hanno pensato bene di sfruttare questa debolezza. Secondo una notizia riportata da diversi organi di stampa internazionali, gli 007 di Gerusalemme hanno ascoltato per mesi tutto quello che veniva detto negli uffici di Arafat. Per farlo hanno sfruttato una nuova e segretissima tecnologia che permetteva di "registrare" anche a telefono spento tutte le conversazioni, utilizzando i telefoni dei suoi collaboratori come registratori remoti. Solo una soffiata avrebbe permesso al leader palestinese di scoprire la causa delle continue fughe di notizie.



IL TELEFONO INVULNERABILE

Il CRIPTOFONINO della torinese CasperTech è uno strumento molto sofisticato ma allo stesso tempo facilissimo da usare. Oltre ad assicurare telefonate non intercettabili, essendo uno smartphone con sistema operativo Windows Mobile 5.0, permette l'utilizzo di molte applicazioni tipiche di un notebook come Word, Excel, Outlook e navigare con Internet Explorer. Tutte queste operazioni pos-



CRITOFONINO

IN PILLOLE

Dimensioni:	107,5x46x17,5 mm
Peso:	106 grammi
Display:	65mila colori, 240x320 pixel
Standard:	Quadribanda GPRS/EDGE Classe 10 (4+2)
Memoria:	64MB RAM, 64 MB ROM
Memoria esterna:	SD/MMC
Processore:	TI OMAP 850 200 Mhz
Connessioni:	USB, Bluetooth e Wi-Fi
Fotocamera:	1,3 Megapixel
Batteria:	ioni di Litio da 1200 mAh

sono essere eseguite con la massima sicurezza; se il Criptofonino viene smarrito o rubato, tutti i documenti cifrati al suo interno non potranno essere decifrati da nessuno senza la password dell'utente. Ogni apparecchio è infatti unico e viene configurato con un software compilato in modo esclusivo per quel dispositivo.

La sicurezza delle comunicazioni viene garantita dalla cifratura con gli algoritmi più robusti (AES 256) e le tecniche più avanzate, senza contare che il team interno è costantemente al lavoro per rendere disponibili nuovi aggiornamenti di sicurezza.

Il prezzo di questo modello è di 1.950 euro + IVA: comprende hardware e software, con la garanzia che se il telefono viene smarrito o rubato, verrà sostituito in tempi brevi con soli 300 euro di spesa.

I clienti sono per la maggior parte manager di grandi aziende con un'età compresa tra i 50 e gli 85 anni, ma non mancano uomini politici e personaggi del mondo dello spettacolo...

E L'SMS, UNA VOLTA LETTO, SI AUTODISTRUGGE

Anche gli SMS possono risultare preda di fastidiose intercettazioni. Di solito le più pericolose sono quelle della fidanzata di turno, ma anche in ambito lavorativo la lettura fraudolenta dei messaggi potrebbe provocare non pochi problemi. Per questo la torinese CasperTech ha lanciato un nuovo prodotto: SmsCrypto. Si tratta di un sistema di messaggistica cifrato con lo stesso algoritmo che utilizziamo per la voce. Si può inviare un messaggio lungo quanto si vuole. Il ricevente (dotato anche lui dell'applicazione) inserirà la password concordata in precedenza con il proprio interlocutore e il messaggio verrà decifrato. Una volta messo in chiaro e letto, il messaggio non può essere salvato o esportato e si autodistrugge senza lasciare alcuna traccia.



I METODI DI INTERCETTAZIONE DIRETTA

Esistono discrete possibilità che una conversazione telefonica possa essere intercettata. Due ricercatori israeliani, Alex Biryukov e Adi Shamir, hanno recentemente dichiarato di aver scoperto come decodificare le conversazioni dei telefoni cellulari GSM senza investire cospicui capitali. Un comune personal computer (basta un Pentium con 128MB di RAM e un capiente disco fisso) collegato a un radio-scanner sarebbe sufficiente a esaminare il segnale di una chiamata di pochi minuti. In questo modo è possibile ricavare la chiave e utilizzarla per decodificare le successive conversazioni.

Un altro metodo molto diffuso è quello di utilizzare sistemi portatili che svolgono funzioni del tutto simili a un ponte radio GSM. Questi apparecchi, introdotti per la prima volta da GCOM Technologies, si sostituiscono in maniera forzata al ponte ufficiale del gestore, consentendo di decodificare il segnale radio. Questo sistema è molto efficace, ma richiede una certa vicinanza con il cellulare da controllare oltre ad avere problemi di costo.

Anche la clonazione della Sim card ha conosciuto un discreto successo, ma presupponeva la possibilità di avere in mano la scheda dell'interessato, che veniva poi duplicata tramite uno speciale software. Basta poi fare una piccola ricerca su Internet per scoprire che diverse aziende (soprattutto straniere) offrono apparecchi per intercettare le telefonate sui cellulari. I costi sono però esorbitanti: una stazione di ricezione può costare fino a 450 mila euro.



PIÙ SEGRETO DEL CODICE DA VINCI

Esiste un vero giallo sull'effettiva solidità del codice A5, l'algoritmo che protegge le nostre conversazioni sul cellulare. Si è sempre ritenuto che il codice fosse basato su una chiave a 64 bit, mentre sembra ormai certo che gli ultimi 10 bit di dati siano sempre volutamente resi pari a "0". Ciò comporta un vantaggio tangibile per i malintenzionati: un codice indebolito artificialmente da una sequenza fissa, richiederebbe "solo" poche ore per essere decifrato. Pare addirittura che già nel 1994 il professor Simon Sherpherd della Bradford University di Londra volesse denunciare la cosa, ma misteriosamente poi tacque. Nel 1998 David Wagner e Ian Goldberg, dell'Università di Berkley in California, comunicarono di avere scoperto anche loro un indebolimento del codice proprio a causa degli ultimi 10 bit. Insomma qualcosa di strano pare ci sia davvero: fantascienza o solo paranoia?



Su diversi siti (in massima parte stranieri, qualcuno italiano) vengono offerti numerosi modelli di telefoni, scelti tra i più popolari, ai quali è stata aggiunta una microspia attivabile anche a distanza

I TELEFONI POSSONO AVERE LE ORECCHIE

Vista la difficoltà nell'intercettare le comunicazioni via etere, molte aziende e servizi di intelligence sono ricorsi a metodi indiretti, sicuramente meno complessi, ma non per questo meno efficaci e ingegnosi. Proliferano così su Internet le offerte di cellulari-spia, veri e propri microfoni in miniatura camuffati da cellulare, in grado di registrare o trasmettere conversazioni e di essere attivati in remoto, anche grazie a un semplice messaggio SMS. I più evoluti permettono persino la localizzazione geografica del cellulare con un margine di errore di soli 50 metri! Inutile però sottolineare come questo tipo di pratica sia assolutamente illegale, come del resto si affrettano a rimarcare anche i gestori dei siti che li vendono, scaricandosi così da ogni responsabilità.

Difficile poi reperire i prezzi di listino, visto che quasi tutti questi rivenditori richiedono un contatto privato, ma in linea generale si parte da circa 700 euro per i modelli base, per superare abbondantemente i 1.000 euro con i modelli più costosi.

Chi li riceve in regalo normalmente non si accorge di nulla, perché il telefono lavora regolarmente: la funzione spia viene aggiunta. L'unica anomalia è la durata della batteria che cala in modo vistoso.



LA SPIA NASCOSTA

Sembra un normalissimo cellulare e solo un tecnico, smontandolo, può scoprire che al suo interno sono stati aggiunti dei componenti-spia



IL MITO DI ECHELON

È stato ridimensionato il ruolo di Echelon, la rete di stazioni di intercettazione che gli Usa e i suoi alleati hanno messo in piedi subito dopo il secondo conflitto mondiale. Da grande fratello che tutto scruta e tutto annota il suo mito è stato sgretolato e ridotto a quello di banale spia commerciale. La rete di intercettazione globale, in altre parole, esiste ma "non sono ancora disponibili strumenti automatici di riconoscimento di una specifica parola nell'ambito di una telefonata" scrive Duncan Campell, il giornalista investigativo inglese incaricato dal Parlamento Europeo di stendere un approfondito rapporto. In più l'uso dei cellulari e di Internet non può essere intercettato dalle stazioni sintonizzate su Intelstat. Così Echelon si riduce oggi a intercettare le comunicazioni fra i grandi gruppi europei per favorire le industrie Usa. I comuni mortali che usano il cellulare possono dormire sonni tranquilli.

LE COSE DA EVITARE

Volete poter conversare al telefono con la ragionevole sicurezza di non essere ascoltati? Stabilito che la garanzia assoluta non esiste, ecco comunque le cose che è meglio evitare di fare:

- Non accettate telefoni in regalo, neanche dal vostro lui (o dalla vostra lei) specie se è geloso
- Non installate programmi di provenienza ignota: potrebbero deviare automaticamente le chiamate a una terza persona
- Disattivate il Bluetooth appena avete smesso di usarlo e rendetelo "invisibile" per renderlo introvabile a PC o cellulari nei dintorni
- Non lasciate la SIM in mano a sconosciuti. Clonarla è un attimo, se si dispone dell'attrezzatura adatta
- Tenete sempre sotto controllo la spesa telefonica. Se si alza all'improvviso e senza apparenti ragioni evidentemente qualcuno lo sfrutta da remoto



TELEFONI CRIPTATI

Se intercettare un telefono tramite una postazione mobile è, come abbiamo visto, un'operazione complicata e costosa è facile intuire come i maggiori pericoli possano provenire dai metodi di controllo indiretto. I costi sono tutt'altro che proibitivi e sapere (regalandole un cellulare truccato) se la nostra fidanzata si intrattiene ancora con il suo ex è un investimento che non ha prezzo!

La necessità di proteggere le proprie telefonate è invece molto importante a livello industriale, quando a viaggiare nell'etere sono le informazioni sensibili delle grandi aziende. Lo spionaggio industriale è una piaga cresciuta a dismisura negli ultimi anni, tanto da giustificare gli enormi investimenti nel settore della sicurezza. È nato così il primo Criptofonino, un marchio registrato da un'azienda italiana con sede a Torino: la Casper Technology. Del tutto simile a un normale telefono cellulare, (ma è disponibile anche in versione palmare) il dispositivo della casa torinese permette la cifratura delle chiamate tramite l'algoritmo AES 256, considerato tra i più robusti sul mercato. Il sistema funziona naturalmente solo se la chiamata è effettuata verso un altro Criptofonino, ma è possibile effettuare telefonate in chiaro anche con i normali telefoni cellulari. I prezzi non sono poi nemmeno proibitivi, se sostenuti da un'azienda, considerato che il costo è di 1.950 Euro + IVA per il modello smartphone e di 2.050 + IVA per il palmare.

CONCLUSIONI

Un'ultima e doverosa precisazione riguarda la possibilità da parte degli inquirenti di intercettare il Criptofonino e la risposta è in questo caso negativa. Nemmeno l'autorità giudiziaria, anche facendo ricorso al gestore telefonico di appartenenza, sarebbe in grado di riprodurre il contenuto delle conversazioni.

Questo perché se è vero che si possono identificare l'intestatario dell'utenza e i numeri del chiamante e del chiamato, (nascondere l'IMEI è infatti un'operazione illegale) il contenuto rimane cifrato e quindi non identificabile. E questo è perfettamente legale visto che non si nasconde l'identità dell'utenza, ma solo il contenuto della conversazione, coperta, come sappiamo, dal diritto alla privacy. In definitiva, quindi, i modi per proteggere le nostre conversazioni esistono, sono perfettamente legali e neppure troppo costosi. E adesso chi lo dice a Luciano Moggi...

La sindrome da intercettazione ci rende prudenti

Non occorrono sondaggi ufficiali, che pure ci sono, per affermare che anche tra noi italiani è abbastanza diffusa la paura che le telefonate via cellulare vengano intercettate e ascoltate con una certa regolarità. Per questo moltissime persone evitano accuratamente di parlare di determinati argomenti quando conversano al telefono. Un po' di prudenza non guasta, specie se parliamo di lavoro, ma occorre comunque evitare di cadere nella paranoia: non è detto che ogni disturbo al telefono indichi la presenza di orecchie indiscrete

