Claudio Ballicu

Le microspie ambientali e telefoniche

Caratteristiche tecniche e metodologie di bonifica

Elaborazione grafica: *Simon Mago*

Le microspie ambientali e telefoniche

Caratteristiche tecniche e metodologie di bonifica

Un'approfondita descrizione delle microspie classiche e dell'ultima generazione

Quali le loro caratteristiche e quali i limiti tecnici?

Quanto è facile spiare le nostre telefonate e come ci possiamo difendere?

Progetto grafico, copertina, ricerche iconografiche, disegni e foto di Claudio Ballicu

Finito di stampare nel gennaio 2014

Edizione digitale PDF del gennaio 2014

Indice

Nota importante
da leggere con attenzione
prima di proseguire:

Gli utilizzi impropri di alcune delle informazioni contenute in questo libro, potrebbero portare alla violazione della Legge 8 aprile ‘74 n. 98, artt. 615bis, 617, 617bis, c.p. e della Legge 226 c.p.p. sulla riservatezza della vita privata e sulle intercettazioni delle comunicazioni, nonché della Legge n. 675 del 31/12/96 sulla raccolta dei dati personali e sul diritto alla privacy.
L’autore declina ogni responsabilità sull'eventuale uso illecito delle informazioni fornite. Infatti, questo libro vuole avere solamente uno scopo didattico ed esplicativo, teso a illustrare le modalità con le quali è possibile effettuare una intercettazione telefonica o ambientale e come è possibile difendersi da queste intrusioni nella sfera del privato, e non vuole essere in alcun modo un invito o un incoraggiamento a mettere in pratica quanto descritto.

Il semplice fatto di proseguire nella lettura, implica l'accettazione di quanto sopra.

N.B.: I dispositivi descritti e/o fotografati, presenti in questa monografia, sono di proprietà dell’autore, non sono in vendita e hanno il solo scopo di chiarire l’argomento di cui trattasi. I relativi fabbricanti e/o distributori, non sono in nessun modo collegati economicamente con l’autore della presente monografia.

Profilo biografico dell'autore

Claudio Ballicu è nato a Roma nel 1949, dove vive e lavora. È perito in elettronica industriale e telecomunicazioni e laureato in Scienze dell'Investigazione.
Autore di pubblicazioni nel campo della meccanica serraturiera e delle casseforti, del misterioso settore dello spionaggio elettronico e dell'indagine sulle cause di incendio, sulla rivista del settore "Force-Security", ha tenuto seminari sul tema della ricerca di tracce forensi nelle serrature sottoposte ad apertura clandestina nelle università di Aquila e Camerino e sulle tecniche di bonifica da microspie, presso la Facoltà di Giurisprudenza e presso la Facoltà di Informatica dell'Università di Camerino e presso il dipartimento di Scienze della Formazione dell'Università di Macerata.

Effettua perizie forensi e consulenze, nel campo serraturiero-casseforti e dei dispositivi elettronici anticrimine per il Tribunale di Roma, ove è iscritto dal 2005 nelle liste dei Consulenti Tecnici del Giudice, e per privati e compagnie assicurative.

Si occupa, inoltre, di tecnologie di ricerca e bonifica di microspie ambientali e/o telefoniche e localizzatori satellitari GPS e di tutto quanto concerne la sicurezza della vita privata.

È autore e curatore del sito internet www.perizieforensi.com, ricco di notizie sul mondo delle microspie, della sicurezza anticrimine e della protezione da intrusioni negli archivi dei dati digitali aziendali.

Collabora, su tutto il territorio nazionale, con importanti Studi Legali effettuando consulenze tecniche e indagini difensive (art.11, legge 7 dicembre 2000, n. 397).

Premessa

In Italia le attività di intercettazione telefonica, ambientale, telematica e informatica, sono rigidamente disciplinate dal Codice di Procedura Penale e consentite alla sola Autorità di Polizia Giudiziaria, eventualmente con la collaborazione del gestore telefonico, su provvedimento motivato del Pubblico Ministero che deve preventivamente richiedere l'autorizzazione al Giudice per le Indagini Preliminari secondo il dispositivo di cui all'art. 266 del c.p.p. (*Intercettazioni di conversazioni o comunicazioni*).

L'autorizzazione può essere concessa, secondo i limiti di ammissibilità contenuti nello stesso dispositivo (comma 1, da lettera A a F-bis e comma 2), con decreto motivato, solo in presenza di gravi indizi di reato, solo quando l'intercettazione sia assolutamente indispensabile ai fini della prosecuzione delle indagini e solo per un periodo di tempo limitato (circa quarantacinque giorni, rinnovabili su richiesta, anch'essa motivata).

A tutto ciò si può, parzialmente, derogare nei soli casi di urgenza: *"Quando vi è fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio alle indagini"*.

In tali evenienze, il P.M. può disporre direttamente questo mezzo di ricerca della prova, con decreto motivato che va comunicato immediatamente, e comunque non oltre le ventiquattro ore, al Giudice per le Indagini Preliminari il quale, entro quarantotto ore dal provvedimento, decide, con decreto motivato, sull'eventuale convalida. Se la disposizione del P.M. non viene convalidata, l'intercettazione deve essere immediatamente interrotta, i suoi risultati non possono essere utilizzati e devono essere distrutti.

1. Le possibilità di intercettazione

I moderni dispositivi elettronici per le intercettazioni telefoniche, ambientali, telematiche e informatiche consentono, non solo teoricamente, a chiunque sia dotato di un minimo di manualità e di conoscenze tecniche anche superficiali, di effettuare con facilità e a costi contenuti, delle intercettazioni.
Anche coloro che non avessero la benché minima dimestichezza con questa tecnologia, possono facilmente trovare qualche tecnico, troppo disinvolto, disponibile a effettuare per loro conto tale incombenza.

Quando parlo di "disinvoltura", mi riferisco al fatto che le intercettazioni, ambientali, telefoniche o telematiche che siano, se abusive, sono perseguite da precise sanzioni del Codice Penale (vedi l'appendice al termine di questo libro), oltre a essere, ovviamente, del tutto inutilizzabili in ambito processuale.

Fino a non molti anni addietro, il costo di una microspia professionale, a differenza di quelle classificabili a livello di "bufala", era a dir poco proibitivo.

Oltre alla microspia vera e propria, infatti, occorreva fornirsi di apparecchi radio appositamente progettati per ricevere le loro frequenze, invero un po' "speciali" e dotati della necessaria sensibilità per far fronte alle basse potenze di emissione proprie di questi dispositivi spionistici.

Al contrario, le microspie a basso costo, poco più che giocattoli, trasmettevano su frequenze ascoltabili con una comune radio o autoradio FM, allo scopo di evitare l'acquisto, e la spesa, di un ricevitore dedicato.

Purtroppo una comune autoradio è progettata per ascoltare trasmissioni commerciali che, di norma, sono emesse con potenze rilevanti, allo scopo di coprire una vasta area geografica e non

hanno bisogno quindi di una sensibilità eccessivamente spinta. Inoltre la selettività, ossia la capacità di separare due emissioni con frequenze vicine tra loro, non ha ragione di essere troppo elevata.

Diversamente da ciò, un ricevitore dedicato all'ascolto delle microspie, o anche un "radio scanner", nasce per ricevere segnali anche debolissimi e/o adiacenti ad altre emissioni di potenza ben maggiore. Quindi la selettività di questi apparati deve essere molto elevata, con conseguente incremento della complessità circuitale e, in ultima analisi, del costo finale.

Oggi le cose sono alquanto cambiate: le ricadute tecnologiche dovute, principalmente, allo sviluppo della telefonia cellulare e dell'informatica, hanno permesso un abbattimento dei costi, anche per gli speciali ricevitori denominati "radio scanners", tali da mettere le microspie alla portata di quasi tutte le tasche.

Modificare un telefono cellulare per trasformarlo in una spia ambientale attivabile da qualunque distanza è un'operazione abbastanza semplice e, tutto sommato, anche poco dispendiosa (vedi cap.14.1). Unica condizione: il telefonino deve essere dotato dall'origine di avvisatore a vibrazione, un dispositivo presente in quasi tutti gli apparecchi.

A questo punto, sorge spontanea una domanda: quanto è lontana la società del "Grande Fratello"? Quanto controlla ogni nostra singola azione?

(…..)

12. Dalla teoria alla pratica: le operazioni di bonifica

Cercare e individuare un'eventuale microspia, che ovviamente sarà stata accuratamente nascosta, non è cosa facilissima. È fondamentale operare con metodo razionale, non affidandosi al caso o a una ricerca empirica, improvvisata o, peggio, tirando a indovinare.

Il rischio è di non individuare il dispositivo e, di conseguenza, dare al cliente una falsa sicurezza che lo spingerà a parlare liberamente, senza il timore di essere intercettato, con le implicazioni che è facile immaginare.

Naturalmente i metodi usati dai tecnici di bonifica sono svariati e non è detto che l'uno sia migliore dell'altro: molto dipende dal tipo di strumentazione usata e, certamente, dal punto di vista strettamente personale, nonché dall'esperienza.

In queste pagine illustrerò il mio metodo personale, evitando accuratamente di criticare altri approcci che potrebbero essere altrettanto validi. Scopo di queste pagine, infatti, è fornire al lettore le cognizioni necessarie per individuare i "praticoni" del ramo, spinti dalla possibilità di un facile guadagno e muniti di strumentazioni piene di lucine lampeggianti e bip-bip più adatti a un videogame che non a una prestazione professionale.

(…..)

12.2 La misura dell'intensità di campo

Il passo successivo consiste nel misurare l'intensità di campo a radiofrequenza nel locale da bonificare, tramite il cosiddetto "spazzolone" (vedi figg.10 e 11), non dimenticando di confrontarlo con la situazione all'esterno. Questo perché al giorno d'oggi l'inquinamento elettromagnetico ha raggiunto livelli notevoli, tali da far rilevare segnali radio praticamente ovunque.
Gli onnipresenti segnali della telefonia cellulare, i vari dispositivi Wi-Fi e Bluetooth, le telecamere di sorveglianza wireless, i segnali delle radio e televisioni private ecc. sono inesorabilmente rilevati dai misuratori di campo, inducendoci a sospettare la presenza di una trasmissione radio dall'interno del locale che stiamo controllando.

2.
3. Fig.10

Un misuratore dell'intensità di campo a radiofrequenza (il cosiddetto "spazzolone") capace di arrivare oltre i 3.000 MHz

4.

5. Fig.11

Un misuratore dell'intensità di campo a radiofrequenza per misure fino a 13 GHz

Per queste ragioni dobbiamo sempre effettuare un confronto fra il campo a radiofrequenza esterno ai locali e quello all'interno poiché non è la sua presenza a essere determinante, ma un eventuale picco improvviso del segnale che indica la presenza di una trasmissione radio a breve distanza, di cui resta ovviamente da stabilire l'origine.

Insieme allo "spazzolone" è utile un frequenzimetro per campi ravvicinati, come ad esempio il "Digital Scout" della Optoelectronics (vedi fig.12), in grado di segnalare con una vibrazione la prossimità di un trasmettitore, indicandone anche la frequenza, con una fulminea analisi che dura meno di un secondo, spaziando da 10 MHz a 2.600 MHz.

Rivela senza problemi tanto i segnali analogici quanto i digitali, anche con impulsi RF (burst) più brevi 300 microsecondi e persino le futuristiche microspie che modulano in "frequency hopping" o "spread spectrum".

(…..)

14. I registratori telefonici

I registratori progettati appositamente per l'uso telefonico, sono facilmente reperibili nei negozi specializzati o tramite internet. In particolar modo, sul sito di aste E-bay, si trova a un prezzo contenutissimo un modello in grado di avviare la registrazione ogni volta che viene alzata la cornetta del telefono interrompendola alla fine della telefonata (vedi fig.16), in modo da ottimizzare lo spazio occupato in memoria, prolungando in modo determinante la durata della registrazione e abbreviando i tempi del successivo riascolto poiché sono stati eliminati tutti gli spazi morti fra le telefonate.

I files che produce, sono in formato MP3, quindi facilmente trasferibili e archiviabili in un computer. La memoria di massa del registratore è una comune scheda flash e da questa dipende la durata totale delle registrazioni che può arrivare anche a parecchi giorni.

Ma attenzione! Non dimentichiamo che le vigenti leggi in materia di tutela della privacy, proibiscono questo tipo di intercettazioni. Ignorarle espone a rilevanti sanzioni penali.

Si vedano, a tal proposito, nell'appendice alla fine di questo libro, le implicazioni connesse all'uso illegale degli apparati di intercettazione e/o registrazione.

Inoltre i regolamenti delle società telefoniche vietano espressamente qualunque tipo di manomissione della linea che non sia eseguita da personale autorizzato.

Malauguratamente, i divieti legali che ho ricordato più sopra sono tali soltanto per le persone oneste mentre, nell'ipotetica azione di qualche "curioso" troppo disinvolto, le cose sono ben diverse.

Fig.16
Un registratore digitale progettato per l'uso telefonico

È successo, infatti, in qualche caso, che tecnici della società telefonica scoprissero, del tutto casualmente, durante una riparazione o una normale manutenzione, un collegamento abusivo e illegale nel doppino telefonico al di fuori di un appartamento o di un ufficio o, peggio, una microtrasmittente all'interno di qualche centralina di derivazione Telecom.

Ma non è ancora tutto: è possibile realizzare facilmente e con una spesa ridicola una semplice interfaccia tra la linea telefonica urbana e un registratore a cassette o digitale (vedi schema in fig.17).

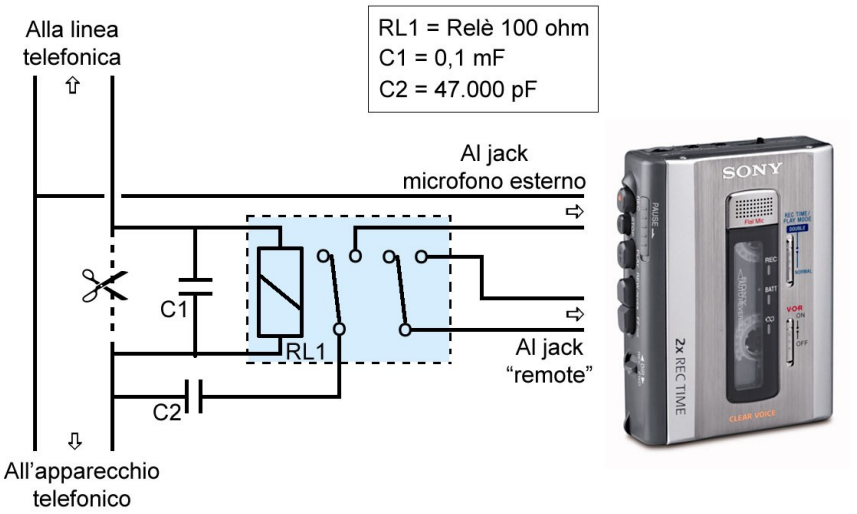

Fig.17

Schema di una semplice interfaccia
tra la linea telefonica urbana e un registratore

Un normale registratore, anche se di modesta qualità, è certamente sufficiente, purché sia dotato d'ingressi jack per il microfono esterno e per il comando a distanza. Quest'ultimo è semplicemente quello denominato "remote", presente su molti apparecchi.

Qui saranno collegati i contatti del relè, visibile nello schema elettrico, denominati "al jack remote". Se in qualche modello di registratore questo ingresso non fosse previsto, niente paura: basta usare lo stesso contatto di scambio per interrompere un polo delle pile di alimentazione ottenendo così lo stesso risultato, ossia far avviare il registratore quando viene sollevata la cornetta del telefono e fermarlo quando la comunicazione termina.

Questa è una condizione essenziale poiché, altrimenti, il nastro si esaurirebbe in poco più di un'ora.

Nota: *L'intercettazione consiste nella captazione, tramite opportuni dispositivi, di conversazioni che si svolgono a distanza mediante telefono (intercettazione telefonica) o fra presenti (intercettazione ambientale) ad opera di un terzo, non presente al colloquio né destinatario dello stesso.*

Non c'è intercettazione quando uno degli interlocutori registra la conversazione cui sta partecipando e quindi non s'intromette di nascosto nella comunicazione fra terzi o viene a conoscenza d'informazioni a lui precluse.

Allo stesso modo, non c'è intercettazione quando uno dei due interlocutori, al telefono, effettua una registrazione della conversazione, purché avvisi l'altro del fatto che sta registrando, ricevendone il consenso.

In ogni caso, tutto questo non implica la libertà automatica e incondizionata di divulgarne i contenuti.

Infatti, la "ratio" che disciplina le intercettazioni ha per scopo la tutela della riservatezza delle comunicazioni impedendo che un soggetto estraneo venga a conoscenza dei contenuti delle stesse.

Al contrario, quando un soggetto partecipa a una conversazione, vi è l'implicito consenso di tutti gli interlocutori alla condivisione delle informazioni espresse.

(…..)

19. Le microspie GSM

Come dicevo nel capitolo precedente, le microspie hanno ampiamente sfruttato i progressi tecnologici nel campo delle telecomunicazioni e non solo.

È il caso delle "cimici" che usano la rete telefonica cellulare per trasmettere a distanze virtualmente illimitate i loro segnali.

Si tratta di dispositivi che si differenziano da un normale telefonino solo per l'assenza di alcuni elementi che sarebbero inutili e inutilmente ingombranti. Ad esempio, il display la tastiera, l'altoparlante e la suoneria ecc. Tuttavia, pur se ridotte all'essenziale, le microspie GSM sono estremamente efficienti, tanto da occupare gradualmente il posto delle "cimici" di tipo classico, quelle di cui abbiamo trattato sinora.

Un'importante caratteristica delle microspie GSM, dal punto di vista della bonifica, è la loro difficile individuazione con i normali strumenti, siano questi dei misuratori di campo o analizzatori di spettro o altro.

Queste "cimici", infatti, trasmettono solo quando ricevono una chiamata dall'esterno, dal cellulare usato per spiare. Di norma, le microspie GSM sono "silenti" ad eccezione di quei modelli progettati per attivarsi automaticamente alla presenza di voci o rumori.

Il problema quindi consiste nella impossibilità di individuare un segnale radio quando non c'è! Come fare, dunque, quando si ha ragione di sospettare la presenza di una spia GSM?

Facciamo un passo indietro: si è detto che queste "cimici" funzionano come un telefono cellulare, pur con le dovute differenze. Dunque, come un cellulare, si attivano a intervalli di tempo più o meno lunghi, per comunicare alla cella telefonica più vicina la loro presenza e posizione in rete.

(…..)

22.1. Le microspie artigianali

Un discorso a parte va fatto per le microspie di realizzazione artigianale. In questo caso non è necessario preoccuparsi del numero di pezzi destinati all'esportazione o di leggi e regolamenti del paese di destinazione o di problemi di natura doganale.

Quasi sempre la microspia sarà realizzata in unico esemplare o comunque in un numero ridottissimo pezzi con l'unica preoccupazione di trovare un canale libero, relativamente alla zona geografica dove è destinata a essere usata.

Le frequenze sono comunque superiori ai 174,000 MHz di cui al capitolo precedente, anche se con alcune eccezioni delle quali si deve tener conto per eseguire una bonifica professionalmente corretta.

Alcune microspie artigianali usano, devo dire molto furbamente, frequenze inserite fra i canali UHF della TV digitale terrestre (DVB-T), magari non utilizzati nella zona.

Non è per niente facile trovare queste "cimici" con le loro piccole potenze, inserite fra emittenti che irradiano potenze molto rilevanti. In questi casi è prezioso l'aiuto dell'analizzatore di spettro purché di ottima qualità.

Le TV digitali appariranno sullo schermo come picchi di segnale intenso, ma con limitata banda passante, grazie alla modulazione di tipo digitale, mentre una microspia apparirebbe con un picco d'intensità modesta, ma con una larghezza di banda maggiore, dovuta alla sua modulazione in F.M.

Si tratta comunque di frequenze molto elevate, comprese fra i 510 e gli 860 MHz, con una notevole efficienza di trasmissione e che consentono l'uso di antenne di piccole dimensioni: l'ideale per una microspia!

Altre frequenze, utilizzate a volte in realizzazioni artigianali, sono quelle riservate agli apparati di debole potenza, deregolamentati da qualche anno in Italia e quindi in libera

vendita, chiamati LPD (Low Power Devices).

Realizzando una microspia sulle frequenze LPD, che vanno dai 433,075 ai 434,775 MHz con 69 canali, si utilizzano, ancora una volta, frequenze elevate e di notevole efficienza con l'uso di antenne di piccole dimensioni.

Inoltre non è necessario munirsi di un ricevitore scanner, che comunque avrebbe un costo notevole, ma si può acquistare un ricetrasmettitore LPD per una cifra molto contenuta.

Certamente qualche ricetrasmittente LPD sarà stata usata come microspia, bloccandola in trasmissione e collegandola con un alimentatore alla rete elettrica per superare il problema della durata delle batterie, nonostante le dimensioni, pur contenute, non siano esattamente minimali e nonostante il microfono sia poco sensibile, poiché progettato per essere tenuto vicino alla bocca.

La portata di queste ricetrasmittenti è, in campo aperto, di 2 o 3 Km. Nell'uso come microspia, dovendo occultare l'apparecchio e considerando la presenza delle pareti e di altro ostacoli, il raggio di azione è sicuramente molto inferiore. Maggiore comunque di una classica microspia.

(…..)

26. Le “microspie” nel computer

In questo capitolo non si parla di microspie “fisiche” nascoste all’interno di computer, anche se in qualche caso è realmente successo di rinvenire sofisticati dispositivi d’intercettazione in macchine da tavolo “desktop” grazie agli ampi spazi e all’alimentazione disponibile.
Non credo di andare troppo fuori tema, descrivendo sistemi d’intercettazione di tipo telematico, costituiti da immateriali quanto insidiosi software maligni definiti, non a caso, “malware”, contrazione dei termini inglesi “malicious” e “software” con il significato letterale di "programma malvagio".

Volendo tentare una prima classificazione di alcune categorie di “malware” che interessano l’argomento di questo libro e tenendo presente che la linea di separazione che le discrimina, quanto mai labile, è basata principalmente sugli effetti negativi sul computer involontario ospite, possiamo trascurare tutti quei codici maligni come:

- Virus: definizione generale di parti di codice maligno la cui specificità è diffondersi, autoreplicandosi, all'interno di programmi, o in particolari settori dell’hard-disk, in modo da andare in esecuzione ogni volta che il file infetto viene aperto. Si spostano fra computers diversi in seguito alla trasmissione di file infetti operato dagli utenti via internet o tramite supporti di memoria esterni.
- Worm: malware che non basano la propria diffusione sull’infezione diretta di altri file, ma agiscono sul sistema

(…..)

29. Alcuni casi reali di bonifica:

Fine di un molestatore:

La signora R.C. abitante in un quartiere residenziale di una città dell'Italia meridionale, era insistentemente molestata da un suo "ex".

Telefonate a tutte le ore del giorno e della notte, messaggi al cellulare, pedinamenti ossessivi, violente scenate in pubblico, avevano costretto la signora a denunciare il molestatore per il reato di "stalking" nella speranza di veder terminare questi atti persecutori. Inutilmente.

Arriva il giorno in cui l'uomo, programmatore informatico presso un'importante azienda di telecomunicazioni, è trasferito in un nuovo centro nel nord dell'Italia.

La signora R.C. trova finalmente un periodo di pace che è presto interrotto dal molestatore che sembra a conoscenza di tutti i suoi movimenti: la rimprovera di non essersi recata al lavoro in un certo giorno, vuole sapere il motivo, cosa ha fatto in casa!

Poi riprendono le telefonate ossessive e i messaggi sul cellulare e nella posta elettronica, finché la signora, esasperata, torna dai Carabinieri e sporge una nuova denuncia.

Neanche un'ora dopo lui le telefona, minacciandola per ciò che ha fatto, perfettamente a conoscenza dei suoi spostamenti. Troppo perfettamente!

Conosce il contenuto delle sue e-mail, sa delle sue telefonate e dei suoi SMS. Troppo perfettamente!

Inizia la bonifica:

Veniamo messi in contatto con il legale della signora R. che ci incarica di bonificare l'abitazione, il cellulare il computer e la macchina.

Dopo un breve esame tecnico, scopriamo che il cellulare era stato regalato alla signora proprio dal molestatore, che aveva provveduto a installare uno speciale software in grado di rinviargli il testo di tutti gli SMS e i numeri telefonici chiamati.

Il computer era affetto da un trojan che rilanciava ogni attività, e-mail, siti visitati ecc. A un server situato fuori dai confini nazionali, al quale l'uomo aveva, ovviamente, accesso.

Poco dopo iniziamo la ricerca di microspie occultate: dopo una breve ricognizione, gli strumenti di analisi dello spettro radio individuano una spia GSM/GPS occultata sotto il pianale della macchina, fissata con un paio di fascette da elettricista.

Si trattava di un dispositivo in grado di telefonare a un cellulare dello stalker segnalando la posizione della vettura su una mappa geografica. (Ovviamente ambedue le SIM, chiamante e ricevente, erano intestate a una persona deceduta!).

Evidentemente l'uomo, che aveva una copia delle chiavi della macchina e del passo carrabile dove era parcheggiata, aveva avuto il tempo di fare un lavoro accurato, collegando persino la microspia con la batteria dell'automobile mediante due sottili fili elettrici.

A questo punto occorreva dimostrare l'identità del molestatore: mi viene un'idea: allentare uno dei fili di alimentazione della spia così che sembrasse staccato a causa delle vibrazioni del motore!

Poi, installiamo tre telecamere nascoste. Una riprendeva l'ingresso del passo carrabile, la seconda l'automobile e la terza, occultata in un furgoncino parcheggiato che conteneva anche un videoregistratore "time-lapse", il cancello dall'esterno.

Passano così venti giorni senza che nulla accada poi, alle tre di una notte, arriva il molestatore… apre il cancello, entra, si sdraia sotto la macchina e controlla la microspia: sembra in ordine, nessuno l'ha rimossa! Apre il cofano e controlla i fili vicino alla batteria. Ah ecco cosa è successo! un filo staccato…bene. Provvede quindi a riallacciare il collegamento, armeggia un po',

forse per fissarlo meglio evitando che si stacchi di nuovo costringendolo a un lungo viaggio per ripristinarne il funzionamento.

Il giorno successivo la signora torna, insieme al suo legale, nella locale stazione dell'Arma. Quando lui la chiamerà, furioso, per sapere cosa è andata a raccontare ai Carabinieri, lei soddisferà la sua curiosità morbosa: "Sono andata a consegnare le prove che t'inchiodano alle tue responsabilità!".

Un molestatore "dilettante"

La signora M.T. di Roma, era molestata insistentemente da un corteggiatore, suo collega di lavoro, nonostante fosse sposata già da qualche anno.

Le solite denunce alle autorità non sembravano sortire alcun effetto positivo.

Improvvisamente, l'insistente corteggiatore sembrava conoscere il contenuto delle telefonate della signora M. i cui argomenti riferiva alla stessa vittima.

I coniugi facevano quindi una ricerca in internet, arrivando al mio sito. Ero quindi contattato con una e-mail per fissare un appuntamento.

Inizia la bonifica:

Il giorno stabilito eseguo una verifica elettronica nell'abitazione della signora, senza trovare nulla. Controllo quindi la sua automobile, con il medesimo risultato.

Mi viene in mente di controllare lo sportello di derivazione Telecom, posto nelle cantine del condominio e… bingo!

La serratura è palesemente forzata e all'interno trovo un microregistratore digitale, incartato in un foglio di alluminio da cucina, collegato ai morsetti telefonici con due pinzette a

coccodrillo. Un lavoro banale e dilettantesco ma indubbiamente efficace.

Dopo aver scattato alcune foto del registratore e della serratura manomessa, decidiamo di piazzare, nella cantina della signora M. T. un videoregistratore di sorveglianza con una telecamera puntata sull'armadio Telecom.

Inoltre, mi viene chiesto di redigere una perizia tecnica asseverata a giuramento che descriva quanto ho trovato, per supportare una successiva denuncia.

A distanza di tre mesi, però, il molestatore non è tornato a sostituire le batterie del registratore. Forse avrà "mangiato la foglia", non lo sapremo mai.

Fatto sta che, dopo la scoperta del registratore, le molestie che andavano avanti da più di un anno, sono improvvisamente cessate. Va bene così!

Una multinazionale troppo curiosa

Il sig. R.N. rappresentante di una grossa multinazionale, mi contatta, su indicazione di un comune amico, perché teme che i suoi spostamenti siano controllati dai suoi superiori diretti.

Alcune sue parole, pronunciate mentre viaggiava in macchina con un collega, sono giunte alle orecchie di un dirigente, così come alcuni suoi itinerari, durante le ore di lavoro.

Bisogna precisare che l'automobile da lui utilizzata è un mezzo di proprietà della multinazionale stessa che lui preleva dalla rimessa aziendale il lunedì mattina, per poi riconsegnarlo il venerdì sera, al termine dell'orario di lavoro. Quindi, se qualcuno che ha accesso al garage volesse nascondere una microspia all'interno dell'abitacolo, non incontrerebbe particolari difficoltà né correrebbe alcun rischio.

Inizia la bonifica:

Invito quindi il sig. R.N. a parcheggiare l'automobile in un mio box, appositamente attrezzato, dove inizio le operazioni di ricerca/bonifica che si risolvono rapidamente in una ventina di minuti con la scoperta di una "cimice" audio GSM inserita nella gommapiuma sotto il sedile a lato del conducente e collegata all'alimentazione del sedile regolabile elettricamente.

Inoltre, sotto al pianale del lunotto posteriore trovo un localizzatore GSM in grado di memorizzare gli itinerari percorsi con un'approssimazione di pochi metri.

Nonostante le apparenze, chi ha piazzato le due "cimici" non era certo un professionista nel campo e non ha saputo nasconderle con sufficiente abilità.

Il mio lavoro termina con la consegna di una relazione tecnica debitamente firmata e con l'invito a rivolgersi alle Autorità di Polizia per formalizzare una denuncia contro ignoti, ma il cliente preferisce lasciare le "cimici" al loro posto.

Conoscendo la loro presenza si comporterà adeguatamente. Inoltre teme che una denuncia possa portare a ritorsioni nei suoi confronti e persino al trasferimento in una sede in altra città.

(…..)

Appendice

Implicazioni sull'uso illegale degli apparati di intercettazione e/o registrazione.

È a tutti noto che anche l'autorità di polizia giudiziaria, qualora nello svolgimento delle indagini debba eseguire un'intercettazione telefonica o un ascolto ambientale, deve essere preventivamente autorizzata dalla magistratura che valuta, per ogni singolo caso, l'opportunità di concedere o meno tale autorizzazione.
Come già scritto all'inizio del libro, l'uso troppo "disinvolto" di microspie o di apparati di registrazione audio o video, può comportare la violazione di precise norme del Codice Penale. Ritengo pertanto utile pubblicare un estratto di tali norme al fine di palesare le implicazioni legali connesse.

Art. 614. Violazione di domicilio

Chiunque s'introduce nell'abitazione altrui, o in un altro luogo di privata dimora, o nelle loro appartenenze, contro la volontà espressa o tacita di chi ha il diritto di escluderlo, ovvero vi s'introduce clandestinamente o con inganno, è punito con la reclusione fino a tre anni. Alla stessa pena soggiace chi si trattiene nei detti luoghi contro l'espressa volontà di chi ha diritto di escluderlo, ovvero vi si trattiene clandestinamente o con inganno. Il delitto è punibile a querela della persona offesa. La pena è da uno a cinque anni, e si procede d'ufficio, se il fatto è commesso con violenza sulle cose, o alle persone, ovvero se il colpevole è palesemente armato.

Art. 615-bis. Interferenze illecite nella vita privata

Chiunque, mediante l'uso di strumenti di ripresa visiva o sonora, si procura indebitamente notizie o immagini attinenti alla vita privata svolgentesi nei luoghi indicati nell'articolo 614, è punito con la reclusione da sei mesi a quattro anni. Alla stessa pena soggiace, salvo che il fatto costituisca più grave reato, chi rivela o diffonde mediante qualsiasi mezzo d'informazione al pubblico le notizie o le immagini, ottenute nei modi indicati nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa: tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o a un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione d'investigatore privato.

Art. 617. Cognizione, interruzione o impedimento illeciti di comunicazioni o conversazioni telegrafiche o telefoniche

Chiunque, fraudolentemente prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo d'informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni o delle conversazioni indicate nella prima parte di questo articolo. I delitti sono punibili a querela della persona offesa: tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale o

di un incaricato di un pubblico servizio nell'esercizio o a causa delle funzioni o del servizio, ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione d'investigatore privato.

Art. 617-bis. Installazione di apparecchiature atte a intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche

Chiunque, fuori dei casi consentiti dalla legge, installa apparati, strumenti, parti di apparati o di strumenti al fine d'intercettare o impedire comunicazioni o conversazioni telegrafiche o telefoniche tra altre persone è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se il fatto è commesso in danno di un pubblico ufficiale nell'esercizio o a causa delle sue funzioni ovvero da un pubblico ufficiale o da un incaricato di un pubblico servizio con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio o da chi esercita anche abusivamente la professione di investigatore privato.

(…..)

Bibliografia

- R. Baroggi: Elaborazione e trasmissione dei dati a distanza: tecniche e metodologie, Angeli, Milano 1984
- L. Bertoni: Le intercettazioni. Mezzo di ricerca della prova nel processo, Nuova Giuridica, Macerata 2012
- J. Gleick: L'informazione. Una storia. Una teoria. Un diluvio, Feltrinelli, Milano 2012
- D. M. Huber: Robert E. Runstein, Manuale della registrazione sonora: Concetti generali, tecnologia audio analogica e digitale, attrezzature, procedure, Hoepli, Milano 1999
- W. Junghans: Il libro dei registratori audio, Franco Muzzio, Padova 1983
- Nazzaro Giovanni: Le intercettazioni sulle reti cellulari, Mattioli, Fidenza
- A. Paoloni, D. Zavattaro: Intercettazioni telefoniche e ambientali, Centro Scientifico Editore, Torino 2007
- G. Praetzel, E. F. Warnke: Il libro dei microfoni, Franco Muzzio, Padova 1979
- U. Rapetto, R. Di Nunzio: L'atlante delle spie: dall'antichità al "Grande Gioco" a oggi, Rizzoli, Milano 2002
- A. Tessitore, C. Marino: Intercettazioni elettroniche e informatiche, le tecniche, Sandit, Albino (BG)

Torna alla Home Page: http://www.perizieforensi.com/