CONSIGLIO SUPERIORE DELLA MAGISTRATURA

Incontro di studi sul tema:
Tecniche di indagine e rapporti tra p.m., polizia giudiziaria, consulenti tecnici e difensori

Roma, 4-8 luglio 2011

Gruppo di studio del 6 luglio 2011 ore 15,00

Le investigazioni con l'impiego di intercettazioni di comunicazioni e di flussi informatici o telematici

I nuovi strumenti di comunicazione telematica ed informatica: aspetti tecnici e questioni giuridiche

coordinatore:
dr Andrea Bonomo
Sost. Procuratore della Repubblica
presso la Procura della Repubblica di Catania

1. Il mutamento delle tecnologie nel settore delle comunicazioni telefoniche ed informatiche: telecomunicazioni digitali e satellitari, comunicazioni telematiche ed informatiche, profili tecnici e giuridici relativi alle intercettazioni.

Il Legislatore Italiano, spesso in adempimento di obblighi di cooperazione europea od internazionale, ha nell'ultimo decennio introdotto nell'ordinamento diverse disposizioni aventi come oggetto la tutela dei "sistemi informatici". A titolo di esempio si possono ricordare:
- L. 547/1993 (modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica);
- L. 197/1991 (norme per prevenire l'utilizzazione del sistema finanziario a scopo di riciclaggio);
- D. Lvo 82/2005 (Codice dell'amministrazione digitale; norme in materia di documentazione informatica e di firma elettronica e digitale)
- L. 248/2000 (modifiche alla legge 633/1941, in tema di diritto d'autore);
- L. 269/1998 (norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, anche condotti per via telematica);
- D. Lvo n. 196 del 30.6.03 (codice in materia di protezione di dati personali, così come modificato dalla Legge n. 45/2004);
- L. 38/2006 (disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet);
- L. 48/2008 (Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica).

Come sovente accade, in nessuna delle norme appena menzionate il Legislatore ha fornito una definizione precisa di "sistema informatico" o di "sistema telematico", e così è stato compito della Giurisprudenza e dell'interprete quello di rinvenirne una nozione unitaria che fosse compatibile con le esigenze di tutela dei diversi beni giuridici protetti, sottese alla copiosa produzione normativa in materia.
La Corte di Cassazione **(Sez. VI n. 3067 del 14.12.1999; Sez. V n. 31135 del 6.7.2007)** si è così pronunciata in materia: *"deve ritenersi "sistema informatico", secondo la ricorrente espressione utilizzata nella legge 23 dicembre 1993, n. 547, che ha introdotto nel codice penale i cosiddetti "computer's crimes", un complesso di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche parziale) di tecnologie informatiche, che sono caratterizzate - per mezzo di un'attività di "codificazione" e "decodificazione" - dalla "registrazione" o "memorizzazione", per mezzo di impulsi elettronici, su supporti adeguati, di "dati", cioè di rappresentazioni elementari di un fatto, effettuata attraverso*

simboli (bit), in combinazione diverse, e dalla elaborazione automatica di tali dati, in modo da generare "informazioni", costituite da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di esprimere un particolare significato per l'utente".

E' dunque sistema informatico ogni macchina che utilizzi un microprocessore per l'elaborazione di dati binari (BIT) per l'esecuzione di una qualsiasi operazione utile all'uomo, purchè sia in grado di svolgere il lavoro comandato in autonomia. Mentre è *"sistema telematico"* l'insieme di più sistemi informatici collegati tra loro per lo scambio di informazioni, purchè siano connessi in modo permanente, e purchè lo scambio di informazioni sia il mezzo necessario per conseguire i fini operativi del sistema.

Una prima domanda a cui rispondere è dettata dallo stato attuale della ricerca e delle tecnologie utilizzate nel campo informatico e delle telecomunicazioni, è infatti corretto continuare a distinguere le comunicazioni telematiche da quelle telefoniche?

Già nella sentenza 13/7/1998, n. 21, Gallieri, RV 211197, la Corte di Cassazione a Sez. Un., si è soffermata sulle innovazioni del sistema telefonico: "*… negli ultimi venti anni si è assistito ad un'evoluzione della telefonia, non solo sotto l'aspetto quantitativo di utenze e di volume delle comunicazioni, ma soprattutto sotto il profilo tecnologico, nella ricerca di nuove prestazioni e nuovi servizi. Lo sviluppo è stato caratterizzato dal prevalere delle tecnologie elettroniche numeriche utilizzate nel trattamento dei segnali telefonici (conversazioni), e dei dati di qualunque tipo convogliati in rete per qualunque servizio, diverso e complementare rispetto alle conversazioni, quali ad esempio messaggi e fax.*

In passato le suddette funzioni erano state svolte da un sistema elettromeccanico (i relé), con funzioni più elementari. Il nuovo sistema numerico è stato adottato in modo completo per la telefonia mobile, di recente diffusione; nella telefonia fissa, invece, la sua introduzione è in corso di completamento, almeno nel nostro paese, richiedendo essa la sostituzione degli impianti preesistenti. Ora, mentre il sistema di tipo elettromeccanico della telefonia precedente, per le sue caratteristiche tecnologiche, non comportava il trattamento dei dati c.d. esterni alla conversazione […] il sistema elettronico della telefonia mobile, in particolare, comprende necessariamente il trattamento dei dati […] esterni alla conversazione, che vengono trattati e registrati ancorché alla chiamata non segua alcun colloquio o conversazione […] Il suddetto flusso di bit comprende -come anticipato – anche dati relativi al traffico dei servizi complementari – alla telefonia mobile – quali il servizio messaggi (es. tipo e-mail o fax) che esulano anch'essi dalla nozione di conversazione tra persone…".

Con la successiva sentenza 23/2/2000, n. 6, D'Amuri, RV 215841, le Sezioni Unite hanno approfondito e puntualizzato gli aspetti

tecnico/giuridici del problema, confermando la tesi della riconducibilità al sistema informatico/telematico del sistema telefonico mobile.
In particolare, la Corte ha sottolineato l'evoluzione della telefonia col sistema digitale GSM (in cui il segnale analogico viene "digitalizzato", cioè trasferito, in forma numerica binaria 0-1, in bit), che consente di effettuare la trasmissione di dati ed anche di inviare e ricevere brevi messaggi, e dell'ulteriore fase di evoluzione rappresentata dal sistema UMTS ("*sofisticata tecnica in via di sviluppo che assicura ottima qualità di ascolto, dà possibilità di accesso ai dati on line e, tra l'altro, consente di inviare e ricevere messaggi video e audio*"); ha poi precisato che "*In concreto, le linee telefoniche, secondo la moderna tecnologia, attuano la trasmissione delle comunicazioni con la conversione (codificazione) di segnali fonici in forma di "flusso" continuo di cifre e detti segnali, trasportati all'altro estremo, vengono ricostruiti all'origine (decodificazione) [...] Trattasi, dunque, di flussi relativi ad un sistema tecnico che s'innesta nella disciplina delle intercettazioni di comunicazioni informatiche o telematiche, captate a sorpresa nel corso del loro svolgimento, che hanno per oggetto anche la posta elettronica (email) da computer a computer collegati alla rete Internet o in forma ibrida a mezzo di messaggi SMS da computer, collegato alla detta rete, ad apparecchi cellulari GSM o viceversa. Il flusso è il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici. Fra strumenti informatici, quindi, è possibile lo scambio di impulsi in cui si traducono le informazioni; scambio che è comunicazione al pari della conversazione telefonica, sicché la relativa captazione nel momento in cui si realizza costituisce intercettazione*".
La giurisprudenza successiva ha confermato l'orientamento, affermando che "la rete di telefonia mobile costituisce un sistema telematico protetto" (Cass.17/1/2003, n. 36288, De Alfieri, RV 226699, a proposito della configurabilità del reato ex art. 615 quater c.p.; cfr. Cass., 17/12/2004, n. 5688, Mbaye ed altro, Rv.230693). Infine, le Sezioni Unite, nella recentissima sentenza 26/6/2008, n. 36359, Carli, RV 240395, occupandosi della c.d. "remotizzazione" dell'ascolto delle intercettazioni, in un passaggio hanno riconosciuto che "*La rivoluzione che ha trasformato la telefonia nel recente passato ha segnato, in estrema sintesi, il progressivo passaggio dalla trasmissione di segnali in maniera analogica a quella di dati in forma digitale, **trasformando il servizio telefonico (a partire da quello di telefonia mobile) in un sistema informatico o telematico**. È dunque mutato lo stesso oggetto fisico della comunicazione telefonica e, quindi, della sua intercettazione. Di conseguenza è stato fatto progressivamente ricorso alla utilizzazione di sistemi di registrazione digitale computerizzata che hanno sostituito gli apparati meccanici*".
A fronte di tali arresti giurisprudenziali che con ogni evidenza sembrano confermare come tutto il moderno sistema di telefonia possa essere

certamente fatto rientrare nella definizione di sistema telematico, anche alla luce di alcune recenti innovazioni legislative si pongono dei rilevanti problemi giuridici.
Invero, con la Legge 547/1993 il legislatore ha provveduto anche ad adeguare la disciplina processuale delle intercettazioni alle nuove esigenze di repressione dei cd. crimini informatici. In particolare, con l'introduzione dell'art.266-*bis* c.p.p. (Intercettazioni di comunicazioni informatiche o telematiche), si è previsto che *"Nei procedimenti relativi ai reati indicati nell'articolo 266* [delitti puniti con l'ergastolo o la reclusione superiore nel massimo a cinque anni, delitti contro la Pubblica Amministrazione puniti con pena non inferiore a cinque anni, delitti in materia di stupefacenti, armi ed esplosivi, delitti di contrabbando, minaccia, usura, abusiva attività finanziaria, abuso di informazioni privilegiate, manipolazione del mercato, pornografia minorile etc.], *nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi."*.
Molto significativamente, è stata quindi consentita la possibilità di disporre intercettazioni informatiche e telematiche non solo per le fattispecie tassativamente indicate dall'art.266 c.p.p. (con l'ulteriore specificazione dei limiti edittali di pena richiesti, per talune fattispecie), bensì per qualsiasi tipologia di reato, ove commesso facendo uso di tecnologie telematiche o informatiche; non solo quindi per i reati "ontologicamente" "informatici", ma per qualsiasi fattispecie per la realizzazione della quale l'autore del fatto abbia utilizzato i "mezzi" informatici. L'opzione legislativa è stata certamente ispirata dalla necessità di ampliare *in subiecta materia* le ipotesi di esperibilità del mezzo di ricerca della prova in oggetto, dovendosi prendere atto della impossibilità di controllare e reprimere seriamente determinate forme di criminalità senza ricorrere a siffatta, peculiare, forma di intercettazione delle comunicazioni.
La lettera della legge consente quindi di ipotizzare un uso estremamente estensivo del mezzo d'indagine introdotto dall'art.266 *bis* c.p.p., anche se è vero che la sua portata innovativa, a ben vedere, è minore di quanto all'apparenza possa sembrare. Infatti l'art.266 c.p.p. già consentiva *"l'intercettazione di conversazioni o comunicazioni telefoniche o di altre forme di telecomunicazione"*: una semplice interpretazione estensiva dell'art. 266 avrebbe infatti consentito di comprendere nelle "altre forme di telecomunicazione" anche le intercettazioni telematiche. Se è infatti "comunicazione" qualsiasi scambio di dati, informazioni, immagini o suoni che intercorre tra due o più soggetti, certamente tutte le comunicazioni che avvengono avvalendosi degli impianti telefonici possono risultare ricomprese nel concetto di "telecomunicazioni", anche laddove le stesse non avvengano più in forma analogica ma digitale.

Diversamente, il contenuto normativo dell'art. 266 c.p.p. non sarebbe stato sufficientemente ampio da ricomprendervi anche le intercettazioni "informatiche", aventi per oggetto più computer in grado di interagire tra loro senza avvalersi dello strumento telefonico: come è noto, infatti, ogni singolo elaboratore può "colloquiare" con altri non solo attraverso un *modem* (quindi avvalendosi del sistema telefonico) ma anche laddove esso faccia parte di una LAN *(Local Area Network*), ovvero di una di quelle strutture in grado di organizzare e collegare tra loro varie postazioni di lavoro informatiche diffuse negli uffici o nelle pubbliche amministrazioni di grandi dimensioni. Poiché infatti la LAN utilizza il sistema telefonico solo per porsi in connessione con reti informatiche esterne alla rete locale, le intercettazioni "interne" alla medesima LAN sono consentite solo per effetto del disposto di cui all'art.266 *bis* c.p.p..

Oggetto delle intercettazioni informatiche o telematiche sono le connessioni tra sistemi informatici o telematici, ossia tra computer tra loro collegati, in rete, via modem od in altro modo. La peculiarità delle comunicazioni informatiche e telematiche è costituita dalla particolare forma "digitale" nella quale si manifestano dati, informazioni, immagini e suoni (composti da un numero variabile di segnali elettronici, detti *bit*).

Occorre però sottolineare che l'art 266 bis c.p.p. si riferisce alle comunicazioni tra "sistemi", senza richiedere affatto che ad essere intercettati siano "dati" (*bytes*) in forma digitale. Dunque, volendo portare alle logiche conseguenze il ragionamento sin qui condotto, si potrebbe certamente affermare che l'art. 266 bis c.p.p. regolamenta oggi non solo le intercettazioni telematiche o informatiche in senso stretto, ma anche quasi tutte le intercettazioni telefoniche, trattandosi comunque di sistemi telematici.

Altra problematica, con riguardo ai presupposti del decreto autorizzativo delle intercettazioni, inerisce l'applicazione dell'art. 13 l. 12.7.1991, n. 203, che tratta come è noto delle intercettazioni necessarie *"per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono"*, prevedendo specifiche deroghe quanto ai presupposti del provvedimento ed alla durata delle operazioni ("*sufficienti* [anziché gravi] *indizi"* e durata di 40 giorni per la prima attivazione e di 20 per ogni proroga [anziché 15 per la prima attivazione e 15 per ogni proroga]). La norma non chiarisce se la possibilità di disporre intercettazioni nei termini previsti dallo stesso art. 13 L 203/91 sia estensibile anche alle intercettazioni informatiche e telematiche di cui all'art. 266-*bis* c.p.p.; la questione è di non poco momento, in quanto proprio la diffusione delle comunicazioni digitali nell'ambito della criminalità organizzata anche internazionale risulta ormai un fenomeno statisticamente rilevante (si pensi alle transazioni monetarie eseguite elettronicamente). Ragioni sistematiche e teleologiche, quali la priorità della lotta alla criminalità organizzata potrebbero invero supportare la tesi

della applicabilità delle citate deroghe anche alle intercettazioni telematiche ed informatiche, considerato anche che il richiamo dell'art. 266 c.p.p. anche ai "mezzi" con i quali l'intercettazione può essere svolta potrebbe essere letto in riferimento a tutti i tipi di intercettazioni previste dall'ordinamento al momento di entrata in vigore della Legge 203/1991. Si potrebbe però obiettare che una tale interpretazione estensiva non sia autorizzata dalla lettera della norma, che fa esclusivo riferimento all' *"autorizzazione a disporre le operazioni di intercettazione previste dall'art.266 dello stesso codice"*.

Ulteriore profilo problematico è quello inerente la modifica processuale più significativa rispetto ai modelli procedimentali preesistenti alla Legge 547/93 e consistente nell'innesto del comma 3-*bis* dell'art. 268 c.p.p., a mente del quale *"quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati"*.

Si tratta di previsione che determina una possibilità espressa di deroga alla rigorosa disciplina prevista dall'art. 268, 3° co., c.p.p., che appunto impone che le operazioni di intercettazione possano essere compiute esclusivamente per mezzo degli impianti installati presso la Procura della Repubblica, ovvero –allorchè tali impianti risultino insufficienti od inidonei ed esistano eccezionali ragioni di urgenza- mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria, con provvedimento motivato del Pubblico Ministero. La violazione di tale disposizione è sanzionata, *ex* art.271 1° co., c.p.p., con l'inutilizzabilità dei risultati delle intercettazioni medesime.

Al contrario, infatti, il comma 3-*bis* dell'art. 268 non richiede alcun obbligo di motivazione, e soprattutto nessuno specifico presupposto per l'esecuzione delle operazioni con impianti diversi da quelli dell'Ufficio di Procura. Sostanzialmente, al Pubblico Ministero è lasciata assoluta discrezionalità nell'uso dei impianti appartenenti a privati, trattandosi di strumenti ad alto "tasso" di tecnologia, di cui le Procure e gli Uffici di Polizia Giudiziaria non sono mai stati effettivamente dotati.

La previsione di un comma autonomo rispetto al comma 3 dell'art.268 c.p.p. consente quindi di ritenere che la facoltà ivi prevista debba ritenersi del tutto autonoma e svincolata dai criteri previsti per l'utilizzo in generale di impianti di pubblica utilità ovvero della polizia giudiziaria, avendo verisimilmente il legislatore preso atto della totale "assenza", al momento di entrata in vigore della legge, di idonee apparecchiature presso gli uffici normalmente deputati alle attività in oggetto.

Il ricorso agli impianti dei privati, pertanto, non costituirà affatto un'eccezione, ma semmai la regola per l'esecuzione di intercettazioni telematiche od informatiche. In punto di motivazione la norma, come detto, nulla prevede. Per il disposto generale dell'art. 267,3° co., c.p.p., pertanto, al Pubblico Ministero basterà indicare nel decreto "dispositivo" delle

intercettazioni le "modalità" di esecuzione, senza che possa derivare alcuna sanzione processuale per il caso che ometta di motivarne la scelta. **E' evidente che, se come già si è detto quasi tutte le intercettazioni telefoniche possono oggi considerarsi intercettazioni "telematiche", l'estensione di tale norma è potenzialmente enorme ed occorre valutarne l'effettiva portata derogatoria rispetto all'art. 268 comma 3° c.p.p.**

A parere di chi scrive, in realtà, la portata innovativa della norma è limitata e, comunque, anche prudenzialmente va preferita una lettura non eccessivamente estensiva della stessa. Invero, se da un lato come detto la norma sembra autorizzare per tutte le intercettazioni informatiche e telematiche (e dunque per quasi tutte le intercettazioni telefoniche) l'utilizzo di impianti appartenenti a privati senza alcuna motivazione, nulla si dice sul luogo dove devono avvenire tali operazioni ovvero se le stesse possano essere effettuate al di fuori della Procura della Repubblica senza alcuna motivazione in ordine ai presupposti richiesti dall'art. 268 comma 3° c.p.p.

A tale proposito di recente la Suprema Corte di Cassazione sez. IV nella sentenza n.33645 del 15.6.2010 Rv248400 in motivazione affermava "… *E' principio affermato che, in tema di intercettazioni telefoniche, l'osservanza della regola ordinaria di esecuzione, per la quale le operazioni devono essere compiute per mezzo degli impianti installati nella Procura della Repubblica, è assicurata ogni qual volta dette operazioni si svolgano (come nella specie è avvenuto) nell'ufficio giudiziario, a nulla rilevando l'eventualità che le apparecchiature utilizzate siano acquisite per l'occasione, anche mediante noleggio presso imprese private. Ne consegue che nei casi indicati, non ricorrendo l'ipotesi delle operazioni effettuate mediante impianti di pubblico servizio o in dotazione alla polizia giudiziaria, il PM non è tenuto a documentare con proprio provvedimento motivato né la ricorrenza di eccezionali ragioni di urgenza né l'insufficienza o l'inidoneità degli impianti preesistenti (Cass. sez. 6 sent. N.2845 dell'1.2.2003 rv.228419)…"* Alla luce di tali principi, pertanto, l'obbligo motivazionale di cui all'art. 268 comma 3° c.p.p. andrebbe riferito non tanto agli impianti utilizzati ed alla proprietà degli stessi, ma al luogo dove avviene la registrazione delle comunicazioni (siano esse telematiche o telefoniche tradizionali), per cui a prescindere dall'applicazione o meno dell'art. 268 comma 3 bis c.p.p. non vi sarebbe alcun obbligo di motivazione se gli apparati di proprietà dei privati si utilizzano presso la Procura della Repubblica, mentre al contrario riterrei che tale obbligo motivazionale debba continuare ad essere adempiuto allorquando tutte le operazioni di intercettazione (anche informatiche o telematiche) inclusa la registrazione dei flussi si svolgano in luoghi diversi dalla Procura.

Tale interpretazione è peraltro ulteriormente confermata anche dalla recente e risolutiva pronuncia della Suprema Corte a sezioni unite (Cass. s.u.

26.6.2008 n.36359 Rv240395) che, intervenendo a proposito della "remotizzazione" dell'ascolto e dei suoi riflessi sul regime dell'utilizzabilità delle intercettazioni ex art. 268 comma 3° c.p.p. ha chiarito che "…*la tecnica dell'instradamento dei flussi sonori captati dagli impianti ritualmente collocati nei locali della Procura della Repubblica, verso punti d'ascolto siti negli uffici della polizia giudiziaria, costituisce una modalità di esecuzione dell'intercettazione pienamente compatibile con lo statuto normativo della medesima, con la conseguenza che gli esiti della stessa intercettazione devono considerarsi pienamente utilizzabili a fini di prova anche laddove la delocalizzazione dell'ascolto non sia stata autorizzata dal pubblico ministero nelle forme previste dall'art. 268 c.p.p., comma 3, per la realizzazione dell'indagine tecnica mediante impianti esterni a quelli in dotazione agli uffici giudiziari*" Partendo da tali premesse, la Suprema Corte ha sottolineato correttamente che "*nella disciplina attualmente in vigore* ***il momento decisivo è quello della registrazione****, ed è a tale segmento - della più complessa attività di intercettazione - che il legislatore ha inteso riferirsi laddove ha stabilito che le operazioni possono compiersi esclusivamente "per mezzo" degli impianti installati nella procura della Repubblica; tuttavia, occorre prendere atto della profonda trasformazione della realtà tecnologica rispetto al 1988, epoca di introduzione delle regime previsto dall'art. 268 c.p.p. …Da qualche anno, infatti, per la registrazione vengono utilizzati apparati multilinea (collegati cioè ad un flusso di linee telefoniche) che registrano dati trasmessi in forma digitale e successivamente decodificati in file vocali immagazzinati in memorie informatiche centralizzate. I dati così memorizzati vengono poi di regola trasferiti su supporti informatici (essenzialmente Cd-Rom o DVD) per renderli fruibili all'interno dei singoli procedimenti. In pratica dunque i supporti costituiscono il corredo documentale in precedenza rappresentato dai nastri magnetici….Le operazioni di "registrazione" ….. consistono, dunque, come è agevole desumere da quanto fin qui detto, nella immissione dei dati (captati presso la centrale dell'operatore telefonico e trasmessi agli impianti in Procura) nella memoria informatica centralizzata (cd. server) che si trova nei locali della Procura della Repubblica a ciò destinati. I menzionati apparati permettono altresì di "remotizzare" agevolmente (attraverso il sistema c.d. client-server) l'ascolto -nonché, volendo, anche una registrazione (ovviamente derivata da quella effettuata in Procura, e da non potersi a questa sostituire) deviando il flusso in entrata anche verso molteplici punti di ricezione, collocabili in qualsiasi luogo (e dunque anche all'esterno degli uffici di Procura) e collegati con il sistema centrale verso cui l'operatore telefonico ha trasmesso il flusso di dati captati*".Così definita la nozione di registrazione, ne deriva, osserva la Corte, che "*Per qualsiasi altra operazione ….. non assume alcun rilievo, ai fini della utilizzabilità delle intercettazioni, il luogo dove la stessa è avvenuta*".

Le modalità operative delle intercettazioni telematiche ed informatiche sono condizionate in primo luogo dalle specifiche caratteristiche del sistema oggetto delle attività di captazione, nonché dal tipo di informazioni ("flussi di comunicazioni") che si intendono acquisire. Occorre perciò in primo luogo accertare il tipo di connessione utilizzata dall'utente (ad es. ADSL o analogica) ma soprattutto conoscere tecnicamente "l'access provider" utilizzato dall'utente.

Infatti ogni volta che l'utente si collega ad un Internet access Provider per avere la connessione alla rete Internet, come si è visto, ottiene uno specifico indirizzo IP: prima dell'attribuzione dell'indirizzo, l'utente viene identificato ("logato") dal *server* come soggetto abilitato a ricevere i propri servizi, previo riconoscimento degli estremi identificativi del *client* (username e password) ed in tal modo accettato ed abilitato alla navigazione in Internet.

Una volta riconosciuto dal sistema, all'utente viene assegnato un numero IP dinamico che seguirà la sua navigazione, e che identificherà univocamente la sua macchina durante il collegamento.

Inoltre, per poter accedere ai servizi offerti da un *server*, ogni *client* deve poter identificare il servizio con precisione, così da inviare una richiesta univoca. I servizi richiesti ai *servers* sono abbinati ai cd. *port numbers*, numeri che caratterizzano ogni specifica funzionalità disponibile su un *server* attivo su un elaboratore: proprio attraverso l'indicazione del *"port number"*, i singoli utenti delle rete possono avere accesso alle varie applicazioni disponibili sul *server* al quale è stata inviata la richiesta.

L'intercettazione telematica si articola su taluni caratteristici passaggi tecnici. Occorre infatti:

- memorizzare il traffico telematico "grezzo" (tutto il flusso dei dati) su un apposito supporto per poi decriptarlo, ove decriptabile;
- individuare il soggetto che abbia avuto in uso la macchina, in ipotesi diverso dall'intestatario delle linea intercettata e che abbia effettuato la connessione durante la quale è stato consumato l'illecito. Di certo non ci si potrà accontentare di identificare il numero di telefono chiamante o chiamato, ma occorrerà approfondire le indagini con accertamenti documentali (contratti) ovvero storici (analisi delle ulteriori chiamate effettuate) nel tentativo di appurare la concreta disponibilità dell'utenza e della macchina ad un soggetto fisico ben individuato.

L'analisi dei dati intercettati, poi, al fine sempre di identificare il soggetto intercettato, si articola tipicamente secondo il seguente modulo:

a) ogni server di accesso alla rete, al momento della connessione (*"login"*) crea un *file* di *log* dell'utente, contenente le seguenti informazioni-base:

- user name;
- data, ora e secondi dell'inizio della connessione (*login*) e del termine della connessione (*logout*);
- IP dinamico assegnato e *caller ID*, cioè numero del telefono chiamante;

b) se l’utente si collega ad un *server* di posta elettronica, esso registrerà a sua volta l’accesso registrando ancora:
- *user name*
- data, ora e secondi del *login* e del *logout*
- IP dinamico.

Sulla base degli elementi sopra indicati sarà quindi possibile risalire all’utilizzatore delle linee telefoniche utilizzate per la connessione (caller ID chiamanti) e quindi agli utenti, incrociando le informazioni derivanti dai dati costituiti dai *file* di *log*, dai dati di registrazione presso il provider e da quelli risultanti dal tabulato telefonico dell’utenza dalla quale risulta effettuato il collegamento al provider.

L’intercettazione può avvenire sull’access provider, nel cui caso sarà posta in centrale una **sonda** detta Front End collegata ad una porta (mirror) che riceve in copia tutto il traffico scambiato (in entrambe le direzioni) dall'apparato di accesso che gestisce la connessione finale dell'utente (una sorta di sniffer). Il flusso di dati è trasferito tramite linea dedicata ad alta velocità verso la postazione della P.G. ove è memorizzato e decodificato (Back End). La postazione di decodifica ha un modulo che interpreta e ricostruisce i protocolli in modo che l'addetto alla postazione possa vedere, ad esempio, i messaggi di posta elettronica inviati e ricevuti, le pagine web visitate, le e-mails, le chat etc..

Esistono, inoltre, dei particolari sistemi hardware denominati **telemonitor**, differenti dalle sonde, di cui la PG ha la disponibilità, che possono essere inseriti anche su più linee e punti. Essi registrano tutte le attività telematiche e non dell'indagato grazie a una sorta di 'bypass' installato tra la linea e la centrale. Non c'è bisogno di un operatore fisso, perché il controllo dei dati non avviene in tempo reale, ma solo quando i file immagazzinati dal tele monitor vengono rielaborati da un operatore della P.G.La macchina tele monitor non rallenta la trasmissione.

In pratica, possiamo eseguire un’intercettazione con una sonda presso il provider di accesso(*access provider*) ad Internet o un’intercettazione sul cavo del segnale di basso livello con ricostruzione completa dei protocolli (telemonitor). Un’intercettazione può essere anche eseguita mediante un trojan (programma malizioso) sul computer dell’utente (vedasi Skype) ovvero se riguarda la posta elettronica ed il service provider che la gestisce collabora reindirizzando su una casella di posta dedicata tutti i messaggi inviati e/o ricevuti.

Infine, un accenno alla cosiddetta intercettazione parametrica cioè quella effettuata sulle dorsali (backbone) di comunicazione o su particolari aree con separazione e filtraggio dei dati. In pratica si tratta di identificare sessioni di traffico generate da un punto imprecisato di un’area geografica che contengono tipicamente parole o frasi chiave, ad esempio il termine “attentato” su tutto il traffico generato dalla Sicilia. Viene, quindi,

impostato un filtro c.d. applicativo e tutti i pacchetti che compongono la comunicazione del canale vengono ispezionati.

Per quanto riguarda l'identificazione certa dell'utilizzatore del pc e quindi del soggetto le cui comunicazioni telematiche vengono intercettate, come detto laddove si presenti la necessità di individuare l'autore (o meglio la macchina dell'autore) di una specifica connessione, l'autorità giudiziaria dovrà acquisire non solo i cd. "*file* di *log*" (ossia le informazioni di identità e tempo memorizzate dal *server*, generati dalle richieste dei singoli *clients*) ma dovrà accertare altresì a quale utente risultava abbinato l'indirizzo IP desumibile dai file di log nel momento in cui sia stata posta in essere l'attività illecita oggetto delle indagini. L'analisi di tali *files* di *log* consente quindi di stabilire se che un determinato utente in un particolare giorno ed ora si è collegato alla rete tramite un *provider*; quale indirizzo IP temporaneo ha avuto in assegnazione per la durata della connessione; quali informazioni (strutturate in "pacchetti") ha inviato o ricevuto per mezzo dell'indirizzo IP assegnato (accessi ai siti, scaricamento di pagine web o di specifici *files*, conversazioni in *chat*, partecipazioni a *newsgroup*, trasmissione o ricezione di posta elettronica).

Anche l'acquisizione processuale dei *files* di *log* ha dato luogo a diverse opinioni giurisprudenziali, specie in seguito all'entrata in vigore del nuovo testo dell'art. **132 del D.Lvo 196/2003** (codice in materia di protezione dei dati personali, come modificato dall'art. 3 della L. 45/2004, ancora modificato dalla L. 155/2005, in materia di contrasto al terrorismo internazionale, e da ultimo ancora modificato con **D. Lvo 109/2008**, di attuazione della direttiva CE 2006/24/CE in materia di *data retention*)[1]. Va

[1] Per la migliore comprensione della terminologia usata, si riporta l'art. 1 del D. Lvo 109/2008:
Art. 1.
Definizioni
1. Ai fini del presente decreto si intende:
a) per utente: qualsiasi persona fisica o giuridica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, senza esservi necessariamente abbonata;
b) per dati relativi al traffico: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione, ivi compresi i dati necessari per identificare l'abbonato o l'utente;
c) per dati relativi all'ubicazione: ogni dato trattato in una rete di comunicazione elettronica che indica la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico, ivi compresi quelli relativi alla cella da cui una chiamata di telefonia mobile ha origine o nella quale si conclude;
d) per traffico telefonico: le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e quelle basate sulla trasmissione dati, purche' fornite da un gestore di telefonia, i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata, la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve, servizi mediali avanzati e servizi multimediali;
e) per chiamata senza risposta: la connessione istituita da un servizio telefonico accessibile al pubblico, non seguita da un'effettiva comunicazione, in quanto il destinatario non ha risposto ovvero vi e' stato un intervento del gestore della rete;
f) per identificativo dell'utente: l'identificativo unico assegnato a una persona al momento dell'abbonamento o dell'iscrizione presso un servizio di accesso internet o un servizio di comunicazione internet;

altresì detto che la vigenza degli obblighi di conservazione ricadenti sugli operatori di comunicazioni elettroniche è stata differita, per ragioni legate agli interventi sulle infrastrutture di rete, al 31 Dicembre 2009 ed al 31 Dicembre 2010 (v. art. 12-ter **L. 38/2009**, in materia di atti persecutori).

La disciplina oggi vigente prevede che l'acquisizione dei dati relativi al traffico telefonico, inclusi quelli concernenti le chiamate senza risposta, nonché i dati relativi al traffico telematico (è appunto il caso dei *files* di *log*), possano acquisirsi con decreto motivato del Pubblico Ministero, anche su istanze del difensore, indipendentemente dal tipo di reato, ma solo con la "profondità" massima di 24 mesi (per i dati relativi al traffico telefonico) e 12 mesi (per i dati relativi al traffico telematico).

Con l'inserimento del comma 1-*bis* del citato art. 132, si è poi stabilito che i dati relativi alle chiamate senza risposta debbano essere conservati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico (o di una rete pubblica di comunicazione) per un massimo di 30 giorni. Poiché i *files* di *log* devono considersi *"dati relativi al traffico telematico"*, dopo la novella legislativa appena ricordata la loro acquisizione seguirà il regime appena menzionato.

Ma la circostanza che ad ogni connessione ciascun *client* (postazione) sia contrassegnato da un indirizzo IP unico al mondo (per quella sessione), non esclude tuttavia che l'identificazione e la localizzazione dei singoli elaboratori collegati alla rete possa essere in qualche modo resa più difficoltosa (se non impossibile) dall'utilizzo di *software* in grado di occultare l'identità della macchina grazie alla quale ad esempio si è portato l'attacco ad un sistema informatico, ovvero da cui è partito un messaggio a contenuto diffamatorio.

È poi possibile imbattersi in interventi che abbiano comportato la cancellazione *ad hoc* dei *file* di *log* al termine delle operazioni illecite condotte sui sistemi attaccati, cosicchè sarà vano tentare di ricostruire a ritroso i vari "passaggi" compiuti dal sistema, così come di risalire all'utenza telefonica dalla quale è partita la connessione nel corso della quale è stata consumata la condotta illecita.

Tra i più diffusi sistemi di "occultamento" dell'identità dei sistemi informatici utilizzati per scopi illeciti vi è quello dell'utilizzo di server denominati *"anonymous remailer"*, che consentono la cancellazione dei dati elettronici dell'utente (rendendone di fatto impossibile l'identificazione) mediante la rimozione e sostituzione delle informazioni concernenti appunto la provenienza del mittente di una qualsiasi comunicazione. Un **anonymous remailer** è un server che riceve messaggi

---

g) per indirizzo di protocollo internet (IP) univocamente assegnato: indirizzo di protocollo (IP) che consente l'identificazione diretta dell'abbonato o utente che effettua comunicazioni sulla rete pubblica.
2. Ai fini del presente decreto si applicano, altresì, le ulteriori definizioni, non ricomprese nel comma 1, elencate nell'articolo 4 del decreto legislativo 30 giugno 2003, n. 196, e successive modificazioni, recante codice in materia di protezione dei dati personali, di seguito denominato: «Codice».

di posta elettronica e li rinvia seguendo apposite istruzioni incluse nei messaggi stessi, senza rivelare la loro provenienza originaria E' così possibile nascondere, per esempio, l'identità dei mittenti dei messaggi di posta elettronica, utilizzando tali *server* di posta che sostituiscono l'intestazione del mittente inviando il messaggio al destinatario con intestazioni fittizie.

Altro metodo per impedire l'identificazione dell'autore di atti/fatti telematici consiste nella possibilità di cancellazione dei *file* di *log*.

Particolarmente diffuse sono poi diverse tecniche di utilizzo fraudolento degli identificativi dell'elaboratore di un soggetto: in questi casi l'autore del comportamento illecito non soltanto nasconde la propria identità, ma addirittura crea le condizioni perché il comportamento sembri apparentemente attribuibile ad un altro utente davvero esistente. L'*hacker* acquisisce l'identificativo e la password di un utente ignaro, e si collega alla rete sotto mentite spoglie. L'acquisizione dell'identificativo e della password possono avvenire o in via "tradizionale" (riuscendo a carpirne gli estremi direttamente dall'utente), ovvero acquisendole per via telematica attraverso l'uso di specifici programmi denominati *"trojan horses"*; si tratta di applicativi apparentemente innocui ed invisibili, che si installano sull'elaboratore con lo scopo di controllare e spiare il funzionamento del sistema, sì da acquisirne appunto i contrassegni identificativi.

Oggi gli obblighi dei fornitori di servizi di comunicazione elettronica in materia di *data retention* sono disciplinati puntualmente dall'**art. 3 del citato D. Lvo 109/2008**, che molto opportunamente distingue le categorie di dati da conservare a seconda che si tratti di telefonia mobile, fissa, di accessi internet, di posta elettronica ovvero di telefonia, fax, SMS ed MMS via internet, e che al comma 2 prevede la possibilità che in futuro tali obblighi siano ulteriormente specificati (anche in ragione della costante evoluzione tecnologica che contraddistingue la materia) con un "semplice" Decreto del Presidente del Consiglio o del Ministero per la Pubblica Amministrazione e l'Innovazione. I dati in questione consentiranno infine di: rintracciare ed identificare la fonte di una comunicazione; rintracciare la sua destinazione; individuare il tipo di comunicazione utilizzato; conoscere la data, l'ora e la durata della comunicazione; individuare le attrezzature impiegate per la comunicazione fra gli utenti; determinare l'ubicazione delle apparecchiature di comunicazione mobile utilizzate[2].

[2] Si riporta il comma 1 dell'art. 3 del D. Lvo 109/2008:

Art. 3.

Categorie di dati da conservare per gli operatori di telefonia e di comunicazione elettronica

1. Le categorie di dati da conservare per le finalità di cui all'articolo 132 del Codice sono le seguenti:

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

1.1 numero telefonico chiamante;

1.2 nome e indirizzo dell'abbonato o dell'utente registrato;

2) per l'accesso internet:

2.1 nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione

sono stati univocamente assegnati l'indirizzo di protocollo internet (IP), un identificativo di utente o un numero telefonico;

3) per la posta elettronica:

3.1 indirizzo IP utilizzato e indirizzo di posta elettronica ed eventuale ulteriore identificativo del mittente;

3.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host, nel caso della tecnologia SMTP ovvero di qualsiasi tipologia di host relativo ad una diversa tecnologia utilizzata per la trasmissione della comunicazione;

4) per la telefonia, invio di fax, sms e mms via internet:

4.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamante;

4.2 dati anagrafici dell'utente registrato che ha effettuato la comunicazione;

b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

1.1 numero composto, ovvero il numero o i numeri chiamati e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata e' trasmessa;

1.2 nome e indirizzo dell'abbonato o dell'utente registrato;

2) per la posta elettronica:

2.1 indirizzo di posta elettronica, ed eventuale ulteriore identificativo, del destinatario della comunicazione;

2.2 indirizzo IP e nome a dominio pienamente qualificato del mail exchanger host (nel caso della tecnologia SMTP), ovvero di qualsiasi tipologia di host (relativamente ad una diversa tecnologia utilizzata), che ha provveduto alla consegna del messaggio;

2.3 indirizzo IP utilizzato per la ricezione ovvero la consultazione dei messaggi di posta elettronica da parte del destinatario indipendentemente dalla tecnologia o dal protocollo utilizzato;

3) telefonia, invio di fax, sms e mms via internet:

3.1 indirizzo IP, numero telefonico ed eventuale altro identificativo dell'utente chiamato;

3.2 dati anagrafici dell'utente registrato che ha ricevuto la comunicazione;

3.3 numero o numeri a cui la chiamata e' trasmessa, nei casi di servizi supplementari come l'inoltro o il trasferimento di chiamata;

c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione;

2) per l'accesso internet :

2.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di accesso internet, unitamente all'indirizzo IP, dinamico o statico, univocamente assegnato dal fornitore di accesso internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;

3) per la posta elettronica:

3.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio di posta elettronica su internet ed indirizzo IP utilizzato, indipendentemente dalla tecnologia e dal protocollo impiegato;

4) per la telefonia, invio di fax, sms e mms via internet:

4.1 data e ora (GMT) della connessione e della disconnessione dell'utente del servizio utilizzato su internet ed indirizzo IP impiegato, indipendentemente dalla tecnologia e dal protocollo usato;

d) i dati necessari per determinare il tipo di comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato;

2) per la posta elettronica internet e la telefonia internet: il servizio internet utilizzato;

e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:

1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati;

2) per la telefonia mobile:

2.1 numeri telefonici chiamanti e chiamati;

2.2 International Mobile Subscriber Identity (IMSI) del chiamante;

2.3 International Mobile Equipment Identity (IMEI) del chiamante;

2.4 l'IMSI del chiamato;

2.5 l'IMEI del chiamato;

2.6 nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e

Le telecomunicazioni satellitari e gli operatori Thuraya, Iridium ed Inmarsat

Le comunicazioni telefoniche satellitari consistono in segnali in radio-frequenza trasmessi e ricevuti da terminali attraverso una rete di satelliti per le telecomunicazioni in orbita geostazionaria.
I principali operatori di telefonia satellitare allo stato sono: 1) **Iridium,** che è un sistema di satelliti per telecomunicazioni il cui nome deriva dall'elemento iridio che nella tavola periodica degli elementi è il numero 77, quanti dovevano essere i satelliti in orbita, anche se allo stato quelli operativi sono 66. Il sistema iridium, che si avvale di satelliti a bassa quota (a differenza dei satelliti in orbita geostazionaria) limita il ritardo tipico di tale forma di comunicazione ed è l'unico servizio di comunicazione satellitare globale esteso a tutta la terra. Tale operatore ha un gateway (stazione radio base che si occupa dell'instradamento del traffico) Italiano ed è titolare di licenza italiana, dunque sarà applicabile la normativa in materia di prestazioni obbligatorie per le intercettazioni. 2) **Inmarsat,** nasce nel 1979 come organizzazione intergovernativa mondiale per lo sviluppo e la gestione di satelliti per comunicazioni, e nel 2000 aderiva anche la società telespazio quale concessionario esclusivo del Ministero delle Poste e telecomunicazioni, successivamente a seguito delle liberalizzazioni dei servizi di telecomunicazione, hanno aderito altre società che in quanto titolari di licenza italiana saranno tutte soggette alla normativa in materia di prestazioni obbligatorie. 3) **Thuraya,** che è l'operatore rispetto al quale si pongono i maggiori profili problematici atteso che, avendo sede all'estero e, quindi, non essendo soggetti alla normativa nazionale in materia di "prestazioni obbligatorie" ai fini di giustizia, non assicura la necessaria collaborazione alle autorità inquirenti. In particolare, l'operatore **Thuraya**, ha sede negli Emirati Arabi Uniti e, a differenza delle altre due aziende, non ha alcun gateway nei Paesi occidentali.
Nell'ambito delle esperienze investigative acquisite dalla **Polizia Postale e delle Comunicazioni** è stato già utilizzato un sistema per il monitoraggio e l'intercettazione delle comunicazioni telefoniche satellitari, in particolare è stato utilizzato un apparato atto alla cattura dei dati di traffico e alla captazione e decrittazione delle comunicazioni telefoniche sulla rete satellitare solo ed esclusivamente del gestore **Thuraya**. Invero, per le

---

l'etichetta di ubicazione (Cell ID) dalla quale e' stata effettuata l'attivazione;

3) per l'accesso internet e telefonia, invio di fax, sms e mms via internet:

3.1 numero telefonico chiamante per l'accesso commutato (dial-up access);

3.2 digital subscriber line number (DSL) o un altro identificatore finale di chi e' all'origine della comunicazione;

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:

1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;

2) dati per identificare l'ubicazione geografica della cella facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.

società Iridium ed Inmarsat, che hanno licenza italiana e gateway in Italia, l'intercettazione sarà possibile tramite collaborazione del gestore (che non potrà rifiutarsi trattandosi di prestazioni obbligatorie).

In tale ambito operativo la Polizia Postale e delle Telecomunicazioni segnala che:

- la società **Thuraya**, con sede negli Emirati Arabi Uniti, ove è attestato anche il gateway principale del proprio sistema di telefonia satellitare (che prevede anche un gateway di back up in Egitto), copre con il proprio servizio ¾ del globo terrestre (Europa, Africa, Asia, Australia), ed ha accordi per il *roaming* sulla rete GSM con oltre 243 operatori nel mondo ed alla sua rete fanno riferimento quasi 400.000 terminali in tutto il mondo;
- i terminali **Thuraya,** che in Italia stanno avendo sempre maggiore diffusione, vengono venduti da distributori autorizzati che, in questo caso, *soggiacciono alla normativa vigente sulla identificazione degli utenti che acquistano traffico prepagato della telefonia mobile*; è tuttavia piuttosto semplice acquistare Sim Card e terminali Thuraya anche attraverso mercati paralleli ed all'estero, con la conseguente impossibilità di avviare investigazioni attraverso la preliminare acquisizione dei dati anagrafici degli intestatari;
- la forte e continua espansione del mercato dei terminali Thuraya deriva, infine, dall'aggressiva politica commerciale della medesima azienda, in virtù della quale viene sensibilmente contenuto il costo della telefonata satellitare;
- dal punto di vista investigativo, come sopra premesso e a differenza di quanto accade con gli altri operatori di settore, sono pressoché nulle le possibilità di ottenere collaborazione dalla società **Thuraya** ai fini dell'acquisizione dei dati di traffico e dell'intercettazione delle comunicazioni telefoniche e tale circostanza rende particolarmente appetibile tale tecnologia di comunicazione per le organizzazioni criminali e terroristiche.

A differenza delle tradizionali modalità tecniche di acquisizione dei dati di traffico e di intercettazione delle comunicazioni telefoniche e dei flussi telematici, che presuppongono l'intervento dei fornitori dei servizi di comunicazione elettronica, il monitoraggio e l'acquisizione del traffico telefonico satellitare vengono eseguiti direttamente dagli apparati atti a tali scopi, non installabili presso le sale C.I.T. delle Procure della Repubblica italiane.

Il sistema in questione è, infatti, composto **da antenne paraboliche di grandi dimensioni e da apparati informatici atti alla cattura ed alla gestione dei dati di traffico, ivi compresi quelli di localizzazione georeferenziata dei terminali, nonché all'intercettazione e decrittazione delle comunicazioni foniche e delle trasmissioni dati**. Tale apparato consente di monitorare un'area precedentemente definita sulla base di

precisi parametri geografici e di configurare il sistema in modo tale da limitare il monitoraggio e l'intercettazione a bersagli predefiniti.
Con riguardo a tale forma di intercettazione, certamente costosa e complessa, per esperienza diretta della Polizia Postale, riferita al solo sistema Thuraya, si possono intercettare tutte le chiamate (entrata ed uscita) senza interessare il gestore del sistema sat, l'importante è che l'utente bersaglio si trovi nella zona geografica di copertura c.d. **spot beam,** così ad esempio per intercettare le comunicazioni in Italia lo spot beam di interesse è il n. 037 ed i sei circostanti. In teoria è possibile intercettare tutta l'area di copertura del satellite abilitando gli spot di interesse. Poiché tali spot beam sono molto ampi e travalicano i confini nazionali tecnicamente sarebbe possibile dall'Italia intercettare anche telefoni satellitari che si trovino in nazioni limitrofe, ponendosi in tali casi ulteriori problemi inerenti la necessità o meno di procedere a rogatoria. A parere di chi scrive, poiché comunque la registrazione dei flussi avverrebbe in Italia, a prescindere da dove si trovi materialmente il telefono intercettato, potrebbero certamente applicarsi i principi giurisprudenziali in materia di instradamento di telefonate provenienti dall'estero e dei quali si dirà in seguito.
Per quanto riguarda le localizzazioni satellitari vengono realizzate solitamente con il ricorso alla tecnologia GPS (Global Positioning System), che è un sistema di posizionamento su base satellitare. La Cassazione si è occupata a più riprese della "localizzazione" o "positioning", affermando il principio consolidato secondo cui tale attività investigativa non può essere equiparata ad una intercettazione di comunicazioni e, pertanto, non necessita di autorizzazione da parte del giudice.
In sintesi: " *…la localizzazione delle persone attraverso l'apparato cellulare in possesso delle stesse, mediante la tecnica detta "positioning", non necessita di autorizzazione giudiziale, risolvendosi in una sorta di pedinamento satellitare e non interferendo sulla libertà e segretezza delle comunicazioni* (Cass., 13/05/2008, n. 21366, Rv. 240092, Stefanini).
"*La localizzazione mediante il sistema di rilevamento satellitare (cosiddetta GPS) degli spostamenti di una persona nei cui confronti siano in corso indagini, costituisce un'attività investigativa atipica, assimilabile al pedinamento, i cui risultati possono entrare nella valutazione probatoria del giudice attraverso la testimonianza degli ufficiali di polizia giudiziaria; tale attività non è assimilabile all'attività di intercettazione di conversazioni o comunicazioni, per cui non è necessaria alcuna autorizzazione preventiva da parte del giudice, dovendosi escludere l'applicabilità delle disposizioni di cui agli artt. 266 ss c.p.p.* (Cass., 11/12/2007, n. 15396, Rv. 239635, Sitzia e altri). Nello stesso senso, cfr. Cass., 29/01/2007, n. 8871, Rv. 236112, Navarro Mongort; Cass., 07/05/2004, n. 24715, Rv. 228731, Massa ed altro; Cass., 27/02/2002, n. 16130, Rv. 221918, Bresciani ed altri.

2. Il fenomeno Skype ed i servizi VOIP

Sicuramente il software VoIP (Voice over IP) più diffuso al mondo è Skype. Esso permette, da un pc o da un telefono cellulare, di effettuare chiamate verso altri pc e cellulari dotati di Skype ovvero di fare chiamate anche verso numerazioni di rete fissa (PSTN) e mobile (GSM, UMTS). In quest'ultima ipotesi si parla di chiamate SkypeOut.
Skype è stato sviluppato da giovani informatici estoni, che come parte del pacchetto software hanno inserito l'algoritmo Advanced Encryption Standard (AES), conosciuto anche come Rijndael, il più avanzato e sicuro disponibile pubblicamente in fatto di cifratura.
Ad oggi, l'algoritmo AES, standard adottato dal National Security Agency (NSA) degli Stati Uniti, non è violabile.
Quando due soggetti intercettati conversano utilizzando Skype, non si riesce ad ascoltare le conversazioni pur intercettando (ricevendo in copia dall'operatore telefonico o fornitore di accesso) il flusso di dati (il cd *grezzo*) che risulta incomprensibile.
Pertanto, per intercettare la voce in chiaro occorre avvalersi di un altro modello di attacco, che non prevede più l'assistenza tecnologica degli operatori che forniscono accesso alla rete. Il modello è applicabile non solo a Skype, ma a tutti i software VoIP che fanno uso di algoritmi di cifratura.
Infatti, la criticità dei software VoIP cifrati è il sistema operativo del computer o del telefono cellulare su cui sono installati. E' lì che è possibile introdurre un programma *"malizioso"* tipo Trojan installandolo con accesso fisico al computer obiettivo (accesso nei locali) oppure in modalità remota, per esempio con l'invio in allegato ad una e-mail. Una volta installato, il software Trojan si occupa di captare la voce dell'utilizzatore del computer su cui è installato prima che venga cifrata dall'algoritmo AES e quella dell'interlocutore dopo che è stata decifrata. Il software di solito agisce fra la scheda audio del computer ed il software VoIP, captando le conversazioni digitalizzate ma in chiaro. Una copia della conversazione può così essere inviata presso la destinazione desiderata.
In sostanza i suddetti software catturano quanto captato dal microfono e, conseguentemente, possono anche operare indipendentemente da Skype, agendo come una sorta di microspia, e teoricamente possono anche abilitare l'eventuale videocamera e riprendere quanto e' visibile.
Le informazioni così captate vengono mandate a server esterni, collocati in una sorta di sala di ascolto. Ovviamente, questo avviene sfruttando la connettività del computer target. Se questo non ha connettività le informazioni sono salvate in locale e vengono in inviate al server non appena un collegamento alla rete risulta disponibile.
Dunque è chiaro che se si ricorre a tale tipo di intercettazione, in sostanza ogni volta che il computer intercettato è acceso con microfoni attivati si realizzerà una intercettazione "ambientale" di tutto ciò che viene captato dallo stesso microfono e, quindi, evidentemente non solo le conversazioni

tramite skype ma anche le conversazioni tra presenti o addirittura video-riprese tramite la telecamera stessa del computer.
Tale dato tecnico, a mio avviso, pone dei rilevantissimi problemi giuridici: infatti come è noto gli artt. 266 e ss. c.p.p. distinguono le intercettazioni delle comunicazioni o conversazioni telefoniche o tramite altre forme di telecomunicazione dalle intercettazioni tra presenti prevedendo, ad esempio, che queste ultime possano svolgersi nei luoghi di privata dimora solo se vi "è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa" (art. 266 ult. comma c.p.p.).
Pertanto, alcuni interrogativi che si pongono sono: laddove l'autorizzazione sia stata chiesta e concessa solo per intercettare le conversazioni telefoniche e telematiche tramite Skype, saranno utilizzabili le eventuali conversazioni tra presenti intercettate e registrate perché avvenute a microfono aperto? E se il computer da intercettare si trova in un luogo di privata dimora si dovrà ritenere applicabile il limite di cui all'art. 266 ult. comma c.p.p.? ed ancora ove il computer sia in un luogo di privata dimora, ma si intendano intercettare le sole conversazioni tramite skype, si potrà chiedere l'autorizzazione entro tali limiti, con conseguente utilizzabilità sono di tali conversazioni?

3. Le intercettazioni telefoniche, telematiche ed ambientali in Italia ed all'estero: problematiche applicative e richieste rogatoriali

La problematica relativi ai confini territoriali inevitabilmente compromessi dalla potenza delle tecnologie attuali è stata ampiamente dibattuta, raggiungendo un punto di sintesi nell'orientamento giurisprudenziale, ormai consolidato, sulla c.d. "canalizzazione" o "instradamento" delle comunicazioni telefoniche che si svolgono in parte in territorio estero (Cass., 3/12/2007, n. 10051, Rv. 239460, Ortiz e altri; Cass., 28/02/2008, n. 13206, Rv. 239288, Volante; Cass., 02/11/2004, n. 7258, Rv.231467, Commisso e altri; Cass., 30/06/2004, n. 37646, Rv. 229149, Romeo; Cass., 13/06/2003, n. 37751, Rv. 226174, P.M. in proc. Lengu e altri; Cass., 16/10/2002, n. 37774, Rv. 222406, PG in proc. Strangio; Cass., 18/01/2000, n. 287, Rv. 215594 Rosmini D e altri).
E' ben noto come con il sistema del c.d. instradamento, oggi si sia in grado di intercettare tutte le comunicazioni che partono dall'Italia e sono dirette verso un'utenza estera determinata, o a un fascio di utenze appartenenti a un distretto geografico, e viceversa. In pratica, l'instradamento sfrutta un accorgimento tecnico che permette di identificare ex post il numero identificativo dell'utenza o delle utenze italiane sulle quali transiteranno conversazioni telefoniche che si vogliono registrare: gli inquirenti, cioè, conoscono un numero di utenza straniero, e l'attività di intercettazione

viene autorizzata con riferimento a tutte le comunicazioni e conversazioni in partenza da utenze italiane, ancora indeterminate, e dirette verso quella utenza straniera, ovvero provenienti da tale ultima ed in arrivo verso qualsiasi, ancora non identificata, utenza italiana.
E' evidente come tale tecnica non riguardi i casi in cui l'intercettazione abbia ad oggetto una utenza cellulare con sim-card di un gestore italiano, che dovesse trovarsi casualmente all'estero. Al riguardo la Suprema Corte ha chiarito che, nel caso in cui le operazioni di intercettazione riguardino un'utenza telefonica mobile, non rileva, al fine della individuazione della giurisdizione competente, il luogo dove sia in uso il relativo apparecchio, bensì esclusivamente la nazionalità dell'utenza, essendo tali apparecchi soggetti alla regolamentazione tecnica e giuridica dello Stato cui appartiene l'ente gestore del servizio. Ne consegue che non è necessario esperire una rogatoria internazionale, se le operazioni di intercettazione di un'utenza mobile nazionale in uso all'estero possono essere svolte interamente nel territorio dello Stato (così Cass., sez. IV, 7 giugno 2005, Mercado Vasquez, in C.E.D. Cass., n. 232080)
La recente sentenza Cass. sez. I n.13972 del 4.3.2009 Rv.243138 ha ribadito tali consolidati principi affermando *"In tema d'intercettazioni telefoniche, il ricorso alla procedura dell'istradamento, è cioè il convogliamento delle chiamate in partenza dall'estero in un nodo situato in Italia (e a maggior ragione di quelle in partenza dall'Italia verso l'estero, delle quali è ceto che vengono convogliate a mezzo di gestore sito nel territorio nazionale) non comporta la violazione delle norme sulle rogatorie internazionali, in quanto in tal modo tutta l'attività d'intercettazione, ricezione e registrazione delle telefonate viene interamente compiuta nel territorio italiano, mentre è necessario il ricorso all'assistenza giudiziaria all'estero unicamente per gli interventi da compiersi all'estero per l'intercettazione di conversazioni captate solo da un gestore straniero"* . Le procedure di rogatoria, conclude la Suprema Corte, sarebbero necessarie soltanto in caso di intercettazione da eseguirsi integralmente in territorio estero.
La giurisprudenza citata si è formata esclusivamente con riferimento alle comunicazioni telefoniche "tradizionali" e non risultano precedenti con riguardo a tutte le "altre" forme di comunicazioni telematiche, coinvolgenti sistemi informatici.
Il problema è di particolare rilevanza, posto che buona parte delle ordinarie attività di fruizione dei servizi informatici/telematici può coinvolgere "server" o comunque postazioni che si trovano fuori dai confini nazionali; è il caso ad esempio dell'utilizzo della "WebMail", cioè della creazione e gestione di un account di posta elettronica attraverso un navigatore web, servizio offerto di solito da Provider o da famosi portali quali Google, Yahoo, ecc., Microsoft.com; in questi casi, le caselle di posta elettronica sono solitamente memorizzate in server posti all'estero.

Altro caso è quello della semplice navigazione Web che spesso si spinge verso siti web con server sparsi nel mondo. In questi casi, qualora l'utente o gli utenti interessati si trovino in Italia, parte delle operazioni tecniche di connessione alla rete telematica avviene comunque in territorio nazionale (tramite i c.d. "Pop", Point of Presence, cioè i punti di accesso alla rete, forniti di solito da un Internet Service Provider), per cui non paiono sussistere motivi ostativi all'applicazione dei medesimi principi giurisprudenziali elaborati con riferimento alla c.d. procedura di "instradamento".

Da segnalare, infine, una recente pronuncia relativa alle intercettazioni "ambientali" eseguite all'interno di autovettura che, partita dall'Italia, si rechi in seguito all'estero. La Suprema Corte ha stabilito al riguardo che "*essendo la microspia stata installata in Italia, ed essendo la captazione avvenuta in Italia, attraverso le centrali di ricezione di Torino, la sola circostanza che le conversazioni siano state eseguite all'estero per lo spostamento dell'autovettura è ininfluente per ritenere la necessità della rogatoria, non potendosi, nel caso di intercettazione ambientale su mezzo mobile conoscere tutti gli spostamenti, così vanificandosi le finalità del mezzo di ricerca della prova [...] le intercettazioni ambientali su veicolo mobile (solitamente autovettura), predisposte con microspia, o altro mezzo di registrazione, non possono poi subire limitazioni per il trasferimento del veicolo in paesi stranieri [...] i continui spostamenti su territori esteri, successivamente al momento dell'inizio delle operazioni che, nella specie, è da individuarsi con certezza in Italia, diversamente comporterebbero una impossibilità tecnica di procedere alla intercettazioni, ben potendo l'Autorità Giudiziaria che le ha disposte ignorare il luogo dove si trova il veicolo, ed essere quindi impossibilità a chiedere la rogatoria* ...." (Cass., sez. IV , 27/02/2008, n. 8588, Rv. 238951, Assisi e altri).

Laddove le operazioni di intercettazione debbano essere eseguite interamente all'estero (perché riguardanti solo utenze straniere o comunicazioni non transitanti su 'nodi' telefonici italiani) è necessario attivare una procedura rogatoriale, disciplinata dalla convenzione bilaterale o plurilaterale ratificata dall'Italia e dal Paese estero interessato, e, in mancanza, dalle norme codicistiche dettate dagli artt. 727 e segg. c.p.p.

In ambito europeo la disciplina applicabile è quella della Convenzione europea di assistenza giudiziaria in materia penale, firmata a Strasburgo il 20 aprile 1959, che, pur non facendo esplicitamente riferimento alle intercettazioni, stabilisce, in generale all'art. 3, che "la Parte richiesta farà eseguire, nelle forme previste dalla propria legislazione, le rogatorie relative ad un procedimento penale che verranno a lei dirette dalle autorità giudiziarie della Parte richiedente e che hanno per oggetto il compimento

di atti istruttori o la trasmissione di corpi di reato, di fascicoli o di documenti".

In base all'art. 14 della medesima Convenzione, la richiesta va tradotta nella lingua straniera dello Stato richiesto, deve contenere l'indicazione dell'autorità giudiziaria richiedente (con gli estremi dei dati che possano favorire le comunicazioni: es. numeri telefonici e di fax, ed indirizzi e-mail); l'oggetto e il motivo della domanda, se possibile l'identità e la nazionalità della persona imputata e del soggetto destinatario dell'atto istruttorio; l'imputazione, con una indicazione delle norme di diritto penale sostanziale violate, ed una sommaria descrizione dei fatti. E' consigliabile anche la indicazione, nella richiesta, delle motivazioni investigative e dei tempi di effettuazione dell'atto istruttorio.

La richiesta va inoltrata per il tramite degli appositi uffici dei ministeri della giustizia dei due paesi interessati, salvi i casi di urgenza, che permettono l'inoltro diretto all'autorità giudiziaria, eventualmente per il tramite dell'organizzazione internazionale di polizia criminale (Interpol). Tuttavia, l'art. 53 della Convenzione di applicazione dell'Accordo di Schengen del 19 giugno 1990 (ratificata ed entrata in vigore in Italia con la legge 30 settembre 1993, n. 388), ammette oggi che, nell'ambito dell'Unione europea, le domande di assistenza giudiziaria possano essere inoltrate e ricevute direttamente dalle autorità giudiziarie competenti. La previa, corretta individuazione dell'autorità destinataria della richiesta è auspicabile, potendo, a tal fine, avvalersi delle informazioni dei Magistrati di collegamento, dei magistrati di Eurojust ovvero degli addetti ai punti di contato della Rete giudiziaria europea.

In materia, la Corte di Cassazione ha chiarito che:

- la richiesta rogatoriale può essere formulata direttamente dal pubblico ministero italiano, spettando al giudice il successivo compito di valutazione della utilizzabilità dei relativi risultati, ed in particolare si è affermato "*La legge consente al pubblico ministero, immediatamente, di richiedere rogatorie all'estero, mediante i previsti canali ministeriali e diplomatici, per comunicazioni, notificazioni e per attività di acquisizione probatoria, espressione da intendere "lato sensu", e cioè comprensiva dell'attività investigativa (indagini) funzionale alla pubblica accusa, che addirittura, alla pari del giudice, potrà inoltrare direttamente la rogatoria stessa, ove ricorrano le condizioni previste dall'art. 727, comma quarto o quinto, cod. proc. pen. (Fattispecie relativa all'acquisizione di intercettazione ambientale e di testimonianza ad opera dell'autorità giudiziaria spagnola su diretta richiesta del P.M., motivata dall'urgenza. Nell'affermare il principio di cui in massima, la S.C. ha ritenuto pienamente utilizzabili i risultati dell'attività investigativa compiuta all'estero al fine dell'emissione di provvedimento di coercizione personale)*". (Cass., sez. I, 25 settembre 1997, Dentice, in C.E.D. Cass., n. 208800);

- in base al principio generale della lex loci, è irrilevante che all'estero le operazioni di intercettazione siano state eseguite senza il rispetto delle prescrizioni dettate dagli artt. 267 e 268 c.p.p., salvo che la violazione non abbia inciso su principi fondamentali del nostro ordinamento: non è necessaria, dunque, la trasmissione dei 'brogliacci di ascolto' redatti dagli ufficiali di polizia straniera, né occorre che la trascrizione delle conversazioni intercettate all'estero sia stata effettuata con perizia (Cass., sez. I, 10 settembre 1998, Bonelli, ivi, n. 211301; conf., in seguito, Cass., sez. I, 30 gennaio 2002, Arben, ivi, n. 220965; Cass., sez. II, 13 dicembre 2001, Borgia, ivi, n. 223918);
- la trasmissione diretta all'autorità giudiziaria italiana della documentazione relativa all'attività di indagine compiuta all'estero, è conforme alle prassi invalse nell'applicazione delle convenzioni internazionali e non comporta alcuna inutilizzabilità ex art. 729, comma 1, c.p.p. (Cass., sez. I, 20 settembre 2002, Monnier, ivi, n. 222863); in questi casi, salvo che l'autorità rogante non abbia espressamente domandato gli originali, è possibile anche la trasmissione di mere fotocopie della documentazione, dato che l'atto formale di trasmissione è idoneo a garantire l'autenticità e la conformità degli atti trasmessi (Cass., sez. IV, 19 febbraio 2004, Montanari, ivi, n. 228355; e Cass., sez. I, 16 ottobre 2002, Strangio, ivi, n. 222406);
- a mente del predetto art. 729, comma 1, c.p.p., l'autorità giudiziaria italiana è vincolata al rispetto delle condizioni, eventualmente poste dallo Stato estero, di utilizzabilità degli atti richiesti (così in un caso in cui il S.C. ha ritenuto utilizzabili in Italia, in un processo relativo al reato di associazione mafiosa, anche dedita alla consumazione di delitti in materia di contrabbando di tabacchi lavorati esteri, le intercettazioni telefoniche effettuate per rogatorie in Svizzera, nonostante la relativa autorità elvetica avesse posto come condizione la loro inutilizzabilità in processi, anche penali, di natura fiscale: v. Cass., sez. VI, 16 maggio 2000, Bossert, ivi, n. 217565);
- è possibile utilizzare in Italia anche i risultati delle operazioni di intercettazione disposte nello Stato straniero nell'ambito di un processo penale pendente in quel paese (Cass., sez. V, 26 novembre 1996, Lavorato, ivi, n. 207867); laddove tale documentazione sia stata trasmessa dall'autorità di polizia straniera alla corrispondente autorità italiana, i relativi atti sono utilizzabili nel processo penale italiano, successivamente instaurato, anche se non siano state rispettate le disposizioni in materia di rogatoria, che non potevano essere applicate in una fase antecedente all'acquisizione della stessa notitia criminis (Cass., sez. III, 6 novembre 2002, p.m. in proc. Pils, ivi, n. 223200; e Cass., sez. I, 17 dicembre 2002, Moio, ivi, n. 222984, in una ipotesi in cui la trasmissione era stata effettuata in Italia dalla polizia straniera ai sensi dell'art. 34 dell'Accordo di Schengen).

Per completezza va segnalato che la materia è stata specificamente disciplinata dalla Convenzione europea di assistenza giudiziaria in materia penale, sottoscritta a Bruxelles il 29 maggio del 2000, che non è stata ancora ratificata dall'Italia. Nell'ambito di una rinnovata regolamentazione dell'attività rogatoriale, la Convenzione prende in considerazione, in realtà, solamente le intercettazioni telefoniche di apparecchi satellitari o cellulari, e prevede quattro casi (artt. 18 e 20): il primo è quello della persona, la cui utenza è da intercettare, che si trova nel territorio dello Stato richiedente laddove le operazioni di captazione necessitino dell'assistenza tecnica di altro Stato membro (ad esempio, perché si tratta di telefoni satellitari); il secondo caso è quello della persona, la cui utenza è da intercettare, che si trova nel territorio di altro Stato; il terzo caso è quello analogo al secondo in cui, però, è necessario il coinvolgimento di uno Stato terzo per potere eseguire le operazioni; ed infine, il quarto caso è quello in cui durante l'esecuzione delle intercettazioni si scopre che la persona, la cui utenza è sotto controllo, si è spostata nel territorio di altro Stato. Ipotesi nelle quali è sempre stabilita l'attivazione di vari schemi rogatoriali, più o meno complessi (sull'argomento v. APRILE-SPIEZIA, Le intercettazioni telefoniche ed ambientali, Giuffrè, 2003, p. 114).

Roma, 6 luglio 2011

Andrea Bonomo