Overview **dei dati che gli operatori telefonici possono fornire al fine di tracciare l'attività e la localizzazione dell'utente, ed un commento alle leggende "high tech" create nel tempo su essi.**

Nanni BASSETTI, laureato in Scienze dell'Informazione, libero professionista specializzato in digital forensics, fondatore di CFI (Computer Forensics Italy) e project manager di CAINE Linux/GNU Live distro per indagini informatiche. Docente, relatore in parecchi corsi ed eventi, autore di molti articoli tecnici e di un paio di libri.

Paolo REALE, ing., consulente nell'ambito dell'ICT ed esperto in Digital Forensics, Presidente della commissione ICT dell'Ordine Ingegneri di Roma. Keynote speaker a conferenze internazionali su tematiche di telecomunicazioni, relatore e docente di Digital Forensics presso Organizzazioni ed Università. Tra gli incarichi affidati e svolti sono presenti casi di particolare rilevanza, anche mediatica.

I DATI TELEFONICI PER FINALITÀ GIUDIZIARIE NELLE APPLICAZIONI REALI

di Nanni BASSETTI e Paolo REALE

Introduzione

Ormai le nostre vite sono tracciate dai dispositivi digitali, onnipresenti e sovrautilizzati, e questo fa sì che i primi oggetti su cui vengono riposte le maggiori attenzioni da parte degli investigatori siano proprio i cellulari e le comunicazioni intercorse. Ma cosa è possibile realmente ricavare dai dati degli operatori telefonici sulle nostre attività?

La richiesta dei tabulati telefonici da parte dell'Autorità Giudiziaria e degli avvocati (per le indagini difensive) è sempre più frequente, anche se con differenze fondamentali sui risultati che si possono ottenere, come vedremo meglio nel prosieguo di questo intervento. Grazie a questi documenti si possono ricavare molte informazioni inerenti le attività da noi compiute nel passato, come i luoghi in cui abbiamo effettuato o ricevute le chiamate, in termini di indicazioni geografiche (ossia le macrozone dove siamo stati insieme al nostro telefonino), chi ci ha chiamato e chi abbiamo chiamato, gli SMS inviati e ricevuti, se ci siamo collegati ad Internet.

In un contesto dove è predominate la tecnologia, e nel quale si vogliono riporre troppe speranze (leggi miracoli) nel cercare le evidenze che magari latitano, possono anche nascere leggende sull'effettivo utilizzo di questi dati al pari delle c.d. "leggende metropolitane". In questo intervento si cercherà di fare chiarezza su alcune di esse, che generano solanto confusione.

Indagini difensive si o no

Per quanto il codice di procedura penale, nell'attuale formulazione, abbia recepito le esigenze e i diritti della Difesa a svolgere le indagini nel proprio interesse, può accadere che questo "diritto" possa trovare qualche impedimento nell'organizzazione degli uffici degli operatori telefonici deputati alla validazione di richieste per la fornitura di informazioni come quelle su menzionate. Al tal proposito è utile ricordare che il Garante della protezione dei dati personali, nel suo documento "Recepimento normativo in tema di dati di traffico telefonico e telematico" del 24 luglio 2008, scrive che "*al difensore dell'imputato o della persona sottoposta alle indagini è riconosciuta la facoltà di richiedere, direttamente, al fornitore i dati di traffico limitatamente ai dati che si riferiscano 'alle utenze intestate al proprio assistito'*". Nella realtà dei fatti, purtroppo, la comunicazione di risposta dell'operatore telefonico può arrivare anche a distanza di molte settimane, o addirittura mesi, dalla richiesta, e può capitare che a fronte della semplice richiesta dei dati sulla posizione geografica della cella telefonica, l'operatore risponda con un messaggio del tipo "*ci duole comunicarLe che non possiamo darvi corso per motivi di riservatezza*".

Traffico telefonico o traffico telematico

Si sente sempre parlare del "traffico telefonico" e dei relativi tabulati, in realtà gli operatori mantengono anche i dati relativi al "traffico telematico"; spesso i relativi tabulati di traffico storico non sono oggetto di analoga attenzione da parte dei consulenti e degli investigatori. Eppure, per quanto riguarda la rete "fissa", questo tabulato consente, per esempio, di conoscere le sessioni ad Internet avvenute tramite la linea telefonica ADSL di casa. Ma è in ambito "mobile" che si hanno i maggiori vantaggi: se un utente telefonico le cui abitudini in termini di quantità di SMS o conversazioni sono piuttosto contenute, riflettendosi in limitatissime (se non addirittura assenti) tracce sui tabulati, è però possibile che questi stia utilizzando un terminale di ultima generazione, uno *smartphone*, che fa generoso accesso alla rete di tipo "dati" per la consultazione della posta elettronica, per le notifiche di Facebook, per i messaggi di WhatsApp e così via. Ciò si traduce in un tabulato telematico di indubbio interesse investigativo, poiché spesso tali connessioni hanno maggiore frequenza e continuità temporale.

Nell'ambito dei servizi di comunicazione elettronica senza distinzione fisso/mobile, nel suo documento "Sicurezza dei dati di traffico telefonico e telematico" del 17 gennaio 2008, il Garante della privacy italiano declina come servizi "telefonici":

- le chiamate telefoniche, incluse le chiamate vocali, di messaggeria vocale, in conferenza e di trasmissione dati tramite telefax;
- i servizi supplementari, inclusi l'inoltro e il trasferimento di chiamata;
- la messaggeria e i servizi multimediali, inclusi i servizi di messaggeria breve-sms;

e come servizi "telematici":

- l'accesso alla rete Internet;
- la posta elettronica;
- i fax (nonché i messaggi SMS e MMS) via Internet;
- la telefonia via Internet (cd. *Voice over Internet Protocol* - VoIP)."

I tempi di conservazione dei dati

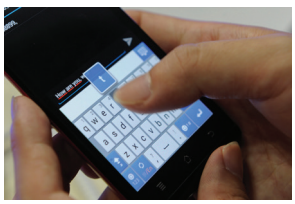
La recente decisione con cui la Corte di giustizia europea, l'8 aprile 2014, ha dichiarato invalida la direttiva europea 2006/24/CE sulla conservazione dei dati nell'ambito della fornitura di servizi di comunicazione elettronica, può essere interpretata come un effetto della c.d. sindrome del "Grande Fratello", secondo cui c'è una generale sensazione che i nostri dati telefonici siano continuo oggetto delle attenzioni degli operatori e dell'Autorità. Se è vero che sono esistiti casi di abuso, portati all'attenzione in noti fatti di cronaca, è altrettanto vero che questo non è quanto dispone la legge. Anzi, per le finalità di accertamento e perseguimento dei reati penali, risulta piuttosto limitato il tempo di permanenza dei cartellini di traffico storico e, come normato dal "Decreto Legislativo 30 maggio 2008, n. 109", che ha recepito in Italia la suddetta direttiva, è esattamente pari a:

- per il traffico telefonico, 24 mesi dalla data della comunicazione;
- per il traffico telematico, 12 mesi dalla data della comunicazione;
- per le chiamate senza risposta, 30 giorni dalla data della comunicazione.

In realtà, va evidenziato che la recente sentenza della Corte di Giustizia Europea, che ha invalidato la direttiva, sostiene che "*[...] adottando la Direttiva sulla Data Retention, la legislatura UE abbia superato i limiti imposti dalla conformità col principio di proporzionalità*". Questo significa che i termini sopra indicati continueranno ad essere i riferimenti legislativi adottati dagli operatori, ma è lecito attendersi una nuova Direttiva che recepisca i rilievi formulati dalla Corte Europea, magari nei termini di un minor tempo di conservazione di questi dati.

Gli operatori telefonici conservano i testi degli SMS

È falso! L'operatore fornisce solamente il numero del mittente, del destinatario, la data e l'ora e la cella utilizzata, l'IMEI, etc., ma i testi degli SMS non sono conservati e nemmeno sono previsti nelle direttive europee e nazionali, oltre che dal codice sulla privacy (Rif. DL 30 maggio 2008 n 109, Direttiva 24/2006 C.E. e D.Lgs 196/03; per un approfondimento si rimanda a "*Gli operatori telefonici non conservano i contenuti delle chiamate e degli SMS*" di Marzia Minozzi, su questa Rivista, n. IV /MMXI).



In particolare, sempre nel DL del 30 maggio 2008, all'art. 3 vengono elencate esattamente le categorie di dati da conservare per gli operatori di telefona e di comunicazione elettronica, che non andremo ad elencare in questo contesto, ma che non contemplano comunque il contenuto del testo del messaggio SMS scambiato.

Come è possibile quindi conoscere questi testi? Esistono solo due modi: l'utenza di interesse è posta sotto intercettazione al momento di interesse (visto appunto che a posteriori non è più possibile recuperare l'SMS inviato in un periodo precedente all'intercettazione), oppure occorre sequestrare l'apparato telefonico che li ha inviati/ricevuti. In questo secondo caso, in funzione della tipologia di terminale e delle sue modalità di utilizzo, è anche possibile tentare il recupero dei messaggi eventualmente cancellati dal proprietario.

Gli operatori telefonici conservano i dati delle navigazioni Internet dell'utente

L'operatore dovrebbe fornire solamente l'indirizzo IP (*Internet Protocol*) fornito al terminale mobile dell'utente, la data e l'ora della connessione ad Internet, la cella agganciata, i dati del terminale e l'APN se è stato utilizzato un cellulare.
È tuttavia utile notare che, al momento attuale, questa tipologia di dato ancora non ha consolidato un minimo di coerenza ed omogeneità di conservazione e rappresentazione tra i vari gestori di telefonia. Il risultato è che si ottengono informazioni a volte lacunose.

Le celle tracciano la posizione del cellulare

Se il cellulare è acceso e riceve/invia chiamate ed SMS o effettua connessioni ad Internet, allora vengono associate a questi eventi le celle che aggancia, le quali potranno esser lette nei tabulati.
Se tuttavia il terminale mobile non riceve/effettua chiamate/sms/connessioni, nessun dato sarà disponibile sui tabulati, quindi non avremo informazioni sulle celle e i relativi spostamenti del dispositivo mobile.

Il posizionamento del cellulare può esser effettuato in due modalità, con riferimento al tempo in cui è effettuato. Se si effettua da un dato momento in poi, allora abbiamo due modi di realizzarlo:

- tramite intercettazione telefonica, i cui cartellini IRI associati al contenuto contengono la posizione dell'utente;
- tramite localizzazione ad evento ("*location updating*") effettuata sul nodo HLR della rete mobile oppure localizzazione di precisione a tempo ("*positioning*").

Se si vuole individuare la posizione del terminale mobile con riferimento ad una data precedente, allora si hanno due possibilità:

- analizzando il telefonino, con un'analisi forense, alla ricerca delle posizioni GPS ed altri dati utili;
- tramite i tabulati del traffico pregresso (come visto in precedenza).

La "triangolazione" delle celle

Il concetto di 'triangolazione' geometrica, ovvero l'individuazione di un punto geografico sfruttando le proprietà dei triangoli è mediamente noto: sfruttando il fatto che più celle - tipicamente - possono esser viste dallo stesso terminale mobile, potrebbe essere possibile calcolare esattamente il punto geografico in cui si trova un utente.
Questa operazione è in realtà possibile effettuarla e viene attivata all'occorrenza nelle procedure di emergenza del Numero Unico Europeo 112: nei casi di emergenza, sono consultate le celle che riescono a "vedere" l'utenza oggetto di richiesta di localizzazione e, sulla base dei loro dati, viene calcolato l'ipotetico punto in cui si trova, tramite operazioni di triangolazione.

Va detto, tuttavia, che l'operazione ha una precisione che, in funzione di diversi fattori, è spesso inadeguata per una determinazione precisa del punto: il caso di Melania Rea è esemplificativo del fatto che - pur in presenza del suo cellulare ancora acceso - il punto individuato distava circa 3Km dal reale punto in cui si trovava il telefonino.

Cellulare spento o non raggiungibile?

Quando un nostro tentativo di chiamata non arriva a far "squillare" il telefono dell'interlocutore, al posto del classico "segnale di

libero", sentiamo un messaggio registrato che ci avvisa che il telefono è probabilmente spento o non raggiungibile. A volte questo messaggio viene prodotto dopo essere rimasti in attesa per diversi secondi, in quello che intuitivamente ci appare come il tempo durante il quale la rete ricerca il telefono per avvisarlo della chiamata in arrivo.

In effetti, solitamente, questa è l'operazione in corso ma sarebbe errato interpretare questa fase come elemento significativo del fatto che il terminale oggetto di nostro interesse sia effettivamente acceso: il telefono, quando viene spento regolarmente tramite pulsante, comunica il "*detach*", ovvero il fatto che si sta disconnettendo dalla rete, quindi alla rete è noto lo stato di "spegnimento". Se invece per diverse cause, come ad esempio la batteria si scarica oppure il cellulare perde il segnale della rete, non avviene la comunicazione di "IMSI *detach*", la rete continuerà per un periodo configurabile a tentare la ricerca del terminale sulle celle telefoniche in cui lo stesso si era registrato poco prima.
Trarre conclusioni sull'effettivo spegnimento o meno di un terminale da queste procedure telefoniche è quindi completamente errato.

Si chiama "cella" o "sito"?

Nel linguaggio comune è frequente sentire parlare di celle telefoniche, vista la loro importanza nelle indagini e nei casi di cronaca: per questo le si trovano negli articoli dei giornali, nelle memorie dei PM e degli avvocati, nelle motivazioni dei Giudici. Spesso però viene troppo "semplificato" il concetto di cella, al punto da confondere i siti delle antenne (le stazioni radio base o BTS) con le BTS stesse. In realtà, un "sito cellulare" consiste in una struttura nella quale trovano alloggio più BTS: la modalità di installazione più comune è quella del sito a 3 celle, in cui ognuna 'illumina' un'area che - a livello di schematizzazione semplificata - corrisponde ad un settore ampio circa 120 gradi. Chiaramente il sito con le 3 celle consente la copertura dell'area a 360 gradi.

Quando si legge "la cella di via Verdi" siamo quindi di fronte sempre ad un dubbio amletico: quale delle 3 celle effettive del sito di Via Verdi sarà quella indicata? In funzione del contesto di indagine il dato non è affatto indifferente!

Com'è fatta una cella

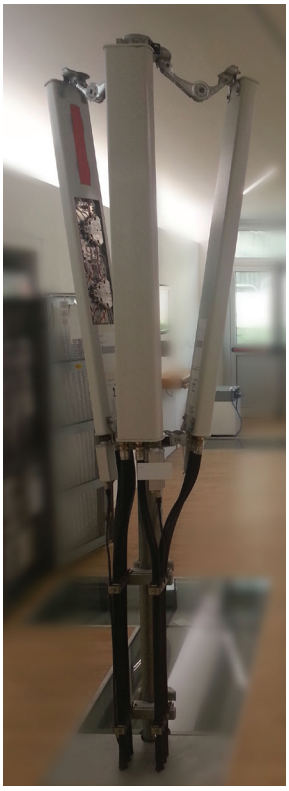
Forse è quindi utile svelare l'arcano, e illustrare con una foto la configurazione tipica di un sito: nella foto accanto si noti la struttura a 3 celle, e - per i più curiosi - come ogni singola antenna è fatta dentro.

I cellulari spenti comunicano con le celle

È falso! Se il cellulare è spento non vi è alcuna comunicazione con le celle telefoniche e non è quindi possibile controllarlo, usarlo come microspia ambientale o sistema di intercettazione abusivo: questo perché manca il mezzo di comunicazione.
L'unico caso in cui potrebbe esser realizzato qualcosa di simile, è quando il cellulare è infettato da qualche *spyware* (*software* installato sul dispositivo), creato *ad hoc* per far credere all'utente di avere il cellulare spento o in modalità aereo.

Qualcuno mi spia dal cellulare

Il caso di cui sopra è possibile solo se qualcuno è riuscito ad infettare il cellulare, e per farlo deve aver avuto accesso fisico al dispositivo o aver utilizzato un SMS di configurazione (o simili) che l'utente ha eseguito e si è auto infettato, come accade per i *computer*.
Nessuna magia: solo un sudbolo trucco, spesso difficile anche da individuare. Attenzione quindi a non lasciare il cellulare incustodito e senza codice di blocco!



Conlcusioni

Insomma tra la fantasia, il complottismo, le leggende e la realtà c'è una bella differenza.
Non tutto si può fare, non tutto è rapido, non tutto è economicamente e legalmente possibile, ci sono limiti tecnologici e legislativi, un bilanciamento tra l'onere dei gestori telefonici e dei costruttori di cellulari e le esigenze della Giustizia che ha bisogno di raggiungere uno stato di equilibrio, rispettoso della privacy degli utilizzatori dei dispositivi oggetto di indagine.

Il problema è che spesso si tende a credere alle dicerie, alle *fiction* della televisione ed alle speculazioni pseudo-scientifiche, senza aver approfondito l'argomento: spesso queste "credenze" ingenerano critiche nei confronti degli inquirenti o paranoie infondate nei cittadini.
Certamente i Governi potrebbero aver mezzi superiori per controllare tutto e tutti, come ci ha rivelato Snowden per gli USA, ma questo è argomento diverso: è spionaggio ad alto livello, costoso e per *target* importanti. Snowden ci ha ricordato che gli strumenti d'indagine sono senz'altro pericolosi se utilizzati senza controllo. Da parte nostra, però, deve sempre alto il livello di attenzione e dobbiamo adottare una "ragionevole prudenza" su quanto della nostra vita trasferiamo nei dispositivi digitali. In tal senso dobbiamo stare attenti a non fare crescere troppo la nostra "ombra digitale", perché se poi sui *social networks* siamo prodighi di *post* dettagliati su tutto quello che stiamo facendo, comprese le foto dei nostri viaggi … beh… allora non sarà una cella telefonica troppo solerte la nostra spia! ©