Che cosa è una “analisi dati” su telefoni cellulari o computer

Le intercettazioni telefoniche e le indagini in campo informatico

L’enorme diffusione dei telefoni cellulari e la possibilità di questi dispositivi di scambiare messaggi brevi, navigare in internet, effettuare foto e filmati ecc. li rendono dispositivi ideali nelle indagini promosse dalla magistratura, che sempre più spesso richiede l’esame, a fini probatori, dei dati contenuti e delle tracce che lasciano nelle reti dei gestori telefonici.

Lo stesso si può dire dei personal computer, anch’essi oramai capillarmente diffusi e sempre più oggetto di analisi alla ricerca di elementi di prova a carico degli indagati.[1]

Per questo, come le notizie di cronaca dimostrano ogni giorno, può accadere che un soggetto, sottoposto ad accertamenti nella ricerca di prove di reato, si ritrovi imputato[2] sulla base di indizi informatici.

La “mobile forensic”, analisi forense della telefonia cellulare

Mi riferisco, in particolare, all’esame dei tabulati telefonici e al prelievo dei dati presenti nella memoria di telefonini, tablet ecc. di proprietà dell’indagato o anche ai dati geografici registrati in un navigatore satellitare.

Da un altro punto di vista, può accadere che un soggetto, che abbia subito un danno, un’offesa o delle minacce tramite telefonate cellulari o attraverso la rete internet, si limiti a sporgere denuncia alle autorità senza preventivamente incaricare un consulente di parte di prelevare e registrare, in maniera conforme ai parametri di ripetibilità, le prove del reato. Può accadere così che il soggetto che ha agito tali minacce riesca a cancellarne le evidenze o che errori commessi durante le indagini modifichino le prove ricercate, portando inevitabilmente all’archiviazione della denuncia.

In tali casi, l’allegazione di una perizia informatica giurata, condotta nel rispetto delle procedure di copia e di custodia, può fare la differenza tra un procedimento destinato all’oblio e la possibilità di veder perseguito l’autore di un reato informatico.

Contrariamente a quanto si è portati a credere, non sono solo i criminali a utilizzare in modo illecito le attuali tecnologie informatiche e/o di comunicazione, ma anche comuni cittadini che, per risentimento, vendetta o altro, usano i telefoni cellulari o internet per aggredire o danneggiare persone o aziende, nella convinzione (illusoria) che un “nickname” di fantasia o indirizzi di posta elettronica anonimi li rendano non rintracciabili.

Ciò non è sempre vero; questo genere di reati trasportano al loro interno, più spesso di quanto si pensi, delle tracce che possono condurre al colpevole.

I “tabulati” telefonici

La capillare diffusione dei telefoni cellulari, le potenzialità delle loro memorie nonché il loro peculiare modo di funzionamento, che registra anche alcuni dati geografici, oltre al traffico telefonico in entrata e in uscita, li rendono dispositivi ideali nelle indagini promosse dalla magistratura, che sempre più spesso richiede, ai gestori di telefonia, i CDR (*Call Detail Records*) ossia la registrazione dei dettagli delle chiamate, comunemente conosciuti come “tabulati”, per esaminare, a posteriori, la posizione geografica di un determinato utente in un preciso segmento temporale, nonché i suoi spostamenti e lo “stato” del suo terminale mobile (telefonino), se spento o se acceso e collegato alla rete telefonica cellulare, sempreché abbia generato del “traffico”, ossia effettuato o ricevuto chiamate, anche senza risposta, sms o altro. I gestori telefonici, infatti, sono tenuti a conservare per ventiquattro mesi, prolungabili di altri ventiquattro in caso di reati, i dati del terminale mobile che ha generato traffico, mentre registrano solo per poche ore la posizione dei telefonini “inattivi”.[3]

Tuttavia, non possiamo trascurare alcune precisazioni che, come vedremo, rivestono un’importanza capitale dal punto di vista della corretta ricerca delle fonti di prova.

L’architettura di tale sistema di telecomunicazione mobile è ingegnerizzata a scopi essenzialmente commerciali, funzionali alla fatturazione degli abbonamenti o di ogni singola chiamata e, contemporaneamente, all’individuazione approssimativa della posizione di ogni singolo terminale allo scopo di metterlo in comunicazione con la cella BTS (base transceiver station) che risulta avere, in un preciso istante, il segnale radio più forte. Questa cella è tecnicamente definita “miglior servente”.

Attenzione! Non sto parlando della cella BTS geograficamente più vicina. Infatti, per le peculiari caratteristiche di propagazione delle onde radio nelle gamme di frequenze usate dalla telefonia mobile, che ricadono nella banda delle microonde, il segnale radio più forte non necessariamente coincide con la trasmittente geograficamente più prossima.

Questo fenomeno è particolarmente rilevante negli ambienti urbani dove uno o più ostacoli, quali possono essere edifici, formazioni orografiche collinari e/o montuose e più in generale qualunque struttura schermante la radiofrequenza, possono rendere momentaneamente “miglior servente” anche una cella BTS posta a distanze rilevanti, a discapito di un’altra posta magari a un centinaio di metri o meno.

L’analisi delle celle si fonda, in realtà, su una valutazione di tipo probabilistico e non deterministico, per cui è prioritario comprendere quali siano i fattori da tenere in considerazione per stimare l’affidabilità dei risultati sul piano tecnico, ancor prima che su quello giuridico. Per questi motivi è di fondamentale importanza affidare l’esame ad un Perito competente in informatica e telecomunicazioni, professionista in grado di apprezzare e vagliare tali fattori.

Tentare di piegare alle esigenze degli inquirenti un sistema progettato per altri scopi, genera spesso risultati impropri, lacunosi e fuorvianti, in grado di distorcere la ricerca della verità, influendo negativamente sulla formazione della prova stessa e sulla costruzione del libero convincimento del Giudice.

In sostanza; non ho la presunzione di contestare *in toto* la pratica dell’esame dei cosiddetti “tabulati telefonici”, anzi, riconosco che spesso hanno portato alla soluzione di complessi casi giudiziari, ma semplicemente ritengo indispensabile evidenziare come, sul piano criminologico-investigativo, si debba tener conto, ai fini della corretta ricerca delle fonti di prova ed a garanzia degli inviolabili diritti della difesa, delle summenzionate numerose ed inevitabili variabili e tolleranze, insite in un sistema progettato per scopi peculiari e, non da ultimo, delle diverse interpretazioni che le parti, legittimamente, offriranno nell’oralità del contraddittorio.

Come si può individuare la posizione geografica di un telefono cellulare

Il funzionamento del sistema telefonico mobile si basa, fondamentalmente, sull’individuazione puntuale di ogni singolo terminale, da parte delle cosiddette “celle” ossia, dei ripetitori radiotelefonici. Più esattamente, ogni terminale, acceso e dotato della sua SIM, aggiorna periodicamente la rete dell’operatore di appartenenza in modo da essere localizzato e quindi

essere raggiungibile dal sistema, anche quando è in “stand-by”, ossia non sta effettuando né ricevendo telefonate o altro.
Questi dati, che possono essere usati anche per la geolocalizzazione, non sono conservati nella rete dell’operatore a causa dell’enorme mole di “bit” che generano e che richiederebbe altrettanto enormi memorie di massa.

L’esame dei tabulati telefonici forniti dall’operatore di appartenenza, basati sui cosiddetti “Call Detail Record” contengono, fra gli altri dati, i “cell ID” che identificano con certezza la stazione base cui il terminale era connesso mentre stava ricevendo/trasmettendo, è dunque, il solo modo per localizzare, a posteriori, la posizione geografica di un telefono in un dato momento, seppure con scarsa approssimazione e con tutte le variabili che possono influire negativamente sulla precisione, utilizzando le mappe di copertura della rete realizzate a cura del gestore telefonico, che rappresentano l’area teorica di copertura di ogni singola cella.

La localizzazione “a posteriori” di un apparato radiomobile all’interno dell’area geografica illuminata dalla relativa antenna non è un dato certo, ma solo probabile. E’ possibile infatti che l’apparato si trovi geograficamente nel settore di una cella, pur essendo comunque servito da una cella adiacente non “prevista” nella mappa di copertura, a causa delle variabili di cui al paragrafo precedente.

Insomma, si può capire se, al momento della chiamata, il telefono si trovasse in centro città o in periferia ma non se si trovasse in una determinata strada, presso un certo numero civico. Questo sarebbe possibile con un dispositivo di navigazione satellitare GPS, ma il sistema telefonico cellulare è tutt’altra cosa.

L’analisi informatica forense o “computer forensic”

A volte, purtroppo, l’attività investigativa svolta dagli inquirenti non è priva di errori, vuoi perché messa in atto da personale non perfettamente addestrato, vuoi perché alcuni software, entrati oramai nell’uso standard nelle perizie, mi riferisco soprattutto all’analisi informatica, possono generare “falsi positivi” suscettibili di interpretazioni arbitrarie che possono essere evitate solo con una
puntuale preparazione nella materia e un aggiornamento continuo nelle tecniche.

Non dobbiamo infatti dimenticare che i responsabili di certuni “files compromettenti”, potrebbero anche essere dei virus informatici o vari tipi di controlli remoti o addirittura potrebbero essere ricondotti alle azioni di precedenti proprietari.

Da qui, l’imprescindibile necessità di verificare pazientemente tutti questi elementi e suffragarne l’esistenza con prove validate a livello forense.

Non dobbiamo inoltre dimenticare che anche le macchine fotografiche digitali, i registratori audio e, più in generale, tutti quei dispositivi elettronici dotati di una scheda di memoria, possono contenere, in forma digitale, foto, video, files audio ecc.

L’uso di questi dispositivi, per archiviare dati illeciti o frutto di attività criminali, è sempre più frequente poiché destano meno sospetti e sono soggetti a minori controlli rispetto ad un computer.

Tuttavia, l’eventuale cancellazione di questi dati, ciò vale anche per i computer, è quasi sempre più apparente che reale. Infatti è spesso possibile recuperarli più o meno integralmente, riportando alla luce prove che sembravano distrutte per sempre.

In conclusione; molte fattispecie di reato in qualche misura legate al mezzo digitale, richiedono l’intervento del consulente informatico per la redazione di una perizia di parte o per l’effettuazione di indagini difensive a tutela dell’indagato (L. 397/2000). Spesso, queste costituiscono la chiave di volta per vedere riconosciuta la propria innocenza in un procedimento penale, anche in contrapposizione con l’elaborato del Perito del P.M. o le proprie ragioni in quello civile, escludendo dal processo prove non pertinenti o frutto di errori interpretativi.

Note:

1 - *Nel nostro ordinamento giuridico, una persona acquista la qualità di indagato nel momento stesso in cui il suo nominativo viene iscritto nell'apposito registro , a norma dell'art. 335 c.p.p. (registro delle notizie di reato) ossia, è sottoposta ad indagini preliminari, all'esito delle quali il P.M. potrà anche chiedere l'archiviazione degli atti.*

2 - *Nel nostro ordinamento giuridico, assume la qualità di imputato la persona che è sottoposta in tutto e per tutto ad un processo penale, nei cui confronti, a norma dall'art. 60 c.p.p. viene formalizzata la richiesta di rinvio a giudizio (Art. 416 c.p.p.), di giudizio immediato (Art. 453 c.p.p.), di citazione diretta a giudizio (Art. 550 c.p.p.), di giudizio direttissimo (Art. 449 c.p.p.), di applicazione della pena nel corso delle indagini preliminari (Art. 447 comma 1), di decreto penale di condanna (Art. 459 c.p.p.). Nel momento in cui l'imputato assume tale qualifica, il suo nominativo viene iscritto nel casellario dei carichi pendenti.*

3 - *Fino all'entrata in vigore del "Codice della Privacy" (01/01/2004) l'ordinamento italiano non prevedeva alcun obbligo di conservazione dei dati di traffico, da parte dei gestori dei servizi telefonici e telematici, né un limite massimo temporale. La questione era demandata alla discrezionalità dei singoli operatori che la usavano ai soli fini commerciali e di fatturazione.*
Successivamente, il Codice in materia di protezione dei dati personali, all'art. 123, stabilì un divieto generale di conservazione di dati relativi al traffico telefonico e telematico, con due eccezioni; Il trattamento di tali dati fu consentito per esigenze di fatturazione dell'abbonato o di commercializzazione consensuale di servizi, mentre la "conservazione" dei dati fu resa obbligatoria per finalità di accertamento e repressione dei reati (art. 132 del Codice).
La disciplina attuale in materia di conservazione dei dati di traffico delle comunicazioni telefoniche e telematiche, necessaria per il buon esito delle indagini, è un obbligo a cui sono tenuti i fornitori di tali servizi ed è la (sofferta) risultante del bilanciamento di due opposti interessi: quello pubblico alla repressione dei reati e quello individuale alla tutela della riservatezza della sfera personale.
Dopo vari decreti, leggi e provvedimenti del garante, succedutisi negli anni, che hanno causato non poche perplessità in ambiente giuridico dove sono in molti a ritenere che non risolvano, ma anzi complichino alcuni aspetti relativi alla data retention, sono state inserite misure di conservazione dei dati di traffico telematico, oltre alle preesistenti norme relative a quello telefonico (art. 132 Codice in materia di protezione dei dati personali), con esclusione del contenuto delle comunicazioni, limitando la conservazione alle sole informazioni che consentono la tracciabilità degli accessi (art. 6) e stabilito un termine di conservazione, per i dati di traffico telematico, di 12 mesi, prolungabile di altri 12 mesi nei casi di delitti più gravi, mentre per i dati relativi al traffico telefonico i termini sono di 24 mesi (per le chiamate senza risposta il termine è di trenta giorni), prolungabili di altri 24 mesi per i delitti di cui all'articolo 407, comma 2, lett. a, del Codice di Procedura Penale nonché per i delitti in danno di sistemi informatici o telematici.

Sitografia:

http://www.dataretention.altervista.org/

http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1482111

https://edu.clusit.it/download1.php?id=105

http://www.interlex.it/675/datitraffico.htm

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