La Data Retention operata dagli Operatori telefonici per fini di giustizia e repressione dei reati è un'attività fondamentale su cui si basa l'attività investigativa condotta dalla Polizia giudiziaria, a cui spetta poi l'analisi dei tabulati di traffico storico. L'analisi tradizionale di questo tipo di dati può realizzarsi con un approccio metodologico articolato in tre *step*: il primo rappresenta la mera lettura in sequenza cronologica delle celle agganciate, il secondo la georeferenziazione su mappa degli indirizzi dove sono ubicate le celle, infine il terzo prevede la rappresentazione, sempre su mappa geo-referenziata, delle aree di copertura teoriche delle celle. L'esperienza maturata dalla Polizia Scientifica in questa tipologia di accertamenti, oltre ad evidenziare i limiti delle tecniche tradizionali finora esposte, ha consento di ampliare le fasi di rappresentazione dei dati di traffico. Le *Best Practices* che ne sono scaturite hanno condotto alla implementazione di un quarto *step* differenziato in base alla tipologia di quesito.

di Gianpaolo Zambonini e Claudio Fusco

GEO-TIMING NEI TABULATI DI TRAFFICO STORICO (II PARTE)

Gianpaolo ZAMBONINI, Primo Dirigente Ingegnere della Polizia di Stato, è Direttore della IV Divisione del Servizio Polizia Scientifica, nonchè Direttore della Sezione Indagini Elettroniche, presso il Dipartimento di Pubblica Sicurezza del Ministero dell'Interno. Nell'ambito della sua attività lavorativa è divenuto un esperto forense nel settore delle intercettazioni, dell'analisi della voce umana, delle localizzazioni, dell'analisi dei telefoni cellulari e dell'elaborazione delle immagini.

Claudio FUSCO, Ingegnere Elettronico, matura un'esperienza ventennale nel settore delle telecomunicazioni prestando servizio in qualità di network engineer presso uno degli operatori nazionali dominanti, curandone l'ingegnerizzazione delle piattaforme di accesso ed autenticazione alle reti dati fisse e mobili. Attualmente in servizio presso la Sezione Indagini Elettroniche della IV Divisione del Servizio di Polizia Scientifica in qualità di funzionario addetto, è referente per le attività di intercettazione, analisi tabulati e radiolocalizzazione.

4. Le possibilità offerte dalle nuove metodologie

L'esperienza maturata dalla Polizia Scientifica in questa tipologia di accertamenti, oltre ad evidenziare i limiti delle tecniche tradizionali finora esposte, ha consento di ampliare le fasi di analisi rappresentazione dei dati di traffico. Le *Best Practices* che ne sono scaturite hanno condotto alla implementazione di un quarto *step* differenziato in base alla tipologia di quesito.

Nell'ambito degli accertamenti, volti alla ricostruzione della posizione delle utenze sulla base dei dati di traffico, sono così state individuate due macro casistiche di studio in cui ricadono i due esempi trattati; quella dell'analisi statica volta a ricostruire la presenza in una data area da parte di un'utenza in relazione a determinati eventi di traffico e quella in cui l'analisi richiede lo studio dinamico spazio temporale degli eventi, soprattutto nei casi di comparazione tra percorsi.

Riprendendo i casi proposti nel paragrafo precedente, le metodologie in argomento saranno riportate di seguito come un quarto *step*, diversamente realizzato in base alle peculiarità del quesito posto.

IV Step - Misurazioni sul campo e analisi statiche/puntuali

La tipologia dei casi di studio che maggiormente beneficiano di questa tecnica è quella dei quesiti riconducibili al caso 1. Lo *step*, relativamente alle celle di interesse ai fini dell'accertamento, prevede l'esecuzione di rilievi strumentali in campo in abbinamento all'utilizzo di una *suite software* integrata e composta dai seguenti elementi:

DBMS per all'analisi del traffico. Si tratta di *software* specifici che riducono gli effetti della produzione non normalizzata dei tabulati da parte dei gestori, facilitando il caricamento dei tabulati, la ricerca delle sequenze di traffico e l'estrazione di tabelle contenenti gli eventi di rappresentativi, comprensivi della fonte informativa (gestore, tabulato e decreto di acquisizione) nell'ottica della permanente conservazione della catena di custodia del reperto anche in materia di tabulati. I dati di cella sono integrati con i dati forniti dall'operatore circa puntamento, apertura angolare ed altre caratteristiche di cella. Con questo strumento è individuato il gruppo di eventi di traffico significativi e le celle ad esso associate con le relative informazioni di puntamento e angolo di irraggiamento

Software di post elaborazione dei dati di misura. Gli strumenti di misura adottati per la rilevazione in campo dei segnali emessi dalle celle sono corredati di un *software* di gestione per l'estrazione dei campioni rilevati, comprensivi della georeferenziazione delle misure condotte.

Soluzioni GIS di allestimento delle mappe. Si tratta di *software* in grado di rappresentare geograficamente le informazioni di interesse, dati di traffico, simulazioni prodotte dai gestori per le mappe di copertura delle celle e misure strumentali. Il

risultato è un *layer* cartografico potenziato a livello informativo da elementi specifici di interesse. Il sistema consente inoltre l'acquisizione di tabelle di traffico (seppure relativamente contenute in termini di numero di eventi) e l'associazione ai singoli eventi delle entità grafiche rappresentative delle celle, consentendone la visualizzazione in sequenza dei coni teorici associati alle singole BTS agganciate.
La particolare soluzione GIS adottata consente di individuare l'intersezione tra elementi grafici associati ad eventi di traffico contrassegnati come di interesse.

Nelle figure seguenti viene riportato un caso di applicazione pratica. Il primo riquadro riporta le tre celle con i tre coni teorici. I successivi tre riquadri riportano la sovrapposizione tra cella teorica e cella reale ricostruita con misure strumentali; la diversa intensità cromatica è rappresentativa della maggiore intensità e qualità del segnale rilevabile nell'area considerata. Gli ultimi due riquadri riportano rispettivamente la sovrapposizione delle aree reali di copertura delle celle e l'estrazione della loro area di intersezione.

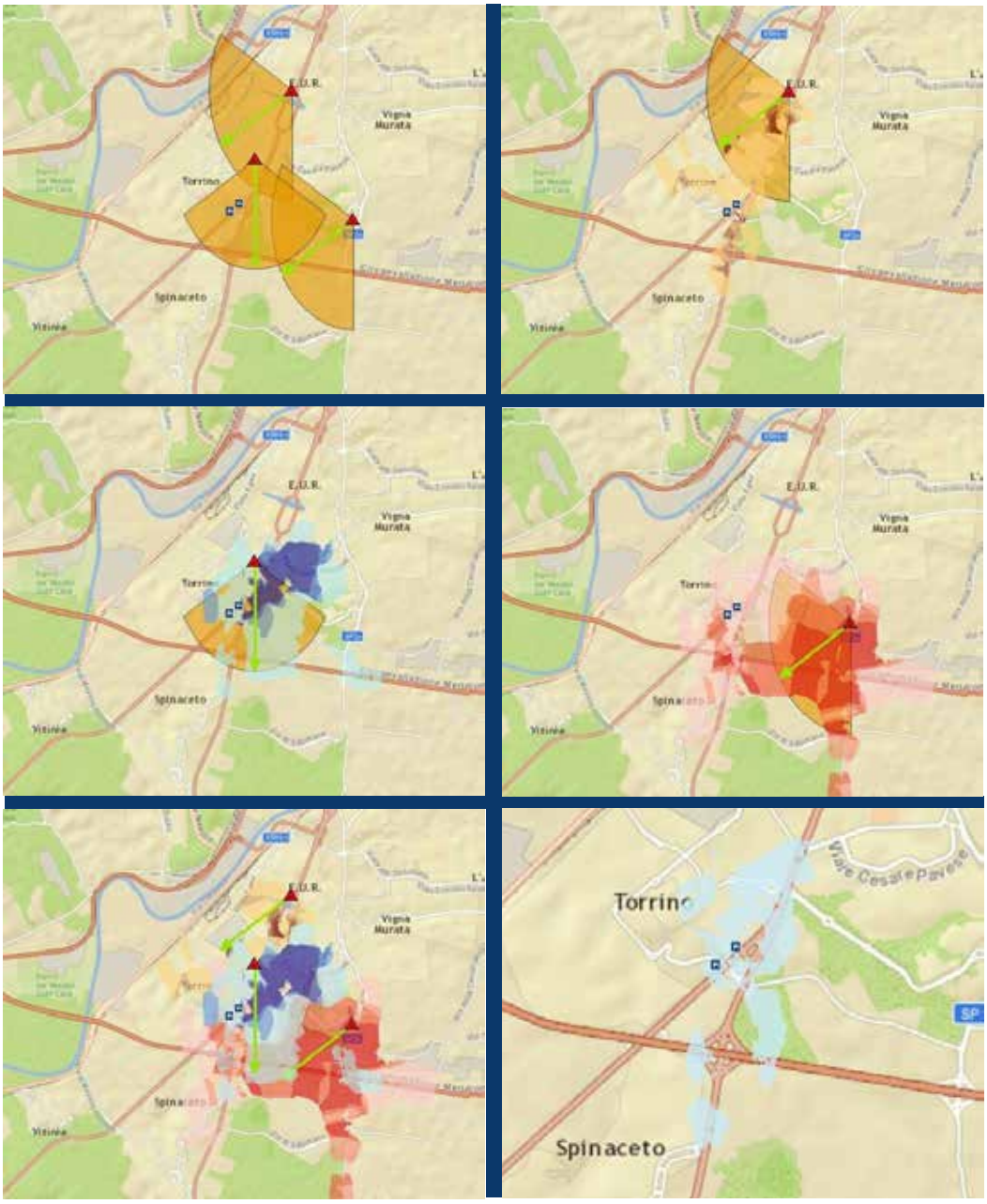

***Figura 1**: Esempio di applicazione pratica.*
Il primo riquadro riporta le tre celle con i tre coni teorici. I successivi tre riquadri riportano la sovrapposizione tra la cella teorica e la cella reale ricostruita con misure strumentali.
Gli ultimi due riquadri riportano rispettivamente la sovrapposizione delle aree reali di copertura delle celle e l'estrazione della loro area di intersezione.

L'analisi del primo caso di studio effettuata con l'utilizzo delle misure reali, ricavando l'intersezione tra le celle, conduce ad un risultato di facile interpretazione, con una maggiore rigorosità scientifica e sostenibilità dibattimentale[1], rispetto alle analisi effettuate soltanto con i primi tre *step* del capitolo precedente.

Nel caso di analisi dinamiche, volta alla comparazione di percorsi estesi nel tempo e nello spazio, questa tecnica, seppure rigorosa, si dimostra difficilmente applicabile. La ricostruzione delle celle per via strumentale è un'attività impegnativa sia in termini di tempo che tecnologici in ragione della difficile raggiungibilità di taluni siti di interesse con percorsi di misura a reticolo sufficientemente regolare e a maglia stretta.

IV Step - *Engine 3D* per la rappresentazione ed elaborazione dei dati GIS e comparazione di percorsi

Si tratta dell'interfacciamento dei precedenti applicativi (DBMS, Soluzioni GIS castomizzate) con un software in grado di riconoscere gli eventi di traffico associati a ciascuna utenza e le relative informazioni di tracciabilità unendoli con la rappresentazione geo-referenziata su mappa delle radio coperture delle celle impegnate. Tutte queste informazioni sono elaborate da un motore di calcolo che ne rappresenta in tempo reale l'evoluzione su cartografia (rappresentazione 3D) degli spostamenti di ciascuna utenza considerata, riproducendo i singoli eventi, eseguendo con delle animazioni le interpolazioni delle posizioni dei terminali ed abilitando dinamicamente la rappresentazione delle aree di copertura delle celle. Il motore di calcolo esegue inoltre l'analisi storica degli eventi, dei percorsi e dei grafi costruiti dalla congiunzione delle celle impegnate nel tempo ricavando interessanti strumenti di analisi come meglio specificato nel seguito.

Con la **rappresentazione 3D,** questa soluzione consente di introdurre la variabile tempo nella rappresentazione statica e cumulativa degli eventi di traffico pur conservando tutte le informazioni di ciascuno di essi. Eventi di traffico che avvengono sullo stesso sito sono ora rappresentati sulla verticale alla rappresentazione geografica dell'indirizzo e sono collocati ad un'altezza proporzionale al tempo che li separa.

Nella figura seguente se ne riporta un esempio. Con una sola immagine si riassume un'intera giornata di traffico su scala temporale graduata e conservando l'identità e le informazioni di ciascun evento di traffico. L'utilizzo statico di un terminale assume ora una diversa leggibilità. Percorsi che si intersecano in modo confuso in rappresentazioni 2D possono ora essere posti in relazione con maggiore immediatezza ad ipotesi di incontro, in quanto la rappresentazione riporta ora anche l'elemento temporale dell'attraversamento delle stesse aree da parte di utenze diverse.

In pochi istanti l'operatore rappresenta su cartografia eventi di traffico relativi ad utenze differenti, con operatori distinti e dispone della rappresentazione dinamica degli impegni di cella e delle rispettive eventuali intersezioni di aree di copertura.

La rappresentazione matematica in un grafo degli eventi di traffico operata dallo strumento consente, inoltre, di automatizzare funzioni di ricerca di notevole valore analitico, velocizzando l'attività dell'operatore, concentrandone l'attenzione su contesti di traffico ordinati in base a criteri selettivi configurabili ed amplificando quindi sensibilmente le potenzialità investigative sia in termini di accuratezza che di volumi di traffico analizzabili nell'unità di tempo; tutti elementi che in un regime di risorse limitate assumono una rilevanza sempre più strategica.

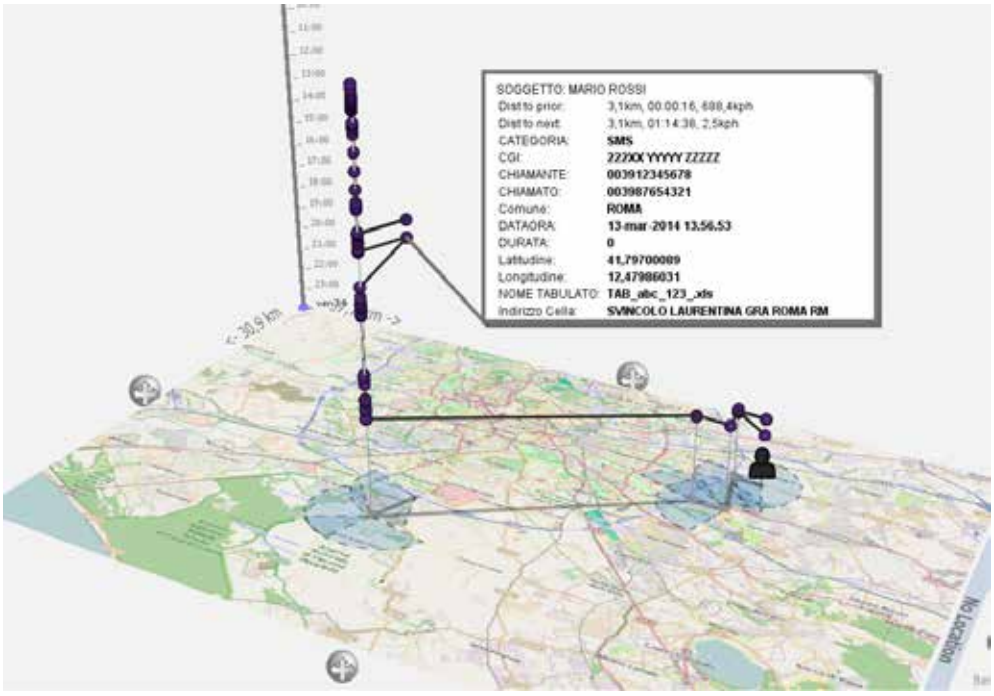

***Figura 2**: Esempio di rappresentazione 3D degli eventi di traffico telefonico.*

1 Ovviamente supportate da adeguati accertamenti presso i gestori circa la confrontabilità della copertura radio rilevabile in campo all'atto delle misure rispetto all'epoca dei fatti a cui l'accertamento è riferito; l'utilizzabilità delle misure è subordinata all'assenza di modifiche intervenute in campo circa la dislocazione e la configurazione delle celle.

Sono state selezionate soluzioni *software* che offrono diverse funzionalità di ricerca e di cui se ne riportano solo alcuni esempi:

- *Rilevamento di incontri*: il *software* elabora il traffico geo-referenziato di tutte le utenze segnalate evidenziando i contesti riconducibili ad incontri secondo criteri di distanza temporale tra flussi, distanza delle celle e numero minimo di utenti distinti coinvolti. Si veda ad esempio la figura 7 in cui si ricercano eventi di almeno due utenze distanti al più 10 minuti ed entro 3 km di distanza.
- *Ricerca di cluster:* evidenza di gruppi di eventi selezionati secondo soglie minime di numerosità e loro accadimento entro certi margini di tempo e spazio.
- *Ricerca di siti di interesse investigativo*: il *software* evidenzia luoghi frequentati almeno "n" volte , da almeno "n" soggetti con eventi di traffico distanti nel tempo e nello spazio secondo margini configurabili. Si pensi ad esempio alla ricerca automatica del covo, dei luoghi di spaccio, ecc.
- *Analisi della mobilità*: il *software* evidenzia i gruppi di eventi dalla cui interpolazione nel tempo e nello spazio emerge una velocità di spostamento dei soggetti compresa entro margini specifici

Le stesse analisi condotte su interi mesi di traffico e con un'automatizzazione meno spinta impegnerebbero un notevole *effort* di risorse umane. Il traffico telefonico assume ora una dimensione intuitiva ed una rappresentazione apprezzabile anche dai non addetti ai lavori. La visualizzazione dinamica "*on demand*" delle aree di copertura, degli orientamenti delle celle e dei reciprochi spostamenti in tempo reale di utenze differenti consente, anche in fase di dibattimento, di affiancare alla potenza della rappresentazione la tracciabilità del dato, sempre associato ad ogni elemento grafico. In affiancamento ai *report* tradizionali in formato tabellare, la soluzione offre quindi la possibilità di realizzare in maniera integrata animazioni ben più intuitive e rappresentative di sequenze di dati e immagini distinte.

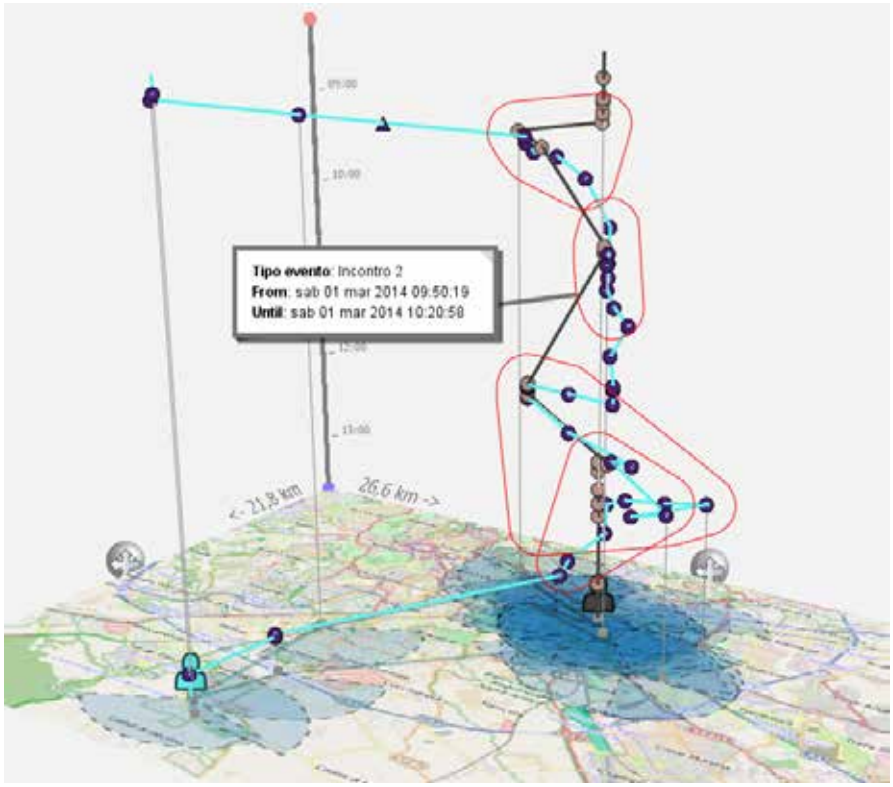

***Figura 3**: Risultati dell'utilizzo di un filtro per il rilevamento di incontri tra soggetti.*

4. Conclusioni

I due *step* descritti come 4ª fase sono due tipologie di accertamento, quella statica e puntuale riferita al primo caso studio e quella estesa e dinamica riferita al secondo, che rappresentano il risultato del continuo aggiornamento delle metodologie di lavoro perseguito dal Servizio di Polizia Scientifica. L'obiettivo è quello di rendere gli accertamenti sul traffico telefonico sempre più oggettivi, restituendo all'esperto forense il suo ruolo originario, ovvero quello di fornire alla magistratura giudicante gli elementi necessari per esprimere il proprio giudizio.

GLOSSARIO

BTS *Base Transceiver Station*. È l'apparatistica elettronica connessa ai tralicci sui cui sono installate le antenne delle celle di telefonia mobile.

CGI *Cell Gobal Identity*. È il codice univoco di identificazione delle celle, composto da 15 cifre rappresentanti la nazione, il gestore, l'aggregato geografico di celle e il progressivo locale della cella specifica.

DBMS *Data Base Management System*. È la categoria di applicazioni che gestisce le basi di dati. In questa classe rientrano strumenti come Microsoft Access Oracle, ecc.

GIS *Geographic Information System*. Applicazioni che uniscono la gestione delle basi di dati ad entità grafiche geograficamente referenziate. In questo modo si ottengono rappresentazioni la cui utilità è apprezzabile ogni qual volta gli elementi del modello, nel loro apporto informativo, hanno una componente territoriale significativa.

RAT *Radio Access Technology*. Questa sigla, valorizzabile con 2G/GSM o 3G/UMTS piuttosto che 4G/LTE è indicativa della generazione tecnologica con cui viene sviluppata la parte radio della piattaforma di comunicazione cellulare

SDR *Software Defined Radio*. È una tecnologia di BTS in cui la configurazione radio degli apparati è configurabile integralmente via software. In questo modo una stessa realizzazione impiantistica può essere agevolmente riprogrammata a coprire la stessa area in generazioni radio diverse (2G/3G/4G) passando dall'una all'altra senza la sostituzione di apparati. ©