filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

L'Open Source Intelligence e le sue declinazioni nell'investigazione privata

05 Giugno 2019
Fabio Mongile

Abstract:
Quando pensiamo all'investigatore privato, l'immaginario collettivo si rivolge subito a figure letterarie e cinematografiche come Sherlock Holmes, che con il solo "*fiuto investigativo*" risolve i casi più complessi, apparentemente, senza un vero e proprio metodo scientifico, ma affidandosi unicamente all'intuizione. Tuttavia l'investigazione è una disciplina con solide basi teoriche e scientifiche che spaziano in numerosi campi accademici, dalla chimica, alla fisica alla biologia e da diversi anni, anche all'informatica. Il presente contributo vuole approfondire una branca dell'intelligence sempre più in uso tra i professionisti del settore, l'**OSINT (Open Source INTelligence**).

Indice:

1. Introduzione;
2. Le Fonti;
3. Il ciclo dell'OSINT;
4. Conclusioni.

1. Introduzione

La figura dell'investigatore privato ha assunto una sempre maggiore professionalità ed il mercato si è fatto sempre più selettivo nella scelta degli operatori del settore, la cui esperienza professionale, è sempre più spesso accompagnata da un titolo di studio.
Il cinema ha da sempre suggerito il cliché dell'ex poliziotto che raccoglie le sue informazioni avvalendosi delle sue vecchia amicizie in polizia, un po' come Dylan Dog e l'Ispettore Bloch. Questa è una prassi oggi sempre più desueta.
Le informazioni raccolte, stante il grado di confidenzialità, non sarebbero riproducibili in nessuna sede ed esporrebbero il nostro confidente a provvedimenti sanzionatori gravi.
È dunque pacifica l'inefficacia sul piano processuale di questa vetusta linea investigativa che ha lasciato il posto all'**OSINT (Open Source INTelligence)**, l'acquisizione legale di informazioni disponibili ad un bacino di utenza illimitato e reperibili tramite le "*fonti aperte*".

2. Le fonti

La letteratura (Vds la ricerca CeMISS C8/Z "Le fonti informative e L'Open Source Intelligence" https://bit.ly/2VVvOb0) individua tre fonti:

1. **Internet;**
2. **La Letteratura Grigia;**

3. **Gli Esperti.**

Personalmente mi sento di elencare una quarta fonte, **i Pubblici Registri**. Non sarebbe altresì errato annoverarli sotto la voce "Internet", in quanto ormai sono tutti accessibili *on line* tramite piattaforme dedicate.

Dal 1994 **Internet**, prima appannaggio della sola intelligence militare, è oggi disponibile al grande pubblico costituendo lo strumento d'informazione più diffuso al mondo. Internet è come un *Paese delle Meraviglie* 2.0, dove sì *Alice* vive le sue avventure in un mondo incantato nel quale però si annidano anche antri oscuri e pericolosi come il ***deep web***, dove tutto è permesso, dall'acquisto di materiale pedopornografico, armi, droga, prostitute, commissione di atti intimidatori, omicidi, finanche attentati terroristici.

> **Una delle iconografie più utilizzate per rappresentare internet nella sue totalità è un iceberg, dove la punta rappresenta il "*World Wide Web*", ovvero Internet così come lo conosciamo tutti, mentre la parte sommersa è il *deep web*. Il *deep web*, con i dovuti accorgimenti, costituisce un valido strumento per un investigatore che segue delle "indagini sotto copertura". Talvolta però il confine tra legale e illegale, nel *deep web*, è molto labile e spesso la norma fatica a stare al passo.**

La **letteratura grigia**, dall'inglese, "*Grey Litterature*", è il materiale proveniente da canali di distribuzione specializzati ed esclusivi.

Si tratta di materiale come: studi accademici; tesi di laurea, relazioni di comitati, atti congressuali, documenti societari, riviste specializzate, ricerche di mercato, procedure standard, relazioni tecniche, working paper, resoconti di viaggio, ***newsletter*** etc.

Al pari delle *newsletter* oggi ci sono anche i canali Telegram o i gruppi privati di Facebook che per l'esclusività che contraddistingue gli utenti è più vicino alla definizione di letteratura grigia che non a quella di Internet.

Un'attività molto cara agli ingegneri sociali, simile nei contenuti alla letteratura grigia, è il ***dumpster diving*** (letteralmente *tuffo nella spazzatura*), che consiste nel frugare nei rifiuti alla ricerca di informazioni gettate incautamente. La raccolta differenziata porta a porta ha agevolato notevolmente questa pratica. È infatti facile andare a colpo sicuro, il giorno del ritiro della carta, alla ricerca di fatture, ricette mediche, corrispondenza etc. consapevoli che ciò che per qualcuno è un rifiuto di cui sbarazzarsi, per qualche malintenzionato potrebbe costituire prezioso materiale informativo per costruire una truffa.

Il *dumpster diving* non ha nulla a che vedere né con la letteratura grigia né con l'OSINT in generale, e peraltro è illegale.

Gli esperti sono una risorsa fondamentale per l'investigatore che, non essendo un tuttologo, avrà bisogno di interpretare le informazioni raccolte, la cui complessità potrebbe esulare dalle sue competenze.

Immaginiamo di seguire un'indagine su un incendio e acquisire la relazione tecnica del *fire investigator*. Il documento è disponibile e contiene tutte le risposte che cerchiamo, ma senza delle solide basi di chimica e fisica sarebbe come leggere un saggio in ostrogoto.

3. Il ciclo dell'OSINT

L'OSINT è un processo suddiviso in 4 fasi, denominato "***le 4 D***". **D** non sta per *Detective*, bensì per:

a. Discovery *(Ricerca)****;***

b. Discrimination *(Selezione)****;***

c. Distillation *(Analisi)****;***

d. Dissemination *(Diffusione)****.***

La **ricerca:** questa fase, se eseguita in maniera grossolana e incompleta rischia di alterare irrimediabilmente le fasi successive del lavoro. Immaginiamo di svolgere un'attività di **SOCMINT** (**SOC** ial **M**edia **INT**elligence), branca dell'OSINT.

Individuato il profilo facebook del nostro presunto target sarà facile individuare anche tutti gli altri profili social, grazie all'immagine del profilo e ad altri riscontri.

Saremo così in grado di ricostruire gli spostamenti dell'utente, le sue relazioni personali, i suoi interessi e a buon bisogno anche gli scambi intrattenuti con altri utenti. Immaginiamo poi di scoprire che l'utente individuato sia un omonimo. Il risultato sarebbe giorni di lavoro buttati se non addirittura conclusioni inconsistenti e fallaci.

La **selezione:** nell'era digitale, in cui le informazioni a disposizione sono milioni e milioni, paradossalmente è proprio la loro sovrabbondanza a renderne difficoltosa l'acquisizione. Difatti le informazioni sarebbero facilmente attingibili da chiunque, ma quello che il committente si attende dall'investigatore è un rapporto tanto esaustivo quanto sintetico.

Per questa ragione, la selezione delle informazioni dovrà ispirarsi a tre criteri cardine: **attendibilità**, **attinenza** e **rilevanza**. La capacità di un bravo investigatore sta appunto nello scegliere e valorizzare le informazioni d'interesse alle indagini escludendo le altre.

L'**Analisi:** questa terza fase è il cuore del ciclo dell'OSINT.

La dottrina oscilla tra due principali orientamenti: da una parte c'è chi pone al centro la macchina, il "*mega cervellone digitale*" in grado di incrociare tra loro tutte le informazioni raccolte; dall'altra c'è chi mette al centro la "*mente umana*", la quale si avvale dell'elaboratore esclusivamente come strumento di ricerca ma analizzando personalmente le informazioni raccolte, con attenzione e spirito critico.

Personalmente propendo per il secondo orientamento. Sono infatti dell'avviso che un'intelligenza artificiale, per quanto elaborata e capace di scandagliare moli infinite di dati, non è in grado di cogliere le mille eccezioni e specificità del caso particolare. Isac Asimov, meglio di chiunque ha ventilato i potenziali pericoli di delegare in toto ad un'Intelligenza Artificiale ogni scelta in capo all'uomo.

La **Diffusione:** è l'ultima fase di questo complesso processo di raccolta, selezione e analisi delle informazioni.

Le peculiarità di un rapporto tecnico investigativo sono: la **celerità**, la **comprensibilità** e la **fruibilità**.

A. Un rapporto deve esser celere e deve giungere al committente nei tempi prestabiliti perché possa essere utilizzato per gli scopi per cui l'indagine è stata commissionata.

Il lavoro migliore del mondo, se giunto tardivamente, non è di alcuna utilità. Un aggiornamento costante del cliente permetterebbe di ovviare ad eventuali ritardi che non dipendono dall'attività dell'investigatore e permetterebbe al cliente di rimodulare l'oggetto della richiesta sulla base di quanto emerso.

B. Il rapporto deve essere comprensibile. È cura di chi scrive resistere alla tentazione di cadere in tecnicismi e terminologie tipiche dei soli addetti ai lavori. Il linguaggio utilizzato deve essere chiaro, sintetico e nel contempo esaustivo.

L'uso di un linguaggio estremamente forbito ed altisonante nasconde il rischio di compromettere l'assimilazione e la comprensione dei contenuti.

C. La fruibilità è la capacità del prodotto di rispondere alle esigenze del cliente. Le informazioni acquisite in maniera confidenziale, in primis *"brucerebbero"* la nostra fonte e non sarebbero producibili in alcuna sede, inficiando lo scopo stesso dell'incarico.

È necessario aver sempre cura di richiamare le fonti di modo che queste siano verificabili in qualunque momento.

La fruibilità non è insita solo nei contenuti del rapporto investigativo, ma anche nel format dello stesso. È importante concordare con il cliente le modalità di condivisione ed il supporto sul quale trasmetterlo (cartaceo/digitale; CD-ROM/pen drive; posta/mail/dropbox, etc.).

La ciclicità è una peculiarità del processo sopra descritto, in quanto il committente, una volta ricevuto il rapporto, deciderà se proseguire o meno le indagini e concorderà con l'investigatore la futura strategia investigativa.

4. Conclusioni

Per queste e molte altre ragioni la figura dell'investigatore con l'impermeabile ed il cappello, che entra in un bar e chiede "*un whiskey e un'informazione*" è una figura tanto romantica quanto *retrò*.

Personalmente ritengo che *"l'investigazione di strada"* non tramonterà mai perché costituisce l'ABC dell'investigazione stessa e in molti casi è necessario un accesso diretto sul territorio.

Tuttavia buona parte della vita relazionale e professionale delle persone passa ormai attraverso il web, ed il progresso tecnologico e la digitalizzazione documentale ci permettono oggi di riservare agli spostamenti fisici il tempo strettamente necessario per espletare quella porzione residuale dell'indagine, laddove le *Open Source* ancora non arrivano.

TAG: *OSINT, investigazione privata, intelligence*
