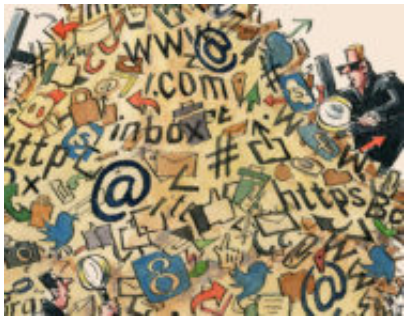
Peculiarità delle perquisizioni dirette alla ricerca di evidenze informatiche: l’ago nel pagliaio

Author : Pier Luca Toselli

Date : 1 Luglio 2019



Non posso negare di avere già trattato l’argomento: tuttavia ritengo il “tema” (come si dice dalle mie parti...) talmente “strategico” per le sorti del lavoro rimesso a coloro che quotidianamente - nella veste di consulenti, ausiliari di P.G. o polizia giudiziaria - si ritrovano “esecutori” di una perquisizione/ispezione informatica delegata dall’Autorità Giudiziaria, da volerlo nuovamente affrontare. Pertanto, scusandomi per le eventuali ripetizioni di alcuni concetti “fondamentali”, invito comunque a un’attenta lettura che, al di là dell’ovvia considerazione "sono cose che si sanno!”, aiuterà ciascuno di quegli operatori nel duro lavoro quotidiano che ogni giorno risulta sempre più complicato.

Ricordo ancora mia nonna che, quando dovevo cercare qualcosa a suo dire impossibile, mi diceva: ***“è come cercare un ago nel pagliaio”***. La metafora spesso abusata rende comunque l’idea e quando mi veniva citata, al di là dell’effetto “demoralizzante” (era meglio lasciar perdere!), era riconducibile a un'“era” (così la definiscono le mie figlie) in cui la media dello *storage* informatico arrivava a… lasciamo perdere; per gli archeologi dell’informatica, avevo un Commodore 64 con un’unità Commodore 1581 per floppy da 3,5… altri tempi.

Ma torniamo a noi, all’oggetto di questo mio articolo.

Volevo introdurre il problema che, da capacità di *storage* che oggi appaiono “ridicole”, siamo passati in pochi decenni a dischi con capacità di diversi TB che oggi ogni utente cd. “medio” può vantare di custodire nella propria abitazione.

Sono sicuro che, se facessi un sondaggio tra i miei lettori, più della metà confermerebbe di avere a casa un HD da qualche TB se non un bel NAS di capacità anche maggiori: del resto i filmini dei compleanni, delle comunioni e cresime, uniti a quelli di matrimoni e viaggi di nozze (soprattutto se in 4K) occupano un certo spazio, e perderli equivale a subire il “processo di Norimberga” con conseguenti condanne degne delle piazze di Parigi nel luglio 1789.

Ecco che allora siamo tutti concordi nel ritenere che oggi lo *storage* medio/personale (tralascio,

per ovvietà, quello professionale e aziendale) sia notevolmente incrementato, a cagione di un ormai inarrestabile progresso tecnologico-informatico che fa sì che oggi la nostra vita sia di fatto pervasa non solo di strumenti tecnologici che ci aiutano in diverse occupazioni ma anche di **un impressionante mole di "dati"** (spesso ridondanti) che siamo chiamati a conservare e custodire.

Capita allora sempre più spesso che, nel corso di una perquisizione e/o ispezione informatica presso un'abitazione - non certo di qualche "smanettone" o "guru" informatico ma di un semplice e ordinario *"user"* - ci si imbatta in capacità di *storage* di alcuni TB. Del resto basti pensare che un desktop medio ormai è accompagnato da dischi di uno o più terabyte, per non parlare degli smartphone che ormai accompagnano non gli adolescenti ma i fanciulli con capacità di 128/256 GB… capacità che all'epoca del mio Commodore 64 erano pura "fantascienza".

Volutamente poi, in quanto ci arriverò poco a poco nel corso dei miei "viaggi" nell'informatica "operativa", tralascio al momento "l'universo" (mai definizione fu più esatta) CLOUD, per il quale non basterà certo qualche articolo, ma serviranno un bel po' di lavori e considerazioni tra tutti i soggetti: esperti, giuristi, polizia giudiziaria e tutti gli altri a vario titolo anche solo "incidentalmente" coinvolti. Qui mi permetto solo di stuzzicare gli appetiti richiedendovi una breve ma doverosa riflessione su quali siano i confini (geografici) del CLOUD e come questi debbano essere considerati rispetto a quei confini geografici che invece regolano la "giurisdizione" di ciascun Paese (su dai che avete capito, ma ci torneremo…).

Torniamo al nostro utente medio, ormai corredato di diversi TB e, tralasciando il CLOUD, caliamoci nella semplicità (è un eufemismo) di una perquisizione informatica che richieda di affrontare solo le problematiche legate allo *storage* fisico presente, ovvero a quei dispositivi dotati di spazio di *storage* che vengono rinvenuti nel corso dell'incombente. Pur apparendo più un caso di "scuola" ormai appartenente a un passato prossimo, vorrei evidenziare come anche tale "caso" già complichi non poco la vita del ***Digital Forensics Expert***.

Tra gli addetti ai lavori si sente spesso rispondere che la soluzione al nostro "caso" sta nella copia *bit to bit* di tutti i dispositivi digitali rinvenuti, riservando poi successivamente un esame analitico dei dati. Per quanto la soluzione appaia la più conveniente, efficace e sulla quale concordo, come ho già avuto modo di far notare[1], non sempre risulta realizzabile e scevra di **problematiche,** in quanto:

a) nel nostro ordinamento giuridico esiste un complesso di norme e tutele giurisdizionali che fanno sì che il cd. "superamento del sequestro" incomba sull'attività della polizia giudiziaria e possa costituire oggetto di "censura" da parte degli organi giurisdizionali deputati al cd. "riesame". Pertanto, quand'anche fosse realizzabile la copia *bit to bit* di tutti i dispositivi rinvenuti (vedi anche il punto successivo), ci si confronterebbe poi con problematiche di natura più squisitamente "giuridica" che potrebbero "cassare" l'acquisizione effettuata. In merito ricordo che le eventuali tesi del tipo "è solo una copia dei dati!" non trovano sempre conforto... nel riportare uno stralcio della sentenza in nota[2], esorto il lettore a una lettura completa della stessa, che ritengo alquanto utile ed interessante per ogni operatore : ""*le Sezioni Unite hanno concluso che* ***la legittimità dell'intrusione nella sfera patrimoniale privata e la legalità***

dell'acquisizione *espletabile nel procedimento incidentale* ***non possano ritenersi soddisfatte mediante la mera reintegrazione del rapporto fisico, materiale****, fra il titolare e l'oggetto dell'ablazione (id est della restituzione del "contenitore" con l'intero "contenuto"),* ***ma presuppongano necessariamente la protezione del rapporto di disponibilità esclusiva dell'informazione acquisita****, facente capo all'avente diritto. Sintetizzando quanto affermato dalle Sezioni Unite Andreucci, i dati informatici acquisiti mediante l'integrale riproduzione di quelli presenti sulla memoria del computer rimangono sotto sequestro anche se il supporto fisico di memorizzazione sia restituito, in quanto permane, sul piano del diritto sostanziale, una perdita autonomamente valutabile per il titolare del dato, che perde la disponibilità esclusiva del "patrimonio informativo" che rientra nella sfera personale dell'individuo. Da tale assunto discende, quale naturale corollario, che non solo la persistenza dell'interesse a ricorrere, ma anche l'osservanza o meno dei principi di pertinenza e di proporzionalità del vincolo reale, debba essere valutata* ***con riferimento non al "contenitore" (computer e supporti informatici) in ipotesi restituito, bensì al "contenuto" (dati informatici in essi memorizzati)****, costituente "patrimonio informativo" ancora assoggettato ad ablazione".*

b) È ancora "credibile", "realizzabile", "possibile" ritenere (nel caso delineato dell'utente medio corredato di alcuni TB e decine di dispositivi digitali) di aver fatto una copia *bit to bit* di **"tutti"** i dispositivi adibiti, anche indirettamente, a *storage* di dati? Oggi esistono ormai dispositivi "intelligenti" che sono tali in quanto dotati di tecnologie che, se da un lato permettono a questi di essere "collegati alla rete", contestualmente permettono anche, quasi sempre, lo *storage* di quantità variabili di dati. Ho di recente acquistato una smart TV con 4GB di storage (ridicolo no?) ma in quei 4GB potrei facilmente occultare (senza essere un Guru dell'informatica) molti dati. Orbene in risposta al principio *bit to bit* ci ritroveremo a fare i *dump* del frigo, della lavastoviglie, dello *smart toy*, dello *smart watch*, della mia smart-TV e anche dell'autovettura che uso per spostarmi quotidianamente da casa al lavoro (*forensic Veichle*!)? In sintesi, l'osservazione ci porta a considerare che oggi e sempre più in futuro (vi ricordo il Cloud) sarà sempre più improbabile per l'operatore essere sicuro o meglio tranquillo di aver provveduto alla copia bit to bit di **tutti** i potenziali dispositivi digitali coinvolti. Oggi ancor più di ieri è richiesto all'operatore di "pronosticare" dove possano trovarsi i dati di interesse per il prosieguo delle indagini, atteso che soluzioni del tipo "prendo tutto e poi lo guardo" sono ormai retaggio del passato e tendono a essere una "chimera" sia sul piano pratico che su quello giuridico (si veda il punto a) che precede).

c) Non vanno poi sottovalutati, in queste ovvie considerazioni, tutti i casi (che ho citato più volte ma che si palesano sempre con maggior frequenza) di "sistemi" che di fatto non possono essere per vari motivi sottoposti a copia *bit to bit*, sia per difficoltà legate alla loro operatività (sistemi di controllo militari, sanitari, di sicurezza etc., ovvero impossibilità di interrompere la loro operatività anche solo momentaneamente) sia per difficoltà legate all'impossibilità, anche a sistema in funzione, di procedere a copia *bit to bit* per problematiche legate alla loro dimensione (si pensi ai sistemi di alcune grandi aziende che si avvalgono ormai di *storage* misurati in Petabyte o Exabyte).

Quindi, per sintetizzare, sarebbe sempre bello fare copie *bit to bit* di tutto lo *storage* rinvenuto ma le difficoltà sono tante e spesso non superabili, soprattutto in sede di perquisizione; l'operatore, poi, ha quella "spada di Damocle" sulla testa costituita dall'affermazione: *"se da un*

lato mi si contesta di aver copiato tutto indiscriminatamente, dall'altro potrei essere censurato proprio per non aver copiato tutto ed essermi lasciato sfuggire qualcosa".

Sulla **seconda** censura, venendo da trent'anni di attività, mi sento di poter affermare che anche nelle perquisizioni informatiche pretendere di aver perquisito "tutto" rimane una "chimera": la storia giudiziaria del nostro Paese è piena di casi in cui quello che si cercava non è stato trovato, perché ben nascosto o non era dove lo si cercava. Del resto, volendo fare un parallelo, perquisire un'intera casa non è perquisire una stanza e una stanza che ci appare con quattro pareti potrebbe celarne altre; o ancora, basta farsi un giro su YouTube per comprendere come i sistemi di "occultamento" superino la normale fantasia e come sia veramente complicato e difficile per l'operatore scoprirli[3] (esempio dei colleghi di Lisbona!). Ma torniamo a noi: il concetto evidente è che "perquisire" tutto spesso è impossibile e, anche quando ci si riesce, molto può sfuggire anche all'occhio più attento. Ecco forse perché le censure relative a quella parte: "*dall'altro potrei essere censurato proprio per non aver copiato tutto ed essermi lasciato sfuggire qualcosa",* siano alquanto rare e per lo più legate a casi di "omissione" veri e propri.

Diverse le valutazioni per la **prima** parte: "*se da un lato mi si contesta di aver "copiato" tutto indiscriminatamente".* Qui occorre prendere in considerazione anche la legge 48/2008 la quale, da molti, fu considerata la norma che "finalmente" avrebbe fatto cessare i sequestri indiscriminati di PC e di tutto ciò che vi era attaccato (stampanti comprese). Di fatto la norma che ha introdotto la possibilità di procedere a "perquisizione" e "ispezione" di un sistema prima di procedere alla copia *bit to bit* dello stesso (qualora contenga elementi di interesse) o al sequestro del dispositivo (qualora sia impossibile procedere sul posto alla copia o all'estrazione dei dati utili), non sembra "aiutare" oltremodo nella soluzione e superamento delle problematiche prima evidenziate che permangono ed incombono (mai termine fu più esatto) sull'operatore.

In questo quadro, tutt'altro che roseo e ricordando ancora le parole della nonna, mi accingo allora a esporre una serie finale e conclusiva di **considerazioni**, sperando che queste possano costituire un sano e costruttivo dibattito tra tutti gli operatori coinvolti.

Certo che ognuno ha le proprie tecniche e stratagemmi per trovare l'ago (il nonno mi consigliava: con la calamita!); orbene, volendo proprio cercarlo, partirei (ormai è un mio cavallo di battaglia!) dalla cd. **"analisi di contesto"**, che qui potremo paragonare al cercare di capire dove sia caduto l'ago. Senza un'adeguata e corretta analisi di contesto si rischia di cadere nel paradosso del "tutto tutto/niente niente", ovvero nel rischio (per quel che ci riguarda più da vicino) di prendere migliaia di dati inutili da dispositivi inutili tralasciando i pochi dati di interesse sul dispositivo "target" utilizzato per la perpetrazione del reato. L'analisi di contesto, al pari di un *"profiling"* qui inteso nel suo doppio significato di:

- ambito psicologico: *metodo di valutazione qualitativa della personalità, delle attitudini comportamentali e delle specifiche abilità di un individuo* **e anche** *la descrizione del profilo psicologico e comportamentale dell'autore di un crimine;*
- ambito informatico: tracciatura;

non potrà che aiutare l'operatore nell'individuare i potenziali "target" tra i molteplici rinvenuti e

ancora lo aiuterà a selezionare tra i molti, sondando le specifiche caratteristiche del reato e individuo responsabile, quali siano le abitudini di quest'ultimo ovvero se possa più facilmente rinvenirsi la traccia del reato in procedimento o il corpo del reato.

Quanto all'Intelligenza Artificiale **(IA)**, se potrà venirci in soccorso in un ormai prossimo futuro non è dato sapere: tuttavia nulla mi impedisce di augurarmi che, di pari passo a evoluti e più veloci sistemi di *triage*, si possa giungere con l'aiuto della IA a risolvere parte delle problematiche evidenziate.

Tuttavia, sul tema mi sia permesso di esprimere alcune perplessità in ordine all'affidare solo all' IA il difficile compito dell'analisi di contesto e *profiling:* spero che l'intelligenza umana sia ancora lungi dall'essere superata e che l'**investigatore 4.0** sia colui che si avvale, certo, di strumenti e potenzialità fino a qualche anno fa impensabili ma che ancora ci mette il suo fiuto e l'esperienza della "vecchia scuola".

Mi ricollego a un esempio pratico: ho assistito nel tempo a decine di workshop *et similia* di presentazione di prodotti innovativi, strabilianti e capaci di fare con un click quello che fino a qualche anno fa realizzavo in lunghe giornate di lavoro e mal di testa. Tuttavia, ciascuno dei prodotti richiede sempre di essere "instradato" sulla "pista giusta", risolvendosi viceversa in un mero per quanto utilissimo "ordinatore di dati" che, senza l'analisi dell'investigatore, rimangono vuoti di significato.

In conclusione, l'ago nel pagliaio non lo si trova facilmente: tuttavia è evidente come un lavoro di *équipe* a più teste e competenze professionali possa aiutare non poco nell'individuare, quantomeno, la balla di fieno sotto il quale è nascosto. Di qui il **consiglio** che ormai è un mantra: non affidare mai al solo *Digital Forensics* (quand'anche *Expert*) il compito di cercare quell'ago, perché spesso, presi dallo sconforto, non si potrebbe giungere al target. Solo un **lavoro di squadra** tra tutti i soggetti coinvolti potrà portare a qualche risultato; e se non troveremo l'ago avremo almeno individuato dove potrebbe trovarsi, e usare poi la "calamita" senza portarci diretro l'intero pagliaio.

Buona estate!

Note

[1] https://www.ictsecuritymagazine.com/articoli/bit-stream-image-dellintero-supporto-digitale-ieri-oggi-domani/.

[2] http://www.ricercagiuridica.com/sentenze/sentenza.php?num=4727.

[3] https://www.youtube.com/watch?v=i3R6FXg1lv4.

Articolo a cura di **Pier Luca Toselli**