Giovedì, 30 Maggio 2013 00:06

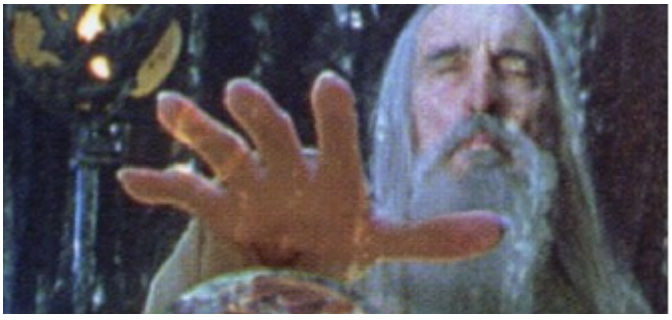
Computer forensics: tra mito e realtà

Parlare di informatica oggi significa discutere di uno strumento irrinunciabile della nostra vita quotidiana tanto che le problematiche giuridiche sollevate dallo sviluppo dell'universo elettronico rappresentano oggi il principale terreno di sfida culturale.

In tale ambito, uno dei temi che più appassionano gli esperti è proprio quello relativo al computer come "prova": che si tratti di acquisire, analizzare o utilizzare in un processo (ovvero nel corso di un'indagine) i dati raccolti il computer si è spesso rivelato un "testimone chiave" per l'accusa o per la difesa.

Sebbene formalmente sarebbe più corretto parlare del computer come "prova" oppure come "fonte di prova", non di rado l'approccio del perito (nominato dal giudice) o del consulente (nominato da una delle parti) con il computer è più simile a quello di chi interroghi un testimone reticente, piuttosto che quello di chi esamini un reperto inanimato: non basta trovare tracce del reato (o non trovarne), occorre interpretarne i silenzi (i dati sono stati cancellati o non sono mai esistiti?) e, persino, le "rivelazioni" (i dati si trovano lì ad insaputa dell'imputato\indagato o vi sono stati consapevolmente collocati da lui?).

Scherzi a parte, proprio per questa ragione l'analisi di un computer non dovrebbe mai ridursi ad un "positivo" o ad un "negativo", ma dovrebbe essere sempre adeguatamente motivata, soprattutto in presenza di reati particolarmente odiosi quali quelli di detenzione, cessione o divulgazione di pornografia minorile o atti persecutori. L'analisi non può essere ridotta ad un'attività meramente informatica ed il consulente dovrebbe sempre cercare di ricostruire il comportamento tenuto dall'imputato di fronte al computer: in questo modo è possibile poter correttamente interpretare i risultati dell'analisi anche alla luce di tale ricostruzione comportamentale tanto che, spesso, è necessario valutare se un determinato atto è stato compiuto volontariamente oppure no ovviamente senza esagerare dato che la sfera di cristallo non dovrebbe rientrare nella dotazione hardware del consulente tecnico...



L'esigenza di avere delle comuni regole, procedure e modalità in grado di garantire un sereno rapporto tra accusa e difesa nella dialettica processuale e preprocessuale è un'esigenza impellente per tutti coloro che si occupano di questo argomento: mai come oggi si avverte la necessità della “certezza delle regole”, soprattutto per quanto riguarda l'individuazione e la conservazione di quei dati che poi costituiranno l'oggetto su cui si fonderà la valutazione dell'organo giudicante. Il rilevamento, la conservazione ed il trattamento di questi dati e delle informazioni che gli investigatori (ma anche, non dimentichiamolo, i difensori) possono rilevare nel corso del normale svolgimento dell'attività d'indagine esigono un protocollo operativo che garantisca la loro integrità e non repudiabilità in sede processuale.

L'indagine relativa ai reati informatici dipende in gran parte dal tipo di crimine che si vuole reprimere e dagli strumenti forniti all'uopo dal legislatore: diverse sono le tracce lasciate dagli autori e, conseguentemente, diverse devono essere le modalità investigative, ma alcune caratteristiche sono comuni:

1) è necessario essere celeri nell'acquisizione di prove ed informazioni: poche cose sono volatili come le prove informatiche. Basta pochissimo per alterarle, modificarle o renderle comunque inservibili;

2) è necessario che l'investigatore sia in grado di ricostruire con precisione le modalità con cui è stato commesso il reato anche al fine di valutare adeguatamente la genuinità di eventuali prove raccolte ovvero di scagionare eventuali coimputati.

In questa fase, in cui l'indagato è generalmente all'oscuro delle indagini, possono essere disposte intercettazioni telefoniche, informatiche o ambientali ovvero essere acquisiti elementi di prova da utilizzare successivamente. Questi elementi possono consistere nell'accesso a siti, in contatti in chat, nello scambio di materiale attraverso le reti p2p: si tratta di attività che devono seguire dei rigidi protocolli processuali la cui violazione potrebbe poi portare all'inutilizzabilità in sede dibattimentale della prova acquisita.

In questa fase sebbene non vi sia nessun obbligo formale di avvisare l'indagato, se quest'ultimo ha il sospetto della pendenza di indagini sul suo conto, può presentare un'istanza presso la Procura della Repubblica per sapere se vi sono procedimenti penali a suo carico (art. 335 cpp). In caso positivo questi gli devono essere comunicati, salvo che l'indagine riguardi reati particolarmente gravi ovvero tale informazione sia stata secretata dal PM, ma, in quest'ultimo caso, il periodo non può superare i tre mesi. In ogni caso, anche in assenza dello status di imputato o indagato, è possibile svolgere indagini difensive in via preventiva, ad esclusione degli atti che richiedono l'intervento dell'autorità giudiziaria e purché il difensore abbia ricevuto un apposito mandato.

Bibliografia e fonti in E.Florindi, *Computer e diritto: L'informatica giuridica nella società dell'informazione e della conoscenza*, (a cura), Giuffré, Torino, 2012