Processo penale, prova informatica e strategie difensive

Date : 11 febbraio 2016

SEMPRE PIÙ NELL'AMBITO DEL PROCEDIMENTO PENALE SI PARLA DI PROVA DIGITALE, OVVERO DEL DATO INFORMATICO DA ACQUISIRE NEL CORSO DELLE INDAGINI PRELIMINARI COME FONTE DI PROVA NELL'EVENTUALE PROCESSO INSTAURATO.

La prova digitale è sicuramente fondamentale nell'accertamento dei cd. reati informatici, introdotti nel codice penale dalla L. 547/93 e, successivamente, dalla L. 48/08, nonché da altre leggi riferibili ai delitti commessi attraverso le tecnologie, come quelle sull'abuso e sfruttamento sessuale dei minori (L. 269/98 e 38/06), che sanzionano la diffusione, cessione e detenzione di materiale pedopornografico realizzata anche per via telematica o informatica. La prova digitale assume un ruolo centrale anche nell'accertamento dei reati che pur non essendo necessariamente informatici possono essere eventualmente commessi attraverso le tecnologie, pensiamo alla diffamazione, all'estorsione o allo stalking perpetrati attraverso internet. La prova digitale diventa essenziale, altresì, per l'accertamento anche di reati comuni, poiché sovente quando si indaga attorno ad un delitto gli inquirenti si imbattono in computer e cellulari che possono contenere elementi di prova e occorre quindi procedere all'analisi dei dati estrapolati.

Più in generale può affermarsi che ormai quasi sempre accanto ad una scena del crimine "tradizionale" ci si trova di fronte ad una scena del crimine "virtuale". A ciò si aggiunga che molti reati vengono oramai commessi all'interno di contesti digitali, quali internet e sue specifiche applicazioni, come i social network.

In casi come questi possono sorgere problemi in ordine all'identificazione dell'autore e del luogo del commesso reato, nonché in ordine all'efficacia probante del materiale presente. Conseguenza è che ci si trova spesso di fronte a nuovi interrogativi. Che valore probatorio ha la stampata di un messaggio diffamatorio diffuso via internet o postato all'interno di un social network? Come si procede al sequestro allorquando un contenuto illecito è rintracciabile nel sito gestito da un provider?

In ambito tecnico giuridico lo studio della prova digitale costituisce una vera e propria scienza, computer forensic, che rappresenta oramai una branca importante delle scienze forensi. Tale scienza trova oggi una legittimazione normativa nella previsione delle ispezioni, perquisizioni e sequestri informatici, introdotti con la L. 48/08 che ha ratificato la Convenzione di Budapest

sulla criminalità informatica.

Senza entrare nel merito dei singoli istituti preme evidenziare come la formazione della prova digitale avviene attraverso tre fasi, che sono quelle dell'acquisizione, dell'analisi e della conservazione del dato (cd. catena di custodia), in cui il ruolo centrale è rappresentato dal verbale, referto, che rendiconta queste operazioni. Ciascuna fase presenta delle criticità che possono accendere il confronto dialettico tra accusa e difesa nell'ambito del processo. Il dato nuovo che emerge è che le indagini informatiche stravolgono le caratteristiche del processo accusatorio perché di fatto le prove vengono raccolte nella fase delle indagini e portate al processo già cristallizzate. Compito della difesa sarà quindi quello di provare a contrastare i contenuti della relazione tecnica, tentando di mettere in discussione le attività svolte in ciascuna delle fasi precedentemente indicate.

Rimangono aperte alcune questioni in ordine ai nuovi mezzi di ricerca della prova. Per quanto concerne l'ispezione informatica, secondo alcuni dovrebbe consistere esclusivamente in una descrizione a verbale di quello che si vede, poiché la stessa intesa come esplorazione porterebbe all'alterazione dei dati, trovandoci, quindi, di fronte ad un atto irripetibile con necessità di tutte le garanzie difensive. Per quanto concerne la perquisizione informatica i problemi maggiori si incontrano rispetto all'attività su un computer che al momento dell'intervento è acceso. Relativamente al sequestro informatico la giurisprudenza già da tempo è contraria ad un'acquisizione indiscriminata dei dati, sottolineando l'esigenza di garantire una continuazione dell'attività ed il rispetto della privacy, anche e soprattutto dei soggetti diversi dall'indagato.

Al di la delle suddette questioni interpretative, fisiologiche rispetto ad una materia nuova ed in continua evoluzione, si può affermare che attualmente l'Italia è dotata di una legislazione, sia sul piano sostanziale che processuale, esaustiva. Allo stesso tempo occorre osservare come c'è stato sicuramente un salto di qualità da parte delle forze dell'ordine e degli organi inquirenti in termini di competenza tecnica e conoscenza dei contesti. Manca ancora, tuttavia, un effettivo coordinamento e la scelta di protocolli condivisi per quanto attiene l'acquisizione, l'analisi e la conservazione del dato. L'esame delle sentenze riguardanti casi accertati anche attraverso acquisizione della prova digitale, evidenziano allo stato due impostazioni differenti. Se da un lato, infatti, si registrano decisioni in cui si predilige il ragionamento eminentemente giuridico, sempre più spesso ci si imbatte in pronunce dove prevalgono argomenti di carattere tecnico.

Al fine di giungere a decisioni il meno eterogenee possibili occorre allora che gli organi giudicanti riescano a coniugare le competenze giuridiche con quelle più specificatamente informatiche in modo da applicare la norma in modo corretto ed efficace.

A cura di **Paolo Galdieri**, *Avvocato e Docente di Informatica Giuridica presso la LUISS Roma*

Articolo pubblicato sulla rivista ICT Security – Maggio 2015