Problematiche giuridiche legate alla computer forensics

di: Avv. Bruno Fiammella[1] (pubblicazione del 2004)

(Sintesi dell'intervento svolto durante il Convegno Internazionale "Pedofilia on-line: strategie di contrasto e di prevenzione" Roma, Aula Magna Ministero delle Comunicazioni, 8 luglio 2004)

Uno dei problemi giunti alla ribalta e all'attenzione dei media negli ultimi tempi, e che irrigidiscono il rapporto esistente tra accusa e difesa nella dialettica processuale, è quello cagionato dalla mancanza di un protocollo tecnico che fornisca delle regole certe per tutti gli operatori giuridici in tema di computer forensic.

Le nuove tecnologie informatiche infatti hanno più che mai posto alla ribalta l'esigenza della "certezza delle regole" soprattutto per l'individuazione dei dati che poi costituiranno l'oggetto su cui si fonderà (o dovrebbe fondarsi) la valutazione dell'organo giudicante. Il rilevamento, la conservazione ed il trattamento dei dati e delle informazioni che gli investigatori (ma anche, non dimentichiamolo, i difensori) possono rilevare nel normale svolgimento dell'attività d'indagine richiedono pertanto l'esistenza di un protocollo operativo che garantisca la loro integrità e non repudiabilità in sede processuale.

Ricercare degli spunti dottrinali o dei riferimenti che consentano ad un avvocato di colmare le carenze del proprio bagaglio culturale, dettate da una formazione giuridica e non tecnico-informatica non è semplice. Da un lato perché occorre addentrarsi in una materia rispetto alla quale mancano spesso le basi scientifiche, dall'altra perché, pur volendo colmare questo *vacuum*, ci si ritrova di fronte alla letteratura principalmente o quasi esclusivamente americana che non consente una facile traduzione e trasposizione sia sotto il profilo didattico che sotto quello applicativo, stanti i vincoli di differenziazione tra i paesi di common law e quelli di civil law.

Una possibile definizione di *computer forensic* è quella con la quale, attraverso questa espressione, ci si riferisce alla disciplina che si occupa della preservazione, dell'identificazione, dello studio, della documentazione dei computer, o dei sistemi informativi in generale, al fine di evidenziare l'esistenza di prove nello svolgimento dell'attività investigativa.[2] La scienza ha poi sottolineato la possibilità di indicare alcune specifiche attività legate alla *computer forensic* ed evidenziate come attività suppletive attraverso cui si esplica la stessa: la c*omputer media analysis, ovvero* l'attività di verifica dei supporti di memorizzazione dei dati e delle periferiche; l'attività di verifica di immagini audio e video generati da un personal computer; la d*atabase visualization,* cioè la visualizzazione dei data base e la *network and internet control: l'*attività di verifica e controllo della attività svolte sulle reti pubbliche e private.

Come avvicinare allora magistrati, avvocati e forze dell'ordine ad una materia ostica *in re ipsa* ?

Occorrerebbe innanzitutto ricordare che i principi del nostro ordinamento giuridico legati alle esigenze di integrità della prova al momento dell'acquisizione e della sua successiva conservazione non sono modificabili nonostante l'evoluzione tecnologica e la diversità tecnologiche di alcuni processi. Occorrerà quindi applicare, con le dovute cautele, gli stessi principi (con

---

[1] Avvocato in Reggio Calabria, Direttore dell'Osservatorio CSIG di Reggio Cal., www.fiammella.it
[2] Andrea "Pila" Ghirardini, CISSP, "Introduzione alla Computer Forensics" 2002.

metodologie necessariamente differenti) che riguardano l'assunzione delle prove relative, ad esempio, ai processi sull'inquinamento e sulla sofisticazione alimentare.[3]

Ma c'è di più, avvicinare gli attori in gioco verso un dialogo costruttivo, significa far loro comprendere le differenziazioni esistenti relative alla *scena criminis.* Normalmente essa è costituita da un ambiente fisico-spaziale ben definito e facilmente identificabile; nei reati informatici invece, quasi sempre l'ambiente è costituito da informazioni, la cui genuinità nella loro acquisizione sta alla base di ogni processo di validazione e dell'elemento probatorio raccolto e sua successiva acquisizione in dibattimento.

In tutto questa matassa non semplicemente districabile, il legislatore non viene incontro all'operatore del diritto. Le recenti modifiche normative all'art. 132 del d.lgs. 196/2003, per come poi combinato con l'art. 123 dello stesso provvedimento creano un quadro che può definirsi, non soltanto a dire delle forze dell'ordine, allarmante.

L'art. 132, infatti, per come riformato dalla legge 45/2004, dispone che i dati relativi al traffico telefonico sono conservati dal fornitore per 24 mesi. Ulteriori 24 mesi sono previsti per finalità di repressione dei delitti di cui al 407 comma 2 lett.a) c.p.c. (ovvero tutte le ipotesi più gravi di delitti previsti dal c.p. terrorismo, armi stupefacenti, associazioni, e quant'altro) oltre ai delitti in danno di sistemi informatici o telematici. Per ottenere questi dati occorre un'istanza al GIP da parte del PM o del difensore affinché emetta un decreto di acquisizione dei dati (e lo fa se ritiene esistano sufficienti indizi per i delitti di cui al 407 c.p.c. sopra richiamato); oppure il difensore stesso chiede al fornitore direttamente i dati relativi al proprio assistito ex. 391 quater c.p.c. (nuova legge indagini difensive).

Alcune delle questioni aperte allora sarebbero: a) non c'è nessun obbligo per le aziende diverse da quelle dei fornitori di accesso alla rete telefonica per la tenuta dei file di log, anzi, esiste l'obbligo di cancellazione dei dati. Quali dati devono esser conservati, visto che la norma fa riferimento ai soli dati relativi alla fatturazione ? b) 24 ed eventuali ulteriori 24 mesi per la conservazione dei dati, sono realmente sufficienti per lo svolgimento delle indagini ? (basti pensare alle eventuali rogatorie internazionali o alle ulteriori richieste di perizie svolte durante il dibattimento).

Le indicazioni che oggi conosciamo e delle quali si è sentito molto parlare, tendono a prediligere la necessità, al fine di salvaguardare il dato, di effettuare una copia bit per bit dell'hard disk con software appropriati, possibilmente davanti a testimoni, protetta con procedura di firma digitale le cui chiavi verranno consegnate al magistrato ed al difensore e memorizzate su un supporto diverso da quello in cui sono custoditi i dati.

Inoltre, baluardo di ogni difesa, è l'esigenza di giustizia di compiere queste attività in contraddittorio tra le parti e quindi con la necessaria presenza del difensore, a sua volta eventualmente assistito da un consulente di parte, in quanto trattasi di accertamenti tecnici sicuramente qualificabili come "irripetibili".

Forse, quello di cui più che mai abbiamo bisogno è, in questa disciplina, di una legislazione chiara che dia agli operatori gli strumenti tecnici, ad esempio, per congelare i dati oggetto di indagine (pratica già diffusa in altre nazioni) e dall'altro tutelare la riservatezza dell'indagato in

[3] A. Gammarota, "Dalla computer forensics all'informatica forense", intervento al Master CSIG in diritto delle tecnologie informatiche, 2003, Bari.

forma più forte rispetto ai normali canoni codicistici oggi attuati.[4] Non si può dimenticare od ignorare la circostanza che l'indagato, per il solo fatto di essere tale, può essere macchiato, in relazione ai procedimenti legati ad attività di contrasto alla pedopornografia on-line, da un'infamia che, prescindendo dall'esito del processo, rappresenta già una condanna preventiva da parte dell'opinione pubblica: una sentenza emessa dai media e dalla collettività prima ancora che il processo vero e proprio si sia svolto. L'eventuale successiva assoluzione processuale rischia di non poter lavare l'onta subita da un'accusa eventualmente infondata.

E' forte quindi l'esigenza di creare un protocollo unico all'interno dell'U.E. per garantire i diritti di tutte le parti in gioco affinché possano avere la certezza giuridica relativa alle modalità seguite o da seguire per il rilevamento dei dati e delle informazioni.

L'ulteriore domanda da porsi, considerato l'oggetto delicato di questo convegno, è quello di capire se, in tema di tutela del minore, possa o meno ancora oggi parlarsi di una differenziazione tra la verità e la verità processuale. L'esperienza nella aule penali spesso dimostra come i due elementi siano non perfettamente combacianti, ma si sa, questa può essere un'arma a doppio taglio nello svolgimento dell'attività difensiva.

Ed allora, come ottemperare in un settore in cui la ricerca della verità è quanto mai indispensabile considerato che il bambino di oggi sarà l'adulto di domani ?

L'interesse, in tutti questi procedimenti, è quello del minore, unica vera vittima di queste esperienze. In casi simili, il problema del rilevamento delle tracce è drammaticamente ribaltato, le uniche tracce che restano, questa volta indelebili, sono quelle riposte nel cuore e nella mente dei bambini, tracce che non potranno essere cancellate dai ricordi di una vita.

Roma,lì 08.07.2004 Avv. Bruno Fiammella

[4] Gerardo Costabile, "Scena Criminis, documento informatico e formazione della prova penale", atti del convegno di Verona del 7 maggio 2004, "Documento informatico: Problematiche di formazione e probatorie"