RASSEGNA DI INFORMATICA GIURIDICA

Laura Nespeca

Questioni terminologiche

Il termine "era digitale" è frutto del quotidiano uso del computer e di Internet in ogni campo di attività: dal lavoro, all'informazione, agli acquisti, alla comunicazione, ai rapporti interpersonali.
Entrando a fondo nella routine quotidiana, non può stupire quindi che gli stessi mezzi tecnologici e informatici siano sempre più oggetto di analisi e di indagine sotto diversi punti di vista. Tra questi, un settore di grande sviluppo e di ancora non prevedibile definizione è lo studio dell'implicazione tecnologica nelle scienze forensi, sia sotto il profilo della commissione dei reati, con la nascita di nuove figure delittuose (*cybercrimes*), sia sotto il profilo delle tecniche di indagini in caso di reati, per la formazione delle prove e la ricostruzione dell'illecito.
Il fenomeno si è imposto con una tale rilevanza da determinare la nascita di una nuova e specifica disciplina giuridica: l'informatica forense.
In Italia, la denominazione racchiude l'insieme delle attività che sono rivolte all'analisi e alla soluzione dei casi legati alla criminalità informatica, comprendendo anche i crimini realizzati con l'uso di un computer, diretti a un computer o in cui il computer può comunque rappresentare una fonte di prova. Informatica Giuridica, Informatica Giudiziaria, Diritto dell'Informatica, Informatica Giuridica Processualistica sono solo alcuni degli indirizzi che si riportano all'ampia area giuridico-tecnologica.
Nei paesi anglosassoni, si avverte la stessa difficoltà terminologica. I campi di indagine si differenziano a seconda dello specifico coinvolgimento della tecnologia in oggetto. Si parla dunque di *forensics analysis*, *computer forensics*, *digital evidence*, *digital forensic practice*, combinazioni semantiche che indirizzano verso la valutazione del coinvolgimento e dell'impatto dello strumento tecnologico (computer, telefono cellulare, iPod, Internet) nella fattispecie legale concreta. Esemplificativa è la definizione fornita da Computer Forensics World: "generally, computer forensics is considered to be the use of analytical and investigative techniques to identify, collect, examine and preserve evidence/information which is magnetically stored or encoded".
Il 1984 può considerarsi l'anno di nascita della disciplina, con la creazione, all'interno dell'FBI, del Computer Analysis and Response Team (CART), gruppo di lavoro incaricato delle indagini laddove si

fosse resa necessaria l'analisi dei contenuti di un computer. Negli stessi anni, la polizia di Scotland Yard pubblica l'*ACPO Guide*, il primo manuale sulla *computer forensics*, stilato dall'ACPO (Association of Chief Police Officer), il cui obiettivo era quello di fornire regole per l'acquisizione, l'analisi e la presentazione delle prove informatiche in dibattimento. Solo dieci anni dopo, in Italia, vengono creati il Nucleo Operativo di Polizia delle Telecomunicazioni (1996) e il Servizio di Polizia Postale e delle Telecomunicazioni (1998).
È probabilmente corretto affermare che fino al 1994 il tema dei crimini informatici o delle modalità di recupero delle prove dai mezzi informatici non era così urgente da richiedere una specifica disciplina strutturata. Viceversa, a partire da allora, l'inarrestabile incremento nell'utilizzo del computer ha spinto il Dipartimento della Giustizia degli Stati Uniti a pubblicare le linee guida che, aggiornate nel 2002, costituiscono ancora oggi la base di riferimento di numerose ricerche e studi del settore.

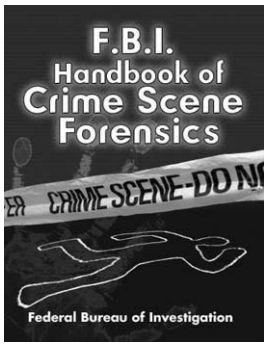


Figura 1.
FBI Handbook
(http://www.skyhorsepublishing.com/Images/Covers/Large/147.jpg)

Temi rilevanti e questioni aperte

A fronte delle numerose pubblicazioni di settore e della letteratura che lo incrementa, l'espressione *informatica giuridica* sembra aprire due questioni fondamentali: la prima attiene alla validità, sicurezza e trasmissione dei documenti giuridici (*informatica giuridica documentaria*); la seconda, riguarda l'acquisizione e l'utilizzo di tali documenti in sede processuale (*digital evidence*).
Evidentemente le due questioni sono connesse, anche se concernono interessi opposti: nel primo caso, si tratta per lo più di salvaguardare la segretezza e la riservatezza dei dati; nel secondo, di recuperare e, soprattutto, di far valere gli stessi dati in sede processuale. Nel

primo profilo, ricordiamo gli aspetti legati alla sicurezza delle reti telematiche (spionaggio informatico, spamming, *hacking* e più genericamente violazione di sistemi informatici). Nel secondo caso, ci si concentra sulle modalità di recupero di dati da supporti danneggiati, cancellati o manomessi, secondo una procedura legale chiaramente definita. Tale duplicità di aspetti si rintraccia anche nei dibattiti tra gli esperti, che possono essere ricondotti a due macro-aree di discussione: una riguardante l'aspetto tecnico-pratico, legato alle modalità di indagine e ai progressi della ricerca scientifica e tecnologica; l'altra relativa all'aspetto puramente teorico-giuridico sulle questioni controverse relative a temi fondamentali come la privacy, la proprietà intellettuale, la trasmissione telematica di documenti ufficiali e la sicurezza informatica, fino al più recente fenomeno del *computer stalking*.

È importante sottolineare che la *computer forensics* è una disciplina fortemente carente di uniformità e standard, e ciò in conseguenza del suo sviluppo tutt'altro che speculativo. Si può affermare che la disciplina sia nata in seguito ad uno sviluppo di tipo *bottom-up*: quindi prodotta dall'esperienza quotidiana e solo successivamente oggetto di una sistematizzazione metodologica. Per di più, nonostante i progressi compiuti in questa direzione, le continue trasformazioni tecnologiche impediscono di considerare risolto il problema metodologico. L'informatica forense non concerne infatti ciò che orbita esclusivamente intorno ad un computer, ma coinvolge ogni strumento passibile di trasmissione e condivisione di dati informatici (telefoni, navigatori satellitari, iPod, iPhone, CD, DVD). Ciò comporta la non applicabilità di un sistema standard di indagine: ogni supporto digitale determina infatti la necessità di individuare specifiche tecniche di investigazione.

L'acquisizione dei dati digitali è, inoltre, un procedimento estremamente delicato che richiede una preparazione tecnica di livello avanzato. Una delle esigenze maggiormente avvertite è pertanto quella di formalizzare le procedure di rilevamento dati, per rendere eventuali elementi probatori da elementi empirici "astratti" a fattispecie legali "concrete". Molte delle community online rispondono proprio a questa esigenza: favorire un proficuo e rapido scambio di risultati di sperimentazioni sul campo e fornire linee guida aggiornate soprattutto per il recupero di dati dai più disparati dispositivi informatici.

Ogni utilizzo di un congegno informatico porta infatti con sé la sua

tracciabilità e cioè la possibilità di ricollegare a soggetti identificabili momenti, azioni e risultati del loro agire. L'estrema volatilità di queste informazioni, facilmente confondibili se non addirittura cancellabili, rende indispensabile il rispetto di determinate procedure ricognitive, che vanno dunque costantemente riviste, verificate e aggiornate.

Topologia gerarchica delle funzioni primarie

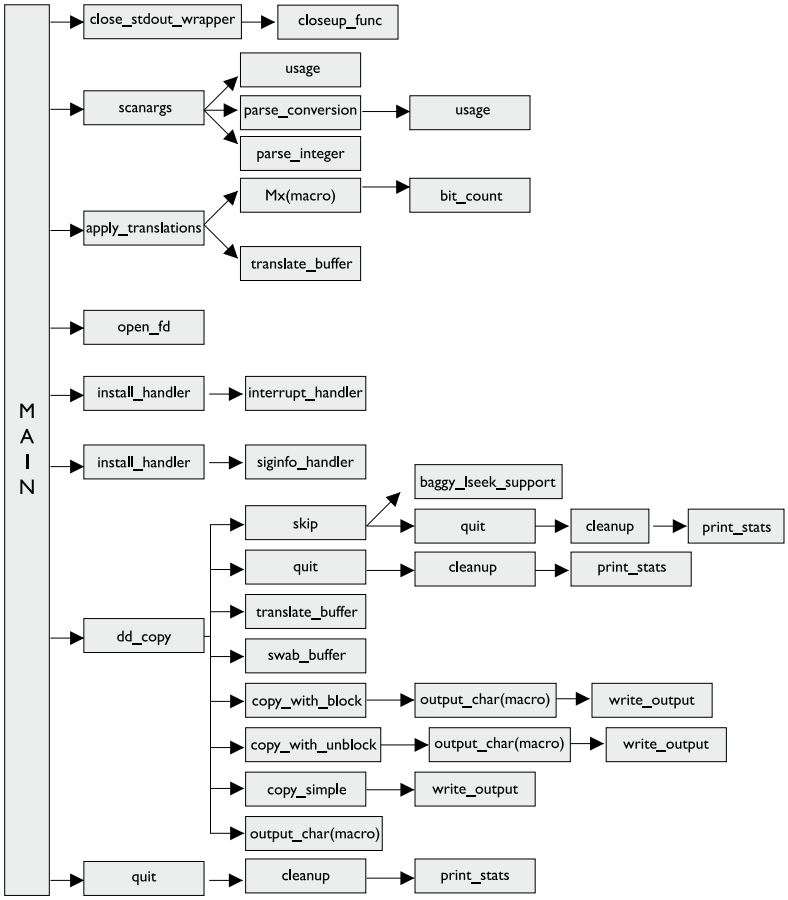


Figura 2.
Esempio di procedura di analisi di dispositivo informatico

VALUTAZIONE DEL CODICE

Riguardo alla seconda macro-area di indagine, inerente alle implicazioni teoriche, filosofiche e giuridiche, dell'informatica forense, il panorama si fa più vasto ed eterogeneo. Nonostante

i tentativi di riportare detta scienza nell'alveo delle discipline puramente tecnico-pratiche, è innegabile che l'informatizzazione dei processi e delle attività umane reca in sé il seme dell'abuso, della non veridicità e dell'attentato alle libertà e ai diritti individuali. Se, infatti, da un lato l'informatizzazione ha reso più facili molti aspetti della nostra vita, dall'altro lato ha determinato l'aumento delle problematiche relative alla gestione delle informazioni e ai criteri di classificazione dei crimini informatici.

Ci si trova cioè a dover fronteggiare i contrastanti aspetti del rispetto della privacy e delle necessità di indagini, il libero scambio di *file* (*peer to peer*) e i diritti d'autore, le enormi possibilità di conoscenza offerte ai giovani dalla rete e i pericoli legati alla pedopornografia.

L'intento di introdurre specifiche fattispecie di *cybercrimes* nel sistema penale italiano si è risolto nella realizzazione di un sistema normativo disarticolato, volto a sanzionare l'accesso abusivo ad un sistema informatico, la detenzione e diffusione abusiva di codici di accesso, la diffusione di programmi diretti a danneggiare un sistema informatico. La lotta al crimine informatico ha però una fondamentale e ineliminabile dimensione internazionale e il Consiglio d'Europa ha approvato, il 23 novembre 2001, la Convenzione di Budapest, ratificata in Senato il 27 febbraio 2008. Tale importante provvedimento introduce numerose fattispecie a tutela e garanzia del corretto utilizzo di Internet, delle banche dati, dell'e-commerce e della riservatezza dei dati personali.

Nell'ambito della riflessione giuridica, uno specifico filone di indagine riguarda l'aggiornamento delle procedure inerenti l'acquisizione e l'ammissione delle prove in sede processuale. Con le dovute differenze, determinate dalla vigenza dei diversi sistemi di *common law* e di *civil law*, sia in Italia che nei paesi anglosassoni l'aumento dei crimini informatici ha reso necessario affrontare il problema del riconoscimento e della validità dei sistemi di acquisizione dell'elemento probatorio al fine del loro utilizzo in sede processuale.

Riferendoci all'Italia, è bene sottolineare le conclusioni cui sono giunti alcuni Tribunali per escludere (TAR di Catanzaro, n. 98, del 9 febbraio 2005, nega il valore probatorio a un documento spedito via e-mail) o ammettere (Tribunale di Milano, 11 marzo 2005, dispone la convalida del sequestro di hard disk di computer disposto durante le indagini preliminari) la prova elettronica.

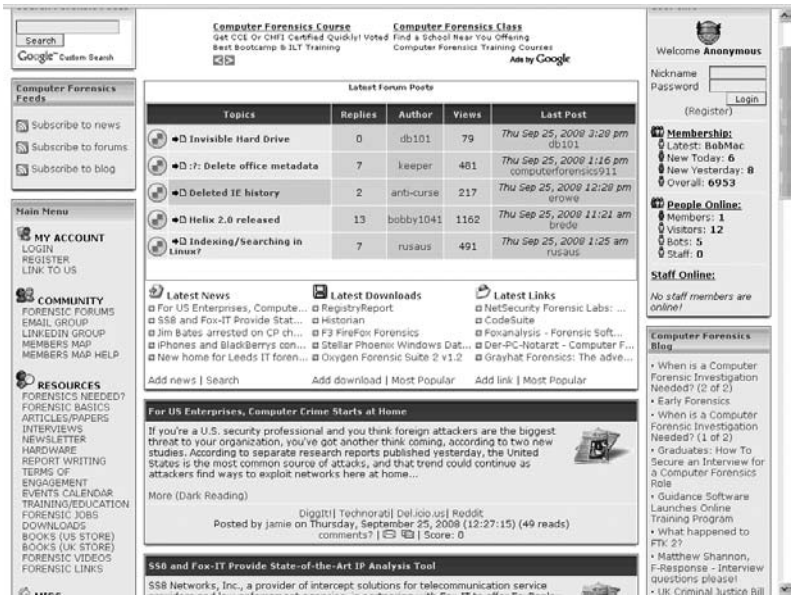
Il nodo comune, rintracciabile nella normativa italiana di riferimento

(Codice dell'Amministrazione Digitale, istituito con D. Lgs. n. 82/05 e aggiornato con D. Lgs. n. 159 del 4 aprile 2006; Regolamento n. 68/2005 sull'impiego della posta elettronica certificata; il Codice per il trattamento dei dati personali e, per alcuni aspetti, anche la Legge antiterrorismo n. 155/05) è sostanzialmente quello di rintracciare gli elementi minimi indispensabili per gli indizi ricavabili dai periti informatici: e cioè gravità, precisione e concordanza.
La questione è piuttosto delicata perché dagli strumenti probatori discende la coerenza di un giudizio. Il sistema di acquisizione probatoria è dunque un nodo centrale dell'indagine: così come un tempo i periti accumulavano gli elementi probatori recuperandoli in modo fisico dalla scena del delitto, ora viene loro richiesto di recuperare gli stessi elementi, sottoforma di bit, dai dispositivi informatici, anche laddove cancellati ed eliminati dal dispositivo stesso.

La letteratura specialistica

La letteratura di settore è in costante sviluppo e la via privilegiata per accedere alle informazioni sulla disciplina è la rete di Internet.
Riferendoci alle macro-aree sopra evidenziate, un nutrito gruppo di siti Internet fornisce elementi base e di riferimento per la salvaguardia e il rilevamento dei dati informatici probatori.
A tal fine, siti istituzionali come il Forensic Science Communications (http://www.fbi.gov/hq/lab/fsc/current/index.htm) o The International Association of Computer Investigative Specialists (http://www.cops.org/), community quali Computer Forensics World (http://www.computerforensicsworld.com/index.php), Crime and Clues (http://www.crimeandclues.com/), National Center for Forensic Science (http://www.ncfs.org/digital_evd.html), HTCIA Online News (http://www.htcia.org/), Computer Crime Research Center (http://www.crime-research.org/articles/), Forensic Focus (http://www.forensicfocus.com/) forniscono un repertorio di agenzie specializzate nell'analisi dei diversi supporti informatici e telematici e le *guideline* per la corretta conservazione delle informazioni. Vengono inoltre offerti concreti riferimenti per il reperimento di *toolkit* necessari per un corretto approccio al rilevamento dei dati.

Figura 3.
Il forum di Forensic Focus
(http://www.forensicfocus.com/
computer-forensics-forums)



L'aspetto più rilevante e proficuo di tali community (in particolar modo Forensic Focus e Computer Forensics World) rimane comunque lo scambio di informazioni e aggiornamenti in materia. In questo contesto, particolare rilievo assume l'International Organization of Computer Evidence (IOCE - http://www.ioce.org/) che organizza convegni in tutto il mondo per aggiornare annualmente le procedure di standardizzazione della prova informatica e favorire il dibattito e lo scambio di esperienze da tutto il mondo.

Numerose sono poi le riviste scientifiche di settore: "International Journal of Digital Evidence" (http://www.utica.edu/academic/institutes/ecii/ijde/), "International Journal of Digital Curation" (http://www.ijdc.net/ijdc/issue/current), "International Journal of Cyber Criminology" (http://www.cybercrimejournal.co.nr/), "Explore Forensics" (http://www.exploreforensics.co.uk/) e "Cybercrimes" (http://www.cybercrimes.it/) sono solo alcune di esse.

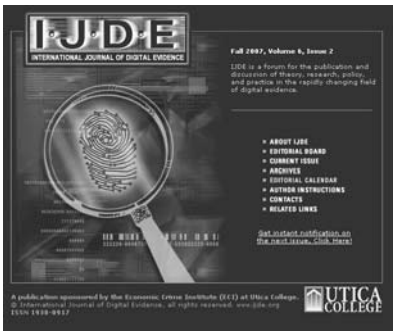


Figure 4 e 5.
Homepage di "International Journal of Digital Evidence" (http://www.utica.edu/academic/institutes/ecii/ijde/) ed "Explore Forensics" (http://www.exploreforensics.co.uk/)

Oltre a riferire delle conclusioni raggiunte nel dibattito su metodologie e ricerche tecnologiche, le rassegne tendono ad ampliare il campo di indagine trattando, ad esempio, delle possibili implicazioni dei diritti umani nella lotta alla repressione del crimine informatico (Russell G. Smith, *Crime control in the digital age: an exploration of human rights implications*, Australian Institute of Criminology, Australia; http://www.cybercrimejournal.co.nr) o analizzando casi giuridici esemplari (è il caso del Regional Computer Forensics Laboratory; http://www.rcfl.gov).

Importanti contributi vengono forniti dal Computer Crime Research Center che offre una considerevole sezione dedicata ai contributi di vari autori e ad un'ampia analisi dei *cybercrimes*. Si forniscono dunque statistiche e casi esemplari, riguardanti in modo particolare gli utenti di Internet, bersaglio di virus, spamming, frodi telematiche (legate principalmente al sempre più diffuso uso dei sistemi di home banking), pedopornografia.

Spunti interessanti sono proposti dall'italiano Cybercrimes.it che offre un importante ponte di collegamento tra l'Italia e il resto del mondo, pubblicando articoli che si riferiscono alle applicazioni e alle innovazioni più stimolanti, come ad esempio il *digital profiling*, metodologia che studia le "caratteristiche umane in una determinata serie di eventi informatici" (Maurizio Acconnelli, *Introduzione al digital profiling*; www.Cybercrimes.it, 1 settembre 2008).

Le scienze forensi si trovano dunque oggi ad una svolta importante. L'emersione di nuovi metodi criminali, più raffinati e occulti, ha reso indispensabile l'aggiornamento dei relativi sistemi di indagine e di tutela del cittadino. La dimensione internazionale del crimine informatico coinvolge gli investigatori di tutto il mondo, che necessitano di luoghi comuni di incontro e di confronto.

La complessità della materia rende peraltro auspicabile il contributo, dottrinario e pratico, di diversi campi del sapere, attinenti non solo alle scienze giuridiche ma anche all'ingegneria informatica o alle scienze archivistiche.