Pubblicata la Legge 18 marzo 2008, n. 48

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalita' informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno (*GU n. 80 del 4-4-2008 - Suppl. Ordinario n. 79*)

INFORMATICA FORENSE NELL'ERA DIGITALE

di Antonio Cilli

LA CONVENZIONE SULLA CRIMINALITA' INFORMATICA

I reati informatici hanno una portata transnazionale, dal momento che possono essere commessi da qualsiasi luogo e a danno di qualsiasi utilizzatore nel mondo. La necessità di combattere la criminalità informatica a livello nazionale e, soprattutto, internazionale è universalmente riconosciuta.

L'esigenza di perseguire i crimini informatici, emerse già alla fine degli anni '80, tanto che, il 13 Settembre 1989, il Consiglio d'Europa emanò una prima "Raccomandazione sulla Criminalità Informatica".

I reati vennero divisi in due liste: facevano parte della prima lista detta "lista minima" quelle condotte che gli Stati sono invitati a perseguire penalmente quali:

- la frode informatica che consiste nell'alterare un procedimento di elaborazione di dati con lo scopo di procurarsi un ingiusto profitto;
- il falso in documenti informatici;
- il danneggiamento di dati e programmi;
- il sabotaggio informatico;
- l'accesso abusivo associato alla violazione delle misure di sicurezza del sistema;
- l'intercettazione non autorizzata;
- la riproduzione non autorizzata di programmi protetti;
- la riproduzione non autorizzata di topografie.

Facevano invece parte della seconda lista detta “lista facoltativa” condotte “solo eventualmente” da incriminare, quali:

- l’alterazione di dati o programmi non autorizzata sempre che non costituisca un danneggiamento;
- lo spionaggio informatico inteso come la divulgazione di informazioni legate al segreto industriale o commerciale;
- l’utilizzo non autorizzato di un elaboratore o di una rete di elaboratori;
- l’utilizzo non autorizzato di un programma informatico protetto, abusivamente riprodotto.

Successivamente, in occasione del XV Congresso dell’Associazione Internazionale di Diritto Penale (AIDP) del 1990, emerse la necessità di incriminare non solo i reati previsti dalla lista minima ma anche le condotte descritte nella lista facoltativa.

Le varie commissioni informatiche che hanno seguito il XV Congresso dell’AIDP hanno tenuto conto delle indicazioni date dall’associazione e nel Settembre 1994 il Consiglio d’Europa ha emanato una seconda raccomandazione che ampliava le condotte perseguibili penalmente inserendo anche:

- il commercio di codici d’accesso ottenuti illegalmente;
- la diffusione di virus e malware.

Nel febbraio del 1997, il Comitato dei Ministri del Consiglio d’Europa incaricava il “Comitato di esperti sulla criminalità nel ciberspazio” di redigere una “Convenzione internazionale sulla criminalità telematica” che esaminasse al tempo stesso la questione delle infrazioni commesse, il diritto penale materiale, il ricorso a poteri penali coercitivi anche sul piano internazionale ed il problema della competenza nei confronti di queste infrazioni informatiche.

Nel dicembre del 1997, i ministri della Giustizia e degli Interni riuniti nell'ambito del G8 adottarono un catalogo di “principi” e redirono un “piano d'azione” articolato in 10 punti

e sottoscritto dai rappresentanti riuniti nell'incontro al vertice di Birmingham di maggio 1998.

Nell’aprile del 2000 il progetto di testo veniva reso pubblico su Internet al fine di raccogliere pareri e proposte finché, non veniva approvato dai Rappresentanti dei Ministri il 19 settembre del 2001 ed aperto alla ratifica degli Stati il 23 novembre 2001 a Budapest. Con la ratifica della Lituania la Convenzione è entrata in vigore il 1° luglio del 2004 per Albania, Croazia, Estonia, Ungheria e Lituania.

La Convezione del Consiglio d’Europa sulla criminalità informatica è, attualmente, l’unico trattato internazionale vincolante. Il Trattato stabilisce le linee guida per tutti gli Stati che vogliano sviluppare una legislazione nazionale completa contro la criminalità informatica; è aperta alla firma degli Stati non Europei e fornisce anche il quadro per la cooperazione internazionale in questo campo. Il trattato è inoltre completato da un Protocollo addizionale relativo all’incriminazione di atti di natura razzista e xenofobia commessi a mezzo di sistemi telematici.

LE PROBLEMATICHE DI DIRITTO SOSTANZIALE

Successivamente al Vertice del Consiglio Europeo di Tampere, del 1999, l'Unione europea ha inserito uno strumento giuridico inteso ad avvicinare il diritto penale sostanziale nel campo della criminalità connessa a danno dei sistemi informatici. L’obiettivo preposto è stato quello di offrire un livello minimo di tutela delle vittime di reati telematici, contribuire a soddisfare la condizione che un'attività debba costituire un reato in tutti i Paesi comunitari perché possa essere richiesta l'assistenza giudiziaria reciproca in un'indagine penale (clausola della duplice perseguibilità) e creare maggiore chiarezza per gli operatori del settore (in merito, ad esempio, alla nozione di contenuto illecito).

Il Vertice ha incluso la criminalità ad alta tecnologia in un ristretto elenco di settori in cui è necessario uno sforzo comune per concordare definizioni di fattispecie, condizioni di perseguibilità e trattamento sanzionatorio. Ciò è riportato nella raccomandazione n. 7 relativa alla strategia dell'Unione europea per il nuovo millennio sulla prevenzione e il controllo della criminalità organizzata, adottata dal Consiglio GAI nel marzo del 2000 e fa parte anche del programma di lavoro della Commissione per l'anno 2000 e del quadro di controllo per la creazione di uno spazio di "libertà, sicurezza e giustizia", elaborato dalla Commissione e adottato dal Consiglio GAI il 27 marzo 2000.

Nella convenzione sulla criminalità informatica vengono specificate quattro categorie di reati penali:

1. Reati contro la riservatezza: numerosi Paesi hanno introdotto norme penali attinenti la raccolta, la memorizzazione, l'alterazione, la divulgazione e diffusione di dati personali. L'Unione europea, ha adottato due direttive per riavvicinare le disposizioni nazionali in materia di tutela della riservatezza con riguardo al trattamento dei dati personali. L'articolo 24 della direttiva 95/46/CE statuisce espressamente che gli Stati membri sono tenuti ad adottare tutte le misure necessarie a garantire la piena attuazione delle disposizioni della direttiva, nonché ad irrogare sanzioni in caso di violazione delle disposizioni della normativa nazionale. Il diritto fondamentale alla riservatezza e il diritto fondamentale alla protezione dei dati sono sanciti inoltre dalla Carta dei Diritti fondamentali dell'Unione europea. In Italia vige il Decreto legislativo 30 giugno 2003, n. 196 "CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI" che all'allegato B) contiene il "Disciplinare tecnico in materia di misure minime di sicurezza";
2. Reati contro il patrimonio, accesso non autorizzato e sabotaggio: numerosi Paesi hanno introdotto norme relative ai reati contro il patrimonio specificamente connessi agli strumenti informatici e definiscono nuove fattispecie legate

all'accesso non autorizzato ai sistemi informatici (ad esempio, la pirateria, il sabotaggio di elaboratori e la diffusione di virus informatici, lo spionaggio informatico, la falsificazione informatica e la frode informatica) e nuove modalità di violazione (ad esempio, manipolazioni di elaboratori invece di inganni a danno di individui). L'oggetto del reato riguarda per lo più denaro in depositi bancari o programmi informatici. Attualmente, non esistono strumenti dell'Unione europea relativi a tali tipi di attività illegale;

3. Reati relativi ai contenuti inerenti la diffusione, soprattutto mediante Internet, della pornografia, e in particolare della pornografia infantile, di affermazioni razziste e di informazioni che incitano alla violenza inducono a chiedersi in quale misura tali atti possano essere affrontati con l'ausilio del diritto penale. La Commissione ha sostenuto la tesi che ciò che è illecito off-line dovrebbe essere tale anche on-line. L'autore o il fornitore dei contenuti può essere chiamato a rispondere in sede penale. È stata adottata una decisione del Consiglio per combattere la pornografia infantile su Internet. La responsabilità dei fornitori di servizi che fungono da intermediari, le cui reti o server vengono utilizzati per la trasmissione o la memorizzazione di informazioni relative a terzi è stata affrontata anche dalla direttiva sul commercio elettronico;
4. Reati contro la proprietà intellettuale: sono state adottate due direttive, relative alla tutela giuridica dei programmi per elaboratore e delle banche dati, che trattano direttamente di temi inerenti alla società dell'informazione e prevedono l'adozione di sanzioni. Il Consiglio ha adottato una posizione comune concernente una proposta di direttiva sul diritto d'autore e sui diritti connessi nella società dell'informazione. È necessario reprimere la violazione del diritto d'autore e dei diritti connessi, così come l'elusione delle misure tecnologiche volte a tutelare tali diritti. Per quanto riguarda la contraffazione e la pirateria, la Commissione ha presentato una comunicazione che tiene conto del processo di

consultazione avviato con il “Libro verde” del 1998 e annuncia un piano d'azione in materia. Con l'aumentare dell'importanza commerciale di Internet, emergono nuove controversie legate ai nomi di dominio, come la registrazione abusiva di nomi di dominio (cybersquatting), l'accumulazione a fini speculativi di un gran numero di nomi di dominio (warehousing) e la riattribuzione controversa di nomi di dominio (reverse hijacking, mediante il quale le imprese di maggiori dimensioni sottraggono i nomi di dominio a concorrenti più piccoli).

Nella Comunicazione n. 173 del 19.04.2002 vengono affrontane le problematiche relative sia ai “reati informatici specifici”, sia ai “reati connessi ai sistemi informatici” (intendendo con ciò qualsiasi reato che comporti il ricorso alle tecnologie informatiche e telematiche). Per i primi è richiesto un aggiornamento delle definizioni riportate nei codici penali nazionali, mentre, per i secondi è auspicabile una cooperazione e misure procedurali migliori.

L’armonizzazione della normativa nell’ottica dell'Unione europea potrebbe spingersi oltre la portata della convenzione del Consiglio d'Europa -che rappresenterà il livello minimo di cooperazione internazionale- e divenire operativo entro un termine più breve di quello previsto per l'entrata in vigore della suddetta convenzione.

In tal modo la criminalità telematica farebbe il suo ingresso tra le materie disciplinate dalla legislazione dell'Unione e verrebbero introdotti meccanismi per garantire il rispetto delle disposizioni comunitarie.

La Commissione ritiene di importanza fondamentale che l'Unione europea sia in grado di agire in maniera efficace, segnatamente contro la prostituzione minorile su Internet, e esprime quindi il proprio apprezzamento nei confronti della decisione del Consiglio che mira a contrastare tale fenomeno, ma condivide il parere del Parlamento europeo, secondo cui sono necessarie ulteriori azioni intese a ravvicinare le legislazioni nazionali.

Conformemente a quanto stabilito nelle conclusioni del Consiglio di Tampere, la Commissione ha presentato una proposta legislativa nel quadro del Titolo VI del trattato

dell'Unione europea che si basa sui progressi compiuti nell'ambito del Consiglio d'Europa al fine di ravvicinare le normative nazionali in materia di accesso abusivo a sistemi informatici e di attacchi che provocano l'interruzione dei servizi.

Altra proposta è quella di individuare linee di azioni comuni nella lotta al razzismo e alla xenofobia su Internet da inserire sempre nell'ambito del Titolo VI del trattato dell'Unione europea nel più ampio quadro dell'attuazione dell'azione comune del 15 luglio 1996.

Infine, la Commissione esaminerà le modalità da seguire per migliorare l'efficacia degli sforzi contro il traffico di stupefacenti via Internet, la cui importanza viene riconosciuta dalla strategia antidroga 2000-2004 dell'Unione europea, adottata dal Consiglio europeo di Helsinki.

Altra problematica è quella inerente gli obblighi in materia fiscale. Le operazioni commerciali in cui il destinatario della prestazione on-line di servizi telematici sia situato nell'Unione europea, gli obblighi fiscali sorgono nella giurisdizione ove si ritiene che il servizio sia fruito. L'operatore che non adempia agli obblighi fiscali è passibile di sanzioni di diritto civile e penale. In ogni caso la cooperazione tra le autorità fiscali costituisce l'elemento chiave per la realizzazione degli obiettivi prefissati.

L'impegno allargato dell'Unione europea si estende anche nel delicato settore della tutela delle vittime dei reati informatici per i quali occorre trattare problemi quali la responsabilità, i rimedi e il risarcimento, che si presentano all'atto della commissione dei reati informatici.

Sono necessari efficaci strumenti giuridici sostanziali e procedurali, armonizzati a livello globale, o almeno europeo, che tutelino le vittime della criminalità connessa ai sistemi informatici e assicurino i colpevoli alla giustizia. Al tempo stesso, le comunicazioni personali, la riservatezza, l'accesso e la divulgazione delle informazioni costituiscono diritti fondamentali delle moderne società democratiche. Per tale ragione, è opportuno

dare priorità alla disponibilità e all'impiego di misure di prevenzione efficaci per ridurre la necessità di applicare provvedimenti che reprimano il fenomeno a posteriori.
La velocità e l'ampia possibilità di commissione di reati informatici e telematici mettono a dura prova le norme procedurali vigenti che, difformi in ogni singolo Stato, necessitano sempre più di una specifica procedura di approvazione.
In particolare, la Corte di giustizia ha più volte affermato che dette disposizioni legislative non possono porre in essere discriminazioni nei confronti di soggetti ai quali il diritto comunitario attribuisce la parità di trattamento né limitare le libertà fondamentali.

COMPUTER CRIMES

All'aumento del trattamento di dati con sistemi informatici consegue l'incremento della domanda di analisi dei dati digitali a fini di investigazione e di giustizia per:

- Reati informatici e telematici (L. 547/93)
- Reati non informatici ma commessi con sistemi informatici
- Reati di cui si rinvengono tracce o indizi nei sistemi informatici
- Conservazione di dati digitali (memorie, supporti, etc)

L'informatica forense è la disciplina che concerne le attività di individuazione, conservazione, protezione, estrazione, documentazione ed ogni altra forma di trattamento ed interpretazione del dato memorizzato su supporto informatico, al fine di essere valutato come prova nel processo. L'informatica forense studia a fini probatori i processi, le tecniche e gli strumenti per l'esame metodologico dei sistemi informatici (memorie, hard disk, dischetti, nastri, cartaceo, rappresentazioni), nonché l'analisi forense di ogni sistema informatico e telematico (computer, rete di computer, e ogni altro dispositivo per il trattamento di dati in formato digitale), l'esibizione della prova

elettronica, l’esibizione del dato digitale, il recupero di dati e la loro esibizione, l’analisi ed esame del sistema informatico e telematico.

REPERTAZIONE DEI SUPPORTI E ACQUISIZIONE DI DATI

Le memorie di massa e ogni dispositivo di memorizzazione devono essere “congelati” il più presto possibile; cioè i reperti vanno raccolti nel tempo più prossimo all’accadere di un evento di interesse e senza che i contenuti dei dispositivi di memoria vengano alterati.

Tutte le procedure utilizzate durante l’esame dei reperti devono essere controllabili e ripetibili; cioè un esperto indipendente deve essere in grado, leggendo i documenti di ripetere tutte le operazioni che sono state eseguite durante le indagini.

Le fasi del trattamento sono:

- ✓ Individuazione
- ✓ Acquisizione
- ✓ Analisi
- ✓ Valutazione
- ✓ Esecuzione della copia integrale, bit per bit, del disco su un altro dispositivo
- ✓ Calcolo dell’hash del disco sorgente e del disco copia e confronto
- ✓ Apposizione della firma digitale
- ✓ Creazione di almeno due copie

L'informatica forense è l'applicazione delle metodologie tecnico scientifiche di analisi dei sistemi operativi e dei file system al fine di raccogliere prove utilizzabili in fase dibattimentale davanti ad un giudice.

L'analisi forense, in generale, è finalizzata all'individuazione delle prove relative ad un caso, alla loro raccolta e conservazione, con metodiche che permettano la preservazione dello stato, in modo da consentire di ripetere gli accertamenti effettuati da inquirenti e/o periti, come previsto dai moderni codici di procedura penale, e all'interpretazione delle

stesse per formulare ipotesi, più aderenti possibile alla realtà dei fatti, su quanto avvenuto.

Le prime indicazioni sulle metodologie da seguire provengono dagli Stati Uniti, dove una più rapida integrazione della tecnologia informatica all'interno della società ha portato le forze dell'ordine e la magistratura a confrontarsi con criminali capaci di usarne le potenzialità per i propri scopi, rendendo inderogabile la necessità perle agenzie di law enforcement di dotarsi di personale (o consulenti esterni) capaci di spiegare come un dato mezzo/strumento informatico era stato utilizzato/coinvolto nella realizzazione di un reato.

Il diffondersi di reati, di natura tecnologica, ai danni di società che della tecnologia informatica fanno ampio uso, ha favorito il nascere di figure professionali, che applicando i principi dell'informatica forense, fossero in grado di analizzare i sistemi vittime, per spiegare le metodiche impiegate dagli aggressori, e suggerire le possibili soluzioni.

In risposta a tali necessità si ebbe una iniziale risposta di alcune società che portarono allo sviluppo di software proprietari quali EnCase, della Guidance Software, e FTK della AccessData. Questi, strumenti funzionati anche in ambiente Windows, possono vantare un utilizzo semplificato, che consente lo svolgimento di operazioni tramite pratici wizard; di contro hanno un costo di acquisto decisamente elevato.

I primi strumenti software sviluppati in ambiente Linux, attraverso i potenti comandi del proprio sistema operativo, offrono la gestione di dati e file system, unitamente al database con la possibilità di esaminare ed acquisire i dati.

Il costo zero dello strumento software sviluppati con licenza GPL, viene controbilanciato dal costo formativo, infatti la natura stessa dei S.O. su cui questi strumenti funzionano implica una maggior difficoltà nell'individuare personale con il background formativo per operare su di essi.

All'inizio degli anni 2000 si presentò rafforzata la necessità, per chi operava nella computer forensic, di intervenire sui sistemi vittima in loco, riducendo i costi di intervento e assicurando il corretto svolgimento delle procedure di acquisizione ed analisi in modo da non inficiare le prove.

Nascono in quel periodo, due distribuzioni specificamente orientate alla computer forensic: F.I.R.E. ed Helix.

Il desktop di Helix 1.8

Si tratta in pratica di sistemi operativi eseguibili da CD-ROM, con i quali è possibile avviare il sistema vittima e procedere alle varie operazioni. Particolare attenzione viene posta dagli sviluppatori per evitare nel modo più assoluto accessi o scritture, anche accidentali, sui supporti di memoria da esaminare, in modo da non causare nessuna alterazione nelle fonti di prova. All'interno di questi sistemi vengono integrati tutti i software necessari per l'analisi forense, svincolando l'utente dalla necessità di installarli risolvendo le dipendenze dalle librerie richieste.

La legge n. 48/2008, tra le diverse novità, introduce, dopo l'articolo 254 del codice di procedura penale, quanto segue:

- *All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».*
- *All'articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente: «1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».*
- *All'articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».*
- *All'articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni: a) il comma 1 è sostituito dal seguente: «1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;*

  b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti: «o alterarli».
- «Art. 254-*bis*. – ***(Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni)***. *L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di*

telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

- *All'articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così è ordinato,» sono inserite le seguenti: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto».*
- *All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».*
- *All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni: a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «anche di carattere elettronico o informatico»; b) al comma 2 è aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».*

Il citato nuovo dettato normativo non solo prevede e promuove l'utilizzo di tecniche che assicurino la ripetibilità delle attività ma impone il tracciamento delle operazioni che consentono la verifica di tutte le azioni espletate. Inaspettatamente e senza formalismi, il nostro legislatore annuncia l'avvento dell'era dei **computer forensics**!