## Il punto sulla normativa contro i crimini informatici

# In nome della Legge!

*In un convegno a Roma sono stati messi a fuoco alcuni aspetti delle nuove norme sul computer crime. Il commento alla legge svolto da Carlo Sarzana*

***di Manlio Cammarata***


Non basta emanare una legge penale per eliminare il reato. Anzi, la legge prevede che il reato sia compiuto e che il colpevole sia identificato, per poi irrogare la pena. Tuttavia le norme hanno anche un valore dissuasivo, perché in assenza di regole i malintenzionati si sentono più liberi di agire. L'effetto di una norma è tanto più alto quanto più la norma stessa è conosciuta, sia dagli aspiranti delinquenti, sia dalle possibili vittime, che in questo modo possono apprestare con cognizione di causa le opportune misure di difesa. Sono quindi opportune le iniziative come quella presa dall'IPACRI nell'organizzare un convegno dal titolo «Le nuove leggi italiane di fronte alla criminalità informatica: problemi e prospettive», per un esame sia delle nuove norme in materia di computer crime (la legge 23 dicembre 1993 n. 547), sia per un ulteriore approfondimento delle disposizioni in materia di protezione del software (il decreto legislativo del 311 dicembre 1992 n. 518, emesso in attuazione della Direttiva 91/250/CEE).

### Evoluzione del crimine informatico

Il professor Giancarlo Martella, del Dipartimento di Scienze dell'Informazione dell'Università degli Studi di Milano, ha tracciato il quadro evolutivo della materia. Secondo Martella *il crimine informatico è caratterizzato da un'oggettiva difficoltà di rilevazione del crimine stesso e di individuazione del perpetratore. Ad esempio, in casi di spionaggio industriale, la presenza di grandi quantità di dati in forma compatta agevola la sottrazione di informazioni segrete, ma rende difficile stabilire, in maniera immediata, che è stato commesso un crimine, in quanto il bene sottratto è ancora presente presso il proprietario. Anche la sottrazione fraudolenta di decimali di unità monetarie da numerosi conti correnti spesso passa inosservata, data l'esiguità della perdita per il singolo correntista colpito. Inoltre, attraverso collegamenti fra elaboratori (reti pubbliche o private, locali o geografiche) è possibile compiere azioni fraudolente in luoghi differenti dal luogo in cui ci si trova fisicamente, o anche inserire nel sistema informativo programmi progettati in modo che il crimine sia portato a termine in tempi successivi a quello dell'inserimento. Questo può contribuire a rendere ancora più complessa l'individuazione del criminale, in quanto «ridefinisce» il rapporto spazio-temporale tra il crimine e il perpetratore (questo non accade nel caso di crimini non informatici, dove, solitamente, è richiesta la presenza del criminale sul luogo e*

*nel momento in cui si verifica il crimine). Le informazioni sui crimini informatici sono generalmente limitate. Molte organizzazioni colpite preferiscono infatti non diffondere la notizia per timore degli effetti di una pubblicità negativa. Per analoghe motivazioni, le organizzazioni preferiscono stabilire e gestire internamente le azioni di condanna, a seguito della rilevazione del crimine e del colpevole (ad esempio, richiami, licenziamenti) evitando, laddove possibile e/o conveniente, la denuncia alle autorità competenti.*

Quindi Martella ha esposto una classificazione dei crimini informatici: sabotaggio, intrusione e sostituzione di identità, falsificazione di dati, aggiramento, ricerca fraudolenta di informazioni, intercettazione, utilizzazione di strutture di servizio, cavalli di Troia, bombe logiche, arrotondamento, virus, simulazione, attacco asincrono.

Per ogni tipo di comportamento, il relatore ha commentato gli aspetti più interessanti. Per il sabotaggio ha messo in evidenza, oltre a quello fisico e a quello logico, il sabotaggio «psicologico»: *Viene usato in una fase preliminare di un successivo sabotaggio di altro genere, o di un altro tipo di crimine, per fare in modo che l'utente collabori, a sua insaputa, alla riuscita dell'azione criminale. Si è verificato un episodio di sabotaggio psicologico in cui gli impiegati di un centro di calcolo, esasperati dai continui falsi allarmi dell'impianto antiincendio, lo disinserirono. L'ultima volta in cui l'allarme fu disinserito si verificò realmente un incendio, che fece supporre, anche se non fu mai provato, che i falsi allarmi erano opera di un sabotatore.*

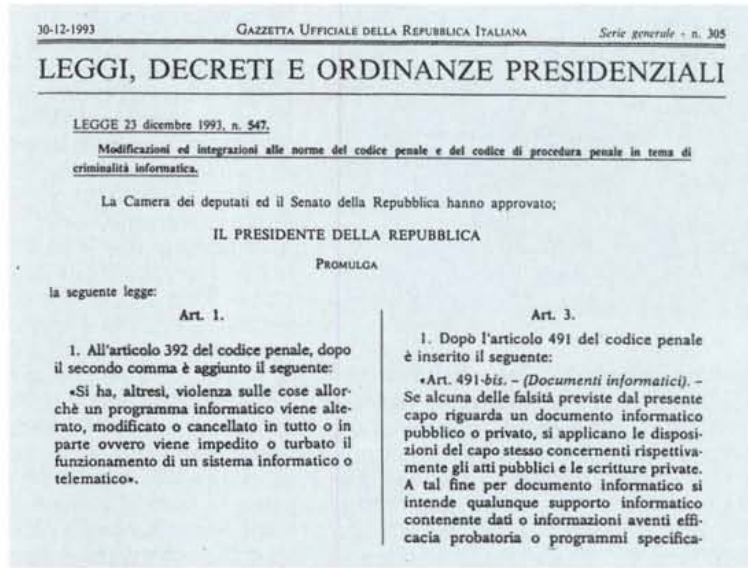
Sull'intercettazione Martella distingue fra intercettazione di tipo passivo e quella di tipo attivo. Nel primo caso l'intercettazione si limita a registrare le informazioni riservate che sono trasmesse sulla rete, nel secondo si aggiunge la modifica delle informazioni stesse. Per quanto riguarda le onde elettromagnetiche, che permettono di ricostruire, per esempio, quello che appare sul monitor, si è scoperto di recente che l'intercettazione può avvenire anche a notevole distanza, anche a centinaia di metri.

Interessante anche la descrizione dell'«attacco asincrono», che consiste nel cambiare l'ordine, o nel ripetere *determinate funzioni, allo scopo di aggirare i controlli del sistema operativo. Le caratteristiche stesse del sistema operativo possono essere utilizzate in modo tale che le condizioni usuali possono essere cambiate, evitando che il sistema operativo registri la variazione... Ad esempio, è possibile alterare una richiesta, sfruttando l'intervallo di tempo esistente tra il momento in cui la richiesta è esaminata per testarne la validità e il momento in cui la richiesta è eseguita.*

## Il parere del magistrato

Analizzati i crimini, ecco un autorevole commento alle norme per la repressione. Per la verità, nei lavori del convegno romano i due interventi si sono susseguiti nell'ordine contrario, ma in questa sede si può recuperare la successione logica.

Carlo Sarzana di S. Ippolito, magistrato di Cassazione e presidente aggiunto della Sezione GIP presso il Tribunale di Roma, è stato membro della Commissione ministeriale che ha redatto il disegno di legge sui crimini informatici che, modificato dal Parlamento, è diventato la legge 547/93. Il suo commento sulle norme penali è particolarmente significativo, perché tiene conto della relazione al disegno di legge che fu preparata dalla Commissione, che offre numerosi spunti per comprendere le ragioni e gli effetti dei diversi articoli. Fra l'altro, Sarzana spiega lo strano iter del provvedimento, che fu presentato al Senato e poi ritirato e ripresentato alla Camera per essere abbinato alla legge sulle banche dati e la protezione dei dati personale. Iniziativa inutile, perché la legge sui crimini è stata approvata, mentre quella, forse ancora più urgente, sulle banche dati dovrà riprendere il suo cammino nella nuova legislatura. Vediamo ora le osservazioni espresse dal magistrato (come per l'intervento di Martella ci limitiamo, per evidenti limiti di spazio, ai punti più interessanti). Sulle modifiche all'art. 420 c.p. (attentato a impianti di pubblica utilità), Sarzana osserva: *L'ipotesi di reato rimane costruita come delitto di attentato ovvero a consumazione anticipata, il cui momento realizzativo coincide con il porre in essere l'azione diretta a danneggiare o distrug-*



30-12-1993 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA *Serie generale* - n. 305

LEGGI, DECRETI E ORDINANZE PRESIDENZIALI

LEGGE 23 dicembre 1993, n. 547.

**Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica.**

La Camera dei deputati ed il Senato della Repubblica hanno approvato;

IL PRESIDENTE DELLA REPUBBLICA

PROMULGA

la seguente legge:

**Art. 1.**

1. All'articolo 392 del codice penale, dopo il secondo comma è aggiunto il seguente:

«Si ha, altresì, violenza sulle cose allorchè un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico».

**Art. 3.**

1. Dopo l'articolo 491 del codice penale è inserito il seguente:

«Art. 491-*bis*. - *(Documenti informatici)*. - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specifica-

*gere* (cioè per configurare il reato non occorre che l'evento si compia, basta il tentativo). *La nuova formulazione della norma, rileva la relazione, è diretta altresì al definitivo chiarimento sulla individuazione dell'oggetto materiale del delitto, essendo sorte... non poche perplessità per l'indicazione alternativa, contenuta nel primo comma dell'attuale testo dell'art. 420, degli impianti di ricerca o di elaborazione dati rispetto a quelli di pubblica utilità. Il testo richiama la prevalente dottrina la quale ha ritenuto che la messa in pericolo degli impianti di ricerca e di elaborazione di dati, ai fini della configurabilità del delitto di cui all'art. 420 c.p., soltanto nel caso in cui tali impianti, pur appartenendo a privati ed essendo adibiti a finalità private, avesse tale rilievo sociale che una condotta diretta a danneggiarli non potesse lasciare indifferente la collettività... Passando a esaminare il secondo comma, si rileva che esso prevede l'inserimento di una specifica previsione di reato, punita con identica pena, per il caso in cui lo stesso fatto di cui al precedente*

-CONVEGNO IPACRI-

# LA LEGGE NR. 547 DEL 1993: PROFILI ESEGETICI DELLA NUOVA NORMATIVA

CARLO SARZANA DI S.IPPOLITO

ROMA - 3 MARZO 1994

*comma, e cioè l'azione diretta al danneggiamento o alla distruzione, riguardi un sistema informatico o telematico, ovvero i dati, le informazioni o i programmi in essi contenuti; anche in questa seconda ipotesi, osserva la relazione, deve trattarsi di sistemi, dati, ecc. appartenenti a soggetti pubblici o privati che abbiano complessità o rilevanza tali da far sì che un attentato agli stessi sia fonte di immediato pericolo per l'ordine pubblico o per gli interessi socio-economici della collettività.*

## Sul «documento informatico»

E passiamo a un punto molto importante (art. 491 bis), nel quale si prevede il «falso informatico» e viene introdotta la nozione giuridica del «documento informatico». *Tale, agli effetti della legge, sostiene la relazione, non deve essere considerato il prodotto dell'elaboratore (tabulato), in quanto lo stesso rientra nel novero dei documenti cartacei contemplati dagli artt. 476 e segg. del c.p. ed essendo ormai pacifico in giurisprudenza che la sottoscrizione meccanica deve essere equiparata a quella manuale. Il legislatore ha ritenuto, invece, di attribuire la natura di documento informatico ai «supporti» - di qualunque specie essi siano - contenenti dati, informazioni o programmi... Come si rileva dalla relazione, la condizione assoluta è che il supporto informatico possa costituire oggetto del reato è, per contro, la destinazione e l'efficacia probatoria dei dati in esso contenuti o alla cui elaborazione sono destinati i programmi registrati sul supporto medesimo.* Questo significa che un qualsiasi dischetto, per esempio, non può essere considerato «documento informatico» se non contiene dati che possano costituire prove in un procedimento giudiziario o programmi per elaborarle.

Un'altra importante novità, per chi si occupa di informatica, è contenuta nell'art. 615 ter, che punisce l'accesso abusivo a un sistema informatico o telematico, o il mantenimento in esso, contro la volontà espressa o tacita del titolare. Afferma Sarzana: *La norma trova la sua collocazione - come osserva la relazione - tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici e telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 del codice penale. La tutela è limitata ai sistemi informatici e telematici protetti da misure di sicurezza perché, dovendosi tutelare il diritto di uno specifico soggetto è necessario, come sostenuto nella relazione, che quest'ultimo abbia dimostrato, come con mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'accesso e la permanenza nel sistema alle sole persone da lui autorizzate.* Qui sorge una domanda molto interessante: se un sistema informativo viene considerato come un'estensione del «domicilio» di una persona, possiamo dire che la legge prevede il riconoscimento di un «domicilio virtuale»? La questione non è banale, perché oggi è possibile svolgere elaborazioni a distanza. Un operatore che si trova fisicamente in un certo luogo, ma opera su un computer remoto, o anche su più computer posti in luoghi diversi, configurerebbe una sorta di «ubiquità» di un individuo. Il problema non è astratto: poniamo il caso in cui l'intrusione in un sistema avvenga attraverso una rete internazionale, e che i sistemi violati si trovino fisicamente in paesi diversi. In quale nazione si consuma il reato, e quale autorità è legittimata a perseguirlo?

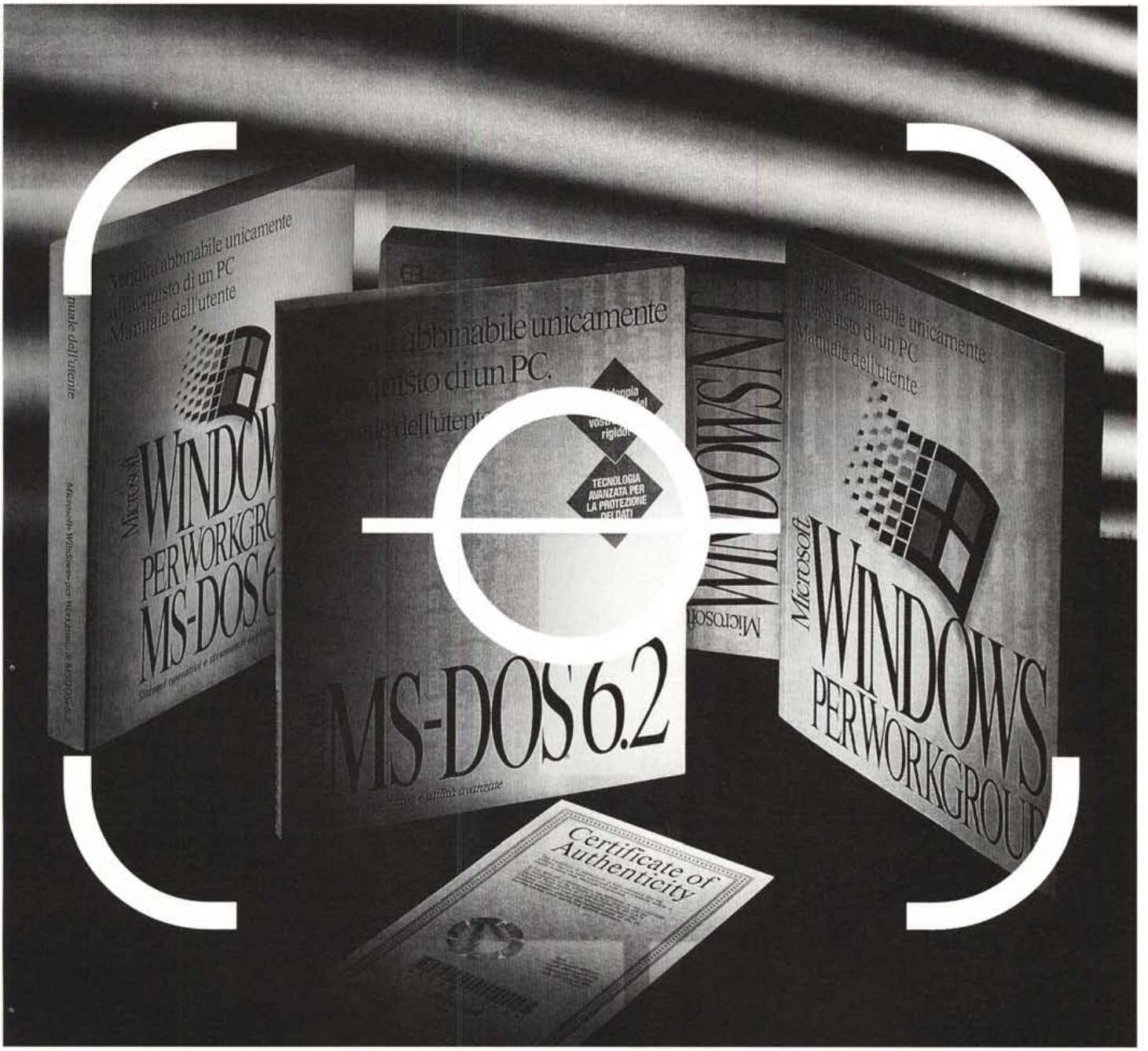
## A proposito di virus

Un'altra domanda viene posta dal magistrato sull'art. 615 quinquies (diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, cioè virus e simili). La norma punisce solo il comportamento doloso, cioè intenzionale, ma nella fase preparatoria era stata contemplata anche la possibilità di punire il comportamento colposo, cioè non deliberato. Dice Sarzana: *A questo proposito vengono alla mente due distinte situazioni. La prima riguarda il comportamento del produttore di software che sia consapevole dell'esistenza nel programma, comunque da fornirsi a terzi, di gravi difetti che, in date circostanze, possono alterare il funzionamento del sistema e pur tuttavia consegna ugualmente il prodotto. Quid juris nel caso in cui l'evento dannoso si verifichi? Ricorre l'ipotesi del dolo eventuale? La seconda si riferisce a colui che, comunque, fornisce ad altri «programmi virus» a scopo di studio o di prevenzione, cioè per la preparazione dei c.d. programmi antivirus. Poiché è richiesto il dolo specifico per la sussistenza del reato, in tal caso il fatto non dovrebbe costituire reato. Non vi è dubbio comunque che sarà molto difficile dimostrare l'esistenza del dolo nel solo fatto di procurarsi o riprodurre programmi virus.* Insomma, non è reato disporre di un virus o copiarlo o consegnarlo a qualcuno, per motivi di studio o per creare un programma per combatterlo. Ma resta il problema del «dolo eventuale», cioè del caso in cui qualcuno fornisca un programma «che può» danneggiare un sistema. Se il danno si verifica, può essere punito chi ha ceduto il programma? Magistrati e avvocati avranno molto da discutere su questo punto.

In conclusione, dall'insieme dei commenti che fino a oggi sono stati fatti sulla legge 547/93, sembra che nel complesso delle norme non vi siano oscurità, incongruenze o altri difetti rilevabili in astratto, cioè senza che si siano ancora verificati casi di applicazione pratica. Si porrà tuttavia un problema di coordinamento quando sarà finalmente approvata la legge sulle banche dati, che conterrà norme penali per la tutela della riservatezza individuale, o richiami alle norme vigenti sulla stessa materia. Un altro problema di coordinamento deriverà dalla creazione di un ufficio di «Garante dei dati», previsto nei diversi disegni di legge sulle banche dati e presente negli altri ordinamenti europei. Il Garante avrà competenza anche sulle banche dati della pubblica amministrazione, e quindi la sua attività potrà incrociarsi con quella dell'Autorità per l'informatica.

Ce n'è abbastanza per capire che il lavoro dei giuristi sulle leggi relative all'informatica si prospetta ancora lungo e complicato. A quando un «Codice delle leggi sulle nuove tecnologie»?

MC




# Importanti rivelazioni per i produttori di PC.

**167-011182 e 167-017267.** Questi sono i numeri verdi rispettivamente di Microtek Italia e Raphael Informatica, i due Delivery Service Partner di Microsoft. E' a loro, e solo a loro, che i produttori di PC devono chiedere i sistemi operativi Microsoft originali.

**Una novità: MS-DOS 6.2.** Da scoprire subito la nuova versione del più collaudato sistema operativo in commercio. Più veloce, più potente, MS-DOS 6.2 ha anche nuove doti operative come la protezione automatica dei dati e nuove utilities quali Scandisk e Antivirus.

**Due certezze per il futuro: Windows NT e Windows per Workgroup 3.11.** Il primo è il sistema operativo a 32 bit per gli anni'90; il secondo, la nuova versione dell'ambiente Windows con funzionalità di rete, disponibile anche insieme al nuovo MS-DOS.

Se li volete subito, o se volete saperne di più, telefonate: scoprirete il sistema più originale per avere tutti i sistemi operativi Microsoft, ma anche il più comodo e il più economico.

**Microsoft®**
**Sempre più facile.**