Approvata la legge sul computer crime

I reati informatici

Anche in Italia, finalmente, ci sono norme penali che puniscono i crimini perpetrati a danno di sistemi informatici e telematici. Quali sono i punti essenziali?

di Manlio Cammarata

Il Senato ha approvato definitivamente il 14 dicembre '93 la legge sui reati informatici, che aggiorna le norme del Codice penale e di procedura penale.

Finalmente! Il Senato ha dato l'approvazione definitiva alla legge sui reati connessi ai sistemi informatici e telematici, colmando un vuoto legislativo che durava da anni.

Mentre scrivo, il testo non è stata ancora promulgato dal Presidente della Repubblica e pubblicato sulla Gazzetta Ufficiale, ma quando questo numero di MCmicrocomputer giungerà in edicola la legge sarà in vigore o sul punto di esserlo. È prematuro fare commenti, che richiedono un'analisi approfondita. Limitiamoci a un elenco delle novità più interessanti.

Il titolo dice: «Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica». E subito notiamo che, ancora una volta, il legislatore non ha formulato un nuovo complesso di norme. Ha scelto di rattoppare le vecchie, secondo quello che i giuristi chiamano «metodo evolutivo», che spesso si risolve in inestricabili guazzabugli (come abbiamo visto con il DL 518 sulla protezione dei diritti sul software). Tuttavia qui la scelta si giustifica con l'opportunità di non modificare sostanzialmente il corpo dei codici. Il testo si compone di tredici articoli.

Novità sostanziali

La nuove norme contengono alcune affermazioni di notevole rilevanza sulla natura giuridica di diversi elementi del mondo dell'informatica. Vediamo i punti più interessanti.

L'art. 1 aggiunge un comma all'art. 392 del CP: *Si ha altresì violenza sulle cose allorché 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.* Questa norma è meno banale di quanto sembra a prima vista, perché l'art. 392 punisce l'esercizio arbitrario delle proprie ragioni, da parte di *chiunque, al fine di esercitare un preteso diritto, potendo ricorrere al giudice...* È chiaro il riferimento a quei programmi che inibiscono il funzionamento del software quando, a una data prestabilita, il licenziatario non provvede al pagamento dei diritti pattuiti. La pena è la multa fino a un milione.

L'art. 2 cambia il testo dell'art. 420 del CP *(Attentato a impianti di pubblica utilità). Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità, è punito, salvo che il fatto non costituisca più grave reato, con la reclusione da uno a quattro anni. La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti. Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema la pena è della reclusione da tre a otto anni.* Qui sembra tutto chiaro. La vera novità e nel fatto che hardware, software e sistemi in genere vengono messi sullo stesso piano, come si era già visto all'art. 1.

L'art. 3 della nuova legge è molto importante, perché, assimilando il documento informatico al documento tradizionale, estende al primo la nozione di «falso». Recita infatti il 491-bis del CP: *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 specificamente destinati ad elaborarli.* Non è la prima volta che il concetto di documento informatico viene accolto nel nostro sistema giuridico, ma da più parti la sua formulazio-

ne non veniva ancora considerata sufficientemente definita per essere applicata, per esempio, ai documenti della pubblica amministrazione. Ora tutto dovrebbe essere molto più chiaro.

L'equiparazione del contenuto informatico alla scrittura ritorna nell'art. 5, che sostituisce il quarto comma dell'art. 616 del CP *(Violazione, sottrazione e soppressione di corrispondenza). Agli effetti delle disposizioni di questa sezione* (Delitti contro l'inviolabilità dei segreti, ndr), *per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.* Ancora, l'art. 7 inserisce un comma nell'art. 621 del CP *(Rivelazione del contenuto di documenti segreti). Agli effetti delle disposizioni di cui al primo comma è considerato documento anche qualsiasi supporto informatico contenente dati, informazioni o programmi.*

Anche l'art. 7, che aggiunge un comma all'art. 621 del CP *(Rivelazione del contenuto di documenti segreti)* considera «documento» *anche qualunque supporto informatico contenente dati, informazioni o programmi.* Lo stesso concetto ritorna nel successivo art. 8, che riscrive l'art. 623-bis: *(Altre comunicazioni e conversazioni). Le disposizioni contenute nella presente sezione, relative alle comunicazioni e conversazioni telegrafiche, telefoniche, informatiche o telematiche, si applicano a qualunque altra trasmissione a distanza di suoni, immagini o altri dati.* E lo stesso concetto è contenuto nell'art. 13.

Il valore di queste disposizioni va molto al di là della semplice previsione di fatti di rilevanza penale, ma innova un intero sistema normativo, attribuendo di volta in volta a contenuti informatici la natura giuridica di documento pubblico o privato, di corrispondenza o di comunicazione.

Contro i pirati

Gli altri articoli della legge si occupano invece di reati strettamente connessi ai sistemi informatici e telematici. L'art. 4 aggiunge al CP gli articoli 615-ter, 615-quater e 615 quinquies. Stabilisce l'art. 615-ter: *(Accesso abusivo a un sistema informatico o telematico). Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni. La pena è della reclusione da uno a cinque anni...* segue l'elenco delle aggravanti, che consistono nell'abuso di poteri o nella violazione dei doveri da parte di un pubblico ufficiale o di un incaricato di pubblico servizio o *da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema; se il colpevole... usa violenza sulle cose o sulle persone ovvero se è palesemente armato; se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione del suo funzionamento ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.* Si arriva a otto anni di reclusione se i fatti riguardano sistemi di interesse militare o comunque di interesse pubblico.

Ancora sugli accessi abusivi è il successivo art. 615-quater: *(Detenzione e diffusione di codici di accesso a sistemi informatici e telematici). Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza... è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni. La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni* in caso di utilizzo di mezzi di intercettazione.

Infine, senza nominarli, l'art. 615 quinquies si occupa di virus: *(Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico). Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.*

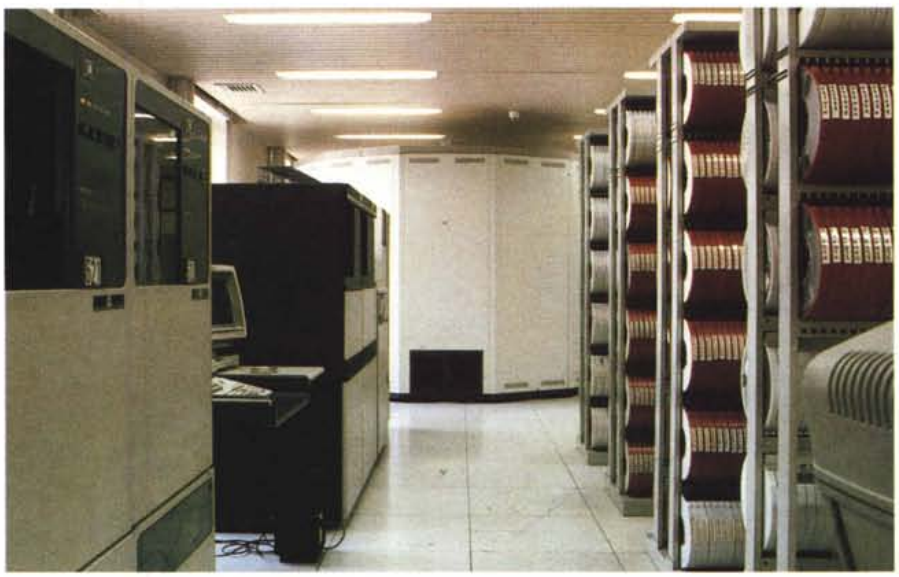
Hacker, pirati, untori di ogni tipo sono finalmente considerati criminali a tutti gli effetti.

Le intercettazioni

Di intercettazioni abusive si occupano gli articoli 6, 7 e 8. L'art. 6 aggiunge tre articoli al CP, il 617-quater, quinquies e sexies. Stabilisce il 617-quater: *(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche): Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.* Seguono le solite circostanze aggravanti (sistema di interesse pubblico, pubblico ufficiale, operatore del sistema, investigatore privato), che portano alla reclusione da uno a cinque anni.

Il 617-quinquies *(Installazione di apparecchiature atte a intercettare, impedire od interrompere comunicazioni informatiche o telematiche)* prevede la reclusione da uno a quattro anni, che diventano cinque con le aggravanti già viste.

Per l'art. 617-sexies *(Falsificazione, alterazione o soppressione del contenuto di informazioni informatiche o telema-*



Le nuove disposizioni proteggono da danneggiamenti, accessi non autorizzati, alterazioni dei dati e dei programmi, quasiasi sistema informativo.

Anche utilizzare un PC all'insaputa del proprietario può costituire reato, se questi ha esplicitamente o implicitamente negato l'accesso a terzi.

tiche) ci sono da uno a quattro anni di galera per chi compie i suddetti reati *al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno.*

Ma le intercettazioni sono consentite, in casi particolari, dal Codice di procedura penale. Fino a oggi i magistrati hanno incontrato non poche difficoltà ad autorizzare le intercettazioni telematiche, ma l'art. 11 della nuova legge aggiunge un articolo al CPC e risolve il problema. L'art. 266-bis dice: *(Intercettazione di comunicazioni informatiche o telematiche). Nei procedimenti relativi ai reati indicati nell'art. 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi.*

Infine l'art. 12 modifica l'art. 268 del CPC, stabilendo norme processuali per i casi di intercettazione di comunicazioni informatiche o telematiche autorizzata dal magistrato.

Danneggiamenti e frodi informatiche

Restano da vedere gli articoli 9 e 10. Il primo aggiunge al CP l'art. 635-bis: *(Danneggiamento di sistemi informatici e telematici). Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici e telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.* Seguono le aggravanti, che comportano la pena da uno a quattro anni. Siamo in presenza di una norma simile a quella dell'art. 1, con la differenza che nel primo caso il reato è la violenza sulle cose, compiuta nell'esercizio arbitrario delle proprie ragioni, nel secondo il semplice danneggiamento di cose altrui.

Anche l'art. 10 della nuova legge aggiunge un articolo al CP, il 640-bis: *(Frode informatica). Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni.* Le aggravanti comportano l'aumento della pena: reclusione da uno a cinque anni e multa da seicentomila lire a tre milioni. Se non ricorrono aggravanti, il delitto è punibile a querela della persona offesa, come prevedono altre disposizioni di questa legge (artt. 392, 615-ter, 616, 617-quater).

In conclusione, la legge non fa altro che estendere all'ambito informatico e telematico una serie di reati previsti dal Codice penale e da norme processuali del Codice di procedura penale. Ci volevano dieci anni?

Comunque, la lunga riflessione sembra aver giovato al risultato finale. La legge appena approvata, che era stata proposta nell'estate scorsa dal Ministro di Grazia e Giustizia, ricalca le linee di molti progetti precedenti. Il testo definitivo sembra chiaro e, a prima vista, non presenta le fumosità o le incongruenze di altre disposizioni, come quelle del DL 518 sulla protezione dei diritti sul software. Le fattispecie, le pene e le aggravanti ricalcano quanto è previsto per i reati «non informatici»; si è resistito alla tentazione di aggravare le sanzioni per il solo fatto che un delitto sia stato commesso con sistemi informatici o telematici o contro i sistemi stessi, pur considerando la loro importanza, sempre più vitale nell'organizzazione della società civile.

In questo primo, sommario esame, non si notano particolari lacune. Sono stati correttamente previsti come reati comportamenti dannosi tipici dell'ambiente informatico, come l'innesco di «bombe a tempo» o la diffusione di virus. Gli organi di polizia non dovranno compiere acrobazie giuridiche per esercitare controlli e intercettazioni di flussi di dati, nei casi e con le garanzie previste dal Codice di procedura penale. E finirà l'imbarazzo di molti magistrati, che

È vietato intercettare flussi di dati intercorrenti tra sistemi diversi, o all'interno di un sistema, al di fuori dei casi previsti dal Codice di procedura penale.

di fronte a comportamenti palesemente illeciti sul piano sostanziale, dovevavo interpretare le norme penali stiracchiandole nei limiti del possibile, per punire i mascalzoni informatici. E qualche volta non ci riuscivano.

Oltre la norma penale

Ma, come ho già accennato, il valore di queste disposizioni non si limita all'ambito del diritto penale. Il riconoscimento formale e sostanziale dell'esistenza di reati in comportamenti che hanno per mezzo o per oggetto sistemi informatici e telematici iscrive le nuove tecnologie nell'intero «corpus iuris» del nostro ordinamento, con riflessi evidenti nell'organizzazione della pubblica amministrazione e nel sistema fiscale, per limitarci ai settori più importanti. È chiaro che, se una norma penale stabilisce che una foglio di carta e un file su dischetto sono la stessa cosa, difficilmente un funzionario potrà disconoscere la validità di una scrittura fatta di bit. Naturalmente si dovranno determinare le caratteristiche di questa scrittura (certificazione della fonte del documento, «firma» elettronica...), ma si tratta di problemi tecnici facilmente risolvibili.

Nell'ordinamento giuridico italiano resta ancora una grave lacuna, che riguarda la protezione delle informazioni individuali contenute nelle banche dati. Anche qui siamo in grave ritardo nei confronti degli altri paesi industrializzati e nell'applicazione delle disposizioni della Comunità Europea. Molti progetti di legge sono stati presentati in questi anni, ma la fine anticipata della legislatura impone che il nuovo Parlamento ricominci da zero. In ogni caso, alcune delle nuove norme penali possono essere applicate anche alle diffusione di notizie riservate contenute in archivi elettronici pubblici o privati (l'art. 615-ter, sull'accesso abusivo, e l'art. 623-ter, che richiama l'art. 621, che punisce la rivelazione del contenuto di documenti segreti).

Ma per le banche dati le norme penali non bastano. Tutta la delicatissima materia deve essere regolamentata organicamente, con la determinazione dei dati che possono essere raccolti, di quelli che possono essere divulgati con o senza il consenso dell'interessato, con l'identificazione dei responsabili e l'istituzione dell'ufficio del Garante.

Dieci mesi fa, sul numero 116 di MCmicrocomputer, scrivevo un «Promemoria per il nuovo Parlamento», nel quale elencavo gli argomenti da affrontare in materia di informatica e telematica: regolamentazione delle banche dati, definizione del documento elettronico, tutela del software e previsione penale dei reati informatici. Le Camere che, con ogni probabilità, saranno elette nei prossimi mesi, troveranno un bel po' di lavoro fatto. Speriamo che lascino passare troppo tempo prima di completarlo.

MB

SENATO DELLA REPUBBLICA

XI LEGISLATURA

N. 1454

DISEGNO DI LEGGE

presentato dal Ministro di grazia e giustizia

(CONSO)

(V. Stampato Camera n. 2773)

approvato dalla II Commissione permanente (Giustizia) della Camera dei deputati il 29 luglio 1993

Trasmesso dal Presidente della Camera dei deputati alla Presidenza il 2 agosto 1993

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

Approvato il 14.12.93

I «requisiti minimi» sono soddisfatti

I riflessi sociali ed economici dei reati informatici sono da tempo all'ordine del giorno in tutti i paesi industrializzati. I sistemi informativi pubblici e privati e le reti di telecomunicazioni costituiscono sempre di più il sistema nervoso dell'organizzazione delle strutture statali e delle economie nazionali e transnazionali. Ogni attacco portato a questi sistemi può avere conseguenze molto gravi. Non è quindi ingiustificata la preoccupazione del Consiglio d'Europa, che da tempo studia il problema e segue l'evoluzione delle legislazioni interne dei singoli paesi. Il risultato di queste ricerche è stato riassunto in due liste di reati, che i paesi membri devono prevedere e reprimere. Una è la cosiddetta «lista minima», che comprende i fatti più gravi, la seconda è una «lista facoltativa», le cui fattispecie dovrebbero essere meno rilevanti. Vediamole.

Lista minima

* Frode informatica
* Falso informatico
* Danneggiamento di dati o programmi informatici
* Accesso abusivo a un sistema o a una rete informatica
* Intercettazione abusiva di comunicazioni
* Riproduzione abusiva di un programma informatico protetto dalla legge
* Riproduzione non autorizzata di una topografia (cioè del circuito di un microprocessore, ndr)

Lista facoltativa

* Alterazione di dati o di programmi informatici
* Spionaggio informatico
* Utilizzazione non autorizzata di un elaboratore
* Utilizzazione non autorizzata di un programma informatico protetto dalla legge.

A una lettura anche superficiale delle due liste sorgono alcune perplessità. Lo spionaggio informatico è da considerare un reato così poco preoccupante che la sua repressione può essere facoltativa? L'utilizzo abusivo di un software (violazione del copyright) è una sciocchezza? E poi, che c'entra in tutto questo la «riproduzione non autorizzata di una topografia»? Qui ci troviamo di fronte a un'eventuale violazione di brevetto, perché i semiconduttori, in quanto prodotti industriali, possono essere brevettati, secondo norme che sono frutto accordi internazionali consolidati. Forse il Consiglio richiede una tutela penale che va al di là del disposto degli artt. 473 e 475 del Codice penale (contraffazione)? Non si vede perché copiare il disegno di un chip sia più grave che copiare qualsiasi altro prodotto industriale.

La sostanza delle raccomandazioni del Consiglio d'Europa è comunque degna di attenzione. Si tratta di vedere, alla luce del DL 518 e della recentissima legge sui computer crime, se l'ordinamento italiano ha recepito tutti i punti elencati. La risposta è positiva. La nuova legge punisce le frodi, i falsi, i danneggiamenti di dati e programmi, il sabotaggio e gli accessi abusivi. Il DL 518, pur con molte incongruenze, protegge il software dalle riproduzioni non autorizzate. Per le topografie possono applicarsi, quando i produttori abbiano richiesto la tutela brevettuale, le norme relative. Anche la lista facoltativa è soddisfatta, con la previsione penale dei reati di alterazione di dati, intercettazione non autorizzata di flussi di dati, utilizzazione non autorizzata di un sistema o (col DL 518) di un software.

Restano fuori da tutte queste previsioni normative la regolamentazione delle banche dati pubbliche e private e la delicata materia della protezione dei dati personali inseriti nelle banche stesse. Per questo settore la Comunità ha emesso raccomandazioni molto più articolate e dettagliate, delle quali ci occuperemo su uno dei prossimi numeri di MCmicrocomputer.