In vigore norme sul computer crime

Molte novità nel Codice penale

Le nuove disposizioni penali in materia di crimini informatici contengono importanti definizioni sulla natura giuridica del documento elettronico, che avranno conseguenze anche nel settore della pubblica amministrazione

di Manlio Cammarata

La legge sui crimini informatici, della quale abbiamo parlato in anteprima sul numero del mese scorso, porta il numero 547 ed è stata pubblicata sulla Gazzetta Ufficiale del 30 dicembre 1993. Dunque è operante. A meno di un mese dalla pubblicazione non ci sono ancora reazioni particolari da parte degli addetti ai lavori, se non di generica soddisfazione. Bisogna considerare che il testo, frutto di una lunga elaborazione, era già noto da mesi e non aveva suscitato critiche sostanziali nella sue stesure più recenti. Dovrà passare del tempo, e forse si dovrà attendere qualche caso di applicazione concreta, prima che possano venire alla luce eventuali incongruenze. In ogni caso non sembra che vi siano problemi della portata di quelli sollevati dal DL 518 sulla protezione del software, che sotto qualche aspetto appare addirittura incostituzionale.

Dopo la prima, rapida lettura di un mese fa, proviamo a esaminare un po' più a fondo le novità più importanti introdotte dalle «Modificazioni ed integrazioni alle norme del Codice Penale e del codice di procedura penale in tema di criminalità informatica». Il primo motivo di riflessione è contenuto nell'art. 2, che modifica il dettato dell'art. 420 del Codice penale: nella sua precedente formulazione (che risale agli anni del terrorismo) si parlava di *impianti di pubblica utilità o di ricerca o di elaborazione di dati*. Il nuovo testo parla invece di *sistemi informatici o telematici di pubblica utilità, ovvero dati, informazioni e programmi in essi contenuti o ad essi pertinenti*. Non è un'innovazione da poco, perché assimila i sistemi telematici a quelli informatici, comprendendo anche i dati, le informazioni e i programmi, cioè il software, che è un bene immateriale, a differenza dell'hardware. In precedenza il «danneggiamento di un bene immateriale» era una nozione che suscitava non poche perplessità nel campo penale, come quella del «furto di programmi», che non comportava la sottrazione di una «cosa» al suo possessore.

Il documento informatico

Ancora più interessante si rivela l'art. 3, che estende le ipotesi di falso in documenti equiparati agli atti pubblici dall'art. 491 C.P. ai documenti informatici, e precisa che *per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli*. La portata di questo comma va al di là della norma penale, perché chiarisce per la prima volta in maniera molto netta, anche se in via generale, la natura giuridica del documento informatico, con riflessi importanti nel campo della pubblica amministrazione. Naturalmente tutto è in relazione all'«efficacia probatoria» dei documenti stessi, e cioè delle informazioni contenute, non del «supporto informatico» in se stesso. In altri termini, un nastro o un dischetto possono essere considerati documenti informatici non per qualche caratteristica particolare del supporto (per esempio, una punzonatura), ma perché le informazioni che contengono provengono da una determinata fonte, o sono in qualche modo «certificate». Si tratta di una previsione generica, che dovrà essere precisata con altre norme. Bisognerà stabilire, per esempio, quando un documento informatico potrà avere la natura di «atto pubblico» o di «scrittura privata». Queste norme dovranno poi essere raccordate con altre, come l'art. 3 del DL 39/93 sull'Autorità per l'informatica nella PA, che dice: *Gli atti amministrativi adottati da tutte le pubbliche amministrazioni sono di norma predisposti tramite sistemi informativi automatizzati*. È chiaro che bisogna stabilire una volta per tutte quali devono essere i requisiti degli atti amministrativi, degli atti pubblici e delle scritture private frutto di elaborazione informatica e custoditi su supporti ottici o magnetici.

Un'altra definizione importante è contenuta nell'art. 5, che innova il 616 C.P. (Violazione, sottrazione e soppressione di corrispondenza): *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 cambia il precedente 623-bis e stabilisce che *è considerato documento anche qualsiasi suporto informatico contenente dati, informazioni o programmi.*

Da tutto questo si deduce che qualsiasi informazione sotto forma di bit viene considerata sulla base del suo contenuto ed equiparata alle informazioni tradizionali corrispondenti (documenti cartacei, lettere, conversazioni telefoniche): forse non è esagerato parlare di una svolta storica.

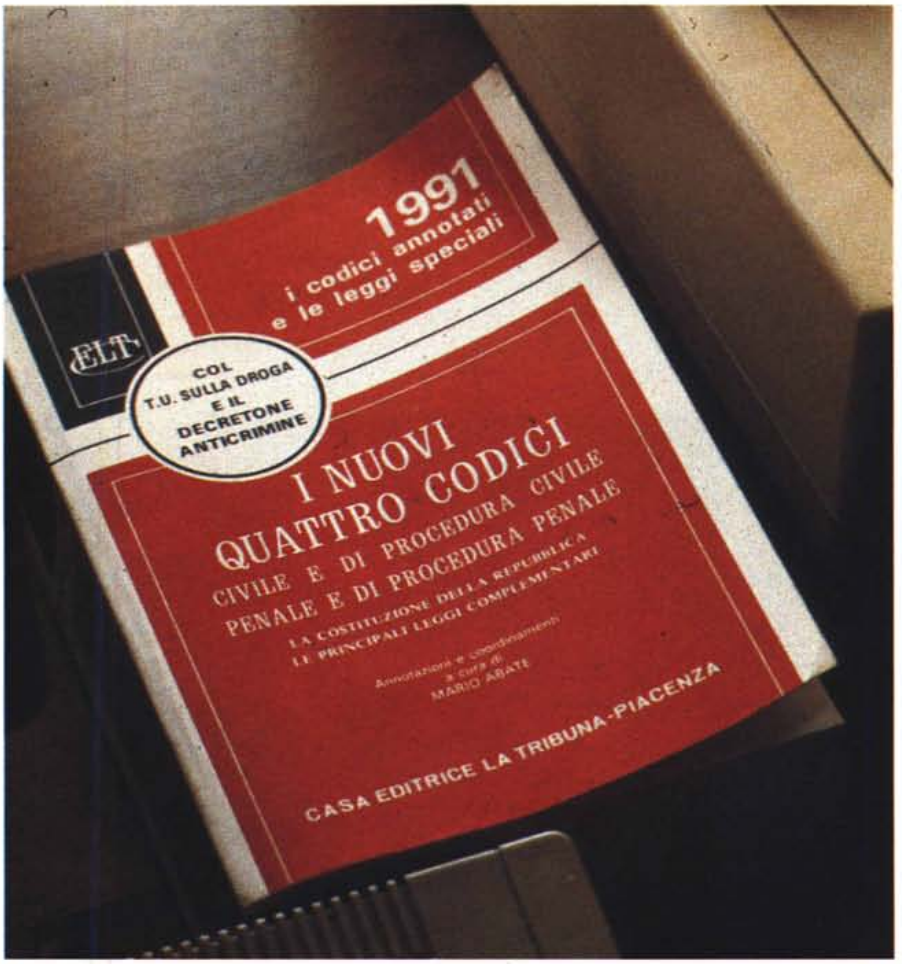
E il furto di software?

Uno dei maggiori problemi che hanno impegnato i giuristi italiani prima dell'emanazione delle leggi sulla protezione del software e sui crimini informatici riguardava il cosiddetto «furto di software». Il problema era semplice, ma insormontabile: la norma penale punisce come furto la sottrazione di un bene materiale al suo possessore, e quindi non può essere applicata a una fattispecie in cui non vi è «sottrazione di una cosa», perché i programmi non sono «cose» e il titolare del diritto non

ne perde la disponibilità. Ora, a un esame superficiale della legge 547/93, non si trovano disposizioni che puniscano i «ladri di bit».

La mancanza è soltanto apparente, per due motivi. Il primo riguarda i programmi, e consiste nel fatto che il «furto di software», non è altro che la copiatura abusiva di un programma, punita dal DL 518/92 sui diritti dell'autore del software. Il secondo riguarda più in particolare il «furto di dati» ed è più sottile. Può essere compreso leggendo la relazione introduttiva al disegno di legge: *La sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto) altro non è che una «presa di conoscenza» di notizie, ossia un fatto intellettivo rientrante, se del caso, nelle previsioni concernenti la rivelazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali, ad esempio, la violazione di domicilio.*

Dunque, per il legislatore, la sottrazione di dati non può in alcun modo costituire una particolare fattispecie di furto (e neanche di «furto d'uso», perché anche questa prevede la sottrazione, temporanea, di un bene materiale alla disponibilità del legittimo possessore). Se ne deduce che, per esempio, un imprenditore che si impadronisca del database di un concorrente contenente i dati relativi ai clienti, commette non un furto, ma una violazione di segreto, punita dall'art. 621 del Codice Penale, integrato dal già citato art. 7 della nuova legge.



A proposito di truffe

Qualche perplessità può nascere dalla lettura dell'art. 10, che aggiunge al Codice Penale l'art. 640-ter, introducendo il concetto di «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...* A prima vista questo articolo sembra del tutto superfluo, perché l'alterazione del funzionamento di un sistema o l'intervento senza diritto sul software potrebbero configurare gli «artifizi o raggiri» previsti dall'art. 640: *(Truffa) Chiunque, con artifizi o raggiri, inducendo taluno in errore, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito*, eccetera. Ma c'è una differenza molto importante. L'art. 640 dice «inducendo taluno in errore», cioè una persona, mentre la truffa informatica si compie inducendo in errore un sistema informativo, cioè una cosa. L'estensione del concetto di «errore della macchina» potrebbe avere conseguenze giuridiche molto rilevanti. Se un malfunzionamento di un hardware o di un software, non riconducibile a colpa o dolo di un individuo, provoca un danno a qualcuno, si può parlare di «responsabilità del sistema informativo»? Evidentemente no, allo stato attuale della tecnologia. Ma la diffusione di macchine sempre più «intelligenti», sempre più in grado di prendere «decisioni» autonome, sottratte al controllo umano per la loro complessità o la loro velocità, potrebbe prima o poi porre problemi di questo tipo, dei quali ora non è possibile prevedere la soluzione.

Un'ultima osservazione va fatta a proposito dell'art. 9, che aggiunge l'art. 635-bis *(Danneggiamento di sistemi informatici o 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.* Il dettato riprende quello dell'art. 635, sul danneggiamento di «cose mobili altrui», ma le pene sono più severe. Il motivo di questa differenza viene spiegato nella relazione introduttiva con il fatto che *il regolare funzionamento dei sistemi informatici e telematici anche privati è di interesse non strettamente singolare ma della comunità intera.* Anche qui ci troviamo di fronte a un'interessante innovazione: il riconoscimento dell'importanza dei sistemi informativi per l'intera società civile, anche quando essi appartengono a privati. Questo significa che l'informazione può in ogni caso essere considerata come un bene di interesse collettivo, e costituisce quindi un aspetto essenziale di quella che chiamiamo appunto «civiltà dell'informazione». MC