CAMERA DEI DEPUTATI N. 1174

PROPOSTA DI LEGGE

D'INIZIATIVA DEI DEPUTATI

CICCIOMESSERE, BARBERA, BONINO, PANNELLA, ELIO VITO, RAPAGNÀ, TARADASH

Introduzione degli articoli 623-*ter*, 623-*quater*, 623-*quinquies*, 623-*sexies* e 623-*septies* del codice penale per la repressione dei reati informatici e telematici

Presentata il 2 luglio 1992

ONOREVOLI COLLEGHI ! — La sempre maggiore diffusione di *computer* e di reti telematiche nelle attività economiche, sociali, politiche ed amministrative ha posto in luce l'inadeguatezza del sistema giuridico al fine di combattere le nuove forme di criminalità informatica o per tutelare le nuove categorie di diritti e di interessi. Si pensi ad esempio alle banche dati della pubblica amministrazione o a quelle degli istituti bancari, che non sono adeguatamente tutelate contro l'accesso abusivo o la falsificazione dei dati, nonostante tali atti possano provocare danni spesso irreparabili o comunque di valore ingente.

Si pensi ancora alle reti di comunicazione telematiche e alla assenza di qualsiasi tutela della riservatezza della corrispondenza o dei dati che vengono trasmessi.

Si pensi infine al pregiudizio nei confronti della identità e immagine personale che può derivare dall'intrusione in sistemi di comunicazione telematica e dalla modifica delle informazioni e delle notizie pubbliche che vi sono contenute.

Nel nuovo quadro tecnologico determinato dallo sviluppo impetuoso dei *computer* e delle reti di comunicazioni telematiche s'impone quindi l'esigenza pressante di tutelare nuovi diritti e nuove forme di libertà personale.

A questo proposito la legislazione italiana vigente appare inadeguata, risultando punibile esclusivamente l'intercetta-

zione o il disturbo della comunicazione telematica (articolo 623-*bis* del codice penale) e rimanendo escluse dalle previsioni di legge le varie ipotesi di reato connesse all'intromissione nelle banche dati e alle frodi informatiche, non risultando comunque applicabili le norme vigenti (per esempio quelle sull'inviolabilità del domicilio, sulla tutela del patrimonio, sulla truffa, sulla falsità in atti) per il generale divieto dell'interpretazione estensiva e analogica alle norme penali. Basti pensare alla non punibilità di chi faccia uso di una *password*, cioè di una sequenza di lettere, numeri e segni di punteggiatura, di cui si sia abusivamente appropriato per accedere ad un *computer* al fine di alterare i dati che vi sono contenuti o di appropriarsene. Il reato di truffa infatti non si concretizza perché l'azione è stata rivolta nei confronti della macchina e quindi non vi è una persona fisica che sia stata indotta in errore come richiesto dall'articolo 640 del codice penale.

E ancora vige la inapplicabilità del reato di furto nei confronti di chi si sia impossessato di informazioni altrui sottraendole al *computer* o del reato di falsità in atti a carico di chi abbia falsificato dati elaborati elettronicamente.

Bisogna inoltre ricordare che il Consiglio d'Europa, con raccomandazione n. R (89) 9 adottata dal Comitato dei Ministri il 13 settembre 1989, ha invitato gli Stati membri ad armonizzare le proprie legislazioni ad alcuni princìpi generali che prevedono una serie di ipotesi di reato fra cui la frode informatica, il falso informatico, il danneggiamento dei dati o dei programmi informatici, il sabotaggio informatico, l'accesso non autorizzato, l'intercettazione non autorizzata di comunicazioni telematiche, la riproduzione non autorizzata di un programma informatico protetto, l'alterazione dei dati o di un programma informatico, lo spionaggio informatico, l'utilizzazione non autorizzata di un *computer* e l'utilizzazione non autorizzata di un programma informatico protetto.

Per porre rimedio ad alcune di queste lacune presenti nell'ordinamento giuridico, si rende urgente un intervento legislativo che provveda alla definizione del termine « elaboratore » o « *computer* », alla introduzione del concetto di comunicazione telematica e alla definizione di nuove tipologie di reato connesse all'uso di banche dati informatiche e di reti telematiche.

Nella proposta di legge che sottoponiamo all'esame del Parlamento, abbiamo innanzitutto scelto, perché ci sembra la più completa e la più ampia, la definizione di « *computer* » adottata dal Parlamento federale statunitense.

Per la sua genericità si presta a comprendere anche elaboratori più sofisticati di quelli attualmente esistenti, che lo sviluppo tecnologico introdurrà nel mercato. La definizione proposta non comprende le macchine da scrivere o le macchine compositrici, i calcolatori portatili e simili congegni. Non è sembrato invece necessario definire i mezzi di trasmissione telematica poiché la trasmissione dei dati fra *computer* può avvenire attraverso i più disparati sistemi: dalle normali reti telefoniche ai satelliti.

Per quanto riguarda la definizione delle nuove ipotesi di reato sono stati previsti tre nuovi comportamenti delittuosi: l'accesso abusivo ed uso non autorizzato di un elaboratore di dati, l'alterazione dell'integrità dei dati, dei programmi e della rete di trasmissione e la falsificazione dei documenti personali informatici.

La prima ipotesi di reato – accesso abusivo ed uso non autorizzato di elaboratore di dati – può in qualche modo essere assimilata al reato di violazione della corrispondenza o di violazione di domicilio. Ma queste due ipotesi delittuose mal si adattano a tutelare quella entità complessa che genericamente definiamo banca dati, che può essere costituita da un semplice *personal computer* dove sono archiviati un numero limitato di documenti o da un sistema integrato e interattivo di archiviazione e comunicazione. Le banche dati infatti sempre più costituiscono un sistema complesso e interconnesso con altre banche dati, nel quale sono custoditi

tutti quei documenti che nel passato erano registrati su supporti cartacei e attraverso il quale si realizzano le diverse forme di comunicazione, dalla messaggistica personale alla stipula di contratti, dalla diffusione di notizie giornalistiche o borsistiche agli ordinativi commerciali e bancari.

Anche le modalità attraverso le quali può essere compiuto il reato non consentono definizioni precise poiché i modi attraverso i quali è possibile accedere ad una banca dati elettronica sono molto diversi fra loro e in continua evoluzione: dall'accesso attraverso connessioni dirette a quello attraverso reti locali, dall'accesso attraverso la rete telefonica commutata o la rete telegrafica o le reti a pacchetto a quello attraverso le onde guidate. In ogni caso per accedere senza autorizzazione ad una banca dati elettronica è necessario forzare le difese fisiche o logiche poste a sua protezione.

A questo proposito bisogna precisare che la previsione di reato copre anche due ipotesi particolari. Una banca dati infatti può prevedere diversi livelli differenziati di accesso e quindi livelli di autorizzazioni: una persona può essere autorizzata ad entrare in alcune parti di una banca dati ma non in altre. Di qui la precisazione sull'accesso totale e parziale contenuta nel primo comma dell'articolo 623-*ter* del codice penale, introdotto dalla proposta. Vi è poi la possibilità che il sistema di protezione della banca dati contenga « buchi » attraverso i quali una persona particolarmente esperta possa accedere a parti riservate o addirittura al sistema operativo. Anche in questo caso si configura il reato di accesso non autorizzato poiché, volendo fare un confronto, in questo caso perfettamente aderente all'ipotesi di reato, con la violazione di domicilio, il fatto di aver lasciato aperta la porta dell'abitazione non legittima l'introduzione e tanto meno la sottrazione di beni da parte di estranei.

La seconda ipotesi di reato – alterazione dell'integrità dei dati, dei programmi e della rete di trasmissione – fa riferimento ad ipotesi di danno molto diverse tra loro, che in qualche modo possono essere assimilabili a quelle previste dai reati di « falsificazione, alterazione o soppressione del contenuto di comunicazioni o conversazioni telegrafiche o telefoniche » o di « interferenze illecite nella vita privata » per lambire anche il vero e proprio furto e il sabotaggio. Infatti la casistica è molto più vasta: l'alterazione dei dati o della rete di trasmissione può infatti riguardare modesti archivi personali come banche dati private o pubbliche di valore inestimabile. Così ancora il danno può essere quantificato in poche centinaia di migliaia di lire o in miliardi.

L'intrusione poi può essere legata a motivazioni le più diverse: la « sfida » tecnologica compiuta da *hackers*, il vero e proprio furto di programmi e di dati o lo spionaggio industriale o militare.

La tutela dell'integrità dei dati ha poi conseguenze che investono gli stessi diritti alla *privacy* e alla tutela dell'identità personale nel caso di banche dati utilizzate per la comunicazione giornalistica o delle cosiddette BBS *(Bolletin Board System)*. Non si tratta solo di tutela della segretezza della propria corrispondenza quanto della necessità di impedire che si realizzino vere e proprie azioni di diffamazione che, per la velocità di propagazione propria del mezzo, possono assumere effetti devastanti.

Per tutte queste ragioni è stato previsto un limite della pena di quattro anni che tiene conto della particolare « potenzialità offensiva » della violazione dell'integrità di una banca dati.

La terza previsione di reato si riferisce alla falsificazione dei documenti personali informatici e cioè delle carte di credito o comunque di quei documenti non cartacei che consentono ad un *computer* il riconoscimento della persona. Questa ipotesi è assimilabile al reato di truffa.

Una particolare aggravante è prevista nel caso in cui questi nuovi reati siano commessi dagli addetti ad un servizio informatico o telematico.

Con l'articolo 623-*septies* si è introdotta una speciale forma di « provvisionale » che richiama in parte quella prevista dall'articolo 24 della legge n. 990 del 1969 (in tema di responsabilità civile derivante dalla circolazione di veicoli); tra i vari casi in sede penale, non si è previsto quello della sentenza conseguente al cosiddetto « patteggiamento », in quanto, ai sensi dell'articolo 445 del codice di procedura penale, tale sentenza non ha effetto nei giudizi civili, e pertanto sarebbe stata contraddittoria la previsione di una provvisionale.

L'inserimento delle nuove previsioni di reato nel titolo XII relativo ai « delitti contro la persona », nel capo III « Dei delitti contro la libertà individuale » e in una nuova sezione « dei delitti in materia informatica e telematica » del codice penale, consegue logicamente dalla volontà esplicita dei proponenti di difendere la riservatezza e l'integrità dei dati gestiti da *computer* e quindi di tutelare i diritti della persona e in particolare la *privacy* individuale contro ogni forma di intromissione e manipolazione da parte di terzi.

PROPOSTA DI LEGGE

—

ART. 1.

1. Nel titolo XII, capo III, del codice penale, dopo la sezione V è aggiunta la seguente:

« Sezione VI-*bis*.
Dei delitti in materia informatica
e telematica ».

ART. 2.

1. Dopo l'articolo 623-*bis* del codice penale, è inserito il seguente:

« ART. 623-*ter* *(Accesso abusivo ed uso non autorizzato di elaboratori di dati).* – Chiunque, fraudolentemente e comunque senza autorizzazione, accede, totalmente o in una sua parte, ad un dispositivo di elaborazione di dati elettronico, magnetico, ottico, elettrochimico e elettromagnetico, o comunque ad ogni dispositivo di elaborazione dati ad alta velocità, incluse le apparecchiature per l'archiviazione dati o le comunicazioni telematiche, ovvero faccia uso dei suddetti dispositivi, è punito con la reclusione da sei mesi ad un anno e con la multa da lire 500.000 a lire 2 milioni. Se il fatto di cui al presente articolo è compiuto a fini di lucro la pena è aumentata.

Il delitto è punibile a querela della persona offesa ».

ART. 3.

1. Dopo l'articolo 623-*ter* del codice penale, introdotto dall'articolo 2 della presente legge, è inserito il seguente:

« ART. 623-*quater* *(Alterazione dell'integrità dei dati, dei programmi e della rete di trasmissione).* – Chiunque, accedendo ad un dispositivo di cui all'articolo 623-*ter*,

preleva o introduce o sopprime o modifica, senza autorizzazione, dati ovvero altera o copia o cancella i programmi di gestione dei dati stessi o manomette i programmi o la rete di trasmissione dei dati o vi introduce interferenze, è punito con la reclusione da 1 a 4 anni e con la multa da 1 a 10 milioni di lire.

Se il fatto di cui al presente articolo è compiuto a fini di lucro la pena è aumentata.

Il delitto è punibile a querela della persona offesa ».

ART. 4.

1. Dopo l'articolo 623-*quater* del codice penale, introdotto dall'articolo 3 della presente legge, è inserito il seguente:

« ART. 623-*quinquies (Falsificazione dei documenti personali informatici)*. – Chiunque falsifica documenti personali informatici e comunque quei documenti che consentono al dispositivo di cui all'articolo 623-*ter* il riconoscimento della persona, quale che sia la loro forma, ovvero fa uso dei suddetti documenti falsificati, è punito con la reclusione da 1 a 5 anni e con la multa da 1 a 10 milioni di lire ».

ART. 5.

1. Dopo l'articolo 623-*quinquies* del codice penale, introdotto dall'articolo 4 della presente legge, è inserito il seguente:

« ART. 623-*sexies (Reati compiuti dall'addetto ad un servizio informatico o telematico)*. – L'addetto ad un dispositivo di cui all'articolo 623-*bis* che, abusando della sua qualità, commette alcuno dei fatti previsti nella presente sezione o viola, sottrae, sopprime la corrispondenza o i dati di proprietà degli utenti del dispositivo o comunque compie atti che provocano danni a terzi, è punito con la reclusione da 1 a 5 anni e con la multa da lire 500.000 a lire 10 milioni.

Se il fatto di cui al presente articolo è compiuto a fini di lucro la pena è aumentata ».

ART. 6.

1. Dopo l'articolo 623-*sexies* del codice penale, introdotto dall'articolo 5 della presente legge, è inserito il seguente:

« ART. 623-*septies* *(Liquidazione provvisoria del danno)*. – Qualora la commissione di taluno dei reati di cui alla presente sezione abbia cagionato un danno patrimoniale di rilevante gravità, il danneggiato che abbia agito in sede civile ovvero si sia costituito parte civile nel procedimento penale, può chiedere, nel corso del giudizio di primo grado, che gli sia assegnata una somma da imputarsi nella liquidazione definitiva del danno.

Tale somma non può essere superiore ai due terzi della presumibile entità del risarcimento che sarà liquidato con la sentenza.

Può altresì richiedere la liquidazione della somma di cui ai commi che precedono, indipendentemente dalla rilevante gravità del danno patrimoniale, il danneggiato che, a causa del reato commesso, si trovi comunque in stato di notevole bisogno.

È competente a decidere sulla richiesta, sentite le parti, in sede civile, il giudice istruttore con ordinanza, ovvero il collegio, con sentenza, se la domanda è proposta all'udienza di precisazione delle conclusioni; in sede penale, il giudice all'esito dell'udienza preliminare, contestualmente e subordinatamente al rinvio a giudizio dell'imputato, ovvero il tribunale qualora la richiesta sia stata riproposta per la prima volta, fino alla discussione finale. In tale ultimo caso, il tribunale decide contestualmente alla deliberazione della sentenza, negli altri casi decide immediatamente con ordinanza.

Sia nel giudizio civile che nel giudizio penale, la richiesta non può essere riproposta innanzi al medesimo giudice e, comunque, non più di una volta.

Nel caso di giudizio abbreviato, è competente a decidere il giudice dell'udienza preliminare, contestualmente alle deliberazioni della sentenza. Nel caso di giudizio immediato, è competente il tribunale.

L'ordinanza, ovvero il capo della sentenza, con i quali si delibera la liquidazione provvisoria del danno sono provvisoriamente esecutivi.

L'ordinanza di cui al quarto comma è impugnabile, in sede civile ai sensi dell'articolo 178 del codice di procedura civile, in sede penale ai sensi dell'articolo 310 del codice di procedura penale. L'impugnazione non sospende l'esecutività dell'ordinanza. Non è ammesso ricorso per Cassazione ».