CAMERA DEI DEPUTATI N. 2773

DISEGNO DI LEGGE

PRESENTATO DAL MINISTRO DI GRAZIA E GIUSTIZIA

(CONSO)

—

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

Già presentato al Senato della Repubblica il 26 marzo 1993 e successivamente trasferito alla Camera dei deputati l'11 giugno 1993.

ONOREVOLI DEPUTATI ! — Lo sviluppo delle nuove tecnologie informatiche e telematiche ed il loro impatto con la società moderna rendono ormai indispensabile una specifica regolazione del fenomeno, affinché siano introdotte più chiare regole alle quali informare i comportamenti.

Il ritardo con il quale vengono di regola affrontati tali problemi dipende essenzialmente dalla maggiore velocità con la quale, rispetto alla produzione normativa, si evolve la tecnologia dei sistemi informatici e telematici.

L'uso di tali sistemi ha tuttavia pervaso le principali attività che vengono svolte nella società moderna, ed una serie sempre più ampia di indicatori lascia prevedere un impatto della risorsa tecnologica più forte e condizionante.

Le conseguenze sono rappresentate dalla maggiore rilevanza dei c.d. sistemi complessi, in quanto basati sull'integrazione delle nuove tecnologie nei principali processi produttivi, che hanno fatto sorgere una domanda di certezza e protezione non prevedibile solo alcuni anni fa.

La tendenza di tali tecnologie ad una convergenza e ad una forte integrazione delle componenti *hardware* e *software* in un processo globale induce ad affrontare la materia con un approccio di ampia portata che consideri:

i sistemi informatici di qualunque tipo o dimensione, comprendendo in tale accezione sia sistemi di scrittura o di automazione d'ufficio ad uso individuale o particolare, sia complessi sistemi di elaborazione dati in grado di fornire servizi e

potenza di calcolo a migliaia di utenti, sull'intero territorio nazionale ed anche oltre i confini del Paese;

i sistemi telematici, includendo in tale accezione reti di telecomunicazione sia pubbliche che private, « locali » o « geografiche », nazionali o internazionali, operanti da e per il nostro paese, ed ogni altra loro componente *(software,* dati, informazioni, flussi di comunicazione, messaggi eccetera);

il *software,* sia esso di base, di supporto, « generalizzato » o « applicativo », inglobando nel concetto qualunque programma informatico realizzato dal costruttore dell'*hardware,* da strutture di produzioni *ad hoc,* da singoli utenti e registrato sui supporti più vari, dal singolo semiconduttore ai supporti di memorizzazione magnetici, ottici o di altra natura;

il patrimonio informatico dei sopradetti sistemi che di essi rappresenta oggi la sfera più esposta in quanto non facilmente ricostruibile in molti dei casi poiché rappresentato, ad esempio, da un puro flusso di comunicazioni scambiato tra due o più utenti senza che ne sia prevista una specifica registrazione; in tale accezione vengono ricomprese informazioni, dati elementari, immagini, suoni e quant'altro possa essere registrato, elaborato o scambiato mediante sistemi informatici o telematici di qualunque tipo o dimensione.

Un elemento da considerare, si è detto, è rappresentato dal valore sempre maggiore che assumono tali sistemi, il *software* ed il patrimonio informatico dei singoli e delle organizzazioni: fortemente dipendenti dalle tecnologie informatiche appaiono, in particolare, taluni settori di rilevante interesse nell'economia nazionale.

Il primo di essi è rappresentato da quello assicurativo ove, accanto alla tradizionale presenza dei sistemi informativi per la gestione delle polizze e delle correlate attività amministrative e contabili, si rileva la tendenza allo sviluppo di dati comuni a tutto il ramo di reti telematiche di notevoli dimensioni e di sistemi di automazione d'ufficio particolarmente evoluti, fino a giungere a sistemi esperti per la valutazione del rischio ed al calcolo dei premi relativi.

Il settore del credito e della finanza, che sembra essere in proposito uno dei più colpiti da fenomeni criminosi, è anch'esso diffusamente ancorato a tecnologie informatiche e telematiche, a causa della necessità, determinata anche dalla globalizzazione o internazionalizzazione dei mercati finanziari, di disporre di informazioni e notizie in tempo reale ed in modo continuativo, attraverso reti interbancarie che ormai collegano il mondo intero. In questi ultimi anni, inoltre, l'ampia diffusione di nuove modalità di pagamento e delle carte a microprocessore (di credito, di debito o di prelievo) ha reso questo settore ancor più dipendente dai sistemi telematici e quindi, entro certi limiti, più vulnerabile nei confronti di azioni delittuose quali l'intrusione nelle reti, l'intercettazione di messaggi, le frodi, i danneggiamenti ed i sabotaggi.

L'area industriale, che è stata tra quelle trainanti dell'automazione in generale, applicata sia ai processi produttivi che a quelli amministrativo-contabili, sta facendo sempre più ricorso all'informatica sia per integrare la totalità delle risorse tecnologiche esistenti attraverso reti « locali » o « geografiche », sia per avviare la realizzazione di un nuovo tipo di fabbrica, c.d. « automatica ».

Nell'ambito della pubblica amministrazione, poi, malgrado il ritardo con il quale le nuove tecnologie sono entrate nel sistema informativo e di governo, si è comunque in presenza di una cospicua diffusione dei sistemi informatici, in particolare nei dicasteri delle Finanze, del Tesoro, della Difesa e della Giustizia, nonché in quello di enti previdenziali quali l'INPS e l'INAIL.

Il settore del trasporto aereo, ferroviario, metropolitano e marittimo è parimenti partecipe di un processo che coinvolge strutture ed infrastrutture vitali per la gestione delle merci e dei passeggeri,

per il controllo del traffico, per i sistemi di sicurezza e di allarme, per la manutenzione e la guida dei mezzi.

I comparti della sanità e dell'ambiente, con specifico riferimento alle funzioni diagnostiche e terapeutiche e al monitoraggio, sia locale che « remoto », si apprestano poi a divenire quelli nei quali l'informatica e la telematica giocheranno in futuro un ruolo sempre più importante, e i problemi di riservatezza e di accesso alle informazioni si porranno sempre più in evidenza.

Da questa breve, e certamente non completa elencazione di settori ove più estesa appare la presenza dell'informatica, risulta evidente come l'intrusione nei sistemi informatici o telematici o il sabotaggio degli stessi, possono provocare danni notevoli alla vita economica e sociale del Paese.

È quindi necessario, in relazione a tale stadio di evoluzione tecnologica, individuare adeguate norme che consentano allo Stato e alla società civile di difendersi da comportamenti che, in quanto incidenti su sistemi di vitale rilevanza, rappresentano un gravissimo pericolo per la collettività intera.

* * *

Il disegno di legge che si propone affronta il compito di delineare alcune nuove figure di reato in riferimento alle più diffuse e gravi attività lesive di interessi di particolare rilievo nel settore informatico.

Con questa finalità, si è dovuto preliminarmente affrontare varie questioni di carattere generale.

Un primo problema è nato a seguito della scelta, nell'ambito del più ampio disegno di politica penale volto ad arginare la sempre più ampia tendenza alla decodificazione, di modificare il codice penale e non di promuovere una legge penale speciale. È stato necessario, quindi, stabilire se le nuove figure di reato da introdurre nel codice penale dovessero essere inserite in un apposito titolo del libro II (ad es. il XIV, ove, naturalmente, si fosse trattato solo di delitti) da destinare esclusivamente ad esse; o se, invece, fosse preferibile ricondurre i nuovi reati alle figure già esistenti che ad essi, pur nella loro autonomia, appaiano più vicine.

Si è ritenuta preferibile la seconda soluzione, nella convinzione che la particolarità della materia non costituisse ragione sufficiente per la configurazione di uno specifico titolo; d'altra parte, il criterio seguito dal legislatore del 1930 nel prevedere i vari raggruppamenti dei reati è ispirato all'unità dell'oggetto giuridico, inteso quanto meno come unico interesse di categoria, mentre le figure da introdurre sono apparse subito soltanto quali nuove forme di aggressione, caratterizzate dal mezzo o dall'oggetto materiale, ai beni giuridici (patrimonio, fede pubblica, eccetera) già oggetto di tutela nelle diverse parti del corpo del codice. Tale ipotesi, poi, appariva anche la sola praticabile per il caso, peraltro non verificatosi, che si fossero dovute introdurre figure contravvenzionali.

Altra questione si è posta in conseguenza della necessità di delimitare il campo dell'intervento di integrazione normativa.

Come è noto, infatti, nel quadro degli illeciti informatici si distinguono i fatti commessi *sul* sistema informatico (o su sue parti o accessori) da quelli commessi *col mezzo* del sistema. Rientra nel primo sottogruppo, ad esempio l'abusiva utilizzazione del *software* mentre si inquadrano nel secondo – anzi ne costituiscono la categoria più importante – quelli commessi tramite abuso delle banche dati e dunque, in prevalenza, lesivi della c.d. *riservatezza informatica*.

Per entrambi le categorie, vi è già, è vero una normativa penale disponibile. Ad esempio, oltre alla specifica ipotesi di cui all'articolo 420 del codice penale relativa all'*hardware*, quanto alla tutela penale del *software*, la Corte di cassazione (Sez. III, 24 novembre 1986, Pompa), ha ritenuto applicabili le disposizioni penali della legge sul diritto d'autore (articolo 171, legge 22 aprile 1941, n. 633). In ordine alla riservatezza, il legislatore italiano non

è del resto apparso insensibile alle esigenze determinate dalle nuove tecnologie, avendo inserita una apposita figura di reato nel nuovo ordinamento della pubblica sicurezza di cui alla legge 1° aprile 1981, n. 121, l'articolo 12 della quale punisce, salvo che il fatto costituisca più grave reato, con la reclusione da 1 a 3 anni (o se il fatto è commesso per colpa, fino a 6 mesi) il pubblico ufficiale che comunica o fa uso di dati ed informazioni in violazione delle disposizioni della stessa legge o al di fuori dei fini da essa previsti.

Ma tali normative non sono certo sufficienti. Quanto alla tutela penale del *software*, infatti, l'indirizzo della Suprema Corte non appare consolidato, onde, a parte la necessità di una adeguata previsione sanzionatoria, le permanenti incertezze sono già ragione sufficiente per intervenire con apposita norma. In relazione alla tutela della riservatezza informatica, poi, il problema resta per le altre banche-dati pubbliche, per quelle private e, comunque, per le ulteriori figure o condotte criminose – diverse da quelle di cui al ricordato articolo 12 – certamente ipotizzabili in proposito.

Un ulteriore aspetto problematico è connesso alla necessità di adeguare la legislazione italiana alle direttive impartite da organismi sopranazionali cui l'Italia aderisce. Nella materia dei reati informatici il Consiglio d'Europa ha proposto due diverse liste di reati da introdurre, una « minima » e l'altra facoltativa: occorreva operare una scelta e, come si vedrà, si è ritenuto di non poter limitare la previsione dei nuovi reati alla prima.

Si è dovuto inoltre avere riguardo alla necessità di coordinare le disposizioni da inserire nel codice penale col nuovo codice di procedura penale: in materia di intercettazioni telefoniche, le disposizioni della legge processuale risulterebbero infatti incomplete ove non integrate in concomitanza delle nuove figure sostanziali di reato. Ed è quanto, appunto, si è fatto con la proposta di introduzione dell'articolo 266-*bis* e di modifica dell'articolo 268 del nuovo codice di procedura penale.

L'operazione più delicata è, peraltro, risultata quella di individuare i comportamenti ai quali attribuire rilevanza penale: ciò sotto vari aspetti.

La scelta normativa conseguente al citato deliberato del Consiglio d'Europa non risultava anzitutto di semplice risoluzione, implicando anche un'accurata valutazione di meritevolezza della sanzione penale rispetto al possibile uso della mera sanzione amministrativa.

Nell'ambito di tale opzione si sono peraltro seguite le indicazioni contenute nella circolare della Presidenza del Consiglio in data 19 dicembre 1983, com'è noto ispirate ai principi di proporzione e di sussidiarietà, e rapportate al rango dell'interesse da tutelare ed al grado dell'offesa (principio di proporzione) nonché alla inevitabilità della sanzione penale, quale ultima *ratio* (principio di sussidiarietà).

Non può, peraltro, omettersi di considerare che la criminalizzazione, quantomeno dei più gravi tra i fatti rientranti nella criminalità informatica, si giustifica anche in riferimento alla cooperazione internazionale. È noto infatti che, sia ai fini della estradizione che di altre forme di collaborazione giudiziaria penale, è di regola richiesta la previsione bilaterale del fatto (c.d. doppia incriminazione) onde, in mancanza di una apposita norma incriminatrice, lo Stato italiano dovrebbe negare la propria cooperazione agli Stati richiedenti che abbiano già previsto i reati informatici, assenti nella nostra normativa. Al riguardo va chiarito che, in questi ultimi anni, numerosi stati europei ed extraeuropei si sono dati una specifica legislazione penale in materia di criminalità informatica (Austria, Danimarca, Finlandia, Francia, Grecia, Irlanda, Norvegia, Regno Unito, Repubblica Federale di Germania, Svezia, Stati Uniti d'America, Australia, Canada, Giappone).

Quanto all'ulteriore scelta circa la configurazione delle nuove figure criminose quali delitti o contravvenzioni, sono stati seguiti gli ulteriori criteri orientativi enunciati nella circolare della Presidenza del Consiglio del 5 febbraio 1986. Ne è derivata l'esclusione di fattispecie contrav-

venzionali non risultando, tra le figure delle quali si ritiene di proporre l'inserzione nel codice penale, nè ipotesi cui destinare norme di carattere preventivo cautelare nè fattispecie concernenti la disciplina di attività soggette ad un potere amministrativo: ciò anche perché la novella proposta non si configura quale intervento penale in sede di disciplina normativo-amministrativistica della materia.

Si è dovuto inoltre verificare quali condotte, tra quelle rientranti nel fenomeno della criminalità informatica, fossero già dotate di rilevanza penale in base alle norme vigenti; operazione esegetica che, per il divieto di analogia in campo penale, ha richiesto un rigoroso confronto tra i fatti emersi dall'esperienza pratica e le norme penali disponibili.

È opportuno ricordare che i comportamenti indicati dal Consiglio d'Europa nella c.d. *lista minima* sono i più significativi nel quadro delle nuove esigenze di tutela e consistono, stando alla terminologia ed ai concetti ivi adoperati, nelle seguenti tipologia di fatti;

frode informatica (intesa quale ingresso, alterazione, cancellazione o soppressione di dati o di programmi informatici, o qualsiasi altra ingerenza in un trattamento informatico che ne influenzi il risultato e che determini, per ciò stesso, un pregiudizio economico o materiale ad un'altra persona, effettuati con l'intento di ottenere un vantaggio economico illegittimo per sè stesso o per altri);

falso informatico (ingresso, alterazione, cancellazione o soppressione di dati o programmi informatici o qualsiasi altra ingerenza nel trattamento informatico, effettuati con modalità o condizioni tali da costituire, secondo il diritto nazionale, un reato di falso qualora i fatti stessi fossero commessi nei riguardi di uno degli oggetti tradizionali di questo tipo di infrazione);

danneggiamento riguardante dati o programmi informatici (cancellazione, danneggiamento, deterioramento o soppressione senza diritto di dati o programmi informatici);

sabotaggio informatico (ingresso, alterazione, cancellazione o soppressione di dati o programmi informatici ovvero ingerenza nei sistemi informatici, con l'intenzione di ostacolare il funzionamento di un sistema informatico o di un sistema di telecomunicazioni);

accesso non autorizzato (accesso senza diritto ad un sistema o ad una rete informatica mediante violazione delle regole di sicurezza);

intercettazione non autorizzata (intercettazione, senza diritto e mediante mezzi tecnici, di comunicazioni inviate, provenienti o esistenti nell'interno di un sistema o di una rete informatica);

riproduzione non autorizzata di un programma informatico protetto (riproduzione, diffusione o comunicazione al pubblico, senza diritto, di un programma informatico protetto dalla legge);

riproduzione non autorizzata di una topografia (riproduzione, senza diritto, della topografia, protetta dalla legge, di un prodotto a semiconduttore o sfruttamento commerciale ovvero importazione a questo scopo, senza diritto, di una topografia o di un prodotto semiconduttore fabbricato con l'aiuto di tale topografia).

Del pari meritevoli di interesse, ai fini della repressione della criminalità informatica, appaiono le ipotesi elencate nella c.d. lista facoltativa, e cioè:

alterazione dei dati o dei programmi informatici (alterazione senza diritto di dati o programmi informatici);

spionaggio informatico (ottenimento, mediante mezzi illegittimi, divulgazione non autorizzata, trasferimento o utilizzazione senza diritto nè altra giustificazione legale, di un segreto commerciale o industriale, con l'intenzione di causare un pregiudizio economico all'avente diritto al segreto o di ottenere per sè stesso o per altri un vantaggio economico illecito);

utilizzazione non autorizzata di un elaboratore (utilizzazione senza diritto di

un sistema o di una rete informatica effettuata:*(a)* accettando un rischio rilevante di causare un pregiudizio a colui che ha diritto di utilizzare il sistema o di arrecare pregiudizio al sistema o al suo funzionamento, ovvero, *(b)*, con l'intenzione di creare un pregiudizio alla persona che ha diritto di utilizzare il sistema o al suo funzionamento, ovvero, *(c)*, causando in tal modo un pregiudizio alla persona che ha diritto di utilizzare il sistema o arrecando un pregiudizio al sistema o al suo funzionamento);

utilizzazione non autorizzata di un programma informatico protetto (utilizzazione, senza diritto, di un programma protetto dalla legge e riprodotto senza diritto, con l'intenzione di ottenere un vantaggio economico illecito per se stesso o per altri, o di causare un pregiudizio al detentore di tale diritto).

Alcuni dei comportamenti sopra indicati possono essere ricondotti a norme penali vigenti. Anzitutto, trovano già riscontro all'interno del codice penale le condotte di impossessamento aventi ad oggetto cose materiali attinenti ai sistemi informatici: e, quindi, parte dell'*hardware* o del *software*, considerati nella loro materialità. A tali comportamenti, infatti, appare applicabile la norma incriminatrice sul furto (articolo 624 del codice penale).

Non così, invece, per le condotte di sottrazione di dati, programmi e informazioni. In tali casi, l'articolo 624 del codice penale appare di dubbia applicabilità, pur nell'ampio concetto di « cosa mobile » da esso previsto: stando alla definizione contenuta nel secondo comma di tale disposizione, l'estensione del concetto non va oltre le « energie » (tra cui quella elettrica) aventi valore economico, tra le quali i dati o le informazioni non sono sussimibili.

Del resto, 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 violazione dei segreti. Ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio (articolo 614 del codice penale), eccetera.

Paiono del pari al di fuori delle attuali previsioni sia l'intercettazione di comunicazioni interessanti sistemi informatici sia l'uso di apparecchiature informatiche per fini personali: la prima, perché le norme penali disponibili (articoli 617 e seguenti del codice penale) riguardano comunicazioni tra persone e non tra persone e macchine o tra macchine; il secondo, perché la norma sul furto d'uso (articolo 626, primo comma, del codice penale) – a parte ogni ulteriore requisito (quale il solo scopo di uso momentaneo e la immediata restituzione) – presuppone pur sempre la sottrazione di una cosa mobile che venga, appunto, usata e restituita, mentre nel caso di specie l'impianto non viene asportato e ciò che l'agente ricava dalla condotta illecita e, in definitiva, « sottrae », è appunto una notizia, di dubbia qualificabilità, agli effetti della legge penale, quale « cosa ».

Anche i fatti di danneggiamento dei sistemi informatici trovano collocazione, sebbene la disciplina merita di essere integrata e adattata alle particolarità dei fatti stessi, nell'ambito delle norme penali esistenti. Risultano, così, utilizzabili sia l'articolo 635 che l'articolo 420 del codice penale.

Queste disposizioni, peraltro, non sembrano sufficienti a coprire l'intera fenomenologia del danneggiamento, restando, ad esempio, fuori delle rispettive previsioni i casi in cui oggetto del reato non sia l'*hardware*. In particolare, quanto alla cancellazione o alterazione del *software*, è opportuno ricordare che la giurisprudenza di merito ha ritenuto talora ravvisabile il delitto di attentato ad impianti di ricerca e di elaborazione di dati (G.I. Firenze, 27 gennaio 1986, Pasqui); altre volte il delitto di danneggiamento, considerando il programma indivisibile dell'*hardware* (Pret. Torino, 23 ottobre 1989, Vincenti ed altro), talaltra infine quello di esercizio ar-

bitrario delle proprie ragioni con violenza sulle cose (articolo 392 del codice penale: Trib. Torino, 12 dicembre 1983, Basile ed altro).

Quanto alle c.d. « truffe » ai danni del *computer*, la loro riconducibilità all'articolo 640 del codice penale è risultata assai dubbia. Vi è di ostacolo la considerazione che il « taluno », al quale la norma in questione riferisce la induzione in errore, non può che essere una persona fisica: onde, quanto l'*output* non è controllato direttamente dall'uomo, un tale estremo non sembra ricorrere. E, malgrado i tentativi di adattare la norma, sostenendo che, in realtà, nei casi in questione l'uomo ha già espresso il proprio consenso, condizionandolo all'operatività di un determinato meccanismo che, invece, nel fatto in questione viene alterato, resta pur sempre valida la obiezione che si tratta di una forzatura della norma, inaccettabile a cagione del divieto di analogia.

Va, comunque, ricordato che, nella giurisprudenza di merito, l'articolo 640 è stato ritenuto applicabile in un caso riguardante l'immissione nell'elaboratore elettronico dell'INPS di dati non veritieri relativi a contributi in realtà non versati (Trib. Roma, 20 giugno 1985, Testa ed altri), ove si è peraltro ritenuto che in tal modo venivano ingannati i dipendenti preposti al controllo del versamento dei contributi e all'esazione degli stessi, e non certo il *computer*.

Ed ancora, è stata ravvisata la truffa aggravata nel caso di un dipendente bancario che, inserendo falsi dati nell'elaboratore, otteneva che risultassero come avvenuti per contanti versamenti effettuati mediante assegni, al fine di occultare il maggior rischio assunto con la negoziazione di assegni prima che ne fosse stata confermata la copertura e per procurare il maggior lucro ai correntisti attraverso il riconoscimento della valuta liquida (Trib. Roma, 14 dicembre 1985, Manenti ed altri). Ma anche in tal caso si è ritenuto che fossero ingannati gli organi di controllo della banca e non il *computer*. Va osservato infine che la tutela di cui agli articoli 420, 635-*bis* e 640-*ter* va estesa anche ai programmi, informazioni e dati archiviati separatamente per ragioni di sicurezza e che hanno lo scopo di consentire, ove del caso, il ripristino del funzionamento del sistema.

Le considerazioni sin qui svolte, alle quali altre potrebbero aggiungersi, in tema di falso documentale, eccetera, sono sufficientemente indicative di come, in sostanza, il sistema penale vigente richieda adattamenti ed integrazioni necessari perché fatti criminosi di rilevante incidenza sociale, attinenti all'articolato e complesso mondo dell'informatica, ricevano finalmente un'adeguata risposta punitiva.

Le norme del provvedimento che si sottopone all'approvazione del Parlamento rispondono alle esigenze sopra indicate per la cui analitica illustrazione si osserva quanto appresso.

Con l'articolo 1 del disegno di legge si inserisce, all'articolo 392 del codice penale, un comma con il quale viene estesa, agli effetti della legge penale, la nozione legale della « violenza sulle cose », già comprensiva dei fatti di danneggiamento, trasformazione o mutamento di destinazione, ad una serie di comportamenti incidenti su programmi informatici o sul funzionamento di sistemi informatici o telematici.

La *ratio* di una siffatta integrazione, che incide anche sulla fattispecie del delitto di esercizio arbitrario delle proprie ragioni commesso mediante violenza sulle cose, risiede nella necessità di non lasciare privi di sanzione comportamenti di sicuro rilievo delittuoso e che appaiono assimilabili alle ipotesi di danneggiamento o di mutamento di destinazione. Si tratta, ad esempio, della « mutilazione » o del rendere, anche parzialmente, inservibili programmi informatici in ordine al quale l'agente vanti pretesi diritti, ancorché si trovino nella disponibilità altrui, ovvero dell'impedire o dell'alterare il funzionamento di sistemi informatici o telematici, azioni realizzate con l'intento di esercitare diritti che potrebbero essere fatti valere innanzi al giudice, e per i quali si ricorra, invece, ad una sorta di autotutela, e cioè a quel

« farsi ragione da sè medesimo » che la norma contenuta nell'articolo 392 del codice penale mira appunto a reprimere.

L'inserimento della disposizione che si propone appare connesso alla già sottolineata difficoltà dell'assimilazione dei programmi informatici alle « cose mobili », ond'è che, nonostante qualche tentativo avutosi al riguardo in giurisprudenza, certamente resta assai problematico il sussumere le manifestazioni del particolare fenomeno cui si è fatto cenno nella previsione di reato contenuta nell'articolo 392 del codice penale.

L'articolo 2 del disegno di legge sostituisce l'intero articolo 420 del codice penale, al fine di estendere la tutela penale apprestata dalla norma, sia nell'ipotesi base del delitto nella stessa previsto, che in quella circostanziata, ai sistemi informatici o telematici, nonché ai dati, alle informazioni o ai programmi in essi contenuti.

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 distruggere.

La nuova formulazione della norma è diretta altresì al definitivo chiarimento sulla individuazione dell'oggetto materiale del delitto, essendo sorte – come è noto – non poche perplessità per la indicazione alternativa, contenuta nel primo comma dell'attuale testo dell'articolo 420, degli impianti di ricerca o di elaborazione di dati rispetto a quelli di pubblica utilità. In via del tutto prevalente la dottrina ha ritenuto che la messa in pericolo degli impianti di ricerca e di elaborazione di dati potesse assumere rilevanza, ai fini della configurabilità del delitto di cui all'articolo 420 del codice penale, soltanto nel caso in cui tali impianti, pur appartenendo a privati ed essendo adibiti a finalità private, abbiano tale rilievo sociale che una condotta diretta a danneggiarli non può lasciare indifferente la collettività.

In questa linea si muove la norma che si propone.

Viene espunto, intanto, dalla formulazione del primo comma il riferimento agli impianti di ricerca e di elaborazione dati in maniera da eliminare in radice ogni possibilità di equivoco: la previsione di reato resta, così, limitata, in questa sua prima ipotesi, ai soli attentati aventi ad oggetto impianti, e cioè complessi di strutture, apparecchiature, congegni eccetera, coordinati e concorrenti ad un unico scopo, che abbiano la connotazione dell'essere destinati o ad essere idonei a soddisfare esigenze di pubblica utilità.

Nel secondo comma viene inserita la specifica previsione di reato, punito con identica pena, per il caso in cui lo stesso fatto di cui al primo 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 deve trattarsi di sistemi, dati, eccetera, che, siano essi appartenenti a soggetti pubblici o privati, abbiano complessità e 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.

Nel terzo comma è contenuta la previsione della fattispecie aggravata, unica per entrambe le ipotesi di cui ai commi descritti in precedenza e cioè concernente sia il caso che dall'attentato derivi la distruzione o il danneggiamento o l'interruzione anche parziale del funzionamento dell'impianto, sia che le stesse conseguenze si producano rispetto ai sistemi informatici o telematici ovvero ai dati, alle informazioni o ai programmi in essi contenuti.

Con l'articolo 3 si inserisce, nel capo III del titolo VII del libro II del codice penale la previsione del « falso informatico », e cioè della falsificazione dei documenti informatici.

Tale, agli effetti della legge penale, si ritiene non debba essere considerato il prodotto dell'elaboratore (tabulato), in quanto lo stesso rientra nel novero dei documenti cartacei contemplati dagli arti-

coli 476 e seguenti del codice penale ed essendo dato ormai pacifico in giurisprudenza che la sottoscrizione meccanica deve essere equiparata a quella manuale.

Si è ritenuto, invece, di attribuire la natura di documento informatico ai « supporti » – di qualunque specie essi siano – contenenti dati, informazioni o programmi.

Per tali documenti, certo, si porrà il problema della individuazione della loro paternità, poiché – come è noto – è requisito imprescindibile per la configurabilità del falso penale la riferibilità del documento oggetto del reato alla persona fisica o all'ente da cui esso proviene: la cosiddetta « riconoscibilità dell'autore ». Su tale aspetto, tuttavia, si è preferito rimettere la soluzione del problema alla disciplina che, in sede pubblica o privata, potrà essere dettata a seconda della natura del documento o del contesto in cui esso opererà.

Condizione assoluta a ché 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. Tale condizione infatti, costituisce l'elemento differenziale tra la falsificazione di documenti suscettibili di produrre situazioni di danno o di pericolo per la pubblica fede e quella incidente su documenti privi di ogni rilevanza probatoria, ipotesi che è del tutto innocua rispetto all'interesse protetto e non giustifica l'applicazione di sanzioni punitive.

In ordine alla soluzione normativa proposta, si chiarisce che è apparsa non opportuna la previsione di una serie di ipotesi delittuose, da inserire in corrispondenza a quelle di falso documentale già esistenti, che avessero ad oggetto le diverse falsità materiali o ideologiche su atti pubblici, certificati, attestati, o la falsità in scritture private eccetera. Nè certo sarebbe stata possibile la configurazione di un unico delitto di falso informatico, nella sola considerazione dell'oggetto materiale del reato: si sarebbe ottenuta la inaccettabile conseguenza di sottoporre, ad esempio, ad identico regime sanzionatorio le falsità incidenti su dati informatici pubblici e su quelli privati e nel contempo si sarebbe creata divaricazione tra falsità omogenee (ad esempio concernenti registrazioni di identiche attività da parte di pubblici ufficiali svolgenti eguali operazioni) soltanto differenziate per lo strumento documentale utilizzato (informatico o cartaceo).

La soluzione che si è ritenuto di privilegiare, allora, è stata quella di far riferimento alle disposizioni sulle falsità di atti disponendone l'applicazione anche alle ipotesi in cui le rispettive previsioni riguardino un documento informatico. In tal modo si raggiunge un duplice obiettivo: quello di non mutare la struttura delle fattispecie in funzione della sola diversità dell'oggetto materiale e quello di sottoporre ad identico regime sanzionatorio fatti criminosi che non si differenziano sul piano dell'oggettività giuridica ovvero della natura dell'interesse violato.

L'articolo 4 prevede l'aggiunta al codice penale degli articoli 615-*ter* e 615-*quater*.

Con il primo si punisce l'accesso abusivo ad un sistema informatico o telematico o il mantenimento in esso contro la volontà espressa o tacita dell'avente diritto. La normativa trova la sua collocazione tra i reati contro l'inviolabilità del domicilio perché i sistemi informatici o telematici, la cui violazione essa reprime, costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale.

La tutela è limitata ai sistemi informatici o telematici protetti da misure di sicurezza perché, dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di 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.

Il reato base è punito con la pena della reclusione fino a tre anni, mentre si applica la pena da uno a cinque anni se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con la violazione dei doveri inerenti alla funzione o servizio, da chi esercita anche abusivamente la professione di investigatore privato, ovvero usando la violenza sulle cose o alle persone o essendo palesemente armato.

Il reato è punito con tale maggiore pena anche quando dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento o la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

I sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile, o comunque di rilevante interesse pubblico, godono di una maggiore tutela: l'abusivo accesso ad essi è infatti punito con la reclusione da uno a cinque anni in riferimento all'ipotesi base del reato e con la reclusione da tre a otto anni, nella ipotesi aggravata indicata nel quarto comma.

Se concorrono due o più delle aggravanti prevedute dall'articolo in esame, o se una di tali circostanze concorre con altra fra quelle indicate nell'articolo 61 del codice penale, tra le quali in particolare va ricordata quella di cui al n. 11, si applica la pena della reclusione da tre a dieci anni.

L'ultimo comma dell'articolo prevede la punibilità a querela della persona offesa per l'ipotesi di reato semplice e la procedibilità d'ufficio in tutti i casi di ipotesi delittuose aggravate.

L'articolo 615-*quater*, che completa la tutela prevista dalla norma precedente, punisce l'abusiva acquisizione in qualunque modo (anche mediante autonoma elaborazione) e diffusione di codici di accesso a sistemi informatici o telematici protetti da misure di sicurezza, da intendersi nel senso già chiarito a proposito dell'articolo 615-*ter*, con la reclusione sino ad un anno e con la multa fino a lire dieci milioni.

Per la configurabilità del delitto è richiesto il dolo specifico, consistente nel fine di procurare un profitto a sè o ad altri, o di arrecare ad altri un danno.

Alle ipotesi precedenti sono equiparate la comunicazione e consegna di codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, o la fornitura di indicazioni o istruzioni idonee allo scopo.

La previsione è, per un certo verso, analoga a quella di cui al terzo comma dell'articolo 9 della legge 8 aprile 1974, n. 98.

L'articolo 4 introduce infine l'articolo 615-*quinquies*.

È apparso infatti opportuno reprimere specificamente anche il comportamento, molto pericoloso nella pratica, di colui che comunque diffonde uno dei così detti « programmi virus », il cui scopo o il cui effetto, come è noto, è quello di provocare un danneggiamento o un'alterazione dell'« hardware » o del « software » o dei dati e delle informazioni contenute nel sistema informatico o telematico ovvero di interrompere o di alterare, in modo totale o parziale, il funzionamento del sistema stesso.

L'articolo 5 del disegno di legge sostituisce il quarto comma dell'articolo 616 del codice penale ed estende la nozione di corrispondenza alle comunicazioni informatiche o telematiche, ovvero effettuate con ogni altra forma di comunicazione a distanza.

L'articolo 6 introduce gli articoli 617-*quater*, 617-*quinquies* e 617-*sexies* del codice penale che estendono la tutela prevista dall'articolo 617 del codice penale per le comunicazioni telefoniche o telegrafiche a quelle informatiche o telematiche.

L'articolo 617-*quater* punisce con la reclusione da sei mesi a quattro anni chi fraudolentemente intercetta, interrompe o impedisce comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi. La stessa pena si applica, salvo che il fatto costituisca più grave reato, a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, le comuni-

cazioni informatiche o telematiche intercettate. Entrambi i delitti sono punibili a querela della persona offesa.

Scatta invece la procedibilità d'ufficio, e la pena è della reclusione da uno a cinque anni, se il fatto è commesso in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico, o da impresa esercente servizi pubblici o di pubblica necessità o se il fatto è commesso da un pubblico ufficiale o da un incaricato di pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero da chi esercita anche abusivamente la professione di investigatore privato.

L'installazione di apparecchiature atte ad intercettare, impedire, o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punita dall'articolo 617-*quinquies* con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni se ricorre una delle circostanze aggravanti di cui all'articolo 617-*quater*.

L'articolo 617-*sexies* reprime la falsificazione, l'alterazione o la soppressione, in tutto o in parte, del contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, qualora se ne faccia uso o si lasci che altri ne faccia uso.

È richiesto il dolo specifico, consistente nel fine di procurare a sè o ad altri un vantaggio o di arrecare ad altri un danno. La pena è della reclusione da uno a quattro anni nell'ipotesi di reato semplice e della reclusione da uno a cinque anni laddove ricorra, anche in questo caso, una delle circostanze aggravanti di cui all'articolo 617-*quater*.

Gli articoli 7 e 8 completano la repressione della criminalità informatica estendendo la tutela dell'inviolabilità dei segreti ai supporti informatici e a qualsiasi altra forma di trasmissione a distanza di suoni, immagini o altri dati.

L'articolo 7 infatti amplia, ai fini della tutela del segreto, il concetto di documento, aggiungendo all'articolo 621 del codice penale un secondo comma per effetto del quale qualunque supporto informatico, contenente dati, informazioni o programmi, è considerato documento.

L'articolo 8 sostituisce il testo dell'articolo 623-*bis* del codice penale stabilendo che le disposizioni sulla tutela dell'inviolabilità dei segreti relative alle comunicazioni e conversazioni telegrafiche, telefoniche e informatiche si applicano a qualunque altra trasmissione a distanza di suoni, immagini o altri dati. Viene così eliminato il riferimento alla trasmissione effettuata con collegamento su filo o ad onde guidate, contenuto nell'attuale testo della norma, che aveva dato luogo a divergenti interpretazioni giurisprudenziali e si era rivelato sostanzialmente inidoneo ad assicurare una adeguata tutela in materia.

L'articolo 9 del disegno di legge introduce nel codice penale l'articolo 635-*bis* il quale, in rapporto di specialità con la comune fattispecie di danneggiamento (articolo 635 del codice penale) e salva la sussistenza di un più grave reato (quale, ad esempio, quello di cui all'articolo 420 del codice penale), sanziona più gravemente ed in via autonoma il reato di danneggiamento allorché l'oggetto materiale della condotta è costituito da sistemi informatici e telematici ovvero da programmi, informazioni o dati altrui. L'accentuato disvalore del fatto rende il reato perseguibile *ex officio* anche nell'ipotesi base. Le circostanze di cui al secondo comma dell'articolo 635 sono, quindi, recettiziamente richiamate nel comma secondo della nuova disposizione al solo fine dell'aumento di pena.

La scelta di rendere comunque perseguibile d'ufficio il reato è determinata dalla esigenza di poter colpire efficacemente questo settore della criminalità informatica atteso che il regolare funzionamento dei sistemi informatici e telematici, anche privati, è di interesse non strettamente singolare ma della collettività intera, e che la più diffusa conoscenza del fenomeno consentirà, come già rilevato in sede internazionale, di rendere sempre più perfettibile da parte dei soggetti interes-

sati, la predisposizione di adeguati mezzi di protezione e l'affinamento delle tecniche investigative.

Riguardato alla luce della nuova formulazione prospettata per l'articolo 420 del codice penale, il rapporto tra le due ipotesi delittuose, soprattutto in riferimento alla problematica dei cosiddetti delitti di attentato, rimane immune data anche la permanente connotazione del danneggiamento quale reato di evento.

La discussa configurabilità del reato di truffa (articolo 640 del codice penale) in caso di analogo illecito « informatico », in particolare come s'è detto per l'aspetto attinente all'induzione in errore, impone per detto illecito la creazione di una nuova figura di reato (articolo 10) nella quale la comune condotta di artificio o raggiro è più specificamente integrata dall'alterazione di un sistema informatico o telematico o dall'abusivo intervento con ogni mezzo effettuato su dati, informazioni o programmi contenuti in detti sistemi.

Per la nuova ipotesi che, al pari della truffa, è collocata nel libro secondo, titolo XIII, capo II del codice (« dei delitti contro il patrimonio mediante frode«) e richiede anch'essa l'avvenuto conseguimento del perseguito profitto, le nozioni di « ingiustizia » del danno e di « altruità » sono mutuabili dalla affine fattispecie di cui all'articolo 640 del codice penale, della quale riproduce altresì il regime di procedibilità ed il profilo sanzionatorio.

L'esigenza, già diffusamente illustrata, di approntare più adeguate forme di tutela penale contro la cosiddetta criminalità informatica impone infine, in simmetria e congiuntamente con la proposta rivisitazione delle fattispecie sostanziali del codice penale, una integrazione delle vigenti norme processuali penali in materia di intercettazione, per ciò che attiene all'oggetto di queste ultime o agli strumenti con cui le relative operazioni possono essere condotte.

L'articolo 11 prevede, quanto al primo aspetto, una positiva regolamentazione delle intercettazioni di comunicazione informatiche o telematiche, sancendone l'ammissibilità negli stessi limiti (di pena edittale o per titolo di reato) entro i quali è oggi consentita l'intercettazione di conversazioni o comunicazioni telefoniche o di altre forme di telecomunicazione, estendendone però l'ambito ad altri illeciti comunque commessi per mezzo di tecnologie informatiche o telematiche.

In ordine al secondo profilo, invece, l'articolo 12 contiene una interpolazione dell'articolo 268 del codice di procedura penale, intesa a far sì che le intercettazioni di comunicazioni informatiche o telematiche, allorché consentite dall'introducendo articolo 266-*bis* del codice di procedura penale (e nel pieno rispetto delle garanzie difensive previste dal capo IV del titolo III del libro III dello stesso codice, debitamente integrate in riferimento a questo tipo di intercettazioni), possano essere effettuate, tenuto conto anche di quanto previsto dall'articolo 348 comma 4 del codice di procedura penale, mediante impianti appartenenti a privati, allorché ricorra l'esigenza di disporre di peculiari strutture o di speciali apparecchiature.

L'articolo 13, per esigenze di coordinamento con il settore delle intercettazioni cosiddette preventive, reca una conseguente interpolazione dell'articolo 25-*ter* del decreto-legge n. 306 del 1992, convertito, con modificazioni, dalla legge 7 agosto 1992, n. 356, estendendo questa forma di intercettazione anche ai casi di comunicazioni relative a sistemi informatici o telematici.

DISEGNO DI LEGGE

—

ART. 1.

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

« 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 ».

ART. 2.

1. L'articolo 420 del codice penale è sostituito dal seguente:

« ART. 420. – *(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 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 ».

ART. 3.

1. Dopo l'articolo 491 del codice penale è aggiunto 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 specificamente destinati ad elaborarli ».

ART. 4.

1. Dopo l'articolo 615-*bis* del codice penale sono aggiunti i seguenti:

« ART. 615-*ter*. – *(Accesso abusivo ad 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:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena

è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede di ufficio.

ART. 615-*quater*. – *(Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici)*. – Chiunque, al fine di procurare a sè o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, 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 lire venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del comma quarto dell'articolo 617-*quater*.

ART. 615-*quinquies*. – *(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 essi 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 ».

ART. 5.

1. Nell'articolo 616 del codice penale, il quarto comma è sostituito dal seguente:

« Agli effetti delle disposizioni di questa sezione, per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza ».

ART. 6.

1. Dopo l'articolo 617-*ter* del codice penale sono aggiunti i seguenti:

« ART. 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.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

ART. 617-*quinquies*. – *(Installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche)*. – Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è

punito con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dall'articolo 617-*quater*, quarto comma.

ART. 617-*sexies*. – *(Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche)*. Chiunque, al fine di procurare a sè o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni.

La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-*quater* ».

ART. 7.

1. Nell'articolo 621 del codice penale dopo il primo comma è inserito il seguente:

« Agli effetti della disposizione di cui al primo comma è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi ».

ART. 8.

1. L'articolo 623-*bis* del codice penale è sostituito dal seguente:

« 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 od altri dati ».

ART. 9.

1. Dopo l'articolo 635 del codice penale è aggiunto il seguente:

« ART. 635-*bis*. – *(Danneggiamento di sistemi informatici e telematici)*. – Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave resto, con la pena della reclusione da sei mesi a tre anni.

Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore di un sistema, la pena è della reclusione da uno a quattro anni ».

ART. 10.

1. Dopo l'articolo 640-*bis* del codice penale è aggiunto il seguente:

« ART. 640-*ter*. – *(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 essi pertinenti, procura a sè 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.

La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal secondo comma numero 1 dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore di un sistema.

Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante ».

ART. 11.

1. Dopo l'articolo 266 del codice di procedura penale è aggiunto il seguente:

« ART. 266-*bis*. – *(Intercettazioni di comunicazioni informatiche o telematiche)*. – *1*. Nei procedimenti relativi ai reati indicati nell'articolo 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 ».

ART. 12.

1. L'articolo 268 del codice di procedura penale è così modificato:

a) dopo il comma 3 è inserito il seguente:

« 3-*bis*. Quando si procede a intercettazione di comunicazioni informatiche o telematiche, il pubblico ministero può disporre che le operazioni siano compiute anche mediante impianti appartenenti a privati »;

b) i commi 6, 7 e 8 sono sostituiti dai seguenti:

« 6. Ai difensori delle parti è immediatamente dato avviso che, entro il termine fissato a norma dei commi 4 e 5, hanno facoltà di esaminare gli atti e ascoltare le registrazioni ovvero di prendere cognizione dei flussi di comunicazioni informatiche o telematiche. Scaduto il termine, il giudice dispone l'acquisizione delle conversazioni o dei flussi di comunicazioni informatiche o telematiche indicati dalle parti, che non appaiano manifestamente irrilevanti, procedendo anche di ufficio allo stralcio delle registrazioni e dei verbali di cui è vietata l'utilizzazione. Il pubblico ministero e i difensori hanno diritto di partecipare allo stralcio e sono avvisati almeno ventiquattro ore prima.

7. Il giudice dispone la trascrizione integrale delle registrazioni ovvero la

stampa in forma intellegibile delle informazioni contenute nei flussi di comunicazioni informatiche o telematiche da acquisire, osservando le forme, i modi e le garanzie previsti per l'espletamento delle perizie. Le trascrizioni o le stampe sono inserite nel fascicolo per il dibattimento.

8. I difensori possono estrarre copia delle trascrizioni e fare eseguire la trasposizione della registrazione su nastro magnetico. In caso di intercettazione di flussi di comunicazioni informatiche o telematiche i difensori possono richiedere copia su idoneo supporto dei flussi intercettati, ovvero copia della stampa prevista dal comma 7 ».

ART. 13.

1. Al comma 1 dell'articolo 25-*ter* del decreto-legge 8 giugno 1992, n. 306, convertito, con modificazioni, dalla legge 7 agosto 1992, n. 356, dopo le parole: « e di altre forme di telecomunicazione » sono inserite le seguenti: « ovvero del flusso di comunicazioni relativo a sistemi informatici o telematici ».

Stampato su carta riciclata ecologica

DDL11-2773
Lire 1000