COMMISSIONE II

GIUSTIZIA

20.

SEDUTA DI GIOVEDÌ 1° LUGLIO 1993

PRESIDENZA DEL PRESIDENTE **GIUSEPPE GARGANI**

INDI

DEL VICEPRESIDENTE **ALFONSO MARTUCCI**

INDICE

PAG.

Disegno e proposta di legge (Seguito della discussione e rinvio):

Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica (2773);

Cicciomessere ed altri: 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 (1174) 149

Gargani Giuseppe, *Presidente* 149

Martucci Alfonso, *Presidente* 150

Cicciomessere Roberto (gruppo federalista europeo) 149

La seduta comincia alle 12,55.

(La Commissione approva il processo verbale della seduta precedente).

Seguito della discussione del disegno di legge: Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica (2773); e della proposta di legge Cicciomessere ed altri: 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 (1174).

PRESIDENTE. L'ordine del giorno reca il seguito della discussione abbinata del disegno di legge: « Modifiche ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica », e della proposta di legge d'iniziativa dei deputati Cicciomessere ed altri: « 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 ».

Ricordo che nella seduta del 29 giugno è stata aperta la discussione sulle linee generali ed il relatore, onorevole Diana, ha anticipato alcune considerazioni della sua relazione riservandosi di integrarla nel prosieguo del dibattito.

ROBERTO CICCIOMESSERE. Signor presidente, i provvedimenti in esame si occupano di una serie di attività gestite attraverso l'uso di *computer* e di reti telematiche a tutt'oggi completamente prive di tutela giuridica.

Come ben sapete, esiste un'obiettiva difficoltà della magistratura nell'applicazione analogica di figure di reato già esistenti: non vi è, dunque, alcuna figura penale che consenta di perseguire queste attività criminose che spesso producono danni rilevanti. Penso soprattutto ai reati di truffa e frode, di cui all'articolo 140 del codice penale nel quale si fa esplicito riferimento ad un soggetto danneggiato. Quando, invece, tali attività criminose sono rivolte ai danni di un *computer*, normalmente non si ritiene – almeno questa è la prassi prevalente – di applicare le disposizioni del codice che le contemplano.

Analogo discorso vale per il reato di danneggiamento, di violazione della *privacy* e soprattutto per quello di violazione di domicilio: una delle principali attività criminose in questo settore consiste nell'introdursi abusivamente in un sistema informatico o telematico attraverso il furto della chiave, cioè della cosiddetta *password*. In concreto, ciò significa entrare nel sistema senza autorizzazione, eppure non esiste alcuna possibilità di tutela perché viene assolutamente esclusa l'applicabilità della figura del reato di violazione di domicilio, anche se in linea di massima potrebbe prefigurarsi una somiglianza o un'analogia.

Ci troviamo, quindi, di fronte ad una serie di comportamenti che si realizzano non attraverso atti materiali – quale può essere il danneggiamento fisico o la sottrazione di un bene o ancora la frode nei confronti di una persona fisica – bensì attraverso comportamenti che riguardano beni immateriali come le informazioni contenute in un sistema o l'interruzione dei flussi di comunicazione che intercorrono fra più reti.

Vorrei far rilevare che ciò spesso comporta danni per miliardi. Farò soltanto un esempio: in questa Commissione

c'è un *computer* collegato alla banca dati della Camera che impegna molte decine di persone che manipolano dati del valore di svariati miliardi; credo, infatti, che si tratti di una delle più grandi banche dati esistenti in Italia. Ebbene, se qualcuno si introducesse abusivamente in questo sistema per danneggiarlo o anche solo per cancellare i dati immagazzinati, allo stato della legislazione e dell'interpretazione che ne viene data, il magistrato non potrebbe far nulla perché non potrebbe disporre intercettazioni telematiche e tanto meno intervenire nel momento in cui l'*hacker* – così vengono definiti coloro che compiono questi crimini – sta per introdursi nel sistema.

A prescindere da questo aspetto del problema – a proposito del quale aggiungerò soltanto che esiste una sorta di « pigrizia » interpretativa della magistratura – resta il fatto che questi comportamenti criminosi non vengono puniti. Inoltre, il Consiglio d'Europa ha chiesto espressamente agli Stati di individuare precise figure di reato per questo tipo di attività criminose e così, in questi ultimi anni, numerosi paesi – non soltanto europei – si sono dotati di una specifica legislazione penale in materia di criminalità informatica che contempla tutti i reati elencati nella lista di cui alla raccomandazione del Consiglio d'Europa.

Bene ha fatto dunque il Governo a recepire integralmente queste indicazioni e, quindi, a procedere alla presentazione di un disegno di legge organico che, da un lato, interviene sulle figure di reato già esistenti, estendendole a quelli compiuti attraverso i *computer* e le reti telematiche e, dall'altro, ne introduce di nuove riferite a quei casi che non avrebbero potuto essere perseguiti tramite un intervento sugli articoli del codice già esistenti. Il disegno di legge, inoltre, prevede la possibilità per il giudice – fino ad oggi esclusa – di effettuare intercettazioni telematiche sia per i reati di cui all'articolo 266, sia per tutti quelli commessi mediante l'impiego di tecnologie informatiche.

In linea generale, dunque, esprimo il mio apprezzamento per il disegno di legge, che ha « stazionato » a lungo presso gli uffici del ministero, evidentemente per un approfondimento di tutte le tematiche da esso implicate. Il solo aspetto sul quale esprimo qualche riserva è quello della prevista trascrizione integrale delle registrazioni conseguenti alle intercettazioni telematiche. Tale obbligo può comportare, nel caso in cui vengano registrati flussi di molti milioni di caratteri, la necessità di riempire intere stanze di pezzi di carta. Ritengo che sarebbe più opportuno, apportando una piccola modifica al disegno di legge, lasciare al giudice, in accordo con le parti, la valutazione del supporto (cartaceo o magnetico) sul quale conservare i risultati delle intercettazioni telematiche. Altrimenti, obbligheremmo gli uffici giudiziari ad un lavoro in parte inutile e comunque assolutamente non gestibile dai nostri tribunali, come d'altronde credo da nessuno in nessun paese.

Ribadisco, quindi, il mio giudizio positivo sui provvedimenti in esame – che mi auguro abbiano un iter particolarmente celere – non foss'altro perché ritengo utile che il nostro paese si allinei in tempi brevi a tutti gli altri – europei e non – che dispongono di una specifica legislazione per contrastare quelli che vengono comunemente definiti come *computer crimes*.

PRESIDENTE. Il seguito della discussione è rinviato ad altra seduta.

La seduta termina alle 13,10.

IL CONSIGLIERE CAPO DEL SERVIZIO STENOGRAFIA

DOTT. VINCENZO ARISTA

IL CONSIGLIERE CAPO DEL SERVIZIO DELLE COMMISSIONI PARLAMENTARI

DOTT. PAOLO DE STEFANO

Licenziato per la composizione e la stampa dal Servizio Stenografia il 2 luglio 1993.

STABILIMENTI TIPOGRAFICI CARLO COLOMBO

Stampato su carta riciclata ecologica

STC11-2LG-20
Lire 500