

FRODE INFORMATICA

Una delle caratteristiche salienti dei computer crimes è rappresentata dall'omessa denuncia di un elevatissimo numero di casi (c.d. *cifra nera*).

Secondo alcuni studi americani -sicuramente i più approfonditi del settore- il numero dei casi non denunciati rappresenterebbe una percentuale oscillante intorno all'85%¹.

Sempre secondo tali stime, *“la possibilità che un reato commesso con l'ausilio di mezzi elettronici venga scoperto è di uno su cento, mentre la probabilità di essere condannati è di uno su cinquecento e quella di subire una pena detentiva dopo la condanna, appena di uno su mille.”*

Se poi si considera che i settori maggiormente colpiti sono quello bancario (46,8% dei casi), la pubblica amministrazione (21,87% dei casi; in Italia soprattutto l'I.N.P.S.) e le case da gioco (6,25%), ben si comprende come l'illecito informatico più ricorrente sia la frode informatica². Infatti, se si ha riguardo alle modalità di attuazione dei computer crimes più diffusi, si può constatare che quasi un terzo di tutti i reati elettronici si compie grazie a manipolazioni dell'input (c.d. *data*

¹ Bequai *“Computer crime: a growing serious problem”*, New York, 1976.

² Stime elaborate dalla Ross-Collins Italia S.p.a. su consultazione della banca-dati *“Crime case”*.

diddling), mentre percentuali minori si riferiscono ai reati compiuti con attacchi al sistema operativo (c.d. *asynchronous attack*), ai programmi applicativi (con il metodo del *trap doors* o del *troyan horse*) e alle procedure di emergenza (metodo del *superzapping*). Tali condotte hanno causato danni per molte migliaia di miliardi e, soprattutto, aumentano proporzionalmente alla diffusione delle tecnologie informatiche in settori di importanza strategica, come quello assicurativo e soprattutto quelli del credito e della finanza³.

Tuttavia, *“una valutazione economica accurata è pressoché impossibile, a causa delle particolari caratteristiche di questo nuovo tipo di criminalità: se il numero dei computer crimes appare ancora trascurabile rispetto a quello dei reati tradizionali, è enormemente maggiore la loro potenzialità offensiva. È stato calcolato che la perdita media derivante dalle appropriazioni indebite commesse con l’uso del computer è dieci volte superiore a quella provocata dagli stessi reati con mezzi tradizionali... Sinora il caso più clamoroso è quello perpetrato nel 1973 ai danni della «Equity Funding Corporation of America» di Los Angeles. Il presidente del consiglio di amministrazione ed altri 21 membri dello stesso, intestarono false polizze di*

³ Ross-Collins Italia S.p.a.: si stima che nel 1985 il costo economico di questi reati abbia raggiunto 1.000 miliardi di lire negli Stati Uniti, 130 miliardi in Francia e circa 80 miliardi in Italia.

assicurazione sulla vita a circa 56 mila persone inesistenti o decedute, creando così delle polizze esistenti soltanto nell'archivio dati del calcolatore elettronico della società, che vennero poi vendute ad altre compagnie di assicurazione. I processi che seguirono la scoperta della colossale truffa accertarono perdite per due miliardi e cento milioni di dollari (cioè oltre tremila miliardi di lire).”⁴

Dati ed accadimenti di tale portata suscitarono, nella dottrina penalistica sia italiana che straniera, un'accesissima disputa circa la possibilità di ricondurre le ipotesi in cui l'agente opera indebitamente sul computer, al fine di trarne un ingiusto vantaggio patrimoniale, all'interno del delitto di truffa. Infatti quest'ultimo postula, sia nella nostra legislazione che in quelle straniere⁵, l'induzione di taluno in errore e rimanda, conseguentemente, ad un rapporto interpersonale, fra agente e vittima, non configurabile per i casi in cui gli artifici o i raggiri siano finalizzati all'alterazione di un processo decisionale interamente condotto dall'elaboratore.

Nonostante tali rilievi trovassero concorde la scarna dottrina che si era occupata del problema⁶, la giurisprudenza, preoccupata del fatto che

⁴ Correras-Martucci *“Reati commessi con l'uso del computer”*, Padova, 1986, pag. 35.

⁵ Correras-Martucci *op. cit.*, pag. 95.

⁶ Borruso-D'Aietti AA.VV. *op. cit.*, pagg. 95 e ss.; Borruso *“La tutela del documento e dei dati”*, Milano, 1994, pagg. 34 e 35; L. Picotti *“La falsificazione dei dati informatici”* in *Diritto dell'Informazione e dell'Informatica*, 1985, pagg. 939 e ss.; C. Sarzana *op. cit.*, pag. 206.

pericolose condotte criminali rimanessero impunte, optò per una diversa soluzione. Emblematica è al riguardo una sentenza del Tribunale di Roma del 20 giugno 1985 secondo la quale la truffa sussiste qualora l'immissione di dati non veritieri all'interno di un elaboratore inganni una persona⁷. In sostanza, l'indefettibile rapporto interpersonale, richiesto per la stessa configurabilità del delitto *de quo*, esisterebbe anche per i casi di frode informatica, poiché le manomissioni sull'elaboratore sarebbero sempre finalizzate a rappresentare una falsa realtà ad un altro uomo.

Quantunque le preoccupazioni che hanno portato la giurisprudenza a formulare questa tesi siano pienamente condivisibili, non si può fare a meno di osservare come numerose frodi correlate all'uso del computer escludano in radice qualsiasi rapporto fra agente e vittima del reato. Ciò avviene tutte le volte che il processo decisionale è delegato per intero ad un elaboratore elettronico. A titolo esemplificativo si possono ricordare truffe molto note, come quelle operate con la c.d. *salami technique*, nelle quali l'agente altera il funzionamento dei programmi applicativi e ne trae un ingiusto profitto patrimoniale.

Il legislatore italiano pose fine alle incertezze sulla “*discussa configurabilità del delitto di truffa in caso di analogo illecito*”

⁷ Pubblicata nella rivista *Diritto dell'Informazione e dell'Informatica*, 1986, pagg. 166 e ss.

*informatico”, sottolineando come si imponesse “per detto illecito la creazione di una nuova figura di reato 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 sui dati, informazioni o programmi contenuti in detti sistemi.”*⁸

Queste considerazioni hanno condotto all’introduzione, nel codice penale, di una nuova norma: l’art. 640 -ter.

In quest’ultima, che è assai simile alla tradizionale ipotesi di truffa, emerge l’assenza del richiamo alla induzione di taluno in errore mediante l’impiego di artifizii o raggiri, proprio per evitare i dubbi antecedenti all’introduzione della norma in commento.

La nuova fattispecie disegna il nucleo centrale della condotta incriminata ricorrendo alle figure di “alterazione” ed “intervento”, in qualunque modo realizzate, su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti.

La formulazione in termini tanto ampi della condotta tipica è tale da poter ricomprendere ogni ipotesi delittuosa fin qui emersa. Infatti, mentre il termine alterazione rimanda ad una modificazione degli

⁸ Cfr. Relazione introduttiva al disegno di legge

algoritmi di cui si compongono tutti i software; con intervento si intende, invece, qualsiasi trasformazione o manomissione compiuta sui dati o sulle informazioni destinate ad essere inserite, per la loro elaborazione, all'interno di un sistema informatico o telematico.

Le affinità strutturali dell'art. 640-ter con la comune fattispecie di cui all'art. 640 impongono di stabilire se anche per la nuova disposizione possa ritenersi sussistente il requisito implicito di fattispecie costituito dal c.d. atto di disposizione patrimoniale, che rappresenta l'effetto dell'errore ed il tramite causale del danno patrimoniale⁹.

Sebbene nel reato di frode informatica manchi qualsiasi riferimento al rapporto fra condotta dell'agente e quella della vittima è sempre sostenibile che l'atto di disposizione patrimoniale sussista; anzi la possibilità che venga ad esistenza dipende proprio dal fatto che l'elaboratore sia chiamato a porre in essere atti di contenuto patrimoniale.

Quanto agli elementi costitutivi della fattispecie, si può facilmente osservare che *“la nuova ipotesi, 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*

⁹ In tal senso Fiandaca-Musco *op. cit.*, pag. 142.

conseguimento del perseguito profitto, le nozioni di «ingiustizia» del danno e di «altruità» sono mutuabili dalla affine fattispecie di cui all'art. 640 del codice penale, della quale riproduce altresì il regime di procedibilità ed il profilo sanzionatorio.”¹⁰

Visto che il reato si consuma nel momento in cui si verifica l'ingiusto profitto, sono configurabili atti idonei ad integrare un tentativo di frode punibile.

L'art. 640-ter prevede, al secondo comma, due circostanze aggravanti che rendono il delitto punibile d'ufficio: la prima rimanda all'ipotesi di cui al numero 1 dell'art. 640 (per il caso in cui il fatto sia commesso a danno dello Stato o di altro ente pubblico); la seconda ha riguardo alla qualità soggettiva rivestita dall'agente (se il fatto è commesso con abuso della qualità di operatore di sistema).

¹⁰ Cfr. Relazione introduttiva al disegno di legge