

VIRUS

L'art. 4 della legge 547/93 ha introdotto, assieme ai reati di accesso abusivo ad un sistema informatico o telematico e a quello di detenzione abusiva di codici di accesso, una specifica ipotesi delittuosa tendente a reprimere il comportamento di colui che in qualunque modo diffonde uno dei cc. dd. programmi virus.

La collocazione topografica di quest'ultima norma è però ingiustificabile. Infatti, mentre i primi due reati possono trovare adeguata sistemazione fra quelli contro l'inviolabilità del domicilio *“perché i sistemi informatici o telematici... costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato”*¹, nel caso dell'art. 615-*quinquies* (Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico) il bene protetto è il buon funzionamento del sistema informatico.

Tale rilievo, però, non vale ad inficiare la portata decisamente innovativa della norma in questione. Infatti, il legislatore ha dotato l'ordinamento di uno strumento utilissimo per reprimere comportamenti molto pericolosi oltre che diffusi. Secondo alcune stime, sarebbero più

¹ Cfr. Relazione introduttiva al disegno di legge

di duecento al mese i nuovi virus messi in circolazione; se a ciò si aggiunge l'altissimo numero di scambi di archivi digitalizzati (cc.dd. files) -all'interno dei quali si annidano i virus - attraverso le reti telematiche mondiali, si può comprendere la portata che ha assunto il fenomeno. Nonostante tali rilievi non possano essere messi in discussione, è pur vero che la reale dimensione del fenomeno non è calcolabile.

Come è stato giustamente osservato: *“la scarsa conoscenza che si ha del fenomeno è spesso causata dalla particolare riservatezza tenuta dai gestori dei sistemi informatici aggrediti, timorosi che la notizia della vulnerabilità del proprio sistema possa nuocere all'immagine di affidabilità del gruppo al quale appartiene il sistema informativo.”*²

Solo pochi ed eclatanti casi assurgono agli onori della cronaca e sono, di conseguenza, denunciati alle competenti autorità.

Ciò premesso, è da dire che i virus sono dei veri e propri programmi (i cc.dd. software) e, quindi, consistono in una serie di istruzioni correlate (cc.dd. algoritmi) eseguibili da personal computer o da un sistema informatico. Le differenze con i programmi applicativi, utilizzati dagli utenti per sfruttare le potenzialità degli elaboratori, si colgono nella “visibilità” e nella possibilità di autoriprodursi, caratteristica principe

² Borruso-D'Aiotti AA.VV. *op. cit.* pag. 82

dei virus. Quanto a quest'ultima capacità, è fin troppo facile rilevare che la pericolosità e dannosità dei virus è tanto più elevata quanto maggiore è la loro diffusione; proprio per tale motivo sono in grado di moltiplicarsi, poiché *“nella loro struttura essenziale (quasi un patrimonio genetico) hanno le istruzioni per riprodursi indefinitamente all'interno della memoria RAM o del supporto magnetico (disco fisso). Ciascun programma infettato assume, a sua volta, il ruolo di virus che infetta tutti gli altri programmi che vengono successivamente eseguiti dal medesimo computer o che si trovano all'interno dei flop-disk (principali vettori delle cc.dd. infezioni virali)”*³.

Secondo elemento differenziatore, oltre ovviamente al fine illecito, rispetto ai comuni software è la visibilità, o meglio l'invisibilità, dei virus che sono abitualmente occultati all'interno di normalissimi software, di modo che né l'utente né il sistema operativo riescono a coglierne la presenza.

La norma *de qua* opera una descrizione dei programmi virus rinviando al fine che essi perseguono, ossia *“il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero l'interruzione totale o parziale, o l'alterazione del suo funzionamento.”*

³ Borruso-D'Aiotti AA.VV. *op. cit.* pag. 84

Venendo all'esame delle condotte tipiche, si può affermare che esse sono tranquillamente riconducibili ai casi di messa in circolazione dei programmi virus.

La soglia della punibilità è assai anticipata rispetto alla lesione del bene protetto, cioè il buon funzionamento del sistema informatico o telematico, e così, integra la fattispecie in esame la diffusione, la comunicazione o la consegna del programma. Le condotte, cui i suddetti termini alludono, sono caratterizzate da attività prive di qualsiasi substrato materiale ad eccezione dell'ipotesi della consegna, in cui è insita un'attività materiale.

Il rispetto del principio di tassatività impone di escludere che la semplice detenzione di un virus integri, di per sé, la fattispecie di cui all'art. 615-*quinquies* del codice penale. Infatti, ciò che la norma reprime è la diffusione dei programmi virus e, pertanto, un'ulteriore anticipazione della soglia del penalmente rilevante -atteso che si tratta di un reato di pericolo- risulterebbe poco consona alla funzione di *extrema ratio* che l'ordinamento riserva al diritto penale.

Trattandosi di un reato di mera condotta, la consumazione coincide con la messa in circolazione del programma "infetto" a prescindere, quindi, da qualsiasi danno da esso cagionato.

Ultimo profilo è quello che attiene all'elemento soggettivo: per la sussistenza del reato, la norma richiede il dolo generico.

La condotta dell'agente non deve essere preordinata al compimento di un determinato evento dannoso, essendo invece sufficiente che sia consapevole di mettere in circolazione un programma virus.