

ACCESSO ABUSIVO A SISTEMI TELEMATICI O INFORMATICI

Nell'ambito dei delitti contro l'inviolabilità del domicilio la legge 547/93 ha introdotto l'art. 615-ter (*Accesso abusivo ad un sistema informatico o telematico*).

La norma reprime l'introduzione abusiva all'interno di un sistema informatico o telematico protetto o il mantenimento all'interno dello stesso contro la volontà dell'avente diritto.

L'articolo in questione costituisce il riconoscimento legislativo più pieno ed incondizionato del valore delle tecnologie informatiche.

Infatti, emerge chiaramente dai lavori preparatori come il nuovo concetto di "*domicilio informatico*" sia stato creato, poiché i sistemi informatici e telematici "*costituiscono un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del codice penale*"¹.

L'inserimento di una tale norma discende dunque dalla necessità di evitare che i vari sistemi informatici collegati in rete possano essere aggrediti da una particolare categoria di computer criminals, i cc.dd. *hackers*. Questi ultimi, utenti particolarmente capaci, collegandosi alle

¹ Cfr. Relazione introduttiva al disegno di legge

reti telematiche - principalmente alla rete INTERNET – possono raggiungere qualsiasi utente collegato.

I fenomeni di *hacking* sono stati a lungo sottovalutati dall'opinione pubblica, anche perché gli *hackers* hanno sempre sostenuto di non voler carpire informazioni per trarne dei vantaggi.

In realtà erano ormai così numerosi i casi di “vandalismo informatico” e di accesso abusivo, che non si poteva non constatare l'inadeguatezza delle norme tradizionali a fronte di tali fenomeni. Accanto ad accessi di tipo, per così dire, ludico furono compiute azioni aggressive che secondo una stima internazionale hanno causato danni, e molto verosimilmente il dato è destinato a crescere nell'immediato futuro, per oltre 10.000 miliardi all'anno.

In Francia, per esempio, un'impresa su dieci ha dichiarato di essere stata vittima di un crimine informatico. Nel 1990 i danni derivanti da crimini informatici furono stimati in oltre nove miliardi di franchi, e la criminalità informatica è la categoria a rischi che aumenta più velocemente: 8,6% nel 1990 contro il 4,8% per incidenti, mentre le perdite dovute ad errori diminuiscono del 2,8%. In Francia i criminali dediti ai fenomeni di *hacking* sono per la maggior parte impegnati (54%) e quadri (30%), non a caso si parla di criminalità da “colletti bianchi”, anche se esistono numerosi raggruppamenti di giovani *hacker*, come il

Chaos Computer Club, dediti alla diffusione di notizie per facilitare accessi abusivi o per generare programmi virus.

Negli Stati Uniti, dove sono stati condotti gli studi più approfonditi sulla materia, il crimine informatico comportava costi a metà degli anni Ottanta tra 100 e 300 milioni di dollari all'anno. Nel 1991, i soli *hacker*, hanno causato danni per oltre 60 milioni di dollari. Nel corso degli anni si è assistito ad una escalation inarrestabile degli *hacker* che ha raggiunto il suo culmine, tra il 1986 e 1987, con un'intrusione nei computer della NASA. È questo l'episodio che, nonostante l'arresto degli autori, rende noti gli *hacker*; il Chaos Computer Club, associazione clandestina con ramificazioni in tutti i paesi industrializzati, edita libri e diffonde la c.d. "cultura dell' *hacking*" il cui caposaldo risiede nell'affermazione che "*compito dell'hacker è quello di individuare sistemi telematici insicuri, penetrarli e pubblicizzare il fatto al fine di denunciare le insidie collegate ad una cieca fiducia riposta nelle tecnologie informatiche.*"²

Data la mancanza di apposita norma incriminatrice, si era invero pensato all'applicazione degli artt. 617 e ss., dettati in tema di intercettazione dei dati trasmessi lungo i cavi telefonici, i quali tuttavia

² Dati e casi sono riportati da F. Berghella e R. Blaiotta "Diritto penale dell'informatica e beni giuridici" in *Cassazione penale*, 1995, pagg. 2338 e ss.

presuppongono che le comunicazioni avvengano fra due soggetti e che rispetto ad essi l'intercettatore si ponga come un terzo; così da non rendersi applicabili nei casi di intercettazione di un flusso di dati fra un elaboratore ed un soggetto ed in tutti i casi in cui l'agente acceda illecitamente ad un sistema informatico.

Altri³ avevano invece ritenuto la configurabilità dell'art. 621 c.p. (*Rilevazione di documenti segreti*), purché i dati, le informazioni o i programmi fossero contenuti all'interno di un documento informatico. Questa tesi, però, dava per scontata la riconducibilità del documento informatico a quello di documento rilevante in ambito penalistico, laddove al contrario essa è stata negata dal legislatore, che ha integrato proprio l'art. 621 estendendo la nozione di documento anche a qualunque supporto informatico contenente dati, informazioni o programmi.

Alla luce delle lacune del diritto positivo e delle esigenze di tutela insorte, è stato così formulato il delitto di accesso abusivo a sistemi informatici.

La relazione spiega perché non si possano tutelare le informazioni abusivamente acquisite⁴ ricorrendo alle tradizionali norme poste a tutela

³ E. Giannantonio *op. cit.*, pag. 76.

⁴ *Contra* Di Pietro "Il furto d'informazioni", Milano, 1990.

del patrimonio come, ad esempio, il furto. Infatti, *“quando la sottrazione dei dati non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il furto), altro non è che una presa di conoscenza di notizie... ciò, ovviamente, a parte la punibilità ad altro titolo delle condotte strumentali, quali ad esempio, quelle di violazione di domicilio...”*

Chiarito ciò, bisogna considerare la condotta in cui si sostanzia l'illecito che il nuovo articolo 615-ter intende reprimere.

Come è stato giustamente osservato, l'accesso cui fa riferimento la norma in discussione non è quello fisico, bensì quello elettronico, che avviene necessariamente attraverso canali telematici.

L'accesso consiste nell'ingresso, da parte dell'agente, all'interno delle memorie di massa del sistema informatico, sfruttando i normali canali usati per la condivisione dei dati a distanza.

Quanto detto sembrerebbe essere smentito da una ipotesi aggravata prevista per il caso in cui il colpevole commette il fatto con violenza sulle cose o alle persone, o qualora sia palesemente armato. Una tale condotta, infatti, non può prescindere da un accesso fisico dell'agente all'interno del luogo dove vi è il sistema informatico. La considerazione di questa ipotesi aggravata lascia molto perplessi dal momento che la

norma intende reprimere esclusivamente l'accesso "virtuale"⁵ all'interno del sistema informatico (posto che quest'ultimo non è penetrabile fisicamente).

Inoltre, la condotta qui prevista come ipotesi aggravata, sarebbe sanzionabile con il ricorso al delitto di violazione di domicilio in concorso, sussistendone i presupposti, con quello di attentato a sistemi informatici di pubblica utilità.

In ogni caso, si deve aggiungere che la tutela non è assicurata indiscriminatamente a tutti i sistemi informatici. Infatti, sono sanzionabili solo quelle condotte di accesso abusivo rivolte a danno di sistemi informatici protetti da mezzi posti a difesa del sistema al fine di rendere evidente la necessità di una autorizzazione per accedere.

L'esistenza di misure di protezione, a prescindere dalla loro concreta efficacia, serve anche a fugare qualsiasi dubbio in ordine alla sussistenza del dolo dell'agente.

Nella maggior parte dei casi, le misure di cui parla la norma, idonee ad innescare la tutela penale, sono costituite da una *password* (o parola chiave) o da codici di accesso.

Detto che la punibilità è subordinata alla presenza di tali misure poste a protezione del sistema informatico, occorre sottolineare che il delitto in

⁵ Borruso-D'Aietti AA.VV. *op. cit.*, pag. 69.

esame è configurabile come reato di pericolo. La sanzione, quindi, è irrogabile indipendentemente dalla effettiva acquisizione di informazioni o dati.

L'accesso abusivo potrebbe essere finalizzato, oltre che all'indebita assunzione di informazioni, anche alla realizzazione di una frode informatica attraverso la manipolazione dei dati, al danneggiamento degli stessi dati o delle informazioni attraverso la diffusione dei cc.dd. *virus* (ipotesi, in verità, molto frequente), all'estorsione, alla falsificazione di documenti informatici o alla rivelazione di documenti segreti. Le suddette ipotesi potrebbero anche non concorrere con il delitto di accesso abusivo. Infatti, per tutti i casi di danneggiamento entra in gioco l'art. 84 c.p. (*Reato complesso*), che esclude l'applicabilità delle norme sul concorso dei reati qualora la legge consideri come circostanze aggravanti di un solo reato, fatti che costituirebbero, per se stessi, reato.

Oltre all'ipotesi aggravata derivante dal danneggiamento delle componenti hardware o software, la norma prevede altre due distinte ipotesi: la prima è correlata alla qualità dell'agente, la seconda alle modalità di condotta. In quest'ultimo caso, la pena è della reclusione da uno a cinque anni se il colpevole per commettere il fatto usa violenza sulle cose o alle persone ovvero se è palesemente armato.

La previsione di una tale fattispecie aggravata suscita, come detto, molti dubbi. Infatti unico caso, assai remoto peraltro, in cui residuerebbe l'applicabilità di questa specifica circostanza aggravante, potrebbe essere l'accesso abusivo a sistemi collegati attraverso "linee dedicate" (cioè linee telefoniche usate esclusivamente da determinati soggetti per la condivisione dei dati). L'aggravante in questione sarebbe configurabile qualora l'agente si allacciasse abusivamente alla linea dedicata, solo in questo caso ricorrerebbe l'indispensabile requisito della violenza sulle cose.

Invero, è assai probabile che il legislatore non abbia pensato affatto alla suddetta condotta, anche perché tale aggravante ricalca integralmente quella prevista dal comma quarto dell'art. 614 c.p. (*Violazione di domicilio*), che si preoccupa di reprimere l'accesso "fisico" al domicilio altrui.

Altra ipotesi aggravata è connessa alla qualità dell'agente: "*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, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore di sistema.*"

L'aggravante si spiega in virtù del particolare rapporto che lega questi soggetti al sistema informatico o telematico. Per gli investigatori privati, invece, la previsione *“intende sanzionare più gravemente l'esercizio scorretto di una professione che si dota sempre di più di raffinati strumenti di intrusione tecnologica.”*⁶

Alcuni sistemi, ad esempio quelli di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità, *“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 ad otto anni nell'ipotesi aggravata indicata nel quarto comma.”*⁷

Ultimo rilievo da effettuare è quello relativo alla nozione di sistema. Infatti i moderni *personal computer* raggiungono prestazioni paragonabili a quelli di un sistema di modeste capacità.

Tuttavia, ribadito che la relazione ministeriale ha inteso punire esclusivamente l'accesso abusivo ad un sistema informatico o telematico e che per sistema si intende un insieme di due o più computer, è da osservare che rimarrebbero al di fuori della tutela gli accessi abusivi diretti contro singoli personal computers.

⁶ Borruso-D'Aietti AA.VV. *op. cit.*, pagg. 73 e 74.

⁷ Cfr. Relazione introduttiva al disegno di legge