Rubrica legale – ICT Security n. 3 – Luglio 2002
Autori: Riccardo Genghini e Daniela Rocca
Studio Notarile Genghini – www.sng.it

Il reato di accesso abusivo ad un sistema informatico o telematico: l'art. 615 ter del Codice Penale

- ***I difficili equilibri legati all'uso delle tecnologie informatiche***
- ***La normativa sulla criminalità informatica***
- ***L'art. 615 ter del Codice Penale: fattispecie e punibilità***

La disciplina dell'informatica tocca aspetti costituzionali molto rilevanti e delicati: da un lato la libertà delle comunicazioni, la libertà di espressione, la tutela della privacy; dall'altro, il diritto dei cittadini di essere difesi da fatti criminosi e fraudolenti.

Il difficile equilibrio fra questi interessi e la rilevanza degli stessi non poteva trovare un'adeguata disciplina senza la garanzia di norme sanzionatorie. Le norme penali, tuttavia, possono costituire un freno allo sviluppo di attività economiche che possono risultare vietate o marginalizzate dalla norma penale.

Gli interventi legislativi che hanno introdotto in Italia i reati informatici non hanno portato all'introduzione di un capo del Codice Penale e di Procedura Penale interamente dedicato alle nuove fattispecie criminali, bensì una serie di norme che si sono aggiunte a fattispecie omologhe già esistenti.

L'introduzione delle nuove norme è stata dettata da una crescente attenzione verso il mondo del commercio elettronico e della nascente criminalità informatica, ma altresì da numerosi richiami e sanzioni dell'UE.

Il quadro che ne è derivato è costituito da varie norme, che hanno novellato il codice penale e alcune leggi speciali e che hanno attenuato, ma certamente non dissolto, le preoccupazioni degli operatori verso l'utilizzo delle reti e, specificamente, verso il commercio elettronico.

L'esistenza di un quadro sanzionatorio ha migliorato la certezza del diritto, ma ha lasciato gli operatori fra Scilla e Cariddi.

- Da un lato, il rischio passivo derivante dall'uso delle tecnologie dell'informazione è quello dell'acquisizione da parte di terzi di dati o addirittura di intere banche dati e del sabotaggio dei propri sistemi.
- Dall'altro lato, il rischio attivo è derivante dalla complessità dei nuovi doveri di tutela dei diritti di terzi, nel campo del diritto d'autore e della privacy.

Le aree di intervento del legislatore italiano hanno riguardato:

(a) *Il Codice Penale e di Procedura Penale*: la L. 23 dicembre 1993 n.547 ha modificato il codice penale e il codice di procedura penale introducendo nuove norme in materia di criminalità informatica tenendo conto delle indicazioni della Comunità Europea che, con la raccomandazione n. 89/9, individuava una lista minima e una facoltativa in materia di reati informatici. la L. 3 agosto 1998 n. 269 ha novellato il codice penale introducendo la disciplina sulla pornografia minorile.

(b) *La normativa sul diritto d'autore.* Il D.Lgs. 29 dicembre 1992 n. 518, attuando le disposizioni della direttiva europea 91/250/CE relativa alla tutela giuridica dei programmi per elaboratore, ha esteso la disciplina del diritto d'autore prevista dalla L. 22 aprile 1941 n.633 anche alla pirateria di software. La normativa è stata poi integrata dal D.Lgs. 6 maggio 1999 n.169, che ha attuato la direttiva europea 96/9/CE relativa alla tutela giuridica

Il reato di accesso abusivo ad un sistema informatico o telematico: l'art. 615 ter del Codice Penale

delle banche di dati. E' poi intervenuta la L. 18 agosto 2000 n. 248 che punisce severamente alcune attività che non sempre la collettività considera eccessivamente gravi.

(c) *La normativa sulla riservatezza dei dati*: la L. 31 dicembre 1996 n.675, come modificata e integrata da ultimo dal D. Lgs. 28 dicembre 2001 n. 467, contiene norme penali a tutela della riservatezza dei dati personali.

Non è questa la sede per un approfondimento di tutte le problematiche legali connesse a tali interventi legislativi. Sembra utile però soffermarsi su una fattispecie del tutto nuova nel nostro panorama giuridico: l'accesso abusivo ad un sistema informatico o telematico prevista dalla L. 547/1993, che ha introdotto l'art. 615 ter del Codice Penale.

Infatti, mentre la frode, il falso informatico, il danneggiamento e i comportamenti criminosi legati alle comunicazioni informatiche affiancano forme di reati esistenti, l'accesso abusivo si riferisce ad aggressioni tipiche delle nuove tecnologie e prima sconosciute.

I fenomeni di accesso abusivo ad un sistema non costituiscono una categoria omogenea: si profilano accessi abusivi per scopi ludici (hackeraggio semplice), con intenti di danneggiamento (all'accesso abusivo consegue la distruzione di documenti o di parte del sistema a cui si ha avuto accesso) o prodromici al compimento di altri reati, quali la frode, la falsità o la violazione della corrispondenza.

Ciò che si vuole qui sottolineare è che il comportamento è considerato illecito indipendentemente dalla sua necessaria dannosità: in termini giuridici, si tratta di un *reato di pericolo* e il danno causato al sistema o ai dati è mera circostanza aggravante. Caratteristico di molti hackers è ottenere soddisfazione semplicemente per aver violato *con dolo* le misure di sicurezza di un sistema.

Due questioni principali si sono poste immediatamente all'attenzione degli operatori.

Innanzitutto, se il singolo PC sia riconducibile alla nozione di "sistema informatico o telematico", vista l'assenza di una definizione legislativa del termine. La dottrina ha risposto finora in senso positivo, sostenendo che, per l'ampiezza e la varietà delle funzioni che un personal computer può svolgere, può essere considerato sistema informatico.

In seconda battuta, la Corte di Cassazione ha più volte qualificato come sistema informatico qualunque servizio televisivo o telefonico che si avvalga si un sistema informatico: ne consegue la tutela dei servizi telefonici da parte dell'art. 615 ter, colmando una supposta lacuna del sistema italiano.

Presupposto oggettivo del reato, quindi non legato all'autore dell'accesso abusivo, è che il sistema sia protetto, ma la legge non definisce la nozione di misure di sicurezza. L'interpretazione corrente considera sufficiente che siano state adottate misure di sicurezza, siano esse logiche o meramente fisiche: non si spiegherebbe altrimenti la violenza sulle cose prevista come circostanza aggravante.

Perché sussista il reato, infine, non è richiesta la violazione delle misure di sicurezza, essendo sufficiente che queste siano predisposte, rendendo palese la volontà dell'avente diritto contraria a qualsiasi forma di accesso non autorizzato. La dottrina e la giurisprudenza (vedi Cass. Pen. Quinta Sezione sent. 12732/2000) sono concordi nel ritenere che, ai fini dell'individuazione di un "sistema protetto da misure di sicurezza" è sufficiente che al medesimo sia applicato un qualsiasi tipo di protezione anche se facilmente aggirabile da persona mediamente esperta, e quindi anche una semplice password apposta dalla casa fornitrice di un programma. Tanto più,

Il reato di accesso abusivo ad un sistema informatico o telematico:

l'art. 615 ter del Codice Penale

sarebbe manifesta la volontà di negare l'accesso aperto al sistema con la presenza di un firewall che protegga i dati: nel caso di un malfunzionamento dello stesso che non riesca a bloccare eventuali tentativi di intrusione, è sicuramente utile da un punto di vista giuridico rendere inevitabilmente percepibile all'intruso il fatto che questi si trovi in un'area riservata del sistema informatico. Ciò è possibile con soluzioni tecniche che variano a seconda della natura dei dati di cui trattasi. Sarebbe sufficiente, per passare da una *protezione tecnica* a una *protezione legale*.

Particolare attenzione va posta alla condotta criminosa, che prende a modello la violazione di domicilio: si punisce chi si *introduce* in un sistema ma altresì chi *vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo*. Questa formulazione consente di considerare illecite le condotte di chi sorpassa i limiti di un'autorizzazione, quindi rende punibili non solo gli estranei al sistema ma altresì gli utenti autorizzati ad accedervi per una determinata finalità che utilizzino il titolo di legittimazione per una finalità diversa o che, da un momento in poi, si vogliono escludere.

La pena prevista è la reclusione fino a tre anni. Da uno a cinque anni se sono presenti una o più circostanze aggravanti. Se il sistema informatico a cui si è avuto accesso è di interesse militare o pubblico, la pena è molto severa e può arrivare fino ad otto anni.

Riccardo Genghini

Daniela Rocca

ART. 615 ter Codice Penale - Accesso abusivo a 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 al 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 essi contenuti.

Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici d'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 d'ufficio.