Del delitto di accesso abusivo ad un sistema informatico o telematico (art. 615ter cp)[1]

di Telesio Perfetti

Il delitto di accesso abusivo è stato introdotto dall'art. 4 della legge 23 Dicembre 1993 n.547, recante *"Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica"*. Trattasi senza dubbio di uno dei reati informatici più importanti e a maggior possibilità di verificazione. Esso, peraltro, ha dato adito alle più significative pronunce giurisprudenziali in materia (non molte per la verità) e alle principali dispute dottrinarie. È bene ricordare fin da subito che, anche in base all'esegesi offerta dalla Corte di Cassazione, l'incriminazione de quo sarebbe sostanzialmente finalizzata *«a contrastare il rilevante fenomeno degli hackers[2], e cioè di quei soggetti che, servendosi del proprio elaboratore, collegato con la rete telefonica, riescono a entrare in comunicazione con i diversi sistemi informatici che a quella stessa rete sono collegati, aggirando le misure di protezione predisposte dal titolare del sistema»*[3].

a) **Soggetto attivo** è "chiunque", onde trattasi di reato comune.

b) **Elemento oggettivo** (**condotte punibili**; nozione di **"sistema"**; concetto di **"misure di sicurezza"**).

Non è unica la condotta penalmente rilevante ai sensi dell'art. 615ter cp. Precisamente essa può attuarsi o tramite **intrusione nel sistema protetto** o tramite **mantenimento nello stesso contro la volontà espressa o tacita di chi ha il diritto di esclusione**.

Sotto il primo profilo, occorre dire che si può accedere o da remoto attraverso apposite apparecchiature (per es. modem) o da vicino tramite mera accensione della macchina, sempre che a tale contatto fisico segua poi l'interazione (una sorta di *"colloquio"*) con il computer stesso, perché solo in tal momento v'è la presa di conoscenza dei contenuti del sistema[4]. Non solo, ma stando alla lettera della norma, l'accesso deve essere "abusivo", il che sembrerebbe colorare la condotta del delitto de quo di una sorta di "illiceità speciale", laddove dunque non solo sarebbe necessaria l'assenza di scriminanti propriamente dette (come quelle previste ex art. 50 e s. cp), ma invero (onde non ridurre l'espressione a mera nota pleonastica) potrebbero venir in rilievo *"pregnanti esigenze morali e di difesa della propria onorabilità o la necessità di contrastare condotte violatrici di specifici principi deontologici"*[5], onde si verrebbe ad allargare la sfera di impunità (al di là per l'appunto delle cause di giustificazione).

L'altra condotta punibile è costituita dalla permanenza nel sistema contro la volontà espressa o tacita del titolare dello *ius excludendi*. In tale ipotesi si sarebbe di fronte comunque ad un comportamento attivo (e non meramente omissivo[6]), concretantesi in un'azione che perdura consapevolmente. Né potrebbe esservi concorso materiale (art. 71 e s. cp) tra la condotta di introduzione e quella di mantenimento in quanto quest'ultimo presuppone un accesso lecito (ma non sempre[7]) nel sistema, che si tradurrà nel trattenersi illecitamente nel medesimo, o perché il titolare ha revocato il consenso inizialmente prestato o perché l'agente ha compiuto operazioni diverse da quelle per le quali era stato autorizzato ad accedere. Tale condotta in genere si verifica o restando nel sistema oltre il tempo consentito oppure prendendo conoscenza di file o di altre informazioni, per le quali non si possedevano i legittimi privilegi o autorizzazioni, oppure compiendo operazioni diverse da quelle originariamente previste. L'abuso può così pertenere a tempi, scopi e aree d'accesso.

L'accesso o il mantenimento illeciti devono avvenire all'interno di *"un sistema informatico o telematico protetto da misure di sicurezza"*. Una definizione di **"sistema"** è stata offerta dalla Cassazione, dovendosi intendere per esso *«una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o "memorizzazione"), per mezzo di impulsi elettronici, su supporti adeguati, di*

dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici ("codice"), in combinazioni diverse: tali "dati", elaborati automaticamente dalla macchina, generano le informazioni costituite "da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l'utente"»[8].

Inoltre il sistema deve essere protetto da **"misure di sicurezza"**, dovendosi intendere per esse (secondo la relazione ministeriale di accompagnamento alla legge 547/93) quei mezzi di protezione logici o fisici, materiali o personali, che rivelino la volontà del titolare dello ius excludendi di riservare l'accesso e/o la permanenza nel sistema alle sole persone da lui autorizzate. Così in tale ampio concetto di m.d.s. rientrano senza dubbio le cd. protezioni logiche atte a proteggere l'elaboratore sia da accessi da vicino (es. le chiavi elettroniche, le password, le sequenze alfa-numeriche, i codici d'accesso, i certificati digitali, le caratteristiche biometriche…), sia da accessi da remoto (es. il *"firewall"*[9]), ma vi rientrano altresì le protezioni "fisiche"[10] come l'adozione di un servizio di vigilanza o di sistemi di videosorveglianza ovvero di porte blindate, chiavi fisiche, lucchetti etc. La S.C. ha chiarito che ha al riguardo rilevanza *«qualsiasi meccanismo di selezione dei soggetti abilitati all'accesso al sistema informatico, anche quando si tratti di strumenti esterni al sistema e meramente organizzativi, in quanto destinati regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi»*[11].

A questo punto si impongono talune precisazioni. In primis, tenendo conto anche della lettera della norma, non è richiesta una particolare efficacia o adeguatezza delle m.d.s. stesse, ergo basterebbe un qualunque strumento di protezione, anche banale o facilmente aggirabile, e ciò in quanto il legislatore, nel richiedere (ai fini della configurabilità del reato) la sussistenza di m.d.s., ha voluto solo specificare che esse debbono considerarsi quale elemento in grado di rendere esplicita o comunque inequivoca la volontà di riservare l'accesso a determinate persone[12]. La violazione dei dispositivi di protezione, se vista in tale ottica, sembrerebbe non assumere rilevanza di per sé, *«bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone. Non si tratta, perciò, di un illecito caratterizzato dall'effrazione dei sistemi protettivi, perché altrimenti non avrebbe rilevanza la condotta di chi, dopo essere legittimamente entrato nel sistema informatico, vi si mantenga contro le disposizioni del titolare»*[13].

È pur vero comunque che un qualche strumento, hardware o software, ovvero fisico, o altresì una particolare procedura organizzativa, deve sussistere acciocché si possa parlare di accesso abusivo ex art. 615ter cp[14]; insomma debbono esservi m.d.s.[15], quali che esse siano e quale che ne sia l'idoneità, sempre che ovviamente siano "attuali"[16], i.e. attive e funzionanti, altrimenti il delitto non sarebbe oggettivamente perfetto in tutti i suoi elementi costitutivi. E infatti la stessa S.C., con una decisione che stranamente non ha avuto la giusta eco che invece le sarebbe spettata, sembra aver abbandonato la precedente impostazione sull'importanza delle m.d.s. solo come *"manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone"*, e ha invece affermato che *«non è ravvisabile la condotta contestata* (quella di cui all'art. 615ter cp, n.d.r.) *in quanto il sistema informatico nel quale l'imputato si inseriva abusivamente non risulta obiettivamente (…) protetto da misure di sicurezza, essendo anzi tale sistema a disposizione dell'imputato in virtù delle mansioni affidategli per ragioni di ufficio»*[17].

c) **Oggetto giuridico** o bene protetto dalla norma è il cd. **"domicilio informatico"**, sebbene in dottrina non vi sia univocità di vedute al riguardo.

Per domicilio informatico, secondo la relazione al d.d.l. sui computer-crimes, devesi intendere *«l'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615 cp»*[18]. E ciò in quanto il computer rappresenterebbe per ogni persona *"una sorta di propaggine della propria mente e di tutte le sue conoscenze, i ricordi, i segreti che essa custodisce"*[19], una specie di proiezione virtuale del proprio io pensante, un'estensione della dimensione della persona, un luogo in cui sono allocati i dati informatici di ciascuno[20]. Ma i dati e le informazioni oggetto di protezione non sono, né possono essere solo quelli a contenuto personalissimo (cioè attinenti alla riservatezza della vita privata), come pure sostiene parte della dottrina in base a una prima interpretazione restrittiva[21]. L'art. 615ter cp invece, secondo un altro indirizzo (maggioritario), assicura tutela a tutti i dati racchiusi nel sistema quale che sia il contenuto di essi, purché attinente alla sfera di pensiero della persona o della sua attività (lavorativa e non). Tale tesi si attaglia tanto alla lettera quanto allo scopo della legge: *«alla*

lettera, perché la norma non opera distinzioni tra sistemi a seconda dei contenuti (esclusivamente limitandosi ad accordare tutela ai sistemi protetti da misure di sicurezza); alla ratio legis soprattutto, perché la prima interpretazione implicherebbe l'esclusione dalla tutela - irragionevolmente e verosimilmente in senso contrario all'interpretazione del legislatore - di aspetti non secondari, quali, per esempio, quelli connessi ai profili economico-patrimoniali dei dati (…), lasciando quindi sforniti di protezione i diritti di enti e persone giuridiche, non tanto per essere incerta l'estensione a tali categorie soggettive della tutela della riservatezza e in genere dei diritti della personalità (…) ma piuttosto perché principalmente fra dette categorie si rinvengono soggetti titolari di sistemi informatici protetti da misure di sicurezza (enti, anche pubblici, grandi società commerciali) per i quali lo ius excludendi è correlato prevalentemente, se non esclusivamente, a diritti di natura economico patrimoniale (…). Pare infatti che una volta individuato nell'accesso abusivo a sistema informatico un reato contro la libertà individuale, il legislatore sia stato quasi "costretto" dalla sistematica del codice a quel tipo di collocazione, senza però che con la collocazione stessa si sia voluto individuare, in via esclusiva, il bene protetto con riferimento alle norme sulla violazione di domicilio, cioè la pax domestica ovvero la quiete e la riservatezza della vita familiare»[22]. In sostanza quel che conta non è la natura personalissima o intima delle attività che si svolgono e trovano allocazione nel domicilio informatico, anche perché sarebbe alquanto rischioso un sindacato del giudice su ciò che potrebbe considerarsi personale (*rectius* personalissimo) e su ciò che tale non sarebbe[23].

Che il bene protetto abbia dunque tale ampiezza, è stato rilevato anche in dottrina[24], anzi sono proprio i sistemi e le banche dati delle persone giuridiche o di enti ad essere quasi sempre protette da m.d.s., soprattutto organizzazioni militari (Comandi, Corpi Armati etc.), amministrative (Ministeri, Università, enti di documentazione e ricerca, scuole di ogni ordine e grado, enti sanitari etc.) ed economiche (società commerciali, banche etc.), tant'è che, così argomentando, si potrebbe addirittura porre in dubbio (come si è detto) l'affermazione secondo la quale il bene protetto sia proprio il domicilio informatico[25].

d) Circa l'**elemento soggettivo**, trattasi di reato (solo) doloso, a **dolo generico** per la precisione, essendo sufficiente la coscienza e la volontà di introdursi nell'altrui sistema protetto ovvero di rimanervi contro la volontà di chi è titolare dello *ius excludendi*. La conoscenza del fatto che sussistano m.d.s. sembra rientrare nel fuoco del dolo.

Non rilevano le finalità che l'agente si propone: curiosità, ricerca di informazioni particolari o riservate o addirittura segrete e di qualsivoglia natura (personale, economica, tecnologica, scientifica, militare, politica etc.), scopo di spionaggio, intento ludico-vandalico ovvero distruttivo o manipolativo e così via[26].

La colpa non rileva (art. 42, co.2 cp), ergo non sarà punibile per es. un accesso meramente imprudente o causato da inesperienza o disattenzione.

Nell'ipotesi della permanenza illecita nel sistema, esclude il dolo l'errore sull'esistenza del dissenso (per es. il non aver udito il divieto verbale o la revoca del precedente consenso)[27]. Mentre per entrambe le condotte previste ex art. 615ter cp la sussistenza di un consenso tacito o implicito vale ad escludere il dolo e dunque il delitto[28].

e) La **perfezione** del reato si ha nel momento e nel luogo in cui avviene l'accesso alla conoscenza dei dati oppure la persistenza in tale accesso contro l'intervenuto dissenso del titolare del sistema. La condotta di intrusione sembra configurare un'ipotesi di reato istantaneo ad effetti permanenti (o più semplicemente istantaneo), mentre la condotta di consapevole mantenimento illecito è certamente reato permanente[29]. Nonostante qualche isolata voce in dottrina, il delitto di cui all'art. 615ter cp è **delitto di danno**, laddove l'offesa è rappresentata dalla lesione del diritto alla riservatezza o alla privacy informatica (intesa *latu sensu*, come si è visto a proposito dell'oggetto giuridico protetto).

Quanto al tentativo, trattandosi di reato di danno e non di pericolo, esso sembra naturalisticamente configurabile, nonché giuridicamente rilevante, ergo punibile. Si pensi all'ipotesi in cui l'agente da remoto cerchi di forzare il *firewall*, ma non vi riesca. Si faccia anche il caso di tentato accesso da vicino, laddove l'agente, sedutosi di fronte al monitor di un P.C. sul quale non ha alcun diritto, provi a scoprire o a *crackare* la password o la chiave logica d'accesso senza esito. Ma il discorso vale anche per le m.d.s. fisiche (si pensi alla manipolazione o forzatura della serratura di protezione apposta sul "case" o involucro del P.C. ovvero all'introduzione in essa di chiavi false ovvero ancora al tentativo di rottura delle chiavi

hardware che bloccano, a seconda dei casi, l'accensione, la tastiera o altre componenti etc.[30]). Ergo è da ricercarsi nel momento in cui l'agente supera (con "rottura" o "aggiramento") le barriere di protezione il discrimen tra perfezione e tentativo, essendo sufficiente per la prima la semplice introduzione nei contenuti del sistema, senza che sia necessario che ne venga presa conoscenza effettiva o totale. A tal proposito, in giurisprudenza si è chiarito che *«la mera duplicazione dei dati acquisiti in occasione dell'accesso abusivo nel sistema è da ricomprendere nella condotta tipica del reato di cui all'art. 615ter cp, potendo l'intrusione informatica sostanziarsi sia in una semplice "lettura" dei dati che nella "copiatura" degli stessi. È noto, infatti, che il legislatore non ha inteso introdurre, con la riforma del 1993, anche una autonoma figura di "furto informatico" allargando i confini del reato previsto dagli artt. 624 e 625 cp»*[31].

f) Alcune considerazioni sulle ipotesi di **aggravanti a effetto speciale (art. 63, co.3 cp)**.

- Per quel che concerne le aggravanti di cui al co.2, n.1 dell'art. 615ter c.p., alcuni problemi definitori ed esegetici li crea l'espressione *"abuso della qualità di operatore di sistema"*. Non esiste una qualifica tecnica univoca di "operatore di sistema", né ne è stata offerta una definizione legislativa o normativa. Pertanto, più che una titolarità astratta di mansioni dal punto di vista tecnico-professionale nel campo dell'informatica, si vuole porre in risalto il collegamento funzionale (anche occasionale) sussistente tra un determinato soggetto, per motivi professionali, e il sistema che egli viola nel mentre che con esso interagisce[32]. La ratio dell'aggravante sta dunque nel fatto che tale soggetto può sfruttare la sua posizione all'interno di un ufficio pubblico o privato ovvero di un'azienda etc., ed eventuali particolari conoscenze (non solo tecniche, ma anche concernenti informazioni riservate quali per es. le password usate da un determinato reparto o divisione organizzativa di cui l'operatore fa parte). Egli è cioè in un rapporto per così dire "privilegiato" col sistema (a prescindere dal fatto che si tratti di un esperto o meno di informatica[33]), in virtù anche della relazione fiduciaria che lo lega al titolare del sistema violato.

  "Abuso" vuol dire "eccesso" ovvero superamento dei limiti che dovevano essere rispettati nell'uso consentito del sistema. Il rapporto che lega operatore al titolare non deve peraltro essere a tempo indeterminato o di lunga durata, bensì può essere anche temporaneo, interinale, breve, persino occasionale. Purtuttavia ciò che conta è che sia attuale rispetto al *tempus commissi delicti*[34], a nulla rilevando che l'agente abbia avuto in passato una determinata qualifica o abbia ricoperto una certa posizione o svolto una specifica attività all'interno della struttura, in cui si trovi il sistema violato.
- Quanto all'aggravante di cui al co.2, n.3 dell'art. 615ter cp, riguardante le conseguenze dannose derivate al sistema dall'accesso abusivo o dall'illecito mantenimento, occorre dire che tale previsione va coordinata con l'art. 635bis cp (Danneggiamento di sistemi informatici e telematici)[35], nel senso che da una parte ricalca le descrizione delle condotte tipiche del danneggiamento, dall'altra può pacificamente ritenersi escluso il concorso tra reati (con assorbimento del delitto di cui all'art. 635bis cp in quello di accesso abusivo aggravato, in quanto sanzionato più duramente e in virtù della clausola di sussidiarietà prevista nell'art. 635bis stesso, sebbene essa potrebbe esser riferita ai soli reati informatici contro il patrimonio). Tuttavia la verificazione di danni al sistema o ai programmi o ai dati in esso contenuti sembra essere ascritta all'agente in base al suo mero accadimento (cd. mero *"versari in re illicita"*), indipendentemente dall'eventuale volontà dell'agente in tale direzione, ergo basta che l'effetto dannoso sia causalmente ricollegabile alla di lui condotta materiale[36].
- Circa l'aggravante di cui al co.3 dell'art. 615ter cp, bisogna distinguere l'ipotesi nella quale è prevista la pena da uno a cinque anni di reclusione, da quella in cui è prevista la pena da tre a otto anni. Nel primo caso i fatti di cui al co.1 dell'art. 615ter vengono posti in essere contro determinati sistemi *"di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico"*. Nel secondo caso invece gli stessi fatti sono commessi su tali particolari sistemi, ma in presenza altresì di una delle aggravanti di cui al co.2 dell'art. 615ter cp.[37]

g) Per quel che concerne la **procedibilità**, l'ipotesi base di cui al co.1 è procedibile a querela, le ipotesi aggravate (co.2 e 3) sono procedibili d'ufficio.

h) **Rapporti con gli altri reati**.

In giurisprudenza è stata espressamente riconosciuta la possibilità di concorso formale con il reato di cui all'art. 640ter cp (Frode informatica)[38]. Infatti nella frode informatica è decisivo l'elemento della manipolazione del sistema, non richiesto né necessario ex art. 615ter cp, mentre nell'accesso abusivo è richiesta la presenza di m.d.s. (non così nella frode informatica). Inoltre sono differenti i beni protetti (patrimonio nella frode informatica, "domicilio informatico" nell'accesso abusivo)[39]. Ovviamente è possibile un concorso con il reato di cui all'art. 615quater cp (Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici[40]), mentre è escluso il concorso con il delitto di cui all'art. 635bis c.p. (v. considerazioni sub lett.f) in riferimento a quanto detto a proposito dell'aggravante di cui al co.2, n.3 dell'art. 615ter cp.

g) **Responsabilità amministrativa delle persone giuridiche (d.lgs. 8 giugno 2001, n. 231)**.

In base alla Decisione quadro 2005/222/GAI del Consiglio U.E. del 24 febbraio 2005 relativa agli attacchi contro i sistemi di informazione, gli Stati membri dovranno adottare le misure necessarie per recepire, entro il 16 marzo 2007, le disposizioni della suddetta decisione concernenti la responsabilità delle persone giuridiche per il caso in cui commetta (tra gli altri) il reato di accesso abusivo nell'interesse della p.g. (art. 8, paragrafo 1 della D.q.) qualsiasi soggetto, che agisca a titolo individuale o in quanto membro di un organo della persona giuridica, il quale detenga una posizione preminente in seno alla p.g. stessa, basata

- o sul potere di rappresentanza di detta p.g.
- o sul potere di prendere decisioni per conto della p.g.
- o sull'esercizio di poteri di controllo in seno a tale p.g.

Peraltro la sussistenza di tale responsabilità per siffatto reato dovrà essere assicurata anche nel caso in cui esso sia stato reso possibile o agevolato dalla mancata sorveglianza o dal mancato controllo da parte di uno dei soggetti di cui sopra (art. 8, paragrafo 2 della D.q.)[41].

---

[1] *"Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero ivi 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 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;*
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 esso contenuti.*

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

[2] *"Hacker"* è parola di incerto etimo, ma in realtà solo in un secondo momento ha assunto il valore dispregiativo di *"pirata informatico"*. In origine l'hacker era colui che cercava di capire il funzionamento di un sistema o di un programma e di studiarlo in modo approfondito e specifico. Indi il termine, come detto, è stato generalizzato per indicare colui che si impegna ad aggirare o a forzare le misure poste a protezione di un computer per accedervi in modo illecito (senza o contro il consenso dell'utente), onde poter prendere visione di dati e di informazioni e poterli utilizzare per scopi personali o per profitto.

Spesso si rischia di fare confusione tra i vari "profili criminologici" di *"cyberdelinquenti"*. Risulta pertanto opportuno effettuare talune distinzioni tra l'hacker propriamente detto e altre figure, che possono assumere le denominazioni più diverse e che nettamente si distinguono dall'hacker *strictu sensu* considerato. Ci si riferisce al *cracker*, al *lamer*, all'*insider*. Ma *procedamus in ordine*:

- *"Cracker"*: parola derivata dal verbo anglosassone "to crack", rompere. È colui che più propriamente può essere considerato il pirata informatico, dacché "spezza", "rompe", "scassina" le misure di sicurezza di un sistema informatico per penetrarvi. In genere agisce per scopi di profitto, talora anche per scopi vandalici e distruttivi. A volte il suo obiettivo è anche quello di sproteggere (*"crackare"* come si dice in gergo) un software coperto da copyright e destinato al commercio, al fine di utilizzarlo senza averne il diritto (né per averlo acquistato, né per averne la licenza o altro titolo per l'uso). Se si vuole mantenere la distinzione tra hacker e cracker, può dunque dirsi che col primo termine devesi indicare colui che, sebbene agisca in modo penalmente illecito, manifesta nel suo *modus operandi* l'assenza dell'intento di conseguire un lucro o comunque un profitto (si parla talvolta di *"ethical hacker"*) e faccia ciò che faccia a scopo dimostrativo o sfida, per es. per "avvertire" che il sistema, che egli ha violato, è insicuro et similia;

- *"Lamer"*: trattasi di un aspirante hacker o aspirante cracker. In gergo i lamer sono conosciuti come *"smanettoni"* e sono in genere adolescenti, spesso minorenni, affascinati dal mito degli hacker famosi e pertanto vorrebbero emularne o imitarne le gesta (ma, viste le limitate conoscenze informatiche, il più delle volte senza successo);
- *"Insider"*: il cd. *"dipendente infedele"*, che in virtù della sua posizione privilegiata all'interno di un'azienda ha la disponibilità di codici d'accesso, password, informazioni riservate. Anche in tal caso i motivi che spingono il soggetto ad agire sono molteplici, per es. la vendetta (a causa di un licenziamento ingiusto o reputato tale, ovvero offensivo o semplicemente mal digerito) o il profitto (nel caso in cui fosse pagato da un'azienda concorrente per boicottare l'azienda di cui l'insider fa parte e dunque a scopo di concorrenza sleale, in modo che venga violato il segreto industriale o vengano rivelate particolari notizie su speciali formule, piani di investimento, organigrammi etc.). È in genere la forma più subdola di *"intruder"*, insospettabile e quindi più pericoloso e più difficile da rilevare e, per ciò stesso, si palesa quale minaccia più frequente per un'azienda, un'amministrazione, un ente, uno studio professionale, una qualsivoglia struttura che tratti dati e informazioni confidenziali e privilegiate.

[3] V. Cass. Sez.III Pen. 31 Luglio 2003, n.32440, reperibile all'URL http://www.eius.it/giurisprudenza/2003/087.asp.

[4] Nel senso che introdursi nel sistema significhi "accesso alla conoscenza" dei dati e delle informazioni memorizzate nel computer, cfr. F.Mantovani, *"Diritto penale. Parte speciale I"*, CEDAM, Padova, 1995, p.453 e, nello stesso senso, G.Pica, *"Diritto penale delle tecnologie informatiche"*, UTET, Torino, 1999, p.41. Secondo il Mantovani non sussiste il reato nel caso di presa di conoscenza senza introduzione nel sistema, come per es. qualora l'agente procedesse a semplice lettura di dati già visualizzati sul video. In dottrina peraltro non v'è uniformità di vedute sulla natura dell'accesso, tant'è che secondo il Borruso (in R.Borruso, G.Buonomo, G.Corasaniti, G.D'Aietti, *"Profili penali dell'informatica"*, Giuffré, Milano, 1994, p.69) sarebbe punito solo l'accesso virtuale. Tuttavia in aderenza alla norma, che prevede anche quale aggravante "la violenza sulle cose o alle persone", altra parte della dottrina ritiene che l'accesso abusivo possa realizzarsi tramite ingresso nei locali dov'è custodito l'elaboratore (cfr. E.Giannantonio, *"Manuale di diritto dell'informatica"*, CEDAM, 1997, p.435).

[5] Cfr. F.Antolisei, *"Manuale di diritto penale. Parte speciale I"*, Giuffré, Milano, 1999, p.237. Contra F.Mantovani, op.cit., p.454 , poiché, se fosse vero quanto affermato dall'Antolisei, più corretta sarebbe stata l'espressione "senza giusta causa" di cui per es. agli artt. 616, 618 e s. cp. Secondo il Pica (op.cit., p.43) l'avverbio "abusivamente" sarebbe da intendersi non solo nel significato di "senza il consenso" del titolare, ma anche in quello di "senza essere a ciò autorizzato da altra specifica norma di legge" (per es. ex art. 266bis cpp).

[6] Nel senso che il secondo tipo di condotta sia a carattere meramente omissivo, cfr. F.Mucciarelli, *"Commento all'art.4 della legge n.547 del 1993"*, in Legislazione Penale, 1996, p.100.

[7] Una forma di accesso illecito prodromica al successivo abusivo mantenimento potrebbe essere attuata tramite l'invio nella casella di posta elettronica dell'utilizzatore del sistema target di una e-mail con allegato "infetto", che contenga cioè un programma cd. *"trojan"*. Il *"trojan horse"*, letteralmente "cavallo di Troia", a prima vista potrebbe apparire come un software normale, contente *"utilities"* e dunque in grado di effettuare una o più operazioni, se non fosse per il fatto che esse sono in realtà occulte o meglio diverse da quelle dichiarate. Ergo ci si trova innanzi a un tipo di *"malware"* (contrazione per *"malicious software"*, letteralmente programma malvagio), le cui funzionalità sono celate all'interno di un programma apparentemente utile o comunque innocuo. È dunque l'utente stesso che, istallando ed eseguendo un certo programma, inconsapevolmente installa ed esegue anche il codice all'interno del trojan (potrebbe trattarsi di uno *spyware* o altro programma malizioso, come un *worm*), per eseguire il quale basterebbe un semplice click sull'allegato stesso. Una volta entrato in funzione, il malware sarebbe sfruttabile da remoto dall'attacker. Quest'ultimo infatti, entrando nel sistema in modo subdolo e non autorizzato proprio grazie al trojan, avrebbe quasi il pieno controllo del P.C. tramite il malware celato all'interno del trojan stesso. Il soggetto agente riuscirebbe così non solo a permanere illecitamente nel sistema, ma anche a visionarne le operazioni, a modificarne le impostazioni di sicurezza, a carpire informazioni delicate e privilegiate etc. In tali casi si è di fronte a un vero e proprio controllo del P.C. da remoto e l'agente potrebbe addirittura far compiere al sistema ogni e qualsivoglia tipo di operazione, fino a giungere al punto di "ricattare" il titolare del sistema stesso, venendosi così a configurare il reato di estorsione (art. 629 cp), che concorrerebbe sia con il delitto di cui all'art. 615ter, sia con quello di cui all'art. 615quater, sia con quello di cui all'art. 615quinquies cp, salvo, nella meno grave delle ipotesi e fuori dei casi di concorso, il reato di danneggiamento informatico (art. 635bis cp).

Talora il trojan viene usato dai cracker, i quali lo inseriscono per es. in videogiochi piratati, ma può essere scaricato anche direttamente (e ingenuamente) dall'utente inesperto, in genere durante la visita di siti pornografici o illegali (siti di virus-writer, di hacker, di cracker o nei quali si pratica la compravendita o il download gratuito di programmi e giochi di provenienza illecita o quanto meno dubbia).

[8] V. Cass. Sez.VI Pen. 4 ottobre - 14 dicembre 1999, n.3067, reperibile all'URL www.ictlex.net/index.php?p=102. La S.C. ha ritenuto che la rete telefonica può essere considerata *"sistema telematico"* ex art. 615ter cp, in quanto le linee di tale rete, nell'epoca moderna, utilizzano normalmente le tecnologie informatiche. Infatti la funzione di trasmissione delle comunicazioni si attua con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all'altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. È poi "sistema" anche il cd. centralino, che abiliti alla chiamata di determinate utenze e non di altre. Ma v'è di più: linee e centralino costituiscono sistemi informatici in quanto consentono di memorizzare e trattare elettronicamente le informazioni relative ai dati esterni alle conversazioni, come il numero dell'abbonato chiamante e di quello chiamato, il totale degli scatti, la data e l'ora della conversazione, che possono essere stampati su appositi tabulati contenenti il flusso di comunicazioni informatiche o telematiche (espressamente contemplato dall'art. 266bis cpp). Nella stessa sentenza è stato anche affermato il principio in base al quale la verifica delle caratteristiche di fatto in ordine alle tecnologie utilizzate spetta al giudice di merito ed è insindacabile avanti al giudice di legittimità se sorretta da motivazione adeguata. Per la definizione di sistema (nello stesso senso di cui sopra), cfr. anche Trib. di Spoleto, 6 Agosto 2001, n.154, reperibile all'URL http://www.ictlex.net/index.php/2001/06/08/trib-spoleto-sent-n-15401/.

In dottrina, S.Aterno (in *"Cassazione Penale"*, 2000, n.535) ritiene invece che potrebbe qualificarsi sistema informatico *"un apparato elettronico in grado di elaborare un numero elevato di dati/informazioni opportunamente codificato e capace di produrre come risultato un altro insieme di dati/informazioni codificato in maniera leggibile grazie ad un programma in grado di far cambiare lo stato interno dell'apparato e di variarne, all'occorrenza, il risultato"*. L'attenzione è qui spostata sulla elevata capacità di elaborazione di dati e/o di informazioni come caratteristica peculiare del sistema. Ponendo ciò come punto di partenza definitorio, si avrebbe una delimitazione e maggior precisazione del concetto, escludendosi per es. dalla nozione la playstation e il decoder, che eppure in passato sono stati considerati sistemi informatici dalla giurisprudenza. Come a dire che non bastano un software operativo e un microprocessore a fare un sistema (altrimenti, paradossalmente, potrebbero considerarsi tali anche la lavatrice e il forno a microonde!), bensì è necessario un quid pluris, che sta proprio nella capacità di svolgere molteplici operazioni, i.e. di elaborare, generare, codificare, decodificare, archiviare, organizzare, selezionare, modificare, estrarre, raffrontare, comunicare, porre in condivisione, interconnettere, cancellare un numero elevato di dati e informazioni.

[9] *"Firewall"*, lett. "muro di fuoco". Trattasi di una delle principali applicazioni della sicurezza informatica e consiste in un programma o software progettato per impedire accessi non autorizzati a computer e reti private (cd. *Intranet*) da parte di utenti remoti, che sfruttano la connessione alla Rete (a Internet, quindi). Il firewall in un certo senso "filtra" i dati che passano da un computer ad un altro sulla rete, in modo tale da tenere fuori tutto ciò che non è necessario far entrare nel sistema.

Esistono tuttavia altre applicazioni di sicurezza altrettanto importanti e in particolare:

- *"router"*: dispositivo software o hardware utilizzato per gestire le connessioni tra reti e per istradare i messaggi che su di esse viaggiano. Può avere la stessa efficacia del firewall, in quanto anch'esso filtra i messaggi, tanto in entrata quanto in uscita, e in genere si trova allocato all'interno del modem;
- *"IDS"* (acronimo per *"Intrusion Detection Systems"*): strumenti hardware e software usati per monitorare e analizzare i flussi di dati e informazioni all'interno di una rete privata con lo scopo di individuare eventi non conformi alla *security-policy* e all'attività istituzionale di un'azienda o di altra struttura. Gli IDS sono in grado, in caso di evento non previsto, di generare i cd. *"warning"* o avvisi di sicurezza (talora anzi trattasi di veri e propri allarmi). Talora gli IDS sono concepiti come *"sniffer"*, i.e. programmi che, connessi a un tratto o segmento di una Intranet, riescono a esaminare, senza essere rilevati, tutti i dati che vi transitano in un determinato frangente temporale, cosicché possano essere scoperte eventuali attività sospette e anomale condizioni di traffico. Altra importante applicazione degli IDS è la registrazione e la conseguente archiviazione dei *"file di log"*, ossia il tracciamento di tutte le operazioni, connessioni, comunicazioni, condivisioni avvenute all'interno di un elaboratore ovvero di una rete;
- *"IPS"* (acronimo per *"Intrusion Prevention Systems"*): sistemi di protezione basati su di un approccio *"proattivo"* (i.e. preventivo) più che reattivo (posteriore rispetto all'attacco). La loro principale funzione è quella di individuare e rilevare anomalie applicative come *"bug"* o *"exploit"* (le cd. "vulnerabilità") ovvero anomalie infrastrutturali (es. malfunzionamenti del router, rischio di blocco o interruzione di comunicazioni a causa di attacchi *"DoS"*, *"flooding"* o *"spamming"* in corso). Gli IPS talora consentono anche di ridurre determinate prestazioni degli elaboratori aziendali e della Intranet, soprattutto in riferimento ad attività che non solo non sono necessarie all'attività istituzionale, ma che potrebbero rilevarsi illecite, anche penalmente (es. violazione dell'e-copyright tramite piattaforme di *"file-sharing"* e *"peer to peer"*, navigazione non autorizzata e visita di siti a rischio come quelli pornografici, visita di siti pedopornografici o gestiti da cracker o inneggianti ad associazioni terroristiche e sovversive…).

[10] Come sopra detto per quel che concerne l'accesso "fisico", la forzatura di m.d.s. anche fisiche come elemento costitutivo del reato risulterebbe dalla previsione dell'aggravante di cui al co.2, n.2 dell'art. 615ter cp Inoltre per una definizione di m.d.s., vedasi l'art. 4, co.3, lett.a) del Codice della Privacy (d.lgs. 196/2003), che però riguarda solo le misure cd. "minime", che devono essere predisposte dal titolare del trattamento dei "dati personali" a protezione degli stessi. La suddetta norma definisce le misure minime di sicurezza come *"il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31"*. Le misure minime sono poi specificate nel *"Disciplinare tecnico in materia di misure minime di sicurezza"* o Allegato B al d.lgs. 196/2003. È appena il caso di dire che le suddette misure sono chiamate "minime" in quanto devono garantire quel minimo per l'appunto di protezione ai dati personali e per ottenere ciò è necessario che presentino determinate caratteristiche e abbiano una certa qual efficacia, oltre al fatto che devono essere periodicamente aggiornate e comunque adeguate alle conoscenze acquisite in base al progresso tecnico.

[11] Cfr. Cass. Sez.V Pen. 7 novembre 2000 (dep. 6 dicembre 2000), n. 1675 (12732/2005 - CED 217743), reperibile all' URL http://www.penale.it/page.asp?mode=1&IDPag=85. Tra gli strumenti organizzativi, cui fa riferimento la decisione, possono rammentarsi indubbiamente i controlli effettuati da guardie particolari giurate (o da parte di altro personale di sorveglianza) prima che sia consentito l'accesso ai locali aziendali, in cui siano collocati sistemi informatici. Altro strumento organizzativo potrebbe essere rappresentato dal servizio di video-sorveglianza, realizzato tramite uso di telecamere a circuito chiuso poste all'ingresso dei suddetti locali.

[12] In tal senso cfr. P.Galdieri, *"Teoria e pratica nell'interpretazione del reato informatico"*, Giuffré, Milano, 1997, p.155.

[13] Cfr. Cass. Sez.V Pen. 7 Novembre 2000 cit. La S.C., nel caso di specie, ha giustificato tale assunto partendo dalla distinzione tra le banche dati offerte al pubblico a determinate condizioni e le banche dati destinate a un'utilizzazione privata esclusiva, come i dati contabili di un'azienda. In questo secondo caso, a detta della S.C., sarebbe evidente infatti che, anche in mancanza di meccanismi di protezione informatica, commetterebbe il reato la persona estranea all'organizzazione che acceda ai dati senza titolo o autorizzazione, essendo implicita, ma intuibile, la volontà dell'avente diritto di escludere gli estranei. Se così fosse però, avrebbe ragione quella parte della dottrina (cfr. Mucciarelli, op.cit., p.99), che sostiene che un sistema meriterebbe tutela penale sol che si sia in presenza di un divieto espresso dal soggetto titolare dello ius excludendi (basterebbe insomma, per es., un cartello con la dicitura "vietato l'ingresso"), a prescindere cioè dal fatto che un computer sia munito o meno di misure di protezione. Tale impostazione sembrerebbe una forzatura delle previsioni di cui all'art. 615ter cp, vista la chiara lettera della norma, in

virtù dei principi di precisione, tassatività e sufficiente determinatezza del reato vigenti nell'ordinamento penale. A tal proposito cfr. di seguito note 14 e 17.

In linea con la suddetta Cass. 7 Novembre 2000 cit., v. Cass. Sez.V Pen. 14 Ottobre 2003, n.44362 (in *"Cassazione Penale"*, fasc.5, 2005, p.1580 e ss., con nota critica di S.Aterno), la quale ribadisce che la violazione delle m.d.s. non assume rilevanza in sé, «*bensì solo come manifestazione di una volontà contraria a quella di chi del sistema legittimamente dispone»*. Partendo da tale presupposto, la S.C. ha stabilito che il titolare di un esercizio commerciale che utilizza sul terminale *"P.O.S."* (*"point of sale"*) in dotazione una carta di credito contraffatta compie il delitto di cui all'art. 615ter c.p. in quanto *«se è vero che il titolare dell'esercizio è legittimato ad utilizzare il terminale P.O.S., non è men vero che nel caso in esame tale utilizzo avviene utilizzando una chiave d'accesso contraffatta, sì che l'accesso assume carattere abusivo»*.

A dire il vero, la decisione della S.C. non convince fino in fondo. Invero duplicare una carta di credito ("clonarla", come anche si dice) attraverso l'utilizzo di un particolare apparecchio, chiamato *"skimmer"* (come è nel caso sottoposto all'attenzione della S.C.), sembrerebbe condotta rientrante in altra e diversa fattispecie criminosa. Ci si riferisce all'art. 12 del D.L. 3 Maggio 1991, n. 143 (convertito con modificazioni nella legge 5 Luglio 1991, n. 197), che qui, per comodità, si riporta per intero:

Art. 12 - Carte di credito, di pagamento e documenti che abilitano al prelievo di denaro contante.

"1. Chiunque, al fine di trarne profitto per sé o per altri, indebitamente utilizza, non essendone titolare, carte di credito o di pagamento, ovvero qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, è punito con la reclusione da uno a cinque anni e con la multa da lire seicentomila a lire tre milioni. Alla stessa pena soggiace chi, al fine di trarne profitto per sé o per altri, falsifica o altera carte di credito o di pagamento o qualsiasi altro documento analogo che abiliti al prelievo di denaro contante o all'acquisto di beni o alla prestazione di servizi, ovvero possiede, cede o acquisisce tali carte o documenti di provenienza illecita o comunque falsificati o alterati, nonché ordini di pagamento prodotti con essi."

Si ricordi che lo skimmer è un lettore che cattura i dati della banda magnetica con la semplice *"strisciata"* della carta di credito su di esso. Questo dispositivo arriva ad immagazzinare, tramite una memoria *eprom*, diverse decine di bande magnetiche. Successivamente lo skimmer viene collegato a un PC, munito di un programma di gestione per bande magnetiche e si trascrivono i dati, presi illecitamente, su un supporto plastico con le caratteristiche di una carta di credito o bancomat (fonte Polizia di Stato; per maggiori approfondimenti cfr. l'URL http://www.poliziadistato.it/pds/primapagina/cartedicredito/skimmer.htm).

14 Sull'importanza delle m.d.s., cfr. F.Berghella, R.Blaiotta, *"Diritto penale dell'informatica e dei beni giuridici"*, in *"Cassazione Penale"*, 1995, p.2334 e s. Ad opinione di tali Aut. la violazione delle m.d.s. costituirebbe anzitutto un chiaro indice dell'atteggiamento psicologico dell'agente, i.e. della sua volontà aggressiva in presenza di una contraria volontà. Inoltre l'abbattimento delle difese predisposte segna il momento dell'obbiettiva e fattuale aggressione al sistema, in ossequio al principio di offensività dell'illecito penale, in un ordinamento, come quello italiano, che bandisce ogni forma di soggettivismo e di "processo all'intenzione" (*"nemo cogitationis poena patitur"*; v. anche art. 25, co.2 Cost.). Ergo è tale momento che traccia il confine tra condotte scorrette, ma nel contempo diffuse e prive di contenuto seriamente antisociale, e condotte da considerarsi propriamente delittuose e da reprimere. Le m.d.s. non possono alfine costituire una simbolica affermazione di esclusività, ma al contrario devono essere un vero e proprio ostacolo, serio e anche difficile da superare. Ma tali considerazioni possono essere estese altresì alla seconda tipologia di condotta (il mantenersi nel sistema contro la volontà dello ius excludendi), poiché anche in tal caso la norma non vuole punire il solo fatto di restare nel sistema e di utilizzarlo oltre il limite temporale stabilito. Orbene, anche in tal caso il *modus operandi* dell'agente deve rivelare una volontà di serio e positivo contrasto nei confronti delle difese del sistema (per es. come nel caso in cui l'utente, che subisca per un qualsivoglia motivo limitazioni temporali nella fruizione di un sistema, disattivi la procedura di espulsione automatica al termine del periodo consentito o eludendo il limite temporale stesso). Solo così possono recuperarsi, nel delitto de quo, insieme col principio di offensività, anche quelli di sussidiarietà e frammentarietà dell'illecito penale e di meritevolezza della pena, in modo che il potere punitivo dello Stato non sia sentito come paternalistico o, peggio, odioso dalla collettività sociale. D'altronde in uno Stato liberale e democratico la sanzione penale (in ossequio ai suddetti principi) non può che costituire l'*extrema ratio*, laddove abbiano fallito tutti gli altri tentativi di contrasto (sanzioni civili, disciplinari, amministrative).

15 In tal senso v. G.I.P. Roma, Sez. 8a, sent. 4-21 Aprile 2000 (reperibile all'URL www.fiammella.it/tribunale_penale_di_roma_GR1.htm). In tale decisione il giudice ha stabilito che con l'art. 615ter cp il legislatore *«ha inteso tutelare non la privacy di qualsiasi "domicilio informatico", ma soltanto quella di sistemi "protetti" contro il pericolo di accessi da parte di persone non autorizzate»*. Ma non solo: sembra che il giudice de quo si sia spinto oltre ed infatti in motivazione si legge che *«i tradizionali mezzi di protezione software, in particolare quelli incentrati sulle cd. chiavi d'accesso non offrono certezza assoluta di impenetrabilità, essendo la loro individuazione soltanto una questione di tempo a livello tecnologico»*, dalla quale affermazione si potrebbe inferire che l'esistenza non di una qualsivoglia m.d.s., bensì di m.d.s. efficaci sia elemento costitutivo della fattispecie incriminatrice.

16 In dottrina, sulla necessità che le m.d.s. siano attuali, cfr. G.Pica, op.cit., p.60.

17 V. Cass. Sez.VI Pen. 27 Ottobre 2004 (dep. 30 Novembre 2004), n. 46509, il cui testo integrale è consultabile all'URL http://www.penale.it/page.asp?mode=1&IDPag=174. Anzi la S.C. ha anche aggiunto che il fatto che l'imputato facesse un uso distorto del computer a fini illeciti e personali, *«non sposta i termini della questione, mancando il presupposto della "protezione" speciale del sistema stesso. Da tale reato pertanto l'imputato deve essere assolto perché il fatto non sussiste»*. Il tutto in evidente omaggio al principio di tassatività, cardine invero del diritto penale moderno.

18 V. Cass. 32440/2003 cit. Ma v. anche Cass. 3067/1999 cit., laddove si afferma che con l'espressione "domicilio informatico" si vuole indicare lo *«spazio ideale (ma anche fisico in cui sono contenuti i dati informatici), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art. 14 Cost.)»*. Sul concetto di domicilio informatico quale luogo anche fisico, cfr. G.Pica, op.cit., p.62, dal momento che i dati informatici, in un certo qual senso, esistono fisicamente sub specie di simboli memorizzati nell'hardware.

19 Cfr. R.Borruso, op.cit., p.28.

[20] Cfr. P.Galdieri, op.cit., p.143.
[21] Cfr. P.Galdieri, op.cit., p.146, secondo il quale dovrebbero escludersi dalla tutela apprestata dall'art. 615ter cp le persone giuridiche e gli enti di fatto. La *"pax domestica"* rientrerebbe dunque nell'oggetto giuridico rilevante e meritevole di protezione da parte della norma de qua, (né più né meno come nel caso dell'art. 614 cp), non così la *"pax aziendale"*. Inoltre secondo l'Aut. il carattere strettamente "personale" dei dati e delle informazioni oggetto di protezione ex art. 615ter c.p. impedirebbe che tramite detta norma possa essere garantita tutela anche a enti o persone giuridiche che non riconoscono al loro interno i diritti del singolo.
[22] V. Cass. 3067/1999 cit. Nella stessa decisione si afferma che *«ove il legislatore ha avuto l'intento di tutelare la privacy vi ha espressamente fatto riferimento in modo inequivocabile, sia nella legislazione meno recente (v. la l. 8 Aprile 1974, n.98, il cui art.1 ha introdotto nel codice penale, sotto la rubrica "interferenze illecite nella vita privata" l'art. 615bis), sia in quella più vicina (v. la l. 31 Dicembre 1996, n.675, sulla "tutela delle persone o di altri soggetti rispetto al trattamento dei dati personali")»*.
[23] Cfr. G.Pica, op.cit., p.65.
[24] Cfr. G.Pica. op.cit., p.61. Tale Aut. peraltro mette in evidenza come con l'art. 615ter cp si sia offerto un contributo non da poco alla tutela preventiva del *"know-how"* industriale, colmando una lacuna dell'ordinamento che vedeva concentrate tutte le forme di tutela (civili o penali) quasi esclusivamente sui momenti successivi alla mera cognizione del segreto altrui (per es. le condotte di rivelazione e diffusione, nonché di uso di segreti scientifici e industriali ex art. 623 cp, ma possono mentovarsi anche l'art. 325 cp e gli artt. 88 e 89 del r.d. 29 Giugno 1939, n.1127).
[25] Secondo F.Berghella, R.Blaiotta. op.cit., p.2333, con l'art. 615ter cp in realtà il legislatore ha inteso tutelare il sistema informatico come bene di straordinario rilievo nell'attuale stato della società. Come nel 1930, in una società contadina, il codificatore proteggeva da ogni possibile turbativa la proprietà fondiaria che allora costituiva bene economico-produttivo preminente, sanzionando (ex art. 637 cp) *"chiunque senza necessità entra nel fondo altrui recinto da fosso, da siepe viva o da un altro stabile riparo"*, così nell'attuale società dominata dall'informatica viene protetto il computer da quelle intrusioni che costituiscono un ostacolo alla esclusiva, indisturbata fruizione del sistema da parte del gestore. E (sempre secondo tali Aut.) la somiglianza tra art. 615ter e art. 637 cp appare tanto più stringente (sebbene con tutte le dovute cautele e distinzioni del caso) sol se si pensi che in entrambi i casi si ha, sotto il profilo della condotta, l'indebita intrusione nell'ambito di un bene alieno protetto da adeguate misure di interdizione.
[26] V. a tal proposito Cass. 3067/1999 cit., che ha affermato che *«con il riferimento al "domicilio informatico", sembra che il legislatore abbia voluto individuare il luogo fisico - come sito in cui si può estrinsecarsi la personalità umana nel quale è contenuto l'oggetto della tutela (qualsiasi tipo di dato e non i dati aventi ad oggetto particolari contenuti), per salvaguardarlo da qualsiasi tipo di intrusione (ius exludendi alios), indipendentemente dallo scopo che si propone l'autore dell'abuso»*.
[27] Cfr. F.Mantovani, op.cit., p.455.
[28] Cfr. G.Pica, op.cit., p.70. L'Aut. porta taluni esempi al riguardo. Il caso di un dipendente d'ufficio il quale, a causa di un improvviso guasto al proprio P.C., vada ad accendere quello (munito di password) di un collega per usare un medesimo programma e continuare così il proprio lavoro. Si pensi ancora alle procedure di test del sistema (sfida ad accedere allo stesso per verificarne il livello di sicurezza o la resistenza delle protezioni), ovvero all'ipotesi in cui un collaboratore dell'azienda titolare acceda al computer con metodi formalmente non regolari per aver dimenticato la password o per aver smarrito la chiave d'accesso hardware etc.
[29] Secondo il Pica (op.cit., p.58) anche la condotta di accesso sostanzierebbe un'ipotesi di reato permanente, sol che si consideri la sequenza introduzione-successivo mantenimento, mentre l'istantaneità potrebbe aversi solo nel caso in cui l'agente, introdottosi nel sistema, ne esca subito per sua volontà o per intervento del titolare che riesca ad intercettarlo per poi escluderlo.
[30] Cfr. G.Pica, op.cit., p.59.
[31] Cfr. Trib.Torino Sez.IV Pen. 7 Febbraio 1998, reperibile all'URL http://www.penale.it/page.asp?mode=1&IDPag=91. Il collegio ha peraltro precisato che *«il reato de quo è da considerarsi perfezionato sia nel caso in cui all'atto dell'introduzione nel sistema informatico già si sia maturata la decisione di duplicare abusivamente i dati contenuti nel medesimo, e sia anche nel caso in cui, possedendo per ragioni di servizio una duplicazione di quei dati, si decida di farne uso ben essendo a conoscenza della contraria volontà del titolare del diritto»*. Si ricordi poi che nella relazione ministeriale al disegno di legge sui computer-crimes può leggersi quanto segue*: «la sottrazione di dati, quando non si estenda ai supporti materiali su cui i dati sono impressi (nel qual caso si configura con evidenza il reato di furto), altro non è che una "presa di conoscenza" di notizie, ossia un fatto intellettivo rientrante, se del caso nelle previsioni concernenti la "violazione dei segreti"»*, dal che può inferirsi che in determinate situazioni potrebbero esser realizzato altresì un altro e diverso reato rispetto al furto o all'accesso abusivo, quale per es. il delitto di cui all'art. 621 cp (ipotesi peraltro presa in considerazione proprio dal Trib. di Torino nella decisione citata).
[32] In tal senso cfr. G.Pica, op.cit., p.74 e ss.
[33] Cfr. R.Borruso, op.cit., p.73. Contra F.Mucciarelli (op.cit., p.102), secondo il quale, acciocché possa configurarsi l'aggravante de qua, sarebbe necessaria qualche conoscenza superiore o comunque ulteriore e specifica rispetto a chi invece possa solo contattare il sistema (almeno la parte meccanica o hardware).
[34] Così G.Pica, op.cit., p. 74 e ss.
[35] *"Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, è punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.*
Se ricorre una o piu' delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni".
L'art. 635bis c.p. è stato introdotto dall'art. 9 della l. 547/1993.
[36] Cfr. in tal senso F.Mucciarelli, op.cit., p.103.
[37] L'aggravante di cui al co.3 fa sorgere altri dubbi sull'oggetto giuridico protetto, vista la particolare natura dei sistemi contemplati e peraltro crea qualche problema di coordinamento con l'art. 420 cp (attentato ad impianti di pubblica utilità).
[38] Cfr. Cass. 3067/1999 cit. e Trib.Spoleto 154/2001 cit.

[39] Contrariamente a quanto si pensa, non è diverso l'elemento psicologico, dacché entrambi i delitti sono a dolo generico. Nella frode informatica infatti lo scopo di profitto (proprio o altrui) con contemporaneo danno della vittima sono eventi finali del reato, mentre l'evento intermedio è rappresentato dall'induzione in errore del sistema informatico, che viene per l'appunto manipolato o alterato o illecitamente sfruttato per raggiungere l'obbiettivo che il malintenzionato (sia questi un hacker, un cracker etc.) si era prefissato, vale a dire per l'appunto lo scopo di profitto (proprio o di terzi) con contemporaneo danno dell'utente. In ciò sta anche la differenza fondamentale con il delitto di truffa (art. 640 cp), laddove ad essere ingannato con artifizi o raggiri è l'essere umano, il quale pone in essere un atto dispositivo patrimoniale, recando danno a se stesso (cd. "artificiosa partecipazione della vittima").

Tipico es. di frode informatica è quella che viene posta in essere tramite l'utilizzo dei cd. *"web-dialer"* (dall'inglese *"to dial"*, comporre). Il dialer è un programma per computer di pochi kilobyte (quindi molto semplice e di facile istallazione), che crea una connessione ad un'altra rete di calcolatori o semplicemente ad un altro computer tramite la comune linea telefonica o tramite un collegamento I.S.D.N. In genere tali programmi sono associati a servizi a valore aggiunto, *rectius* a tariffazione elevata o speciale. Se è vero che esistono dialer legittimi (in quanto richiesti e voluti dall'utente), ne esistono tuttavia di illegali, poiché *"manipolano"* il sistema, lo alterano, intervengono su di esso in modo illecito, senza consenso dell'utente, a sua insaputa, istradandolo a numeri telefonici ad alto costo. Molti siti Web promettono di fornire gratuitamente loghi e suonerie per telefoni cellulari ovvero canzoni e altri file in formato "mp3", ma anche ricette culinarie, software, film e immagini pornografiche, a patto che il cybernauta istalli un certo programma, anch'esso offerto gratuitamente. Ma tale programma è in realtà un dialer, che dunque, una volta istallato nel sistema, può provocare danni patrimoniali notevoli (per es. bollette telefoniche di svariate migliaia di Euro). Talora i dialer sono contenuti in software trojan.

[40] Il delitto di cui all'art. 615quater cp è tipico reato di pericolo o se si vuole di "sospetto" o "ostativo", laddove vengono punite condotte meramente preparatorie rispetto al reato di cui all'art. 615ter cp. Ergo trattasi di norme complementari e integrative miranti alla tutela dello stesso interesse (il domicilio informatico per l'appunto).

[41] In base alla Decisione quadro, la responsabilità delle p.g. andrà prevista anche per il reato di danneggiamento informatico (art. 635bis c.p.) e, probabilmente, di interferenza illecita su dati e sistemi (presumibile, nel nostro ordinamento, il riferimento al delitto di cui all'art. 617quater cp). L'art.5 della Decisone quadro prevede poi che rilevino come reati anche l'istigazione, il favoreggiamento nonché la complicità e il tentativo in ordine alla commissione dei reati suddetti (oltre a quello di accesso abusivo ovviamente) e che anche in tali casi sussista la responsabilità delle p.g.

La Decisione quadro si occupa poi anche di altre problematiche e stabilisce l'introduzione di alcune particolari aggravanti per i reati informatici di cui si è detto (art.7) e detta linee-guida per risolvere problemi di giurisdizione e di estradizione (art.10).

È appena il caso di dire che in Italia già è prevista la responsabilità delle p.g. (v. d.lgs. 8 giugno 2001, n.231) per taluni crimini informatici specifici commessi nel loro interesse, quali:

- la frode informatica aggravata ex art. 640ter, co.2, 1a parte cp (tramite il rinvio alla figura generale dell'art. 640 co. 2, n. 1 cp: truffa aggravata dal fatto che il delitto sia stato commesso a danno dello Stato o di altro ente pubblico);
- il delitto di cui all'art. 270ter cp, nella parte in cui sanziona chiunque, fuori dei casi di concorso nel reato e di favoreggiamento, offre strumenti di comunicazione a taluna delle persone che partecipano ad associazioni sovversive (art. 270 cp) o con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270bis cp);
- i delitti di pornografia minorile di cui all'art. 600ter, co.3 e 4 cp (quando realizzati per via telematica) e il reato di detenzione di materiale pornografico di cui all'art. 600quater cp (sempre se realizzato tramite tecnologie info-telematiche).