COMMENTO AL REATO DI ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO, DI CUI ALL'ART. 615-TER C.P., ALLA LUCE DELLE PRONUNCE GIURISPRUDENZIALI

Dott. Giovanni Modesti[i]

SOMMARIO. INTRODUZIONE. 1. IL PANORAMA NORMATIVO ITALIANO. 1.1 VIOLAZIONE DI DOMICILIO. 1.2 LA LEGGE N. 547 DEL 23.12.1993. 2. IL REATO DI ACCESSO ABUSIVO. 2.1 LA NOZIONE DI MISURA DI SICUREZZA. 3. LE PRONUNCE GIURISPRUDENZIALI. CONCLUSIONE.

INTRODUZIONE

A partire dalla seconda metà degli anni ottanta è stata avvertita la esigenza di elaborare una disciplina normativa in materia di criminalità informatica[ii].

I primi Paesi a sollevare il problema e a porlo alla attenzione non solo del mondo giuridico ma anche di quello dei media furono gli Stati Uniti[iii] e, successivamente, la Gran Bretagna.

Gli USA cominciarono con il definire i concetti base di tale disciplina, computer[iv], dispositivo elettronico[v], sistema informatico[vi], sistema telematico[vii], per poi procedere ad una loro normazione. A tale proposito va distinta la normativa adottata dalla legge federale e quella prodotta dai singoli stati; a livello della prima vanno citati in particolare due atti adottati, rispettivamente nel 1984 e nel 1986, che hanno consentito di estendere la disciplina in questione oltre che ai computer ai sistemi telematici, mentre hanno escluso dal novero della normativa sistemi elettronici con modeste capacità di elaborazione.

In merito al reato di accesso abusivo si registrò un diverso approccio al problema, infatti: mentre la legge federale disciplinava delle ipotesi di accesso abusivo ai dati, in base ai concetti di riservatezza, a livello di singoli stati, invece, la figura di reato veniva ricondotta alle fattispecie di danneggiamento e di alterazione dei dati.

In Gran Bretagna, con legge del 1990 furono individuate tre ipotesi di reato: "l'accesso abusivo finalizzato alla apprensione di informazioni riservate di tipo politico, militare, energetico, l'accesso abusivo finalizzato ad ottenere informazioni

di tipo finanziario , e l'accesso abusivo finalizzato a rilevare o distruggere dati contenuti in computer governativi[viii]"

1. IL PANORAMA NORMATIVO ITALIANO

Nel nostro Paese è necessario distinguere, sostanzialmente, due fasi: quella precedente la introduzione della legge n. 547 del 1993 e quella ad essa successiva.
Nella prima fase mancando una esplicita disciplina normativa della fattispecie oggetto di studio di questo contributo, la dottrina si vide costretta ad accostare la figura del reato di accesso abusivo a norme che disciplinavano fattispecie analoghe, pur tenendo a mente che in materia penale il ricorso alla analogia è vietato.
Le teorie esplicitate furono sostanzialmente tre: 1. una che riconduceva l'accesso abusivo al reato di violazione di domicilio, ex art. 614 c.p.; 2. la seconda che riteneva essere l'accesso abusivo una particolare ipotesi del reato di sostituzione di persona, ex art. 494 c.p.; 3. la terza elaborazione dottrinale chiamava in causa l'art. 632 c.p. in materia di intercettazione delle comunicazioni telefoniche e telegrafiche.
Merita un cenno di riflessione la prima teoria in quanto la più vicina a descrivere la fattispecie oggetto di questo studio.

1.1 VIOLAZIONE DI DOMICILIO

Il reato di violazione di domicilio comune[ix], ex art. 614 cp, può presentarsi in due forme:

a. quando taluno si introduce nell'abitazione altrui o in altro luogo di privata dimora o nelle appartenenze di essi, contro la volontà espressa o tacita di chj ha il diritto di escluderlo, o vi si introduce clandestinamente o con inganno;
b. allorché un individuo si trattiene nei detti luoghi contro l'espressa volontà di chi ha il diritto di escluderlo, o vi si trattiene clandestinamente o con inganno.

L’elemento oggettivo del reato presuppone che il soggetto attivo si introduca o si trattenga nell’abitazione altrui o in un altro luogo di privata dimora o in una loro appartenenza.
Titolare del diritto di esclusione deve ritenersi colui che attualmente e legittimamente abita o dimora in un certo luogo o chi lo rappresenta in caso di impedimento.
Il delitto si consuma, nella prima forma, quando l’agente si introduce nel luogo di privata dimora contro la volontà del titolare del diritto di escluderlo o in modo clandestino o con l’inganno; nella seconda forma, allorché l’agente comincia a trattenervisi contro tale volontà o in uno dei detti modi.
La violazione di domicilio è un reato eventualmente permanente.
Per la sussistenza del dolo occorre nell’agente:

a. la volontà di entrare o di soffermarsi in un luogo di privata dimora;
b. la consapevolezza che tale luogo è altrui;
c. che la permanenza o l’ingresso avvenga invito domine.

1.2 LA LEGGE N. 547 DEL 23.12.1993

Recependo le indicazioni contenute nella Raccomandazione[x] del Consiglio d’Europa del 13.9.1989, precisamente la “Reccomandation n° R899 du Comitè des Ministres aux etats membres sur la criminalità en relation avec l’ordinateur (adoptè pour le Comitè des Ministres le 13 septembre 1989, lors de la 428° reunion des Delegues des Ministres”, il nostro legislatore promulgò la legge n. 547/93.
Con tale legge si riconobbe un valore giuridico a tutta una serie di condotte illecite poste in essere su elaboratori elettronici che fino a quel momento non potevano essere pienamente perseguiti e introdusse il reato di frode informatica.
Attraverso tale norma si apportarono modifiche ed integrazioni al codice penale e a quello di procedura penale, in materia di crimini informatici.
Da rilevare che di fronte alla scelta se licenziare una norma penale specifica oppure introdurre le nuove fattispecie di reato all’interno del Codice Penale, il legislatore ha

adottato la seconda soluzione andando a novellare gli articoli del codice. Tale scelta finisce per avere una valenza ideologica, oltre che sistematica, in quanto sancisce la negazione – da un punto di vista giuridico – del concetto di bene informatico, al quale quindi non è riconosciuta una autonoma tutela penale, e, la contestuale assunzione dello strumento informatico al rango di mezzo.

I reati informatici si distinguono, solitamente, in due categorie a seconda che la presenza dell'elemento informatico – computer, elaboratore, sistema telematico, ecc. – sia conditio sine qua non per la venuta ad esistenza del reato stesso o meno. Si distinguono così i reati necessariamente informatici dai reati eventualmente informatici. Inoltre, i delitti contro i sistemi informatici o telematici sono raggruppabili in tre categorie: a) accesso[xi] ad un sistema informatico, b) attacco[xii] ad un sistema informatico, c) virus[xiii].

Da rilevare che la legge 547/93 omette la definizione di sistema informatico, dandola per presupposta. Riteniamo, quindi, di potere fare riferimento a quanto sancito dalla Cassazione, Sezione penale VI, con sentenza n. 3067/99, secondo cui "Sulla base del dato testuale pare comunque che si debba ritenere che l'espressione "sistema informatico" contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime…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.

L'art. 4 della legge 547/1993, introduce tre figure di illecito e lo fa attraverso altrettanti articoli del codice penale, precisamente: l'art. 615 ter, che tutela l'accesso abusivo ad un sistema informatico o telematico, l'art. 615 quater[xiv] che punisce la detenzione e la diffusione abusiva di codici di accesso a sistemi informatici o telematici e, l'art. 615 quinquies[xv], che punisce la diffusione di programmi diretti a danneggiare o interrompere un sistema informatico.

In merito all'art. 4 sopra menzionato, la Cassazione[xvi] ha stabilito che, "il legislatore ha dettato un sistema completo di norme in tema di criminalità informatica, considerando i sistemi informatici e telematici alla stregua del domicilio".

2. IL REATO DI ACCESSO ABUSIVO

Art. 615 ter Accesso abusivo ad 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 volonta' espressa o tacita di chi ha il diritto di escluderlo, e' punito con la reclusione fino a tre anni. La pena e' della reclusione da uno a cinque anni: 1) se il fatto e' 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 qualita' di operatore del sistema; 2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se e' 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 sanita' o alla protezione civile o comunque di interesse pubblico, la pena e', rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni. Nel caso previsto dal primo comma il delitto e' punibile a querela della persona offesa; negli altri casi si procede d'ufficio".

Sono state previste due distinte condotte che consistono, rispettivamente, nell'accesso[xvii] e nel mantenimento all'interno di un sistema informatico.

L'accesso abusivo ad un sistema informatico si verifica, quindi, nella ipotesi in cui un soggetto si introduce in un sistema informatico o telematico protetto da misure di sicurezza. La seconda ipotesi si verifica allorché un soggetto autorizzato ad accedere

ad un sistema informatico vi si trattenga successivamente al periodo temporale necessario a giustificare la presenza nello stesso sistema per il quale aveva ricevuto la autorizzazione.

In entrambi i casi si può parlare di reato di azione[xviii] in quanto il reato consiste nel semplice compimento dell'azione e, precisamente, dui un reato di azione commissivo poiché la condotta tipica è rappresentata da un agire positivo..

Oggetto della condotta incriminata può essere tanto un sistema informatico quanto un sistema telematico; si tratta, adesso, di stabilire quale sia il bene giuridico[xix] protetto dall'art. 615 – ter c.p. e, precisamente, se debba farsi riferimento al concetto di domicilio informatico oppure a quello di riservatezza informatica.

La nozione di domicilio informatico[xx] è stata sviluppata prendendo a prestito quella di domicilio comune, così come esplicitata dalla Costituzione, mentre il concetto di riservatezza informatica[xxi] lo si desume attraverso la normativa che disciplina il trattamento dei dati personali. Appare, in prima battuta, preferibile l'adozione del secondo concetto che certamente offre una più compiuta forma di tutela[xxii].

La dottrina ha elaborato in proposito una serie di teorie che andiamo ad esporre, per sottoporle alla attenzione di chi legge:

1. poiché l'art. 615 –ter c.p. è stato inserito tra i delitti contro la inviolabilità del domicilio, si desume che oggetto della tutela è il bene giuridico del domicilio informatico;
2. le fattispecie incriminate si concretizzerebbero nella aggressione, sotto diverse forme, del bene relativo alla integrità dei dati e dei programmi; oggetto del reato sarebbe il patrimonio.
3. oggetto di disciplina dell'articolo in questione sarebbe la tutela contro la violazione della riservatezza dei dati e dei programmi contenuti in un sistema informatico. Questa ultima teoria che ha ricevuto l'avallo da parte di autorevole dottrina[xxiii] sembra essere la più rispondente alla definizione della fattispecie.

Circostanze aggravanti disciplinate dall'art. 615 ter cp sono:

a. 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 sua funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore di sistema[xxiv];
b. se il colpevole per commettere il fatto usa violenza sulle cose o alle persone ovvero se è palesemente armato;
c. 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.

Tale reato può essere commesso da chiunque ed è di tipo mono soggettivo, non richiedendo la partecipazione di una pluralità di soggetti agenti.

Esso è un reato di tipo comune, in quanto può essere commesso da chiunque.

L'illecito si consuma con la introduzione nel sistema informatico o telematico, contro la volontà del titolare, nella prima ipotesi; con la permanenza contro tale volontà nella seconda ipotesi.

In merito alla forma, il reato è sicuramente a forma vincolata perché la sua realizzazione presuppone una determinata condotta, che si realizza con l'introduzione abusiva o con il mantenimento abusivo.

Trattasi di un reato di pericolo[xxv], poiché esiste il rischio che chi accede abusivamente a un sistema abbia la capacità di impadronirsi o venire a conoscenza dei dati in esso contenuti. In merito alla successiva suddivisione, approntata dalla dottrina, tra reati di pericolo concreto e reati di pericolo presunto: nei primi il pericolo è elemento costitutivo della fattispecie incriminatrice mentre nei secondi il pericolo si presume. Il reato di accesso abusivo di cui all'art. 615-ter cp risulta essere, quindi, un reato di pericolo presunto.

Trattasi, inoltre, di un reato doloso[xxvi], dolo generico in quanto colui che accede abusivamente o si intrattiene contro la volontà del dominus, ha in sé la coscienza e la volontà di realizzare gli eventi costitutivi di un reato.
Il reato di cui sopra è procedibile a querela di parte, in merito al comma 1, d'ufficio per gli altri commi.

2.1 LA NOZIONE DI MISURA DI SICUREZZA

Dal testo normativo si evince che il reato si concreta non semplicemente a seguito dell'accesso tout court ad un sistema informatico ma richiede che tale sistema sia "protetto da misure di sicurezza". La presenza di misure di sicurezza atte a proteggere l'elaboratore è da considerare, quindi, come elemento costitutivo della fattispecie.
Per la definizione di tale concetto ci viene in soccorso il legislatore attraverso la disciplina della materia inerente il trattamento dei dati personali precisamente il Decreto Legislativo n. 196/2003 e l'All. B a tale Decreto, denominato "Disciplinare tecnico in materia di misure di sicurezza".
E' l'art. 31[xxvii] del decreto a stabilire l'obbligo a carico del titolare della adozione delle misure di sicurezza al fine di proteggere i dati personali che sono oggetto di trattamento. Ma le misure di sicurezza, di tipo tecnico, informatico, organizzativo, logistico e procedurali, sono oggetto di disciplina anche attraverso l'Allegato B al Codice.
Il legislatore ha stabilito che le misure di sicurezza vadano distinte in due categorie: le misure di sicurezza idonee e le misure di sicurezza minime. Le prime non sono elencate nel testo di legge ma vanno estrapolate dal titolare sulla scorta delle conoscenze tecniche ed organizzative esistenti al momento in cui il danno si è avuto[xxviii]. Le seconde sono state elencate dal legislatore nell'Allegato B e riguardano, in estrema sintesi: le credenziali di autenticazione, l'autenticazione informatica, l'autorizzazione, la protezione da programmi maligni, la prevenzione dalle

vulnerabilità, il salvataggio dei dati, il backup e il ripristino dei dati, l'adozione del documento programmatico sulla sicurezza, la certificazione delle misure minime di sicurezza, ecc.. La violazione delle prime comporta a carico del titolare ed, eventualmente , del responsabile se è stato espressamente incaricato di curare tale aspetto, l'applicazione di sanzioni penali. La violazione delle misure idonee comporta, invece, la comminazione di sanzioni civili.

Dalla lettura della normativa sopra richiamata si evince che le misure di sicurezza si inseriscono nell'ambito di un generale obbligo di proteggere i dati e i sistemi informativi che trattano tali dati.

L'adozione di misure di sicurezza deve effettuarsi in base al principio dinamico per il quale le misure variano con il tempo, a seguito –soprattutto- dell'evoluzione tecnologica.

In merito al reato di cui all'art. 615-ter c.p., per prevenire accessi abusivi volontari dall'interno o dall'esterno dell'azienda, occorre adottare i firewall[xxix], gli screening router[xxx] e gli Ids[xxxi].

Ebbene, è su tale concetto, o meglio, sulla definizione di misure di sicurezza e, soprattutto, del grado che tali misure debbono raggiungere., che si registrano a livello giurisprudenziale delle divergenze.

3 LE PRONUNCE GIURISPRUDENZIALI

Ci limitiamo a citare una serie di sentenze, espresse in merito a tale fattispecie di reato, tra loro non sempre concordi, ma che risultano utili al fine di fare luce su alcuni dei più importanti aspetti della materia.

La **Cassazione penale con sentenza n. 3067 del 4.10.99[xxxii],** ha fornito una serie di delucidazioni in merito all' estensione del reato in trattazione disponendo che " …l'espressione sistema informatico" contenga in sé il concetto di una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all'uomo, attraverso l'utilizzazione…di tecnologie informatiche. Queste ultime… sono caratterizzate dalla

registrazione…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;…" in merito all'oggetto giuridico della tutela approntata attraverso l'art. 615 ter in tale pronuncia si è sancito che il legislatore – inserendo la norma nella sezione IV del capo III del titolo XIII del libro II "Ha preso a parametro il "domicilio fisico" dell'individuo…" ed in questo modo ha inteso "…assicurare la protezione del "domicilio informatico", quale 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.)…".

In merito alla estensione da attribuire alla tutela garantita dall'art. 615 ter la suprema Corte individua due teorie che riporta nella sentenza de quo: " …lo scopo avuto di mira dal legislatore (è) stato quello di tutelare soltanto i contenuti personalissimi (cioè attinenti al diritto alla riservatezza della vita privata) dei sistemi informatici…mentre vi è chi riconosce che la norma in parola debba estendersi nel senso che essa abbia ad oggetto lo jus escludendi del titolare del sistema informatico, quale che sia il contenuto dei dati racchiusi in esso, purchè attinente alla propria sfera di pensiero o alla propria attività…". La Corte adotta il secondo indirizzo poiché, a suo dire, la norma non opera distinzioni tra sistemi a seconda dei contenuti.

Il **Tribunale Penale di Roma con sentenza del 21 aprile del 2000**[xxxiii], ha disposto quanto segue: " Considerato che l'esistenza di mezzi efficaci di protezione è elemento costitutivo della fattispecie incriminatrice di cui all'art. 615-ter c.p., deve dichiararsi il non luogo a procedere…". In altre parole il giudice non ha ritenuto sufficiente per la realizzazione del reato la esistenza di misure di sicurezza ma ha ritenuto che tali misure debbano essere adeguate ad un determinato standard al di sotto del quale non si configura il reato in oggetto.

La **Cassazione Penale, sez. V, con sentenza n. 12732 del 6 dicembre 2000**[xxxiv], , si è espressa in merito alla natura delle misure di protezione che rilevano ai fini della configurabilità del delitto previsto dall'art. 615 ter c.p. ed ha sancito che: "…la violazione dei dispositivi di protezione del sistema informatico non assume 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…ma si tratta di un illecito caratterizzato appunto dalla contravvenzione alle disposizioni del titolare, come avviene nel delitto di violazione di domicilio, che è stato notoriamente il modello di questa nuova fattispecie penale, tanto da indurre molti a individuarvi, talora anche criticamente, la tutela di un domicilio informatico. …certo è necessario che l'accesso al sistema informatico non sia aperto a tutti…Ma deve ritenersi che, ai fini della configurabilità del delitto, assuma 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 a regolare l'ingresso stesso nei locali in cui gli impianti sono custoditi".

La suprema Corte voleva fare riferimento all'uso di porte allarmate o regolate da dispositivi per l'accesso, ad esempio i badge; così come all'adozione di telecamere per la sorveglianza oppure di porte di sicurezza, ecc. .

Continuando, "L'analogia con la fattispecie della violazione di domicilio deve indurre a concludere integri la fattispecie criminosa anche chi, autorizzato all'accesso per una determinata finalità, utilizzi il titolo di legittimazione per una finalità diversa e, quindi, non rispetti le condizioni alle quali era subordinato l'accesso. Infatti, se l'accesso richiede un'autorizzazione e questa è destinata a un determinato scopo, l'utilizzazione dell'autorizzazione per uno scopo diverso non può non considerarsi abusiva." E' chiaro il riferimento alla ipotesi che si realizza qualora ad un accesso autorizzato, ad es. ad opera di un operatore di sistema, faccia seguito una permanenza all'interno del sistema per un fine diverso da quello che ha legittimato l'accesso stesso.

Sempre la **Cassazione, Sezione III penale, con Sentenza 31 luglio 2003, n. 32440**[xxxv]**,** ha fornito un ulteriore interessante spunto di riflessione per l'oggetto della nostra materia, stabilendo che i " delitti di cui agli articoli 615-quater, 615-ter (sono stati)…collocati entrambi tra quelli contro l'inviolabilità del domicilio perché si è ritenuto che i sistemi informatici costituiscano "un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantito dall'articolo 14 della Costituzione e penalmente tutelata nei suoi aspetti più essenziali e tradizionali agli articoli 614 e 615 del c.p." Inoltre, "…l'incriminazione dell'accesso abusivo al sistema informatico altrui (articolo 615-ter c.p.) è sostanzialmente finalizzata a contrastare il rilevante fenomeno degli hackers, e cioè di quei soggetti che, servendosi del proprio elaboratore, collegato con la rete telefonica, riescono ad 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".

Di conseguenza, la nostra attenzione, a questo punto, deve spostarsi sul problema inerente la tutela dei dati contenuti nel sistema elettronico o telematico, atteso che lo stesso legislatore ha disciplinato quale circostanza aggravante la provocazione, a causa del reato, della "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, e dei programmi in esso contenuti".
Nella necessità di definire il concetto di dato ci viene in aiuto il legislatore che attraverso l'art. 4 del D.Lgs.vo n. 196/03 ha identificato il "dato personale" come "qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".
Trattasi, a ben vedere, di una definizione notevolmente estesa comprendente: il nome e cognome, l'età, il codice fiscale, l'indirizzo, la voce, le caratteristiche biometriche di una persona, ecc.

CONCLUSIONE

Come giustamente è stato rilevato[xxxvi], l'avverbio "chiunque" che apre l'art. 615-ter cp vuole indicare che tutti possono essere i potenziali soggetti attivi della fattispecie criminosa

L'interesse tutelato dal legislatore è la privacy informatica e la riservatezza dei dati memorizzati nei sistemi informatici e telematici.

La norma vuole colpire chiunque si introduce nei pc di altri soggetti senza dirlo e, a ben vedere, tale condotta non viene posta in essere solo dagli hacker ma anche da chi utilizzando sistemi di monitoraggio è in grado di accedere ai sistemi. Ci riferiamo, quindi, ai provider, alle ditte di software, alle aziende, alle stesse istituzioni[xxxvii]!.

Ottobre 2005

Dott. Giovanni Modesti

---

[i] L'Autore, funzionario presso l'Ausl di Pescara, è referente aziendale per la applicazione della privacy ed in tale veste svolge da anni attività di formazione presso il personale in servizio, oltre che di consulenza presso la Direzione Generale della Azienda. In materia è autore di una pubblicazione dal titolo "Commento breve al Decreto Legislativo n. 196/2003, Codice in materia di protezione dei dati personali" apparso sul sito WWW.dirittosuweb.com, 2005 e sul sito: www.diritto.it

[ii] Bibliografia di riferimento: **Corrias L.**, Informatica e Diritto Penale: elementi per una comparazione con il diritto statunitense; 1987; **Tonelli G.,** Il delitto di accesso abusivo a sistemi informatici o telematici con particolare riferimento alla tutela dei dati personali; in Filodiritto.it; **Frediani V.,** Quando ricorre il reato di accesso abusivo ad un sistema informatico?, in www.commercialistatelematico.com; ; **Stalla G.,** L'Accesso abusivo ad un sistema informatico, in Penale.it; **Vaccaio D.,** L'evoluzione del concetto di misura di sicurezza a protezione del sistema informatico alla luce dell'art. 615-ter e del Disciplinare Tecnico; in www.computerlaw.it,; 2004; **Stilo L.,** Accesso abusivo ad un sistema informatico e telematico; Alla ricerca della definizione di "Accesso ad un sistema informatico" ai sensi dell'articolo 615 ter C.P., su WWW.leostilo.it; **La mia privacy**, **Guida normativa Il sole 24 Ore,** AA.VV., 2004; **Limone A.,** Il delitto di accesso abusivo a sistemi informatici o telematici con particolare riferimento alla tutela dei dati personali, in www.diritto.it; **Rossi D.,** Personal computer…home sweet home, in WWW.filodiritto.com; **Farolfi F.,** I crimini informatici, in www.ei.unibo.it/materie/pdf/reati_informatici.pdf

[iii] L a espressione "computer crimes" sta a significare l'insieme di reati perpetrati attraverso i computer, i sistemi informatici e quelli telematici. Trattasi di in crimine che vede un sistema di elaborazione quale oggetto o soggetto oppure strumento del reato. Nell'anno 2003 il costo degli "e-crime" è stato stimato in 666 milioni di dollari! Da un Dossier di repubblica del 24.1.05, si è appreso che, nell'anno 2004 uno studio condotto negli Usa da parte di una rivista specializzata, la

Cso, in collaborazione con il Cert (centro ricerche sulla sicurezza informatica della Carnegie Mellon University) ha rilevato che che il 43% delle aziende interpellate ha registrato un aumento dei crimini elettronici e delle intrusioni rispetto all'anno precedente e il 70% ha dichiarato di avere subito almeno un attacco diretto.

[iv] Il computer è una macchina elettronica statica programmabile strutturata attorno ad un microprocessore, in grado di eseguire calcoli ad altissima velocità. Le applicazioni dei computer sono infinite ma, da un punto di vista oggettivo, il computer è utile e applicabile in tutte quelle situazioni in cui esistono problemi che possono essere tradotti in formule di tipo matematico.
Gli elementi minimi costitutivi di un computer sono: microprocessore; memoria di tipo RAM; memoria di tipo EPROM; interfaccia per l'immissione dei dati (per esempio tastiera); interfaccia per l'output dati (per esempio monitor). Le due interfacce comunemente non sono considerate parte del computer, ma comunque senza di esse il funzionamento risulta impossibile... o meglio, per quanto il funzionamento in termini di elaborazione possa essere possibile, senza le interfacce risulta impossibile ottenere i risultati del lavoro eseguito e immettere comandi al fine di controllare il funzionamento della macchina. Un esempio completo di computer è una normale calcolatrice di tipo scientifico. Esistono alcuni microprocessori particolari, detti *microcontrollori*, che oltre a contenere al loro interno un microprocessore semplice, contengono anche una certa quantità di memoria RAM ed EPROM, nonchè vari tipi di interfacce, per esempio seriali, parallele o addiritura di conversione analogico/digitale: questi circuiti integrati realizzano in un solo chip un computer completo. [di Marco Steccanella]

[v] Si differenzia dal sistema informatico in quanto non consente, di per sé, la organizzazione né la elaborazione dei dati; ci si riferisce, quindi, ad es. ad un video registratore, ecc.

[vi] Si caratterizza per consentire di elaborare ed organizzare dei dati, che potranno essere utilizzati per svariate finalità. Tale termine comprende anche il software di base (che consente all'elaboratore di funzionare), quello applicativo (che permette all'utente di scrivere testi, disegnare grafici, ecc.).

[vii] E' cos tituito da una pluralità di sistemi informatici tra loro collegati onde consentire la trasmissione e la comunicazione a distanza delle informazioni.

[viii] Tonelli G, op. cit. al quale si rimanda per una esauriente rassegna di diritto comparato sui crimini informatici.

[ix] Per tutti, **Antolisei F.,** Manuale di diritto penale, parte speciale – I;

[x] In questa Raccomandazione il legislatore comunitario indicò due liste di reati informatici; la lista minima contemplava le ipotesi di reato più diffuse (quali ad es.: la frode informatica, il sabotaggio informatico, l'accesso non autorizzato, ecc.) ed una lista facoltativa che conteneve ipotesi delittuose che, probabilmente 16 anni fa non apparivano particolarmente rilevanti ma che invece oggi hanno una loro pregnante attualità, ci riferiamo ai reati di: alterazione dei dati o dei programmi informatici, allo spionaggio informatico, ecc.

[xi] L'accesso si verifica attraverso la introduzione all'interno di un sistema.

[xii] L'attacco viene perpetrato o per accedere ad un sistema informatico o per diffondere un virus oppure per renderlo meno funzionale.

[xiii] Si tratta di un programma che si riproduce all'interno del sistema ed infetta altri programmi all'interno del sistema medesimo. Più precisamente è un codice informatico capace di replicarsi in modo autonomo attraverso programmi, messaggi di posta elettronica, ecc. può danneggiare l'hardware, il software e le informazioni contenute su pc e periferiche.

[xiv] Art. 615 quater Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici Chiunque, al fine di procurare a se' o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, e' punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni La pena e' della reclusione da uno a due anni e

della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617 quater.

[xv] Art. 615 quinquies Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto 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, e' punito con la reclusione sino a due anni e con la multa sino a lire venti milioni

[xvi] Corte di Cassazione, Sezione V Penale, Sentenza n. 4389 del 2 luglio 1998.

[xvii] L'accesso ad un sistema informatico e telematico sembra fare riferimento non alla semplice ipotesi di chi effettua un collegamento fisico con il computer ma a chi instaura un dialogo con l'elaboratore (c.d. collegamento logico), sulla scorta del quale assume il dominio dell'elaboratore potendone copiare e/o alterare e/o distruggere i file.

[xviii] **Fiandaca Musco, Diritto penale , Parte generale.** "I reati di azione consistono…nel semplice compimento dell'azione vietata, senza che sia necessario attendere il verificarsi di un evento casualmente connesso alla condotta medesima."

[xix] **Fiandaca Musco,** op. cit, "assurge a bene giuridico soltanto quell'interesse, o quell'accorpamento di interessi, idonei a realizzare un determinato scopo utile per il sistema sociale o per una sua parte".

[xx] La Cassazione con sentenza n. 3067/1997, definì il domicilio informatico quale "…luogo fisico…nel quale è contenuto l'oggetto della tutela, per salvaguardarlo da qualsiasi tipo di intrusione (ius excludendi alios), indipendentemente dallo scopo che si propone l'autore dell'abuso…"

[xxi] La dottrina ha adottato una serie di definizioni del termine "riservatezza ", ricorrendo ai concetti di "right to be let alone", inteso come il diritto a restare solo, o di "right to privacy", diritto alla privacy, altri ancora hanno inteso tale termine come il diritto di evitare la diffusione di notizie attinenti la vita privata della persona a prescindere che la loro diffusione possa concretare fattispecie penalmente rilevanti quali l'offesa all'onore, alla reputazione, ecc.

[xxii] Entrambi i concetti esplicitano dei diritti tutelati sia dall'ordinamento internazionale (vedasi la Dichiarazione universale dei diritti dell'Uomo, del 1948: Articolo 12: Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, nè a lesioni del suo onore e della sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente e la Carta dei diritti fondamentali della U.E. del 2000: Articolo 8**,** *Protezione dei dati di carattere personale* Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano) sia dal diritto interno (Decreto Legislativo n. 196/2003, Codice della protezione dei dati personali).

[xxiii] Per tutti si cita **Mantovani,** Manuale di diritto penale.

[xxiv] L'operatore di sistema è il professionista che, in qualità di operatore, programmatore, analista, per espletare le proprie mansioni deve, necessariamente, introdursi nel sistema informatico e che, quindi, rischia di incorrere nella ipotesi sanzionata come aggravante. A tale proposito la Cassazione ha sancito che il reato viene a concretarsi quando l'operatore di sistema, introdottosi nel sistema per una determinata finalità, utilizzi tale titolo di legittimazione per una diversa finalità non contemplata nell'incarico che espleta.

[xxv] **Fiandaca Musco,** op. cit.**,** “I reati si distinguono in illeciti di danno e illeciti di pericolo, a seconda che la condotta criminosa comporti la lesione effettiva ovvero la semplice messa in pericolo o lesione potenziale del bene giuridico assunto a oggetto di tutela penale”.
[xxvi] **Fiandaca Musco,** op. cit.”…la nozione del dolo si incentra su tre elementi: previsione, volontà, evento dannoso o pericoloso.” Ai sensi dell’art. 43, c. 1, cp “il delitto è doloso, o secondo l’intenzione, quando l’evento dannoso o pericoloso, che è il risultato della azione od omissione e da cui la legge fa dipendere l’esistenza del delitto, è dall’agente preveduto e voluto come conseguenza della sua azione od omissione”.
[xxvii] Art. 31: “I dati personali oggetto di trattamento sono custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l’adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta”.
[xxviii] Ciò sta a significare che tali misure vanno adottate in base al tipo di dato trattato, se sensibile o comune, alla modalità di trattamento: informatizzato, cartaceo o misto ed, infine, in base alle conoscenze acquisite.
[xxix] Firewall: (*ingl. lett.*) muro di fuoco. Un rete LAN connessa ad Internet deve difendersi da attacchi esterni (*cfr.* DoS), da accessi non autorizzati o da connessioni attivate da malware. Un firewall, composto ad esempio da un router e da una application gateway, ha il compito di separare due o più reti per consentire alcuni tipi di traffico e bloccarne altri. Il router analizza tutti i pacchetti entranti ed uscenti della rete aziendale, leggendo la provenienza di ciascun pacchetto IP (l'indirizzo IP). Un firewall è, come suggerisce il suo nome, un sistema progettato per impedire accessi non autorizzati a (e da) reti private. Esso può essere realizzato sia via software che via hardware (o anche con una combinazione delle due). Il suo utilizzo tipico è quello di impedire agli utenti provenienti da Internet l'accesso non autorizzato ad una Intranet. Successivamente il router dotato di alcune funzioni può controllare a quale tipo di servizio appartengono quei pacchetti, analizzando il numero di porta della connessione TCP per controllare se si tratta ad esempio di un'operazione FTP. In tal caso potrebbe disattivare la porta 21 per difendere la rete dal servizio di trasferimento di file provenienti dall'esterno. L'*appliction gateway* invece opera ad un livello più alto, controllando non i singoli pacchetti entranti od uscenti, ma analizzando i messaggi e-mail oppure i file importati dalla rete, prima di inviarli all'interno della LAN. *cfr.* NAT-PAT. [di Marco Lizza]:
[xxx] Router: (*ingl. lett.*) instradatore. Dispositivo che interconnette reti e instrada datagrammi IP. Le sue funzioni sono definite all'interno del terzo livello del modello ISO/OSI (Livello Network). Ogni router ha una *tabella di routing* con due tipi di indirizzi IP, il primo indica come raggiungere reti distanti [*rete, 0*], il secondo tipo è della forma [*questa rete, questo host*] e indica come raggiungere gli host di una LAN, attraverso un'interfaccia di rete (NIC) indicata ad esempio con *eth0*. Diversamente, se il pacchetto non è indirizzato ad un host della rete locale, il router (o gateway) lo inoltra ad un'altro router con una tabella più estesa, attraverso l'interfaccia appropriata, per esempio *eth1* o *eth2*, …, *ethN*.Mentre un hub opera da ripetitore, ossia riproduce ogni segnale che riceve anche se distorto, il router rigenera solo i pacchetti corretti, modificando l'intestazione e non il payload, poichè ricalcola il campo *checksum* per il decremento del campo *Time To Live del pacchetto IP*. Diversamente dagli hub, se il pacchetto è danneggiato viene scartato, demandando l'affidabilità della connessione all'entità TCP che si occupa di ritrasmettere la parte scartata Anche un server con più schede di rete, e quindi con altrettanti indirizzi IP, può connettere più reti ed agire da router. Un router, sia esso un dispositivo special purpose da rack o un server PC, ha almeno due interfacce di rete, una per ogni reteI router inviano e ricevono pacchetti anche se le reti sono dissimili, sia nei protocolli sia nella grandezza dei pacchetti. In questo caso, per rispettare l'MTU di una rete, i router possono frammentare l'informazione in pacchetti più piccoli. Un router multiprotocollo concettualmente è simile al bridge, ma ha una visione molto più estesa della rete, poichè il bridge opera solo localmente al Livello Data Link. *Cfr.* ARP

[xxxi] IDS SAS: software creato nel 1976 da un gruppo di ricercatori dell'Università di Cary (North Caroline) e la sua originaria funzione fu di strumento orientato all'analisi statistica. SAS System è attualmente a livello mondiale il sistema di IDS (*Information Delivery System*) per la trasformazione dei dati in utili e rilevanti informazioni per il business più diffuso nelle aziende. Gli Ids, intrusion detenction system, sono anch'essi strumenti elettronici che permettono di analizzare e verificare le attività in corso sulla rete e sui sistemi al fine di individuare eventuali segnali di pericolo. In buona sostanza, essi svolgono una azione di monitoraggio atta ad evidenziare eventuali pericoli alla integrità dei dati.

[xxxii] Il caso verteva su una ipotesi di truffa perpetrata a danno della Telecom., in merito ad un traffico telefonico verso l'estero, compiuto da un dipendente della filiale di Brindisi.

[xxxiii] Il Tribunale era stato chiamato a pronunciarsi in merito alla introduzione abusiva nel sito telematico della RAI , rinominando con lo stesso nome di quello autentico e sostituendo il file contenente il radio giornale audio con un altro file contenente una serie di critiche alla Microsoft. Con l'aggravante che l'attore si era inserito in un sistema telematico di pubblico interesse.

[xxxiv] La sentenza in commento attiene al caso di chi dopo essere uscito dalla società per intraprendere analoga attività ne aveva copiato i dati contenuti nell'impianto informatico, ciò in quanto non gli era stato concesso di potere utilizzare come locatario l'impianto informatico della società stessa.

[xxxv] Tale sentenza verteva sulla condotta del soggetto che ricarichi il proprio telefono cellulare servendosi di un codice di accesso indebitamente ottenuto.

[xxxvi] **Crespi,Stella,Zuccalà, Commentario breve al codice penale, 2003.**

[xxxvii] P**almieri N.W., Usa: lo spyware protetto dalla libertà di espressione?** in www.interlex.it; al quale si rimanda per una puntuale disamina dei pericoli rappresentati dall'utilizzo della rete, con particolare attenzione alla situazione presente negli Stati Uniti.