Accesso abusivo a sistema informatico o telematico

Avv. Stefano Aterno

Docente di diritto penale dell'informatica
presso la LUMSA di Roma
e di
Aspetti giuridici delle nuove tecnologie
presso il Dipartimento di informatica
dell'Università La Sapienza

615 ter cp
Accesso abusivo ad un sistema informatico o telematico

comma 1

Chiunque abusivamente si introduce in un *sistema informatico o telematico* protetto da **misure di sicurezza** ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo,

è punito con la reclusione fino a tre anni.

Segue 615 ter:

La pena è della reclusione da uno a cinque anni:

- 1) se il fatto è commesso da un **pubblico ufficiale o da un incaricato di un pubblico servizio,** con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della **qualità di operatore del sistema**;

- 2) se il colpevole per commettere il fatto usa **violenza** sulle cose o alle persone, ovvero se è palesemente **armato**;

- 3) se dal fatto deriva la **distruzione** o il **danneggiamento** del sistema o l`interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il **danneggiamento dei dati**, delle **informazioni** o dei **programmi** in esso contenuti.

- Segue 615 ter cp

- 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

Definizione di sistema informatico/telematico:

- Nel codice penale non esiste una definizione:

-PC, un server, il bancomat, una rete LAN, una rete Wireless etc etc

- Il decoder ?
- Il cellulare? TACS o GSM ? 3 ? UMTS ?
- La Playstation ? 1 o 2, 3.. ?
- X – BOX ?
- Agendina elettronica ?

-Forno a micro-onde ?

-il sistema di allarme ?

Sono accesso abusivo le seguenti condotte ?

- Connessione (accesso ?) tramite access point a sistemi wireless non protetti adeguatamente ?

- penetration test (IP, range di IP, errori possibili) ?

- Port scanning ? È tentativo ?

È accesso abusivo ?

- Se ci sono Honeypots e Honey nets ?

- Se c'è un sistema di file sharing o peer to peer e quindi "condivisione" di alcune cartelle/file ?

La definizione della cassazione nella sentenza Piersanti - 1999

"Sulla base del dato testuale pare comunque 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 di tecnologie informatiche ovvero caratterizzate dalla registrazione o memorizzazione per mezzo di impulsi elettronici, su supporti adeguati di dati, di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici (codice), in combinazioni diverse; tali dati elaborati automaticamente dalla macchina, generano le inforamzioni 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".

Tentativo di definizione

- Potrebbe ritenersi 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.(cass. Pen. 2000, n. 535, in cass pen 11, 2000)

Reato di danno o di pericolo ?

Quale bene giuridico viene tutelato ?

- domicilio informatico = 614 cp

  (Se fosse solo domicilio informatico ……vi sarebbe il problema delle aggravanti dell'art. 615 ter c.p.)

A ben vedere… anche

- "riservatezza informatica"come riservatezza dei dati, delle informazioni e della **sfera non personale** ma comunque **riservata ed inviolabile** (fondamento normativo nell'art. 2 costituzione) in cass. pen. n. 11 del 2000)

Introdursi in un sistema…….

- prendere il possesso, il controllo, la gestione (anche parziale)di un sistema ponendo in essere una serie di operazioni o facendole fare al sistema;
- cognizione della struttura interna e non necessariamente dei documenti contenuti (è comunque una informazione “riservata” o considerata tale dal titolare o comunque un suo spazio che desidera mantenere riservato (misure di sicurezza)

Ovvero vi si mantiene,…..

- Qualcuno entra con il consenso dell'avente diritto MA al momento della cessazione della volontà non esce,

Oppure :

- Va oltre i limiti imposti dal mandato/contratto (IP diversi e penetration test);
- Ovvero fa altre cose oltre quelle per le quali è stato fatto accedere

C’è una lesione concreta del bene giuridico

- Introdursi significa ledere già di per sé il bene giuridico tutelato (sia esso domicilio informatico e/o riservatezza informatica, intangibilità informatica);

- Non c’è una messa in pericolo del bene perché il bene giuridico viene subito leso, danneggiato.

……è un reato di danno e non di pericolo

e ciò è una garanzia importante perché:

- non c'è anticipazione della soglia di punibilità;

-si configura più agevolmente il **tentativo**, mentre viceversa il reato sarebbe sempre consumato (es : invio di un trojan non eseguito)

un po' di Giurisprudenza sull'accesso abusivo

- Cass. 4 ottobre 1999, P., in Cass. Pen 2000, p. 2990, con nota di ATERNO p. 2994 e con nota di Cuomo p. 2998
- Cass. 7 novembre 2000, Zara, in Giust.pen.2001, 548,
- GUP Roma, 4 aprile 2000, G.C. in www.penale.it
- Cass. 14 ottobre 2003, n. 44362, M., in cass.pen.2005, n. 5, con nota di ATERNO (615 ter e clonazione carte di pagamento)
- Cass. 5 FEBBRAIO 2004, N. 4576 (non è frode informatica)
- Corte di Cassazione, Sez. VI, 27 ottobre 2004 n. 46509
  Non e' ravvisabile il reato di accesso abusivo in quanto il sistema informatico nel quale l'imputato si inseriva abusivamente non risulta obiettivamente protetto da misure di sicurezza.
- Tribunale di Bologna luglio 2005 (dep. dicembre 2005) caso "Vierika",

Alcune più recenti sentenze

- Tribunale di Milano – caso “Banca on line” – 6 giugno 2006 (dep. 10.11.06)
- Cass. Sez. 5, del 15.2.2007, n. 6459 (trascinamento cartella)
- Cass., Sez. 5, 20.3.2007, 11689 (non è necessario violare la riservatezza dei legittimi utenti; caso Telecom)
- Triunale di Nola GUP 11.12.2007 (caso Agenzia delle Entrate e dati famiglia PRODI)
- Corte appello Milano – caso “banca on line” – 2 aprile 2008 (dispositivo)
- Corte appello di Bologna – caso Vierika – 9 aprile 2008 (?)

Seguono sentenze recenti:

- **Migliazzo**
- **Scimi.**
- **Studio legale**
- **Genchi**
- **Casan.**

Il centralino è un sistema informatico ?

Cass. 4 ottobre 1999, P.,

- Centralino con blocco telefonate interurbane
-Alcuni numeri consentiti
-i sistemi di gestione traffico telefonico TELECOM sono (già allora ?) gestiti da sistemi informatici/telematici

La Suprema Corte e le misure di sicurezza ex art. 615 ter c.p.

- GUP Roma, 4 aprile 2000, G.C. in (sistema RAI winmix – cartella condivisa) Idoneità della protezione ?
- Cass. 7 novembre 2000, n. 12732, Zara (misure organizzative)
- Cass. 27 ottobre 2004 (dep. 30 novembre 2004), n. 46509 (inedita, non massimata) sistema deve essere **oggettivamente** protetto
- Cass.15 febbario 2007, n. 6459 (il trascinamento della cartella del "capo")

GUP Roma, 4 aprile 2000, G.C

- Accesso in un sistema informatico della Rai (Radio) sfruttando una vulnerabilità del sistema Windows (Win mix) che consentiva condivisione di alcune cartelle e quindi una loro totale visione in Rete.

- Il ragazzo installa un messaggio con la propria voce al posto del *gingle* del GR….
- Viene dichiarato NPD perché il sistema non è protetto da misure di sicurezza

Contra:

Cass. 7 novembre 2000, n. 12732, Z.,

- <<.. la violazione dei dispositivi di protezione non assume rilevanza per sé, ma solo come eventuale manifestazione di una volontà contraria a quella di chi dispone legittimamente del sistema>>

- <<che il reato si può realizzare anche quando, in assenza del titolare, un soggetto supera strumenti esterni meramente organizzativi e diversi rispetto al sistema informatico ma tali a denotare la volontà del titolare di negare l'accesso agli estranei e, anche se il computer è privo di misure di sicurezza (sia logiche e sia fisiche),
- tale volontà sarebbe <<..implicita, ma intuibile … >>.

(massima ufficiale, C.E.D. 217743); si veda, per gli stessi fatti, Tribunale di Torino, 4 dicembre 1997, Dir. Inf., 1998

- Qualche dubbio in seguito alla sentenza del 2000 :
- - lo *ius excludendi alios* va considerato anche in assenza di misure si sicurezza informatiche ?

- - devono fornire obiettiva protezione ?

- **le misure di sicurezza devono essere in modo chiaro ed inequivocabile a protezione del sistema e …..non di altre cose e ciò deve essere percepibile….. da chiunque**

Perchè i problemi sorgono tra misure fisiche e misure informatiche e percezione da parte dell' attaccante della volontà di bloccare l'accesso…

Cass. sez. 6, 27 ottobre 2004 n. 46509 (dep. 30 novembre 2004)

<<… non è ravvisabile il reato di accesso abusivo se il sistema informatico o telematico nel quale l'imputato si inserisce non risulta obiettivamente protetto da misure di sicurezza >>

Cassazione Sez. 5, Sentenza n. 6459, del 15.2.2007 (il trascinamento della cartella del “capo”)

- Un soggetto avrebbe, secondo l'accusa, utilizzando indebitamente il "nome utente" e la "password" del datore di lavoro B. Giuseppe, acceduto alla cartella personale riservata di costui e scaricato dalla stessa una serie di "files";

- NON vi erano prove che fosse stato l'imputato l'autore dell'indebito trasferimento della cartella riservata del B. nella cd. "area comune" del sistema informatico in uso alla ditta "B.S." di cui era titolare lo stesso B.

- Vi era stata la concreta possibilità che a quella cartella accedessero tutti i dipendenti della ditta:

- era emerso che la mattina del 12 giugno 2001, all'inizio dell'orario di lavoro, l'unico "personal computer" collegato al sistema era quello del l’imputato, giunto in precedenza ed al momento assentatosi, e che da esso erano stati scaricati e trasferiti su di un dischetto, ritrovato piegato nel cestino della carta, diversi "files" tratti dalla cartella riservata del B;

- Segue Cass 2007 su misure di sicurezza:

- **la configurabilità del reato di cui all'art. 615 ter c.p. postula, alla stregua del letterale tenore della norma incriminatrice, che trattisi di un sistema "protetto da misure di sicurezza" e che l'agente, per accedervi, abbia in qualche modo neutralizzato tali misure,**
  nulla rilevando, invece, sotto il profilo penale, che una volta avvenuta detta neutralizzazione, **altri, senza avervi concorso, ne approfittino** avvalendosi soltanto degli strumenti e dei dati di cui siano legittimamente in possesso;

  ragion per cui deve ritenersi, nella specie, legittimamente escluso che, **in assenza di prova circa l'avvenuta effettuazione, da parte dell'imputato, dell'operazione di trascinamento della cartella** contenente i dati riservati dall'area protetta a quella comune, potesse affermarsi la responsabilità dell'imputato stesso per il solo fatto che, trovandosi ormai la cartella in detta ultima area, egli, **utilizzando la "password" di cui era legittimamente in possesso** avesse preso visione del suo contenuto e lo avesse trasferito sul dischetto poi rinvenuto nei cestino della carta usata;

La Cassazione sul 615 ter c.p. sembra oggi più convincente……

…..un po' meno i tribunali di merito

- **Tribunale di Catania, 9/5/2003,** in sede di riesame, confermava l'ordinanza cautelare emessa dal G.I.P. di Siracusa, con la quale veniva disposta la misura cautelare in carcere nei confronti di N. S., indagato per **furto aggravato** per avere sottratto dal C/C xxxxx, acceso presso la Banca Telematica Intesa "121", 30.000,00 euro, **accedendo tramite Internet e operando immediati bonifici in favore del proprio C/C.**

su ricorso dell'indagato

interviene

Cass. Sez. V, 5 febbraio 2004, n. 4576 :

- al più, ricorre l'ipotesi di cui all'art. 640 ter c.p., la c.d. frode informatica, …..

- la norma e' posta a tutela sia della riservatezza e della regolarità dei sistemi informatici che del patrimonio altrui …….
- trattasi di reato a forma libera che prevede, alternativamente una condotta consistente nell'alterazione del funzionamento del sistema informatico o telematico**, ovvero in un intervento non autorizzato (che e' possibile effettuare con qualsiasi modalita') sui dati, informazioni e programmi ivi contenuti.**

L’invio di un worm particolare……

Tribunale di Bologna luglio 2005

(dep. dicembre 2005)

caso “Vierika”

art. 615 quinquies (diffusione di virus)

e art. 615 ter (accesso abusivo)

- Un ragazzo italiano crea un virus worm nuovo che riesce per alcune ore a diffondersi
- Vierika
- 1 ° script + 2 ° script (programma) che determinano nel sistema una serie di modifiche consentendo in ultimo l’invio involontario di una serie infinita di email a tutti gli indirizzi in rubrica

Sentenza Vierika 1° grado

- Condanna per 615 quinquies

- Condanna per 615 ter …. (?):

  perché attraverso il worm l'imputato è entrato nel sistema …..(sentenza interessante anche sotto il profilo della computer forensic)

Commenti e note critiche su Vierika:

Il virus “worm” che si introduce alla stregua di una *longa manus* del soggetto “attaccante”.....

ma chi è che si introduce ?

è vero che abbassa le misure minime di sicurezza del browser (internet explorer)

ma è anche vero che altera più che consentire l’intrusione… (640 ter cp ?)

Commenti e note critiche - vierika

è una interpretazione che lascia molte perplessità :

- principio di tassatività della norma penale
- principio di precisione
- concetto di intrusione
- domicilio informatico e riservatezza violati da un programma ?
- attività unica / NON più attività diverse e assolute

Corte appello di Bologna 2008
caso vierika

- Conferma condanna per il 615 quinquies cp (diffusione di virus e programmi diretti a danneggiare)

- NDP per il reato di cui al 615 ter cp per mancanza di querela (essendo caduta l'aggravante della violenza sulle cose)

"Accesso abusivo a un sistema informatico - Concorso di persone - presupposti - condizioni artt. 110 e 615 ter c.p.

Cassazione Sezione V, sentenza 22 febbraio - 12 aprile 2006 n. 12962 - Pres. Calabrese, rel. Ferrua; Pm. (parz. diff.) Salzano; ric. Rizzetti e altro "

Poiché la figura del concorso di persone nel reato (art. 110 del c.p.) postula che il concorrente che non commette l'azione tipica voglia la stessa, quantomeno sotto il profilo del dolo eventuale, e si sia adoperato, anche solo nella fase preparatoria, proprio per la sua commissione ad opera del correo, ne discende **che la richiesta di informazioni rivolta ad un operatore di polizia** di notizie riservate può costituire **concorso morale nel reato** di accesso abusivo a sistemi informatici protetti (articolo 615 . ter c.p.), materialmente posto in essere da detto operatore, avente la possibilità di accedere agli stessi, solo nel caso in cui la richiesta sia specificatamente rivolta ad **ottenere detto accesso o nel caso in cui comunque risulti la consapevolezza del richiedente in ordine alla circostanza che il soggetto al quale ci si rivolge ricorrerà a tale azione.**

- **TRIBUNALE DI MILANO GIUDICE PER LE INDAGINI PRELIMINARI**
-
- **Ha pronunciato la seguente**
- **SENTENZA**
- Nel procedimento a carico di:
- P . Anna Maria, nata 11 ago 1961 a Milano, PRESENTE, residente in Milano via Nicola n. 3, elett. domiciliata in Milanopresso lo studio del difensore, presente
- - difesa di fiducia dall'avv. del Foro di Milano, PRESENTE
-
- F)- del reato p. e p. dagli artt. 81 cpv, 615 ter commi I, II n. 1 e III c.p. perché, con più azioni esecutive del medesimo disegno criminoso, abusando dei poteri inerenti le funzioni di PG presso l'Ufficio del Sost. Proc. dott. G. presso la Procura della Repubblica e di operatore del sistema utilizzando , all'insaputa della titolare ed avendola ricevuta dal collega PINCO PALLO la password assegnata al Proc. Aggiunto dottoressa Maria Luisa , in violazione dei compiti alla stessa delegati e senza alcuna autorizzazione interrogava il Registro Re. Ge. 2.2 circa alcuni nominativi di persone dalla medesima conosciute ed appartenenti al Corpo di Polizia Locale di Milano , venendo così a conoscenza di informazioni relative a procedimenti penali a carico di taluni di questi, ancora in fase di indagine preliminare e trattati da Ufficio e da Dipartimento diverso da quello di appartenenza
- In particolare:
- - interrogava in almeno due occasioni il sistema , digitando il cognome "TOPI" corrispondente a TOPI…. ed il cognome "ASCOL….. (o inserendo il relativo numero di procedimento) , entrambi imputati nel procedimento penale n. 2523/04 RGNR;
- - interrogava in almeno due occasioni il sistema , digitando " MONFRE….. o "MONFR…… LUCIANO" (o inserendo il relativo numero di procedimento), imputato nel p.p. n. 27716/04 RGNR;
- - interrogava il sistema in due occasioni, digitando "ARGEN……, corrispondente ad Arge…… coimputato di Topi Roberto nel p.p. n. 2523/04 RGNR;

- - interrogava il sistema in più di una occasione, digitando il cognome “RICCIA……“, corrispondente a Vittorio ……Aggiunto della Polizia Locale , in servizio presso la Squadra Investigativa della Polizia Locale;
- - interrogava il sistema più volte digitando il cognome “ Barba…..” , appartenente alla Polizia Locale;
- - interrogava in numero almeno pari a tre occasioni il sistema , digitando il cognome NAPOL…… (o inserendo il relativo numero di procedimento) , imputato nel p.p. n. 27687/04 ed appartenente alla Polizia Locale

- In Milano, dal 4 dicembre 2003 al luglio 2005
-
- **In cui risulta persona offesa dal reato:**
- MINISTERO DELLA GIUSTIZIA – in persona del Ministro pro-tempore – domiciliato ex lege presso l’Avvocatura dello Stato – Uffici di Milano – Via Freguglia 1 – NON PRESENTE

- *Sez.* 5, ***Sentenza*** *n.* 11689 *del* 06/02/2007 Cc. (dep. 20/03/2007) Rv. 236221

- *Presidente:* **Pizzuti G.** *Estensore:* **Fumo M.** *Relatore:* **Fumo M.** *Imputato:* **Cerbone e altro.** *P.M.* **Febbraro G.** *(Conf.)*
- (Rigetta, Trib. lib. Napoli, 26 Luglio 2006)

- REATI CONTRO LA PERSONA - 032 VIOLAZIONE DI DOMICILIO - IN GENERE
- REATI CONTRO LA PERSONA - DELITTI CONTRO LA LIBERTÀ INDIVIDUALE - VIOLAZIONE DI DOMICILIO - IN GENERE –
- Accesso abusivo ad un sistema informatico - Reato di mera condotta - Perfezione del reato - Introduzione in un sistema informatico - Sufficienza - Violazione della riservatezza dei legittimi utenti - Finalità di insidiare detta riservatezza necessità - Esclusione.

- Il delitto di accesso abusivo ad un sistema informatico, che è **reato di mera condotta**, si perfeziona con la violazione del domicilio informatico, e quindi con l'introduzione in un sistema costituito da un complesso di apparecchiature che utilizzano tecnologie informatiche, **senza che sia necessario** che l'intrusione sia effettuata allo scopo di **insidiare la riservatezza** dei legittimi utenti e che si verifichi una effettiva lesione alla stessa. (Fattispecie in cui il reato è stato ravvisato nella condotta degli imputati, che si erano introdotti in una centrale Telecom ed avevano utilizzato apparecchi telefonici, opportunamente modificati, per allacciarsi a numerose linee di utenti, stabilendo, all'insaputa di costoro, contatti con utenze caratterizzate dal codice 899).

- Massime precedenti : N. 3067 del 1999 Rv. 214945

Tribunale di Nola
GUP 11.12.2007
(i dati della famiglia PRODI)

- Elemento oggettivo:

accesso e mantenimento nel sistema informatico **contro la volontà tacita dell'amministrazione finanziaria,** per **finalità diverse** rispetto a quelle per le quali vale la sua autorizzazione – irrilevanza della natura delle informazioni captate;

condotta di **intrattenimento** nel sistema per pochi secondi, non per prendere cognizione di dati sensibili, quali le informazioni fiscali, bensì puramente e semplicemente per prendere visione di dati, quali quelli anagrafici, di pubblica conoscenza e conoscibilità e non sottoposti dall'ordinamento ad alcuna forma di tutela della riservatezza;

esclusione **dell'elemento soggettivo** atteso che il reo non si è nemmeno reso conto che vi potesse essere una tacita volontà contraria da parte dell'amministrazione finanziaria per la consultazione dei dati anagrafici

Il 615 ter cp..ad unaBanca on line”

- CNR e Infostrada come sistemi “ponte” per fare l’attacco su sistemi di “Banca on Line”
- Stanza di albergo e internet cafè per preparare e ultimare l’attacco
- Port scanning e Penetretion test
- Il contratto di consulenza”
- Il ruolo della secuity in questi casi

Sentenza Tribunale Milano
caso “Banca on line”
6 giugno 2006 (dep. 10.11.06)

- capo a) b) c) e) : 615 ter (accesso abusivo) aggravato dalla qualità di operatore del sistema;
- nel capo c) aggravante di aver commesso il fatto ai danni di un sistema di interesse pubblico
- Capo D : danneggiamento informatico aggravato dalla qualifica di operatore del sistema;

- SENTENZA
- Condanna per a)b)c)e)
- Assoluzione per D (il sistema non è risultato danneggiato)
- Cadono anche le aggravanti di operatore del sistema (tutti i capi)

Corte appello Milano – caso “banca on line”
2 aprile 2008

- Non riconoscimento delle aggravanti di sistema di interesse pubblico (il PC del CNR- sistema informatico di test, non particolarmente protetto, contenente dati campione).
- Ma Infostrada ? Non è sistema di interesse pubblico ? …..(aspetteremo le motivazioni)
- Non è operatore di sistema

- Ndp per mancanza di querela
- Assoluzione per 530 comma 2

Qualche mese fa…..

2 sentenze Cassazione destinate a cambiare molte cose

- *Sez.* 5, ***Sentenza*** *n.* 2534 *del* 20/12/2007 Cc. (dep. 17/01/2008) Rv. 239105
- *Presidente:* **Colonnese A.** *Estensore:* **Dubolino P.** *Relatore:* **Dubolino P.** *Imputato:* **P.M. in proc. M. e altri.** *P.M.* **D'Angelo G.** *(Conf.)*

- (Rigetta, Trib. lib. Torino, 17 Luglio 2007)

- 603 REATI CONTRO LA PERSONA - 032 VIOLAZIONE DI DOMICILIO - IN GENERE
- REATI CONTRO LA PERSONA - DELITTI CONTRO LA LIBERTÀ INDIVIDUALE - VIOLAZIONE DI DOMICILIO - IN GENERE - Introduzione, in qualità di ispettore della Polizia di Stato e di appartenente all'Arma dei Carabinieri, nel sistema informatico denominato SDI e trasmissione dei dati riservati acquisiti ad un'agenzia investigativa - Integrazione del reato di cui all'art. 615 ter cod. pen. - Esclusione - Ragioni.

Non integra il reato di accesso abusivo ad un sistema informatico (art. 615 ter cod. pen.) la condotta di coloro che, in qualità rispettivamente di ispettore della Polizia di Stato e di appartenente all'Arma dei Cararbinieri, si introducano nel sistema denominato SDI (banca dati interforze degli organi di polizia), considerato che si tratta di soggetti autorizzati all'accesso e, in virtù del medesimo titolo, a prendere cognizione dei dati riservati contenuti nel sistema, anche se i dati acquisiti siano stati trasmessi a una agenzia investigativa, condotta quest'ultima ipoteticamente sanzionabile per altro e diverso titolo di reato. (segue) ./.

Segue Cassazione 17 gennaio 2008, n. 2534 – M.

- Nella fattispecie la Corte ha rilevato l'**ininfluenza** della circostanza che detto uso sia già previsto dall'agente all'atto dell'acquisizione e ne costituisca la **motivazione esclusiva**, in quanto la sussistenza della volontà contraria dell'avente diritto, cui fa riferimento l'art. 615 ter cod. pen., ***ai fini della configurabilità del reato, deve essere verificata solo ed esclusivamente con riguardo al risultato immediato della condotta posta in essere dall'agente con l'accesso al sistema informatico e con il mantenersi*** al suo interno e non con riferimento a fatti successivi che, anche se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente).

la sussistenza della volontà contraria dell'avente diritto

deve essere verificata solo ed esclusivamente con riguardo al risultato immediato della condotta posta in essere dall'agente con l'accesso al sistema informatico e con il mantenersi

<u>e non con riferimento a fatti successivi</u> che, anche se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente)…..

Cassazione V, 3 luglio 2008,n . 26797 - proc. c/ Scim. + altri

Il reato contestato consiste nell'accesso abusivo o nell'indebito (*invito domino)* trattenimento in un sistema – per quanto qui interessa – informatico. Nel caso in esame è pacifico che lo Scimia, autore (per quanto s'è detto e si dirà) della interrogazione incriminata, in quanto Cancelliere dell'Ufficio del Giudice delle indagini preliminari del Tribunale di Milano aveva accesso ai registri informatizzati dell'Amministrazione della giustizia e l'interrogazione risulta effettuata con la utilizzazione della chiave logica (o *password* che dir si voglia) legittimamente in suo possesso. E non solo non esiste norma o disposizione interna organizzativa che inibisca al cancelliere addetto alla singola sezione di consultare i dati del registro generale e le assegnazioni ai diversi uffici, ma tale inibizione sarebbe contraria ad ogni buona regola organizzativa, attese le necessità di consultazione di un ufficio giudiziario. Non può dunque affermarsi che lo Scimia abbia effettuato un accesso che non gli era consentito. Neppure può affermarsi che si sia trattenuto nel sistema oltre modi o tempi permessi, giacché nessuna limitazione di tal genere è prevista per la lettura dei dati ad opera degli utilizzatori del sistema. Di tanto erano d'altronde consapevoli i giudici del merito, i quali hanno ritenuto tuttavia sussistente il delitto avendo lo Scimia «agito in violazione dei doveri del suo Ufficio», e cioè per dare l'informazione ottenuta mediante l'accesso a Re.Ge. all'avvocato Colaleo.

Siffatta violazione non attiene però alle modalità che regolano l'accesso al sistema e la consultazione dei dati in esso registrati, concernendo l'uso successivo che di tali dati s'è fatto e l'infedeltà dell'agente ammesso in via privilegiata al sistema, ed è tutta assorbita nella, pure contestata, condotta di rivelazione di notizie (dati) d'ufficio destinati a rimanere segreti.

La norma in esame garantisce invece la riservatezza del domicilio informatico quale spazio ideale (ma anche fisico) in cui sono contenuti i dati informatici, per salvaguardarla da qualsiasi tipo di intrusione non autorizzata, «indipendentemente dallo scopo» che si propone l'autore dell'accesso abusivo (così Cass. sez. 6, n. 3067 del 14.12.1999, Di Zenzo). Ed è mediante l'apprestamento dei mezzi di protezione e l'erogazione delle correlate chiavi d'accesso che il titolare dello *ius exludendi* seleziona gli ammessi, il cui dovere di riservatezza è altrove assicurato.

Non può non condividersi, perciò, quanto recentemente affermato da Sez. 5, n. 2534 del 20.12.2007, Migliazzo, secondo cui «la sussistenza o meno della contraria volontà dell'avente diritto» necessaria alla configurabilità del reato «va verificata solo ed esclusivamente con riferimento al risultato immediato della condotta posta in essere dall'agente con l'accedere al sistema informatico e con il mantenersi al suo interno e non con riferimento a fatti successivi che, pur se già previsti, potranno di fatto realizzarsi solo in conseguenza di nuovi e diversi atti di volizione da parte dell'agente medesimo», che integreranno autonome violazioni, diversamente sanzionabili a seconda degli specifici connotati delle ulteriori condotte (abusive o d'infedeltà) realizzate. Agli

…..non sempre si può parlare di accesso abusivo a sistema informatico…

La verifica deve riguardare solo ed esclusivamente il risultato immediato della condotta posta in essere dall'agente

Cassazione ud 8.7.2008 (1.10.2008), n. 37322, Sal. + altri

- S. , B, M. R, avevano costituito un'associazione profesionale – studio associato ragionier Sala
- Sala era socio di maggioranza relativa e amministratore
- M, B, R, decidono di dare vita ad una nuova associazione professionale
- Nei giorni del passaggio dalla vecchia alla nuova associazione B. e M. si recarono presso la sede dello Studio S., associazione della quale facevano ancora parte non essendo stata sciolta, e si introdussero nel sistema informatico dello studio prelevandone l'archivio.

- 1° grado Condannati ; 2° grado assolti; riccorre il SALA.

- Fatto storico ricostruito

- I due professionisti, erano ancora soci dello Studio associato S. non ancora sciolto,

- effettivamente si introdussero nel sistema informatico dello studio costituito da due servers e da due computers portatili, sui quali trasfusero i dati contenuti nei servers;

- i due portatili furono poi portati in altro luogo ove i dati vennero copiati ed, infine, i computers furono restituiti allo studio a richiesta del liquidatore.

- È necessario ricordare che la norma in esame tutela, secondo la più accreditata dottrina, ***molti beni giuridici ed interessi eterogenei***, quali il diritto alla **riservatezza,** diritti di **carattere patrimoniale**, come il diritto **all'uso indisturbato dell'elaboratore per perseguire fini di carattere economico e produttivo**, **interessi pubblici rilevanti**, come quelli di carattere militare, sanitario nonché quelli inerenti **all'ordine pubblico ed alla sicurezza**, che potrebbero essere compromessi da intrusioni o manomissioni non autorizzate.

- a tutelare i contenuti personalissimi dei dati raccolti nei sistemi informatici, ma prevede uno *ius excludendi alios* quale che sia il contenuto dei dati, purché attinenti alla sfera di pensiero o alla attività lavorativa dell'utente;
- Ergo vengono tutelati anche gli aspetti economici e patrimoniali,

- nei servers in questione erano custoditi i dati relativi ai clienti dello Studio S., del quale il S. era non solo socio di maggioranza relativa, ma anche amministratore ed in quanto tale garante del corretto utilizzo degli strumenti esistenti nello studio, e, quindi, anche del sistema informatico, per le finalità tipiche dello studio associato.
- È del tutto evidente che la copiatura dei dati, necessaria per fare funzionare lo studio concorrente creato dai due imputati, non era affatto compiuta nell'interesse dello Studio S., ma al fine di avvantaggiare uno studio concorrente; da ciò è lecito desumere che detta copiatura sia avvenuta con il dissenso, in verità anche espresso perché mediante una guardia giurata il S. impedì, anche se successivamente alla consumazione dei fatti contestati, l'accesso ai locali dello studio al B. ed al M., quanto meno tacito dell'amministratore dello studio che aveva il dovere di garantire il raggiungimento dei fini dello studio associato.
- Cosicché appare priva di pregio la considerazione che i due imputati, in quanto ancora formalmente associati, avevano il diritto di accesso al sistema, perché il problema e, quindi, la violazione della norma consiste nel fatto che i due non avevano il diritto di accesso al fine di sottrarre dati importanti per lo studio associato, con i quali fare concorrenza allo stesso;

Cassazione n. 40078/2009 (ud 26.6.2009) dep. 14.10.2009, Genchi

- Non ha commesso un accesso abusivo nè ha violato la privacy il consulente tecnico nominato incaricato di svolgere indagini sulla scomparsa di Denise Pipitone.
- Al tecnico - che aveva ottenuto l'autorizzazione dal comune di Mazara del Vallo a entrare nel sistema informatico dell'Agenzia delle Entrate - la procura di Roma aveva sequestrato supporti informatici relativi a posizioni di persone, circa 2.600, che nulla avevano a che fare con l'inchiesta.
- L'accusa del pm romano era di **reato di accesso abusivo e trattamento illecito di dati personali**.
- annullato dal tribunale del riesame della Capitale che ordinò il dissequestro del materiale
- Secondo i giudici della Cassazione Genchi NON ha compiuto un accesso abusivo, avendo ricevuto il mandato dal comune siciliano in quanto consulente tecnico del pm di Marsala che si occupa del sequestro di Denise Pipitone.
  Non ha quindi messo in atto nessun sistema per neutralizzare e superare le misure di sicurezza, apprestate dal titolare dello 'ius excludendì", al fine di impedire accessi indiscriminati.
- Devono essere quindi considerate irrilevante sia le finalità che si propone l'autore sia l'uso successivo dei dati che, se illeciti, integrano eventualmente un diverso titolo di reato.
- L'assenza di un "**vulnus" significativo** arrecato alle persone offese esclude anche la violazione della normativa sui dati personali.

Segue motivazioni Genchi 2009

Quanto all'ipotesi ex art. 615 ter c.p., va esclusa la qualifica di abusività attribuita all'attività svolta dal Genchi, avendo questi effettuato l'accesso, a seguito dell'autorizzazione ricevuta dal comune di Mazzara del Vallo nel sistema informatico dell'Agenzia delle Entrate . Nel caso in esame, essendo Genchi abilitato a consultare i dati presenti nel sistema informatico dell'Agenzia delle entrate, non è ipotizzabile una volontà contraria del titolare dello *ius excludendi* .Il Genchi era stato nominato consulente tecnico dal p.m. di Marsala nel procedimento relativo al sequestro della piccola Denise Pipitone e che per lo svolgimento di tale attività ricevette l'abilitazione all'accesso al sistema Siatel, dietro richiesta della procura al comune di Mazara del Vallo. Secondo un condivisibile orientamento giurisprudenziale, la qualificazione di abusività va intesa in senso oggettivo, con riferimento al momento dell'accesso e alle modalità utilizzate dall'autore per neutralizzare e superare le misure di sicurezza, apprestate dal titolare dello *ius excludendi*, al fine di impedire accessi indiscriminati. Non hanno quindi rilevanza la finalità che si propone l'autore e l'uso successivo dei dati che , se illeciti, integrano eventualmente un diverso titolo di reato (Cass. sez. VI, n. 39290 dell'8.10.2008, Peparaio, in Cass. pen. 2009, n. 863; conf. N. 2534/2007 e sez. V 26797 del 29.5.2008, Scimia). Quest'ultima decisione, correttamente rileva come la formula "abusivamente si introduce" sia ambigua e foriera di pericolose dilatazioni della fattispecie penale, se non intesa in senso restrittivo di "accesso non autorizzato", secondo la più corretta espressione di cui alla cosiddetta lista minima della Raccomandazione del Consiglio d'Europa, attuata in Italia con la legge n. 547 del 1993 , e di "accesso senza diritto", impiegata nell'art. 2 della

Non può pertanto condividersi la lettura della norma sottesa alla contestazione qui in esame, che individua l'abusività della condotta nel fatto di chi, abilitato ad accedere al sistema informatico, usi tale facoltà per finalità estranee al compito ricevuto. Oltre ad essere contrastante con l'indicato testo della Raccomandazione del Consiglio d'Europa, tale interpretazione porta alla creazione di una nuova fattispecie, frutto dell'intreccio delle due ipotesi descritte nell'art. 615 ter c.p., che il legislatore ha previsto disgiuntamente, come differenti e alternative. Sarebbe stata pleonastica la descrizione della seconda condotta , se la prima fosse realizzata anche da chi usa la legittimazione dell'accesso per fini diversi da quelli previsti (Cass. sez. VI, Peparaio cit.).

Le Sezioni Unite della Cassazione - 2012

- *Sez.* U, *Sentenza n.* 4694 *del* 2012 – **Sentenza n. 4694 del 27 ottobre 2011 - depositata il 7 febbraio 2012 -** *(Sezioni Unite Penale, Presidente E. Lupo, Relatore A. Fiale)*
- REATI INFORMATICI – ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO – MANTENIMENTO ABUSIVO NEL SISTEMA – REATO – SUSSISTENZA – CONDIZIONI
- Nel risolvere il contrasto in proposito insorto nella giurisprudenza di legittimità le Sezioni Unite hanno stabilito che la condotta di introduzione o di mantenimento in un sistema informatico protetto integra il delitto previsto dall'art. 615-ter cod. pen. qualora l'agente, pur essendo abilitato, violi le condizioni ed i limiti risultanti dal **complesso delle prescrizioni impartite dal titolare del sistema per delimitare oggettivamente l'accesso al medesimo**, senza che possano in alcun modo rilevare, ai fini della sussistenza dello stesso reato, gli scopi e le finalità che soggettivamente hanno motivato l'ingresso nel sistema. Nell'occasione il Supremo Collegio ha altresì precisato che la fattispecie di abuso delle qualità specificate nel n.1 del comma secondo del menzionato articolo costituisce una circostanza aggravante del

  delitto descritto nel primo comma dello stesso e non già un'ipotesi autonoma di reato.

- Caso di accesso allo SDI da parte di un appartenente alle forze di polizia

Sono a disposizione per eventuali vostre domande

www.studioaterno.it

STUDIO LEGALE ATERNO

s.aterno@studioaterno.it

SAPIENZA UNIVERSITÀ DI ROMA