Proc. n. 11577/01 R.G.N.R.

TRIBUNALE DI BOLOGNA
IN COMPOSIZIONE MONOCRATICA
IN NOME DEL POPOLO ITALIANO

Il Giudice Dott. Pier Luigi di Bari, all' udienza dibattimentale del 21/07/2005, con l'intervento del P.M. Dott. Giylapian e con l'assistenza del cancelliere Proietti, ha pronunciato mediante lettura del dispositivo e della seguente

SENTENZA DIBATTIMENTALE

nei confronti di:

1) C. G., nato a ***** il **/**/****, ivi residente in via *********

- contumace -

2) C. S. nato a ***** il **/**/****, ivi residente in via *********

- contumace -

Svolgimento del processo

Con decreto notificato il 25/03/03, C. S. e C. G. venivano citati in giudizio per rispondere, davanti a questo Tribunale, della violazione degli artt. 615 ter e quinquies, 81 cpv., 110 c.p., come da rubrica.

All'udienza del 13/6/03, dichiarata la contumacia degli imputati, venivano ammesse le prove orali richieste dalle parti: il Tribunale si riservava di disporre eventualmente la perizia, richiesta dalla difesa in ordine al funzionamento del codice virale, all'esito delle prove espletande.

Alla successiva udienza del 27/11/03, il Tribunale respingeva la richiesta della difesa di assoluzione ex art. 129 c.p.p. per mancanza di querela per la prima fattispecie criminosa, ritenendo che nella descrizione, contenuta nel capo di imputazione, del fatto integrante il reato di cui all'art. 615 ter c.p., vi fosse il riferimento al danneggiamento di programmi ed al loro malfunzionamento: si riteneva, pertanto, che il reato fosse procedibile d'ufficio, stante la contestazione, in fatto, dell'aggravante di cui all'art. 615 ter, secondo comma n. 3 c.p.

Nella medesima udienza venivano assunte le testimonianze del Cap. G.d.F. R. D. sulla attività generale di p.g. svolta per la individuazione dell'autore del programma, del M.llo. G.d.F. D. F. G. sulle operazioni di p.g. svolte presso Tiscali s.p.a., di B.C., responsabile di Tiscali s.p.a. per i rapporti con l'A.G., sull'attività di esecuzione del decreto di esibizione di tracce telematiche della Procura di Milano, del M.llo G.d.F. M. G. sulla attività di p.g. svolta presso l'abitazione dei C..

Nel corso dell'udienza si acquisiva, con il consenso delle parti, il decreto di esibizione ed il verbale di sequestro relativi al provider Tiscali s.p.a., nonché - previa emissione di apposita ordinanza - la comunicazione della predetta società relativa agli accessi effettuati per amministrare lo spazio web contenente il worm.

Veniva altresì prodotta memoria difensiva ex art. 121 c.p.p. per motivare le precedenti istanze istruttorie dirette ad ottenere l'ammissione di una perizia e l'esibizione del corpo di reato (che

veniva depositato all'udienza successiva).

All'udienza del 27 maggio 2004 venivano assunte le testimonianze di Ferrero Roberto, responsabile dell'Ufficio supporto Enti Istituzionali di Wind Telecomunicazioni s.p.a. (ex Infostrada), sull'attività di esecuzione del decreto di esibizione di tracce telematiche della Procura della Repubblica presso il Tribunale di Milano, e dell'ex M.llo G.d.F. F. D. sul sequestro operato presso il C. e l'analisi del materiale rinvenuto: nel corso di questa testimonianza, con il consenso delle parti, si acquisiva l'allegato n. 1 alla nota di p.g. del 28/3/01 e copia delle regola di condotta e procedura forense I.A.C.I.S.

Alla stessa udienza venivano letti ed acquisiti ex art. 513 c.p.p., stante la loro contumacia e la non opposizione delle parti, i verbali di interrogatorio resi dagli imputati il 07/09/01: veniva, inoltre, depositata memoria difensiva ex art. 121 c.p.p. con i relativi allegati.

All'udienza del 23/9/04, con il consenso delle parti, si acquisivano le note di p.g. della G.d.F. di Milano del 13/03/01, 19/03/01, 28/3/01, 15/5/01 e veniva depositata altra memoria difensiva ex art. 121 c.p.p. a sostegno della richiesta di perizia, che, all'udienza successiva del 20 ottobre, veniva respinta con ordinanza, in quanto ritenuta non necessaria.

Infine, dichiarata terminata l'istruttoria dibattimentale, nelle udienze del 24/2/05 e del 21/7/05, il P.M. ed i difensori concludevano rispettivamente come da verbale.

Motivi della decisione

1. Fatto e fonti di prova

L'imputato C. G. va ritenuto l'esclusivo colpevole dei reati di cui al capo di imputazione, avendo diffuso il programma informatico denominato "Vereika" di sua creazione, avente per effetto l'alterazione del funzionamento di sistemi informatici, ed essendosi introdotto abusivamente in sistemi informatici altrui in modo aggravato ai sensi dell'art. 615 ter, co. 2 n. 2-3, c.p..

Si perviene a tale conclusione processuale in forza delle seguenti fonti di prova: 1) verbali di perquisizione e sequestro operato il 21 marzo 2001 dalla Polizia Tributaria della Lombardia a carico di C. G. e S.; 2) verbale di acquisizione di tracce telematiche del 14 marzo 2001 eseguita presso Infostrada s.p.a. dalla Polizia Tributaria della Lombardia; 3) documento prot. SEI 010313009355 e SEI 010314009405 di Infostrada s.p.a. relativo all'amministrazione dello spazio web digilander.iol.it/vierika/index.html (fax del 16/3/01); 4) verbale di esibizione e sequestro del 14 marzo 2001 eseguito presso Tiscali s.p.a. dalla Polizia Tributaria della Sardegna; 5) comunicazione e-mail Tiscali s.p.a. del 14 marzo 2001 relativa all'amministrazione del sito web.tiscalinet.it/krivojrog/vierika/Vindex.html; 4) annotazioni di p.g. della Polizia Tributaria della Lombardia del 13/3/01, 19/3/01, 28/3/01 (con all. n. 1), 15/5/01; 5) testimonianze di F. D., R. D., B. C., M. G.; 6) verbale di interrogatorio dell'imputato del 7 settembre 2001.

2. Il worm Vierika

L'istruttoria dibattimentale, in particolare le testimonianze di F. D.[1] e R. D.[2], e le annotazioni di

p.g. agli atti[3], hanno permesso di accertare che Vierika[4] è un internet worm programmato in Visual Basic Script, i cui effetti derivano dalla interazione di due script differenti.

Il primo, di piccole dimensioni, è allegato come attachment ad una e-mail: tale lettera contiene infatti il file Vierika.JPG.vbs, mentre il subject è "Vierika is here" e nel testo viene indicato "Vierika.jpg".

Una volta eseguito, il programma agisce sul registro di configurazione di Windows[5], abbassando al livello minimo le impostazioni di protezione del browser Internet Explorer ed inserendo come home page del predetto browser la pagina web http://web.tiscalinet.it/krivojrog/vierika/Vindex.html.

Il secondo script in Visual Basic, di dimensioni maggiori, è contenuto nel documento html Vindex.html[6], e si attiva quando l'utente, collegandosi ad Internet, viene automaticamente indirizzato dal browser sulla nuova home page sopra indicata: il basso livello di protezione impostato dalla prima parte del codice, permette l'automatica esecuzione dello script contenuto nel documento html.

L'effetto di questo secondo script è quello di creare nella prima partizione del primo disco rigido del computer il file c:\Vierika.JPG.vbs, contenente la prima parte del codice, e di produrre un effetto di mass-mailing, inviando agli indirizzi contenuti nella rubrica di Outlook una e-mail contenente l'attachment sopra descritto, in modo tale che il programma Vierika si autoreplichi[7].

3. Individuazione dell'imputato ed accertamento della sua condotta

Alla identificazione dell'imputato la Guardia di Finanza di Milano perveniva attraverso una indagine iniziata il 5 marzo 2001 dopo aver ricevuto una e-mail contenente il primo script del programma, come sopra descritto: la p.g. individuò due siti web, uno sul server di Tiscali s.p.a. (contenente il secondo script), e l'altro sul server di Infostrada s.p.a.[8], aventi nella propria url il nome Vierika[9].

Lo stesso giorno Tiscali s.p.a., su segnalazione informale della G.d.F. di Milano[10], provvedette a sospendere l'accesso al sito web.tiscalinet.it/krivojrog/vierika/Vindex.html [11]: vennero poi emessi dalla Procura di Milano, ed eseguiti, due decreti di esibizione e sequestro delle tracce telematiche relative ai due siti indicati.

Dai dati forniti dal gestore Tiscali s.p.a., la cui documentazione è agli atti, risultavano interventi di gestione del sito web.tiscalinet.it/krivojrog/vierika/Vindex.html relativi all'11/12/00 ed alla notte del 3/3/01[12] ad opera dell'utente con username krivoj, registrato presso il provider con i dati di identificazione e di residenza di C. G.: utente che si connetteva al server mediante una linea telefonica risultata intestata a C. S..

Dai dati forniti dal gestore Infostrada s.p.a. risultava che nella notte del 3 marzo 2001 l'utente avente come username krivoj[13] - registrato anche presso questo provider con gli estremi di identificazione e di residenza di C. G. - realizzava sei interventi di amministrazione sul sito digilander.iol.it/vierika/index.html, connettendosi al server mediante la medesima utenza telefonica sopra indicata.

L'ultimo intervento di gestione risultava effettuato, dal medesimo utente e con la stessa linea telefonica, nella notte del 12 marzo 2001: alle ore 9,01 del 14/03/01 l'utente disattivava il proprio account presso il provider Infostrada s.p.a.

Sulla base dei dati acquisiti, in esecuzione di attività delegata dalla Procura di Milano, il 21 marzo 2001 la G.d.F. di Milano eseguiva una perquisizione presso l'abitazione dei fratelli C., ove C. G., di professione consulente informatico, risultava avere anche la sede della propria attività: in quella circostanza l'imputato, assuntasi la paternità del programma, indicava alla p.g. i files relativi al programma Vierika contenuti nel proprio disco rigido[14], masterizzandone copie da sottoporre a sequestro sotto il controllo degli agenti[15].

In sede di interrogatorio, il 7 settembre 2001, C. G. confermava di avere creato e diffuso il programma Vierika.

4. Il problema del metodo e gli accertamenti tecnici di parte

La difesa dell'imputato sia nel corso dell'istruttoria, che nell'arringa finale ha reiteratamente posto in discussione la correttezza sia del metodo utilizzato dalla p.g. per estrarre i programmi dal computer del C., che di quello applicato dalla p.g. e dalle società Infostrada s.p.a. e Tiscali s.p.a. per individuare l'amministratore degli spazi web (uno dei quali contenente il secondo script del programma Vierika).

Il tema è, in termini generali, di non poco momento e certamente dovrà essere affrontato in maniera approfondita anche dalla giurisprudenza, ma appare nella fattispecie in esame di seconD. rilievo.

Occorre innanzitutto precisare che non è compito di questo Tribunale determinare un protocollo relativo alle procedure informatiche forensi, ma semmai verificare se il metodo utilizzato dalla p.g. nel caso in esame abbia concretamente alterato alcuni dei dati ricercati.

In altre parole, non è permesso al Tribunale escludere a priori i risultati di una tecnica informatica utilizzata a fini forensi solo perché alcune fonti ritengono ve ne siano di più scientificamente corrette, in assenza della allegazione di fatti che suggeriscano che si possa essere astrattamente verificata nel caso concreto una qualsiasi forma di alterazione dei dati e senza che venga indicata la fase delle procedure durante la quale si ritiene essere avvenuta la possibile alterazione.

In termini generali, quando anche il metodo utilizzato dalla p.g. non dovesse ritenersi conforme alla migliore pratica scientifica, in difetto di prova di una alterazione concreta, conduce a risultati che sono, per il principio di cui all'art. 192 c.p.p., liberamente valutabili dal giudice alla luce del contesto probatorio complessivo (fermo restando che maggiore è la scientificità del metodo scelto, minori saranno i riscontri che il giudice è chiamato a considerare per ritenere attendibili gli esiti delle operazioni tecniche).

Facendo applicazione di tali principi nel caso in esame, deve evidenziarsi come la difesa si sia limitata ad allegare che i metodi utilizzati, non essendo conformi a quelli previsti dalla (supposta) migliore pratica scientifica, conducono a risultati che non possono essere ritenuti ab origine attendibili, senza peraltro allegare che nel caso concreto si è prodotta una qualche forma di alterazione o che avrebbe potuto prodursene alcuna, indicandone la possibile fonte, forma e fase di azione.

Gli accertamenti compiuti dalla p.g. in ordine alle tracce telematiche possono ritenersi pienamente attendibili alla luce del contesto probatorio complessivo (confermando, indirettamente, che il metodo utilizzato non ne ha alterato gli esiti).

Da una parte, infatti, i dati consegnati alla p.g. dal provider Tiscali (gli interventi di amministrazione sul sito http://web.tiscalinet.it/krivojrog/vierika/Vindex.html avvenivano da parte

dell'utente con username krivoj, registrata presso il provider con i dati identificativi del C.; le connessioni avvenivano per mezzo della utenza telefonica intestata al fratello, S., di C. G.) trovano un riscontro incrociato con quelli forniti dal provider Infostrada[16] (gli interventi di amministrazione sul sito digilander.iol.it/vierika/index.html avvenivano da parte dell'utente con username krivoj, registrata presso il provider con i dati identificativi del C.; le connessioni avvenivano per mezzo della utenza telefonica intestata al fratello del C.; l'imputato, in sede di interrogatorio, ha confermato di operare ancora sul sito digilander.iol.it/vierika), dall'altra, l'assunzione della paternità del programma fatta dal C. in sede di interrogatorio, rende puro esercizio accademico l'affrontare più approfonditamente la questione del metodo.

Il C., infatti, in sede di interrogatorio dichiara espressamente di aver creato e diffuso il programma denominato Vierika, e già in precedenza, al momento della perquisizione domiciliare, lo aveva indicato alla p.g. operante, masterizzandone le copie da sottoporre a sequestro sotto il controllo degli agenti.

Quanto al funzionamento del programma, non sembra che la complessiva impostazione difensiva abbia posto seriamente in discussione il meccanismo sopra descritto, avendo appuntato le proprie critiche, anche con l'ausilio di tecnici, su aspetti del funzionamento e degli effetti del programma, ipotizzati o ritenuti dalla p.g., che in questa sede non sono stati ritenuti rilevanti ai fini dell'affermazione della penale responsabilità dell'imputato.

Le attenzioni della difesa, nella memoria depositata alla udienza del 23/6/04, si sono concentrate sul fatto che il programma interagisce solo con Outlook e non con la più diffusa versione Outlook Express; su correzioni terminologiche (come il riferimento improprio ai programmi "sorgente" sequestrati all'imputato) o sulle valutazioni del teste F., in particolare in ordine alla potenziale diffusività del programma; sulle generalizzazioni ed esemplificazioni contenute nelle note di p.g.

Dalle stesse considerazioni della difesa si ricava, peraltro, che "Vierika è un codice autoreplicante in due parti...in grado di infettare...le macchine con Windows 95 o 98 con istallato il software "Outlook Professional" della piattaforma "Microsoft Office", p. 2; si legge ancora che "se andiamo a leggere il codice di Vierika, troviamo che esso chiama funzioni dell'interfaccia MAPI completa, in particolare per acquisire gli indirizzi dalla rubrica", p. 3; a p. 5 si contesta la sussumibilità delle impostazioni di protezione di Internet Explorer nel concetto normativo di misure di sicurezza, ma non che il programma apponesse tali modifiche, tanto più che - si spiega - per ripristinare le impostazioni originarie sarebbero bastati "quattro click del mouse"; si contesta la ingannevolezza del messaggio e-mail portatore del programma, ma non il fatto che abbia una doppia estensione e contenga un codice eseguibile; si contesta che il programma abbia un funzionamento di tipo "troiano" con appropriazione e diffusione di dati riservati, ma si ammette che esplica "funzioni di mailing del software Outlook installato sulla macchina al fine di autoreplicarsi", p. 9; a p. 22 si riconosce che Vierika è un worm che si autodiffonde utilizzando gli indirizzi di posta elettronica e che si manifesta come allegato di posta elettronica.

Conferma del fatto che le operazioni di copiatura del programma Vierika, avvenute nel corso della perquisizione domiciliare, non ne hanno in concreto prodotto alcuna alterazione, deriva dal fatto che i risultati dell'analisi della copia sequestrata sono del tutto conformi alla descrizione del suo funzionamento operata dalla p.g.[17] e da una società produttrice di antivirus[18] in un momento antecedente al sequestro operato presso l'abitazione del C.: descrizione, come sopra riportata al punto 2, che non poteva, pertanto, risentire di ipotetiche ed astratte alterazioni dovute alle successive operazioni tecniche poste in essere dalla p.g.

Non può, inoltre, non evidenziarsi che la difesa si è limitata a porre suggestivamente la questione in ordine alla metodologia di sequestro del programma: non ha, invece, allegato la sua avvenuta

alterazione in concreto, nonostante la disponibilità della versione da cui fu copiato il programma successivamente analizzato dalla p.g., rimasta nel possesso dell'imputato, le avrebbe permesso l'accertamento e l'allegazione di eventuali anomalie.

Non solo il disco rigido dell'indagato non fu sottoposto a sequestro, ma non risulta che vennero nemmeno rimossi i files trovati nel computer del C.: venne, infatti, sottoposta a sequestro una loro copia masterizzata su cd, lasciando gli originali nella disponibilità dell'imputato (teste F. p. 22).

Appare in questa sede opportuno precisare che non si è ritenuto necessario disporre una perizia volta ad esplicare il funzionamento del programma: da una parte, infatti, i testi di p.g. (in particolare, F. D.) avevano le competenze tecniche necessarie per la decifrazione del codice, dall'altra si è ritenuto che la difesa non abbia in sostanza contestato i meccanismi di funzionamento del programma, come esplicitati dai testi escussi e sopra descritti al punto 2, nonostante si sia servita anche della collaborazione di un esperto informatico (per criticare e contestare, come si è detto, aspetti della deposizione del teste F. che non sono stati valorizzati in questa sede).

Deve inoltre sottolinearsi che gli elementi di conoscenza probatoria di cui dispone il Tribunale poggiano anche su produzioni documentali assunte con il consenso delle parti, come la cd. analisi tecnica redatta da F. D. ed allegata alla nota di p.g. del 15/5/01 e la documentazione relativa ai files sequestrati nel computer dell'imputato (all. 1 alla nota di p.g. del 28/3/01).

Si ritiene, pertanto, che il contraddittorio si sia svolto anche su di essi, mettendo il giudice in condizioni di poter ricostruire adeguatamente gli aspetti rilevanti della condotta materiale del C. e di compiere le opportune valutazioni di tipo giuridico, comprese quelle inerenti l'elemento soggettivo del reato.

Non ignora il Tribunale l'emergere di un orientamento della Suprema Corte, non consolidato, che sembrerebbe adombrare una qualche forma di cogenza della perizia, ogni qual volta la ricognizione del reato presupponga accertamenti di tipo tecnico (Cass. pen., sez. III, n. 4686/05, Corsi; Cass. pen., sez. V, n. 5672/05, Scoppa).

Deve peraltro constatarsi che tale orientamento pretermette, senza alcun accenno motivazionale, il tradizionale insegnamento secondo il quale la perizia è un mezzo di prova essenzialmente discrezionale, essendo rimessa al giudice di merito, anche in presenza di pareri tecnici e documenti prodotti dalle parti, la valutazione della necessità di disporre indagini specifiche (cfr. Cass. pen., sez. VI, n. 34089/03, Bombino).

Nella fattispecie in esame la difesa, nonostante abbia presentato quattro memorie ex art. 121 c.p.p., non ha prodotto alcun documento o parere che disconosca il funzionamento del worm nei suoi aspetti delineati al punto 2, gli unici valorizzati in questa sede: a fronte della descrizione del codice operata dalla p.g., non ha invero allegato un diverso funzionamento del programma, chiedendone l'accertamento ad opera di un perito.

Sotto altro aspetto, il menzionato orientamento giurisprudenziale non consente un agevole coordinamento tra il principio del libero convincimento del giudice e quello del contraddittorio tra le parti.

Tradizionalmente, infatti, in forza del primo principio, il giudice può valorizzare un accertamento di parte che sia ritenuto esaustivo, corretto ed appropriato, senza necessità di accertamenti ulteriori.

In tal caso, la tutela delle parti, siano esse pubbliche o private, si esplica in primo luogo a livello motivazionale, dovendo l'organo giudicante dare compiuta contezza dei risultati raggiunti: qualora

ritenga di aderire alla prospettazione tecnica di una delle parti, non è peraltro gravato dell'obbligo di fornire autonoma dimostrazione dell'esattezza scientifica delle conclusioni raggiunte e dell'erroneità di tutte quelle espresse, dovendosi considerare sufficiente che egli dimostri di avere comunque valutato le conclusioni e le argomentazioni delle parti (cfr. su tale tematica Cass. pen., sez. IV, n. 34379/04, Spapperi).

Del resto non avrebbe senso imporre una sorta di accertamento vincolato mediante perizia, lasciando poi libero l'organo giudicante, peritus peritorum, di disconoscerne motivatamente i risultati, come da sempre viene riconosciuto in giurisprudenza.

Tali conclusioni potrebbero trovare conferma indiretta anche dalla analisi della fattispecie concreta sottoposta al giudizio di una delle pronunce innovative sopra richiamate (Cass. pen. n. 5672/05, cit.): il risultato a cui essa perviene si fonda, infatti, sulla censura di difetto di motivazione della sentenza di appello in ordine al rigetto di una istanza di perizia dibattimentale e sul fatto che un teste riferisse de relato le conclusioni a cui era giunto personale di p.g., esprimendo considerazioni tecniche riferite ad un'attività da lui non direttamente espletata (a differenza del caso in esame, in cui i testi sono stati escussi sulla attività da loro condotta).

Quanto al principio del contraddittorio, la parità di armi fra accusa e difesa si garantisce non solo con il controesame del teste esperto addotto da una delle parti, ma con la facoltà di dedurre testimoni e produrre documenti e memorie, anche avvalendosi di consulenti tecnici (per la considerazione che il diritto alla controprova non può, invece, avere ad oggetto l'espletamento di una perizia, essendo questo mezzo di prova di per sé neutro, cfr. Cass. pen., sez. VI, n. 275/96, Tornabene).

Ed è proprio uno dei pochi passaggi argomentativi di Cass. pen., n. 4686/05, cit., che conferma come la perizia non possa ritenersi cogente, laddove, richiamando l'art. 360 c.p.p., ricorda che, in caso di accertamenti tecnici irripetibili, il PM deve consentire alla parte di parteciparvi con un proprio consulente.

Il fatto che anche nel caso degli accertamenti non più ripetibili eseguiti da una delle parti non sia prevista l'obbligatorietà della perizia, nonostante nessuna operazione tecnica ulteriore potrà più essere disposta in dibattimento, dimostra che il legislatore ha essenzialmente concepito il contraddittorio come sufficientemente garantito dalla possibilità per le parti di partecipare, in proprio o mediante consulenti, agli accertamenti tecnici.

La facoltà che esse hanno di promuovere incidente probatorio non mina tale ragionamento, ma trova spiegazione nel fatto che, mentre nel caso di accertamenti ripetibili le risultanze di parte saranno sottoposte alla valutazione imparziale del giudice, il quale potrà disporre un nuovo accertamento peritale qualora le ritenga insufficienti od inidonee, nel caso degli atti urgenti, l'impossibilità di ripetizione dell'atto ed il principio del contraddittorio suggeriscono l'immediato riconoscimento alle parti della facoltà di sollecitare ed anticipare la funzione di terzietà e controllo che è propria dell'organo giudicante.

5. Il reato di cui all'art. 615 quinquies c.p.

Deve ritenersi che C. G. abbia commesso il reato di cui all'art. 615 quinquies c.p., avendo diffuso il programma denominato Vierika, da lui creato, avente per scopo ed effetto l'alterazione di alcune delle funzionalità telematiche di sistemi informatici.

La diffusione del programma, oltre che dalle circostanze che nel prosieguo verranno indicate e dalle

quali si desumono gli accessi abusivi commessi[19], si evince dalle dichiarazioni dell'indagato che, in sede di interrogatorio, ammette di averlo diffuso, inviandolo ad alcuni indirizzi di posta elettronica reperiti sulla bacheca elettronica del sito www.sexualcyber.com/annunc.htm.

Non vi è dubbio, a parere del Tribunale, che il programma creato dall'imputato abbia come scopo ed effetto quello di alterare una parte del funzionamento dei sistemi informatici aggrediti.

Infatti, gli effetti complessivi creati dai due script di cui è composta Vierika, integrano una modificazione dell'ordinario modo di funzionare dei programmi Internet Explorer ed Outlook, dal momento che l'invio automatico di e-mail e l'autonoma modifica dei parametri di protezione del browser, senza alcuna conoscenza da parte dell'utente ed in assenza della digitazione degli appositi comandi da parte sua, costituiscono comportamento anormale del sistema.

L'impostazione accolta sembra trovare riscontro nella fattispecie sottoposta all'esame di Cass. pen., sez. II, n. 17295/04, Nicolai, ove viene avallata l'interpretazione dei giudici di merito, secondo i quali la modifica dei parametri di connessione ad internet occultamente realizzata da un software dialer integra il concetto di alterazione rilevante agli effetti di cui all'art. 640 ter c.p.

Quanto all'elemento soggettivo del reato, si ritiene sufficiente l'accertata volontà dell'imputato di diffondere il programma con la consapevolezza dei suoi effetti (conoscenza derivante dall'esserne il C. l'autore), non esigendo la norma che il fine dell'agente sia diretto alla distruzione od al danneggiamento del sistema.

Non sembra che il dolo possa venire escluso dalle motivazioni che hanno spinto il C. a realizzare Vierika, da lui ricondotte, in occasione dell'interrogatorio, a fini di studio e ricerca, e dal suo difensore a fini ludici: infatti, esse non elidono, ma anzi presuppongono, la volontà di diffusione del programma con la conoscenza dei suoi effetti ed integrano, semplicemente, il movente del reato (apprezzabile in sede di trattamento sanzionatorio).

Né, per il principio ignorantia legis non excusat, ha alcun rilievo scriminante la convinzione dell'imputato, quale si ricava dall'interrogatorio, che gli effetti del programma dai lui creato non integrerebbero gli elementi oggettivi delle due fattispecie criminose contestategli.

Peraltro, un'analisi cronologica degli accadimenti, alla luce dell'esame di tutti i programmi rinvenuti nel computer dell'imputato[20], consente di dare maggiore intensità alla volontà dell'imputato di realizzare il fatto delittuoso.

Il C., infatti, nella notte del 3 marzo 2001, dopo aver effettuato un lungo accesso sul sito ospitato da Tiscali s.p.a., si collega con l'altro sito web presente sul server di Infostrada s.p.a.: al termine di queste connessioni, dopo le nove del mattino, apporta le ultime modifiche ai files Vierika.jpg.vbs e Valecalda.vbs, entrambi rinvenuti nel suo pc e contenti il codice Vierika.

Il 5 marzo, su segnalazione di clienti e della G.d.F. (che, oltre a ricevere in proprio il programma con una e-mail, ha constatato che su internet ne è già stata segnalata la presenza), Tiscali s.p.a. impedisce agli utenti l'accesso al sito contenente la seconda parte dello script, in modo da bloccare la diffusione del programma.

Il 7 marzo, dopo aver probabilmente rilevato che il sito sul server di Tiscali s.p.a. era stato oscurato, C. modifica cinque programmi aventi il medesimo codice di Vierika, ma nei quali il comando relativo alla modifica della home page del browser fa riferimento al sito ospitato sul server di Infostrada s.p.a. (Edit1.txt, Edit2.txt, Edit4.txt, Finale.txt, Copia di edit2.vbs).

Nella notte del 14 marzo, qualche ora prima che vengano notificati i decreti di esibizione e sequestro ai due provider, l'imputato apporta le ultime modifiche ad alcuni programmi rinvenuti nel suo computer.

Fra questi i files Newvirus.txt, NewVirus2.txt, Vierika.jpg.txt (contenenti le istruzioni per impostare come home page la pagina digilander.iol.it/vierika e far comparire come soggetto delle e-mail la significativa scritta "Vierika è tornata"), ed il file Newvirus2.vbs, contenente le istruzioni per far inviare dai computer infetti una e-mail anche all'indirizzo abuse@libero.it (attraverso il quale Infostrada s.p.a. gestisce le segnalazioni relative alla sicurezza informatica): e-mail avente nel soggetto "ragazzi non scherzate..." e nel testo "certe cose non si dovrebbero mai fare...", nonché un attachment (autoexec.bat).

Nella notte del 14 marzo le ultime operazioni C. le svolge su tre programmi (Laura.jpg.txt, Viruslibero.txt, Copia di Viruslibero.vbs) aventi l'effetto di far inviare dai computer infettati 300 e-mail all'indirizzo di posta elettronica abuse@libero.it (nota di p.g. G.d.F. Milano del 28/3/01, p. 3.).

Alle nove del mattino del 14 marzo C. disattiva il proprio account presso Infostrada s.p.a. (l'ultimo accesso al sito digilander.iol.it/vierika/index.html era avvenuto nella notte del 12 marzo).

La sequenza temporale descritta, oltre a dimostrare la piena consapevolezza dell'imputato in ordine agli effetti prodotti dal proprio programma, induce a ritenere che il C. stesse progettando interventi sempre più complessi e pregiudizievoli.

6. Il reato di cui all'art. 615 ter c.p.

Esistono indizi gravi, precisi e concordanti dell'avvenuta introduzione del C., per mezzo del programma da lui creato, all'interno di sistemi informatici altrui protetti da misure di sicurezza.

Tale introduzione si ricava dalle segnalazioni sulla diffusione del virus che vennero fatte da alcune società di sicurezza informatica[21], dalle lamentele che alcuni clienti presentarono a Tiscali s.p.a. poiché ospitava il programma sui propri spazi web[22], e dai dati numerici presenti nel counter del sito web.tiscalinet.it/krivojrog/vierika/Vindex.html, dal quale risultavano 829 visite (cfr. teste Cap. R. p. 27; nota di p.g. G.d.F. Milano del 13/3/01, p. 3).

Non vi è dubbio che l'introduzione - la quale sussiste ogni volta che vengano sorpassati gli ostacoli che presidiano l'accesso al sistema e che non presuppone necessariamente che il reo sia in grado di poter richiamare e disporre dei dati e programmi contenuti nel computer violato - sia avvenuta abusivamente, dovendosi a tal fine apprezzare la natura, le finalità e le modalità della condotta del C., volte ad aggirare il jus prohibendi dei titolari.

Vengono in rilievo soprattutto le modalità dell'azione, dirette a manipolare con l'inganno (primo script del programma) e clandestinamente (secondo script) la volontà dell'utente.

L'abusività discende, innanzitutto, dalla fraudolenta induzione in errore dell'utente che riceveva l'e-mail sull'esistenza di un'immagine: infatti, il file Vierika, presentava una doppia estensione che, all'epoca, secondo le impostazioni di default di Outlook, non veniva visualizzata dall'utente per intero (salvo questi avesse cambiato le impostazioni predefinite)[23], poiché il sistema mostrava solo la prima, relativa al formato jpg.

L'estensione jpg indicava la presenza di un'immagine allegata al messaggio e quest'ultimo ne suggeriva l'inerenza ad una figura femminile (nel soggetto compariva, infatti, la scritta "Vierika is

here"), sicché l'utente era portato ad acconsentire alla esecuzione del file associato (richiesta di esecuzione che non pare venisse, peraltro, formulata in modo esplicito, ma mascherata dietro l'innocua richiesta all'utente di esprimere il suo consenso a vedere la foto)[24]: immagine non presente nell'allegato, che conteneva solo uno script in Visual Basic[25].

Indipendentemente, pertanto, dalla visualizzazione completa del file, la maliziosa scelta del C. di impostare quale prima estensione dell'attachment quella relativa ad un oggetto che stimolava la curiosità dell'utente e che non sussisteva, doveva ritenersi volta ad aggirare fraudolentemente la volontà del destinatario.

Sintomi di tale fraudolenza si ricavano, inoltre, dal fatto che il C. non si presentava come l'effettivo mittente della e-mail, ma ne celava la paternità attraverso il meccanismo di funzionamento del worm, il quale si autoreplicava sfruttando gli indirizzi contenuti nella rubrica di Outlook: in tal modo, il destinatario erano indotto a ritenere l'e-mail proveniente da un mittente diverso da quello effettivo, il C., ed a fare affidamento sulla bontà del messaggio ricevuto nel caso ne conoscesse l'apparente autore (dal cui computer veniva inviato il messaggio).

L'abusività della introduzione, oltre che con l'inganno insito nelle modalità di presentazione del primo script, è integrata anche dal sistema occulto con il quale agiva il secondo script, posto che l'abbassamento delle impostazioni di protezione del browser comportava l'esecuzione della seconda parte del codice senza che l'utente ne avesse alcuna consapevolezza.

Le modalità di introduzione descritte rendono pertanto inappropriato il riferimento che la difesa ha ripetutamente fatto al funzionamento di alcuni cd autoinstallanti per la connessione ad internet fornita da infostrada, kataweb ed altri: in tali casi, infatti, l'esecuzione del programma deve essere volontariamente attivata dall'utente mediante l'introduzione del supporto nel terminale e le modifiche apportate dal programma – spesso funzionali al risultato che l'utente si prefigge con la sua installazione – sono da lui immediatamente percepibili.

Come sopra anticipato, deve ritenersi che le introduzioni abusive avvennero in sistemi informatici presidiati da misure di sicurezza, considerato che il programma Vierika era destinato proprio ad abbassare le impostazioni di protezione del browser.

Nelle versioni più diffuse nel 2001, Internet Explorer consentiva di suddividere i siti internet in quattro differenti aree di protezione (internet, intranet locale, siti attendibili e siti con restrizioni) all'interno delle quali era possibile impostare livelli di sicurezza diversi (da alto a basso) [26], in base alla provenienza ed al grado di attendibilità delle informazioni sul Web: quello predefinito dal produttore Microsoft era quello medio.

Il primo script del programma Vierika agiva su queste misure di protezione abbassando al livello minimo le impostazioni di default presenti nell'area Internet, affinché fosse poi possibile, collegandosi alla pagina web presente sul server di Tiscali s.p.a., l'esecuzione del secondo script del programma.

Deve ritenersi che le impostazioni di protezione di Internet Explorer rientrino a pieno titolo nel concetto di misura di sicurezza di cui all'art. 615 ter c.p., poiché, regolando le finestre a comparsa e l'esecuzione automatica di download e contenuti attivi (fra i quali gli script ed i controlli Active X di cui si è parlato nel corso del dibattimento), costituiscono la protezione minima per gli utenti di internet contro l'occulta installazione di cavalli di Troia, spyware, virus, worm, dialer e l'apertura di backdoor (strumenti attraverso i quali, oltre che captare informazioni e dati, si può ottenere il controllo remoto del terminale infettato).

Nella nota depositata all'udienza del 23/6/04 la difesa non nega che le impostazioni di protezione di Internet Explorer abbiano "...dei riflessi, anche molto, rilevanti, sulla sicurezza della navigazione in rete dell'utente..." e che tali parametri consentono di "...scaricare o non scaricare varie tipologie di oggetti...che, contenendo codice eseguibile, potrebbero potenzialmente dare fastidio" (p. 5).

Del resto è sempre la difesa ad avere evidenziato, in sede di perorazione finale, come l'impostazione del massimo livello di protezione impedisca di scaricare persino le patch di aggiornamento di Microsoft: non si vede, pertanto, come si possa negare che tale strumento costituisca la prima basilare difesa – spesso insufficiente – dei fruitori della rete internet.

Né, come rilevato dalla giurisprudenza e dalla dottrina, è necessario che le misure di sicurezza abbiano un elevato grado di efficacia, rimanendo tali anche nel caso siano facilmente superabili da una persona mediamente esperta, poiché la loro funzione è solo quella di manifestare lo ius excludendi dell'avente diritto (Trib. Torino 7/2/98, Giur. mer. 1998, p. 708; Trib. Torino 4/12/97, Giur. it. 1998, p. 1923), in conformità con il bene giuridico protetto dalla norma, da ravvisarsi nella tutela del domicilio informatico (cfr. Cass. pen., sez. VI, n. 3065/99, De Vecchis)[27].

Proprio per tale loro funzione, si è ritenuto in dottrina e giurisprudenza che, prescindendo dalla manipolazione, non necessaria, delle misure di sicurezza, integri il reato anche chi abusi per tempi, finalità od aree di accesso delle autorizzazioni dell'avente diritto e che, in tale concetto, possano farsi rientrare anche barriere materiali[28], quali l'esclusiva disponibilità dei locali contenenti il sistema informatico violato.

Sviluppando l'insegnamento di Cass. pen., sez. V., n. 12732/00, Zara, non risulta pertanto peregrino affermare che, poiché l'illecito non si sostanza nell'effrazione dei mezzi di protezione, ma nella violazione delle disposizioni del titolare, l'introduzione nei sistemi informatici mediante strumenti di intrusione o di controllo remoto che sfruttano canali telematici, quando avviene in sistemi di privato ed esclusivo utilizzo custoditi in locali ad accesso riservato, privi di una qualsiasi propaggine pubblica e visibile nella rete internet, deve considerarsi effettuata in violazione della volontà del titolare (sicché, ad esempio, si dovrà accertare l'effettiva esistenza di misure di sicurezza nel caso della abusiva introduzione in una banca dati consultabile on-line, ma non nel caso di introduzione in una utenza informatica domestica utilizzata per soli fini di esplorazione del web).

Nel fatto commesso dal C. devono ravvisarsi le aggravanti previste dall'art. 615 ter secondo comma numeri 2 – 3 c.p., poiché l'introduzione è avvenuta mediante violenza sulle cose ed il programma Vierika ha apportato effetti pregiudizievoli ai sistemi informatici colpiti: sebbene non sia stato fatto un espresso riferimento normativo, deve ritenersi che le aggravanti siano state contestate con la descrizione del fatto contenuta nel capo di imputazione, in particolare nel riferimento al danneggiamento dei programmi ed al pregiudizio del loro corretto funzionamento.

Quanto alla prima aggravante, secondo quanto già esposto in relazione alla fattispecie di cui all'art. 615 quinquies c.p. e tenuto conto della definizione di violenza fornita dal terzo comma dell'art. 392 c.p. per ogni effetto penale, deve ritenersi che l'ingresso abusivo avvenne mediante l'alterazione dell'ordinario funzionamento del browser Internet Explorer, al quale il programma Vierika forniva istruzioni per l'abbassamento del livello di protezione, senza che l'utente impartisse il relativo comando, realizzando così una modificazione delle normali modalità di comportamento del programma che consente l'esplorazione del web.

Quanto alla seconda aggravante, deve rilevarsi che il worm produce alcuni effetti negativi, per quanto di minima entità, sulla memoria del computer e sui tempi di connessione ordinariamente necessari per l'invio e la ricezione della posta elettronica (con eventuale conseguente aggravio di

spese telefoniche).

Rilevato, inoltre, che la norma non prescrive che il danno debba avere natura esclusivamente patrimoniale, deve osservarsi che il programma produce anche una pregiudizievole veicolazione di informazioni che sono nella disponibilità esclusiva dell'avente diritto: l'invio di una e-mail a tutti gli indirizzi presenti nella rubrica di Outlook, infatti, rende edotto il destinatario di informazioni che l'apparente mittente potrebbe volere non rivelare (quali, ad esempio, la sua avvenuta connessione ad internet; la conoscenza del suo recapito e-mail che il destinatario può ricavare dal messaggio ricevuto[29]; il fatto, che può essere ignoto al destinatario, che il mittente abbia la disponibilità del suo indirizzo e-mail).

Occorre infine osservare che la modifica occulta e stabile dei livelli di protezione del browser, esponeva l'utente al rischio di ulteriori e più gravi infezioni informatiche, poiché, non essendo a conoscenza della modifica apportata e facendo ragionevole affidamento nell'ordinario comportamento del sistema, avrebbe potuto compiere operazioni o visitare siti pericolosi con il nuovo livello di protezione impostato.

Non vanno, inoltre, sottovalutate le eventuali conseguenze a cui sarebbe stato esposto l'utente del computer infettato per avere inconsapevolmente contribuito alla diffusione del worm: l'essere, infatti, additato quale veicolo del contagio avrebbe potuto giustificare l'applicazione nei suoi confronti di misure di contenimento, come, ad esempio, la sospensione della partecipazione a mailinglist o l'inserimento, da parte dei destinatari, nella lista dei mittenti bloccati.

L'elemento soggettivo è integrato dalla intenzionale volontà del C. di introdursi nei sistemi informatici altrui protetti dai sistemi di sicurezza, quale si desume dalla volontaria diffusione del programma da lui creato a tali fini, con la consapevolezza di averlo fatto mediante inganno e clandestinamente.

Quanto alle aggravanti, la volontà della violenza sulle cose discende dall'aver predisposto il codice affinché alterasse il browser per introdursi nei sistemi altrui, mentre per l'aggravante di cui all'art. 615 ter comma secondo n. 3 c.p. sussiste la necessaria rappresentazione della capacità di danneggiamento del sistema correlata agli effetti del programma creato.

Né, come si è già detto con riferimento all'altra fattispecie criminosa, hanno efficacia esimente le arbitrarie opinioni espresse dall'indagato nel corso dell'interrogatorio, secondo cui gli effetti del programma non sarebbero intrusivi.

7. Estraneità del coimputato

Per quanto concerne il coimputato C. S. va accolta la richiesta del P.M. e della difesa di assoluzione per non aver commesso il fatto.

Infatti, dagli atti processuali non emergono indizi gravi di un'attività di concorso nei reati commessi dal fratello, il quale in sede di interrogatorio si è assunto l'esclusiva responsabilità di essi.

In sostanza, l'unico elemento riconducibile a questo imputato è quello, in sé poco concludente e, comunque, da solo inidoneo, dell'intestazione delle utenze telefoniche usate dal fratello per le connessioni.

L'esclusiva assunzione di responsabilità da parte del fratello G., come si è sopra detto, è invece riscontrata sia dalla riferibilità a lui delle operazioni di amministrazione dei due siti internet, sia dal

possesso – che non risulta avere il fratello - delle idonee capacità di programmazione: del resto i programmi sequestrati presso la comune residenza familiare furono trovati nei dischi rigidi presenti nella stanza nella disponibilità esclusiva di G..

È, dunque, attendibile l'affermazione di estraneità ai fatti contestati effettuata dal coimputato C. S. già in sede di perquisizione domiciliare (negativa quanto alla sua stanza) e reiterata in sede di interrogatorio.

8. Trattamento sanzionatorio

Passando all'esame del trattamento sanzionatorio, in applicazione dei criteri di cui all'art. 133 c.p., si reputa equa la condanna dell'imputato C. G. alla pena di mesi sei di reclusione così determinati:

- pena base per il reato di cui all'art. 615 ter c.p. - ritenuta la sua maggiore gravità a causa della pena edittale per esso prevista - di mesi tre, in ragione dell'intensità del dolo e delle modalità descritte dell'azione, valutate equivalenti le circostanze attenuanti ex art. 62 bis c.p., applicate a causa della incensuratezza dell'imputato e del comportamento collaborativo tenuto in occasione della perquisizione domiciliare, alle ritenute aggravanti;

- aumentata tale pena base di un mese per la continuazione interna al capo A) e di due mesi ex art. 81 cpv. c.p. a causa della plurima commissione del reato di cui all'art. 615 quinquies c.p., collegato con il vincolo della continuazione - stante la evidente medesimezza del disegno criminoso - alla fattispecie criminosa sopra indicata.

Sussistendo le condizioni di cui agli artt. 53 ss. l. 689/81 e ritenuta la maggiore idoneità della pena sostituiva al reinserimento sociale della imputato, stante la sua estraneità a circuiti delinquenziali, si ritiene di giustizia sostituire la pena detentiva di mesi sei di reclusione, con la pena pecuniaria corrispondente a € 6.840 di multa, avuto riguardo ai criteri di ragguaglio di cui agli artt. 135 cp e 57 l. 689/81 (38 euro per 180 giorni).

Si ravvisa, inoltre, l'opportunità, considerati i criteri di cui all'art. 133 c.p. e l'incensuratezza del C., di concedere il beneficio della non menzione della condanna previsto dall'art. 175 c.p., mentre quello della sospensione condizionale non è stato chiesto nelle subordinate dalla difesa e non corrisponde all'interesse dell'imputato, in ragione delle caratteristiche e dell'entità della pena irrogata.

Visto l'art. 544, 3° comma c.p.p., si indica in giorni 90 il termine per il deposito della motivazione della sentenza, trattandosi di questione nuova in giurisprudenza e che, quindi, richiede particolare cura nella esplicazione della ratio decidendi.

P.Q.M.

Visti gli artt. 533-535 c.p.p., dichiara C. G. colpevole del reato continuato ascrittogli e concesse le attenuanti generiche, valutate equivalenti rispetto all'aggravante contestata al più grave reato ex art. 615 ter c.p. in forma aggravata, lo condanna alla pena di mesi sei di reclusione, sostituita ai sensi dell'art. 53 l. 689/81 con la corrispondente pena pecuniaria di € 6.840,00 di multa.

Non menzione ai sensi dell'art. 175 c.p.

Visto l'art. 530 c.p.p., assolve C. S. dal reato continuato ascrittogli per non aver commesso il fatto.

Visto l'art. 544 terzo comma c.p.p. indica in 90 giorni il termine per il deposito della motivazione

Bologna, 21/7/2005.

Il Giudice
Dott. Pier Luigi di Bari

[1] Pag. 6 ss.

[2] Pag. 16 ss.

[3] Si veda altresì il riferimento che a p. 3 dell'analisi tecnica redatta dal M.llo F. viene fatto alla circostanza che le conclusioni a cui pervenne la G.d.F. sul meccanismo di funzionamento del programma, trovarono conferma nelle corrispondenti analisi effettuate dalla società F-Secure Corp.

[4] Vierika è il nome di una ragazza che l'imputato ha conosciuto nella città ucraina di Krivoj Rog ed alla quale ha dedicato il sito digilander.iol.it/vierika: cfr. verbale di interrogatorio e teste F., p. 91.

[5]In particolare con i seguenti comandi: HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\StartPage","http://web.tiscalinet.it/krivojrog/vierika/Vindex.html" HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\1201", 0 , "REG_DWORD"

[6] Come accertato anche dal servizio di sicurezza informatica di Tiscali s.p.a., che provvedette ad oscurare il sito il 5 marzo 2001: cfr. teste B., p. 68-69.

[7] Dalle deposizioni del Cap. R. e del M.llo F. si evince che le versioni circolanti in internet del programma Vierika erano in realtà due: poiché una versione utilizzava per la diffusione del secondo script uno spazio web presente sul server di Geocities, provider estero, la p.g. non ritenne opportuno estendere le indagini anche a tale programma. Come si ricava dall'all. 1 della nota di p.g. del 28/3/01, nel computer dell'imputato vennero rinvenute anche le istruzioni contenute nelle pagine html relative a questa versione (Vindex2.html).

[8] Sul quale, peraltro, non venne rinvenuto il secondo script del programma.

[9] Teste Resetti, p. 5.

[10] Nota di p.g. della G.d.F. di Milano del 19 marzo 2001, p. 2.

[11] Teste B., p. 55; verbale di esibizione e sequestro G.d.F. Cagliari del 14/3/01.

[12] Questa connessione ha la durata di circa h. 2,30. La connessione del 3 marzo risulta sia dai dati estrapolati dalla p.g. dai cd sequestrati presso il provider e contenenti i log di amministrazione e navigazione del sito (dei quali vengono riportate due stringhe nella nota di p.g. del 19/3/01 a p. 2), sia dalla successiva comunicazione fatta dalla B. alla G.d.F. di Milano in esecuzione del decreto di esibizione e sequestro della Procura di Milano.

[13] Il nickname completo di C. G. è Krivoj Rog, nome della cittadina ucraina dalla quale proviene sua moglie; tale termine si rinviene anche nel url di un sito che l'imputato, in sede di interrogatorio, ha dichiarato di amministrare (web.tiscali.it/krivoj).

[14] Testi Cap. R., p. 12; M.llo M., p. 75, 79, 86; F., p. 45, 77 ss.

[15] Teste F., p. 22.

[16] Sullo spazio web di tale provider la p.g. riteneva che avrebbe potuto essere inserita la seconda parte del codice del worm: tra i programmi successivamente sequestrati, rinvenuti nel pc dell'imputato, ve ne erano nove contenenti il comando diretto ad impostare come start page del browser il sito digilander.iol.it/vierika.

[17] Cfr. note Polizia Tributaria della Lombardia del 13 e del 19 marzo 2001; per la constatazione che la prima descrizione del funzionamento del programma era conforme con i risultati della successiva analisi tecnica cfr. teste F. p. 25.

[18] Si noti che le immagini utilizzate nella prima nota di p.g. del 13/03/01 sono state tratte da materiale della società di sicurezza informatica F-Secure Corp., come si desume dal copyright delle stesse immagini.

[19] L'e-mail contenente il worm venne ricevuta anche dalla G.d.F. di Milano: cfr. teste F., p. 6.

[20] Si fa riferimento all'all. 1 alla nota di p.g. del 28 marzo 2001.

[21] Teste Cap. R., p. 4-5; teste F., p. 89, teste B., p. 68, per quanto concerne la segnalazione che la società F-Secure Corp. fece a Tiscali s.p.a.. La stessa difesa dà atto nella nota difensiva dep. all'udienza del 23/6/04 (p. 12) che "la diffusione registrata del worm Vierika, secondo una fonte non smentita, ma anzi citata dal M.O. F. stesso, è arrivata a circa 1500 infezioni nell'arco di 24 ore" e che "sia F-Secure Corporation, sia Symbolic s.p.a. hanno dichiarato che è stato il loro intervento a consentire il blocco del worm..." (p. 16), che evidentemente doveva essersi diffuso.

[22] Teste B., p. 68; verbale di esibizione e sequestro G.d.F. Cagliari del 14/3/01.

[23] Teste F., p. 51-53.

[24] Teste F., p. 31.

[25] Nota di p.g. G.d.F. Milano del 15/5/01, p. 5.

[26] Teste F., p. 55.

[27] Suggestiva è, peraltro, l'impostazione dottrinale che, accostando la fattispecie in esame al reato di cui all'art. 637 c.p., piuttosto che alla violazione di domicilio, ravvisa il bene giuridico protetto nella integrità e nel diritto alla esclusiva fruizione dei sistemi informatici.

[28] Trib. Torino 4/12/97, cit., dove si fa riferimento alla sistemazione dell'impianto in un locale munito di serrature; accenna alle misure di protezione esterne al sistema anche Trib. Gorizia 19/02/03, Riv. pen. 2003, p. 891. Cfr. Relazione ministeriale alla legge n. 547 del 1993, che ha introdotto nel codice penale gli artt. 615 ter e ss., secondo cui "dovendosi tutelare il diritto di uno specifico soggetto, è necessario che quest'ultimo abbia dimostrato, con la predisposizione di mezzi di protezione sia logica che fisica (materiale o personale) di voler espressamente riservare l'acceso e

la permanenza nel sistema alle sole persone da lui autorizzate".

[29] Non è un caso che l'Autorità Garante della Privacy abbia statuito nel 2001 e nel 2003 che gli indirizzi e-mail, attenendo alla sfera di riservatezza individuale, non sono di pubblico dominio e che, senza il consenso del destinatario, non deve considerarsi lecita l'attività di spamming.