REPUBBLICA ITALIANA
IN NOME DEL POPOLO ITALIANO

LA CORTE D'APPELLO DI BOLOGNA
SEZIONE SECONDA PENALE

composta dai magistrati:
1 - Dr. Guarino Salvatore PRESIDENTE
2 - Dr. Ricchi Jolanda CONSIGLIERE
3 - Dr.Pasquariello Domenico CONSIGLIERE

Udita la relazione della causa fatta alla pubblica udienza odierna dal consigliere relatore Dr. Pasquariello Domenico
Inteso l'appellante
Inteso il Procuratore Generale, dr. Posini
ed i difensori, ha pronunciato la seguente

SENTENZA

nella causa penale
CONTRO
XXXX
nato a XXXX
con domicilio dichiarato: XXXXXXXX

agli artt. 110 c.p.. 615 ter e quinquies ep, 81 cpv, poiché in concorso tra loro, creando un "virus" (programma atto a danneggiare sistemi informatici) denominato "Vierika" trasmesso in via informatica al provider "Tiscali" e tramite questo a circa 900 utilizzatori del provider, si introducevano nei sistemi informatici di tali utenti e acquisivano dati anche riservati contenuti nei loro personal computers -tra i quali indirizzari e-mail- a loro insaputa, inoltre per mezzo del virus danneggiavano i programmi contenuti nei personal computers e ne pregiudicavano il corretto funzionamento.

In Bologna l'imputato: XXXX

avverso la sentenza emessa dal TRIBUNALE MONOC. di BOLOGNA in data 21/07/2005 che ha pronunciato il seguente dispositivo:

Visti artt. c.p.p., dichiara XXXX 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 euro 6.840,00 di multa. Non menzione ai sensi dell'art. 1 c.p. Visto l'art. 544 terzo comma c.p.p. indica in 90 giorni il termine per il deposito della motivazione.

MOTIVAZIONE

Sentenza impugnata.

Con sentenza n. 1823 del 21.7.0S il Tribunale di Bologna, in composizione monocratica, ha giudicato XXXXX e YYYYY per i delitti p. e p. dagli artt 615 ter e 61S quinquies c.p.

Secondo l'imputazione essi avevano creato un cosiddetto "virus", cioè un programma dall'unica funzione di introdursi e danneggiare sistemi informatici, da loro chiamato "Vierika", e l'avevano trasmesso in via informatica al provider "Tiscali"; attraverso questo il virus si era introdotto nei sistemi di circa 900 utenti, acquisendo dati riservati nei relativi personal computers, danneggiandone i programmi e pregiudicandone il corretto funzionamento; in Bologna "nel corso del 2001".

Nell'accertamento compiuto in sentenza "Vierika" è un "internet worm" programmato in Visual Basic Script, i cui effetti derivano dalla integrazione di due script differenti (gli script sono stringhe di comandi, ed il visual basic è un linguaggio di programmazione).

Il primo script (la prima parte del virus) era inviato come attachment ad una email, dall'oggetto "Vierika is here", cui era appunto allegato il file "infettante" Vierika.jpg.vbs; nella mail ricevuta dal destinatario appariva però solo il nome Vierika.jpg, dall'estensione (".jpg") ingannevole in quanto caratterizzante files di immagini.

Il destinatario della mail, accettando l'allegato, mascherato con il nome che suggeriva l'immagine di Vierika, installava invece a sua insaputa nel proprio computer il file Vierika.jpg.vbs.

Questo era in realtà un file di programma, che agiva sul registro di configurazione del sistema Windows (di massiccia diffusione, come è noto), riconfigurando al livello minimo di protezione il browser Internet Explorer ed inserendo come home page predefinita la pagina web con indirizzo http://vveb.tiscalinet.it/krivojrog/vierika/Vindex.httlll.

Il secondo script in Visual basic (la seconda parte del virus) era costituito dal suddetto documento Vindex.html; l'utente, avviando la navigazione in Internet, veniva inviato al suddetto indirizzo, automaticamente apriva il documento e "scaricava" quella che era invece una stringa di comandi.

Per effetto di questo secondo script nel disco rigido dell'utente veniva creata una specifica partizione, in cui veniva annidata la prima parte del codice virale; successivamente, sempre in maniera occulta, il programma installato produceva un comando di mass-mailing, inviando a tutti gli indirizzi del sistema di posta elettronica Outlook una e-mail contenente l'allegato virale Vierika.jpg.vbs, con diffusione esponenziale del virus ed effetto autoreplicante.

A questo accertamento si era arrivati in quanto l'email virale "Vierika is here", contenente l'allegato suddescritto Vierika.jpg.vbs, era arrivata anche ad un indirizzo in uso alla Guardia di Finanza di Milano.
Le indagini erano proseguite attraverso l'acquisizione di documenti riepilogativi di tracce informatiche conservate nel server del gestore Tiscali, che dimostravano che XXXX, di professione consulente informatico, con il nick name "Krivoj" con il quale egli si era registrato presso detto provider, era l'amministratore (cioè colui che aveva creato e gestito) del sito con indirizzo http://web.tiscalinet.it/krivojrog/vierika/Vindex.html contenente la seconda scritta del programma virale.
Nel corso di perquisizione e sequestro presso l'abitazione dei fratelli XXXX e YYYYY (il secondo era risultato essere l'intestatario dell'utenza telefonica usata per i collegamenti al web) il primo riconobbe di essere il creatore di "Vierika" (come del resto fece in seguito in sede di esame) e collaborò con la polizia giudiziaria, indicando egli stesso i files di programmazione di Vierika contenuti nel disco rigido del proprio personal computer, e masterizzandone copie, che erano sottoposte a sequestro.

Il suddetto meccanismo di funzionamento del virus Vierika, i cui files di programmazione sono stati

così acquisiti agli atti, è stato riportato in sede dibattimentale dal M.llo Forte, all'epoca dei fatti in servizio presso il Nucleo Crimini Informatici della GdF Milano.

Il giudice ha ritenuto esaustive le risultanze probatorie così sommariamente ora riassunte, senza ravvisare la necessità di accertamenti peritali, richiesti dalla difesa sin dalla fase predibattimentale, ed esplicati con memoria tecnica prodotta all'udienza del 23.6.04, giacché sostanzialmente la stessa difesa non aveva messo in discussione il funzionamento del programma come sopra descritto, ma ne aveva offerto in definitiva una lettura non penalmente rilevante.

Per altro profilo la sentenza di primo grado motivatamente si discostava da certo orientamento di legittimità che proprio in materia pare indicare necessaria la perizia, in ragione dell'accertamento di natura tecnica imprescindibile per la ricognizione delle fattispecie dei "computer's crimes". Pertanto il Tribunale di Bologna, accertata la materiale estraneità ai fatti di YYYYY, riteneva il coimputato XXXXX responsabile di entrambi i reati a lui ascritti, con l'aggravante -ritenuta di fatto esplicitata nell'imputazione- di cui all'art. 615 ter, c.2 nn. 2 e 3) (violenza sulle cose e danneggiamento del sistema o dei suoi dati, od alterazione parziale di funzionamento), che comporta la procedibilità d'ufficio.

Quanto al reato p. e p. dall'art. 615 ter c.p., il counter del sito http://web.tiscalinet.it/krivojrog/vierika/Vindex.html aveva registrato 829 visite, che corrispondevano ad altrettante pregresse installazioni della prima stringa di Vierika, altrettante abusive introduzioni in sistemi informativi dei personal computers di utenti, altrettante elusioni di sistemi di protezione ed altrettante "infezioni", con correlativa integrazione della fattispecie in contestazione.
Le aggravanti erano ravvisate integrate dalla alterazione dell'ordinario funzionamento del browser Explorer, integrante violenza sulle cose, e dagli effetti di allungamento dei tempi di connessione, con aggravio di spese telefoniche, per effetto dell'occulto mass mailing, nonché dal danno non patrimoniale della veicolazione di informazioni private (invio agli utenti in rubrica) e dell'apparire mittente di mail con allegati virali, integranti danneggiamento di sistema e di dati.

Quanto al reato p. e p. dall'art. 615 quinquies c.p. Vierika, inizialmente inviato dall'imputato -per sua espressa ammissione- ad alcuni indirizzi di posta elettronica reperiti sulla bacheca virtuale del sito www.sexualcyber.com alterava la funzionalità telematica del sistema infettato, per effetto della alterazione dei parametri di protezione del browser, all'oscuro dell'utente, e dell'invio automatico e massiccio di email, con ciò integrandosi anche detta fattispecie.

Per tali motivi il giudice irrogava la pena di mesi sei di reclusione, previa:

- concessione di attuanti generiche in valutazione di equivalenza con le aggravanti ad effetto speciale;
- pena base di mesi tre di reclusione per il reato art. 615 ter;
- aumento di pena ex art. 81 cpv c.p. di mesi uno per la continuazione interna e di mesi due per la plurima commissione del reato concorrente.

La pena veniva sostituita con la sanzione pecuniaria nella misura corrispondente ex art. 53 L. 689\81, con il beneficio della non menzione.

Motivi d'appello.

Il difensore di XXXXX ha proposto appello, eccependo, con il primo motivo, la nullità del decreto di citazione a giudizio per indeterminatezza della imputazione, in ragione della omessa indicazione delle identità delle 900 presunte parti offese, nonché della descrizione "cumulativa" della condotta, effettuata con riferimento a due diverse norme incriminatici, e con la conseguente incertezza circa la riferibilità del fatto ad una specifica norma di legge asserita violata.

Con secondo motivo è stata impugnata 1'ordinanza, resa all'udienza 27.11.03, di diniego di

pronuncia ex art. 129 c.p.p. sulla richiesta di declaratoria di improcedibilità per difetto di querela in relazione al reato di cui all'art. 615 ter c.p., contestato espressamente non aggravato.

Con il terzo motivo è stata dedotta l'inutilizzabilità di annotazioni di servizio della GdF, costituenti nella sostanza accertamenti tecnici ripetibili.

Con il quarto motivo sono stati denunciati il percorso motivazionale della sentenza impugnata, viziato da ricostruzione tecnico informatica priva di fondamento peritale, ed il correlativo ingiustificato diniego dell'espletamento di perizie, chieste dalla difesa, sulle modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore Tiscali ed Infostrada, nonché sull'originale del codice sorgente del software per cui è causa.

Con il quinto motivo, connesso ed in parte reiterativo del precedente, si è protestata la imprescindibilità per l'accertamento dei fatti e per la decisione dell'espletamento delle perizie suddette, che avrebbero permesso altresì di verificare le tesi difensive sull'effettivo funzionamento del software, e su quali fossero gli applicativi (ad esempio Outlook, e non il più diffuso Outlook Express) con i quali Vierika era in grado di interagire, nonché sulla integrità dei dati telematici raccolti nel corso delle indagini.

Con il sesto motivo si è argomentato che la condotta, pur nella denegata ricostruzione dei fatti operata in sentenza, non integra il reato di cui all'art. 615 ter c.p..

Secondo la prospettazione difensiva infatti non è ravvisabile il requisito essenziale del reato 615 ter, costituito dall'accesso al sistema dell'utenza, giacché realizzato dal programma, ma non da XXXXX, nel senso che questi rimaneva all'oscuro degli utenti, dei computers che scaricavano il programma e dei dati in essi contenuti.

Altro elemento caratterizzante la fattispecie incriminatrice, e non integrato, è costituito dall'assenza di elusione di misure di sicurezza informatiche, tali non potendo definirsi semplici opzioni di configurazione di un applicativo.

Con il settimo motivo si è dedotta l'assenza di prova circa la effettiva introduzione nei sistemi delle pretese 900 parti offese, nessuno dei quali era stato individuato ed esaminato.
Con l'ottavo motivo è stata dedotta l'insussistenza delle aggravanti; il programma Vierika, che è semplicemente autoreplicante, non provoca alcuno degli eventi richiesti per la sussistenza delle aggravanti, quali alterazioni, danneggiamenti o distruzioni di programmi informatici.

Esso si installa e si diffonde, senz'altro risultato che questo, ricercato per motivi di studio dall'appellante, programmatore di professione; la corretta terminologia informatica intende per modificazione (posto che la distruzione non è in questione) di un programma l'accesso ai codici sorgente del programma per l'alterazione del funzionamento.

Nessun pregiudizio, o variazione, di funzionamento era inoltre percepibile dall'utente.

Con il nono motivo, attinente la fattispecie di cui all'art. 615 quinquies c.p., sono state richiamate le precedenti argomentazioni, rilevanti anche per escludere la sussistenza del danneggiamento, o dell'alterazione di funzionamento, dei sistemi, dati o programmi, richiesti dalla norma incriminatrice.

Vierika insomma non era stato progettato per danneggiare, ed era stato scritto proprio nella consapevolezza della innocuità, il che anche si rifletteva sull'elemento soggettivo del reato.

Con il decimo motivo è stata dedotta la non correlazione tra fatto contestato e fatto ritenuto in sentenza, in violazione del disposto dell'art. 521 c.p.p., in quanto la prima condotta di ritenuta diffusione del preteso virus, attraverso la posta elettronica, era del tutto assente nella contestazione.

Per tali motivi l'appellante ha chiesto:

- in via principale l'assoluzione con la miglior formula;
- in gradato subordine:

- declaratoria di nullità del decreto di citazione a giudizio;
- nullità della sentenza impugnata per violazione dell'art. 521 c.p.p.;
- rinnovazione dell'istruttoria dibattimentale, con espletamento di perizie;
- declaratoria di improcedibilità per il reato di cui all'art. 615 ter c.p.p. per difetto di querela, e rideterminazione della pena, ferme la sua conversione e la non menzione.

DECISIONE DELLA CORTE

All'esito dell'odierna udienza, svoltasi in contumacia dell'imputato XXXXX, pronunciando sulle conclusioni delle parti che sono trascritte in epigrafe la Corte ha deliberato la presente sentenza di parziale riforma della sentenza impugnata.

Nullità del decreto di citazione a giudizio, dedotta violazione dell'art. 521 c.p.p.

L'eccezione di nullità del decreto di citazione a giudizio è fondata sui rilievi della mancata indicazione dell'identità delle parti offese e della descrizione "cumulativa" della condotta incriminata.
In proposito si deve ritenere che nella descrizione della condotta incriminata, come esplicitata nella imputazione, nessun equivoco sul fatto storico contestato o sulle norme di legge violate, né alcuna indeterminatezza nella imputazione, né alcuna vulnerazione della possibilità di comprendere l'accusa e di adeguatamente potersi difendere, è dato rinvenire.

Avuto riguardo alla specificità del reato in esame, in danno di un numero indiscriminato e potenzialmente esponenziale di soggetti (suscettibile di cosiddetto danno diffuso), l'indicazione delle generalità, anziché del solo numero complessivo delle parti lese, è del tutto irrilevante ai fini defensionali e di comprensione dell'oggetto del giudizio penale circoscritto dalla contestazione, elementi questi di esauriente rilievo per valutare la nullità dell'atto, secondo quanto disposto dall'art. 429, c.1 lett. c), e c.3, c.p.p.

Identiche considerazioni si impongono in relazione alla censura della descrizione cumulativa, e riferita a due norme incriminatici, della condotta, stante il parziale concorso formale (ovvero coincidenza in fatto degli elementi costitutivi essenziali previsti dalle fattispecie astratte). L'eccezione di nullità del decreto di citazione in giudizio va pertanto disattesa. Parimenti non è ravvisabile alcuna violazione della necessaria correlazione tra fatto contestato e fatto ritenuto in sentenza; nella prospettazione dell'appellante ciò sarebbe dovuto alla mancata esplicitazione, nella imputazione, dell'invio in rete della e-mail con l'allegato contenente la prima parte di Vierika.

Si ritiene di osservare, in proposito, che ciò invero attiene ad elementi di dettaglio della condotta non riferibili ad elementi costitutivi essenziali delle fattispecie incriminatici (condotta di abusivo accesso a sistema informatico, elusione di misure di protezione, diffusione di programma avente determinati scopi od effetti vietati), in ordine ai quali debba esser condotto il giudizio di corrispondenza imposto dall'art. 512 c.p.p.

Sull'accertamento istruttorio.

Nel corso del dibattimento di primo grado (udienza 23.9.04) con l'accordo delle parti, sono state acquisite ex art. 493, c.3, c.p.p., e dichiarate utilizzabili per la decisione le annotazioni di polizia giudiziaria (Guardia di Finanza) del 13.3.01, 19.3.01, 28.3.01, 15.5.01.
Già il rilievo dell'acquisizione con dichiarazione di utilizzabilità, avvenuta con l'espresso consenso della difesa, è esaustivo della infondatezza dei motivi di impugnazione in proposito, relativi alla natura di accertamento tecnico non ripetibile delle annotazioni.

Va aggiunto che, comunque, l'attività di accertamento compiuta è stata ripercorsa, con analogo risultato di acquisizione di fonti di conoscenza del fatto, nel corso delle deposizioni testimoniali degli ufficiali di polizia giudiziaria D. Rasetti, G. De Filippo, G. Mazzaraco (udienza 27.11.03), D. Forte e di C. Broi, responsabile di Tiscali SpA per i rapporti con l'autorità giudiziaria (udienza 27.5.04).
Anche dalle suddette deposizioni risulta univocamente ricostruibile, nel termini descritti nella sentenza impugnata e sopra riportati, il funzionamento del programma informatico "Vierika"; è d'obbligo rilevare che si è trattato di testimoni (ufficiali di polizia giudiziaria appartenenti al Nucleo Crimini Informatici, forniti di specifica preparazione e formazione in materia informatica) che, in forza della ricordata particolare preparazione tecnica, hanno risposto su fatti e circostanze concernenti la loro attività professionale d'indagine.

In tema di prova testimoniale, va aggiunto, il divieto di esprimere apprezzamenti personali non vlge qualora il testimone sia persona particolarmente qualificata, in conseguenza della preparazione professionale, quando i fatti in ordine ai quali viene esaminato siano inerenti alla sua attività, in quanto, in tal caso, l'apprezzamento diventa inscindibile dal fatto, dal momento che quest'ultimo è stato necessariamente percepito attraverso il "filtro" delle conoscenze tecniche e professionali del teste (vedi Casso n. 12942 de116/01/2007).

Pertanto sia le annotazioni di polizia giudiziaria, anche nelle parti relative ad accertamenti ripetibili, per effetto del ricordato consenso dibattimentale, e sia le deposizioni sono pienamente utilizzabili quali fonti di conoscenza per la decisione.

Altra questione è, all'evidenza, costituita dalla esaustività ed attendibilità di dette fonti di conoscenza, questione connessa alla dedotta necessità di accertamento peritale, negato dal giudice di prime cure.

Anche in proposito i motivi d'appello non paiono fondati.

La prima questione è relativa alla "correttezza" della acquisizione delle cosiddette "tracce informatiche" o delle prove documentali di natura informatica.

In proposito è necessario previamente precisare, richiamando espressamente quanto esattamente osservato nella sentenza impugnata, che non è compito del giudicante determinare una sorta di protocollo delle procedure informatiche forensi, ma solo verificare se nella fattispecie l'acquisizione probatoria sia fidefaciente, o se abbia subito alterazioni.

E nella specie, quanto alla tracce informatiche, i dati consegnati alla polizia giudiziaria dal provider Tiscali, relativi agli interventi di manutenzione ed amministrazione del sito con indirizzo http://web.tiscalinetit/krivojrog/vierika/Vindex.html ed alla individuazione dell'utente con username "Krivoj" sono stati confermati dalle dichiarazioni dello stesso XXXXX.

Questi ha espressamente e correttamente riconosciuto (vedi verbale esame delegato del 7.9.01) di aver realizzato "Vierika", di averlo diffuso, di aver creato il sito web con il nome "Krivoj". Non si vede come possa esser messa in dubbio la fidefacienza di una risultanza documentale (tale è la traccia telematica, seppur necessitante di appositi strumenti per la fruibilità), coincidente con le ammissioni dello stesso imputato.

Identica considerazione va svolta in relazione alla prova costituita dal sequestro informatico eseguito presso l'abitazione di XXXXX; come ricordato nella circostanza fu questi stesso -così evitando il sequestro dell'hardware- ad indicare alla polizia giudiziaria i files dì programma rilevanti per l'accertamento, masterizzandone la copia ora in atti.

I rilievi mossi alla metodologia del sequestro informatico peraltro mai sono stati attinenti all'effettivo funzionamento e scopo del programma "Vierika", come accertato nella sentenza impugnata e sopra ripercorso, in realtà mai messi in discussione, neppure nelle memorie "tecniche" depositate dalla difesa; in esse, e del pari nei motivi di appello, mai è allegato o prospettato un funzionamento del programma diverso da quello sopra descritto. Le stesse richieste di perizia

attengono ad aspetti non rilevanti per l'accertamento del funzionamento di Vierika, quali le modalità di generazione e conservazione dei log (registri di collegamento), acquisiti presso il gestore Tiscali ed Infostrada (rilevanti per individuare le generalità di "Krivoj", fatto non in discussione, od il numero di accessi al sito infettante), ovvero concernono l'originale del codice sorgente del programma e pertanto (atteso che esso era nel 2001 nella memoria del computer dell'imputato) non più espletabili, oltre che non necessarie.

Nel difetto di effettive necessità istruttorie -secondo il parametro dell'assoluta necessità richiesto dall' art. 507 c.p.p.- volte a colmare lacune o contraddizioni nell'accertamento dei fatti, va confermata l'ordinanza del Tribunale di rigetto della richiesta di integrazione probatoria; per i medesimi motivi, riportati anche al disposto dell'art. 603 c.p.p., va disattesa la richiesta di assunzione della prova nel giudizio di appello.

Reato di cui all'art. 615 ter c.p.

La norma, come è noto, è posta a tutela del cosiddetto "domicilio informatico", inteso sia come spazio fisico in cui sono contenuti dati informatici personali, sia quale spazio ideale di pertinenza della sfera individuale e privata.

L'accertamento istruttorio condotto nel giudizio di primo grado offre piena contezza di come XXXXX, creando il programma "Vierika" e poi diffondendolo occultamente per mezzo di mass mailing e del sito web ….....Vindex.html, secondo il meccanismo sopra descritto, abbia integrato il reato in contestazione.

In proposito vanno richiamate le puntuali osservazioni svolte nella sentenza impugnata, relative alla sussistenza degli elementi costitutivi e tipizzanti del delitto di accesso abusivo a sistema infonnatico.
In primo luogo si pongono indubbie la materialità dell'accesso attraverso il worm "Vierika" e la diffusione indiscriminata del medesimo.

Esse sono state provate dalle deposizioni citate Broi, Rasetti e Forte, in merito alle segnalazioni sulla diffusione del virus effettuate da alcune società di informatica (F-Secure Corporation, Symbolic SpA), alle lamentele pervenute al provider Tiscali poiché il programma era annidato sugli spazi web da esso gestiti, nonché dal counter del sito http://web.tiscalinet.it/krivojrog/vierika/Vindex.html dal quale risultavano 829 accessi (vedi annotazione GdF 13.3.01); agli accessi corrispondono necessariamente altrettante ricezioni della mnail "Vierika is here", altrettante installazioni automatiche, immediate ed occulte degli script contenuti nell'attachment alla mail, altrettante occulte riconfigurazioni di registro di Windows, altrettante involontarie ed indesiderate "navigazioni" al sito suddetto, scaricando il secondo script di programma.

Tale meccanismo ha indubbiamente il carattere dell'abusività richiesto dalla norma incriminatrice, ravvisabile prima nella fraudolenta induzione in errore dell'utente che riceveva la mail "Vierika is here", ingannato dall'estensione ".jpg" dell'attachment, che indicava un file immagine, il quale conteneva invece la prima stringa di comandi, e poi nel sistema occulto di scarico del secondo script, realizzato attraverso la riconfigurazione occulta della protezione, e la reimpostazione della home page del browser, il tutto sempre all' insaputa dell'utente.

Sempre all'insaputa dell'utente, e contro la sua volontà, il programma "clandestino" insediato nel sistema informatico provvedeva ad inviare a tutti gli indirizzi della rubrica della posta elettronica (se gestita con l'applicativo "Outlook", peraltro di larga diffusione) l'email con l'allegato vitale Vierika.jps.vbs, con il cosiddetto effetto autoreplicante.

Prova ne sia che, in brevissimo tempo, dall'invio da parte di XXXXX della mail virale a pochi indirizzi trovati sulla bacheca virtuale del sito sexualcyber.com (come da quegli riconosciuto), il sito "trappola" ….Vindex.html era stato involontariamente aperto da oltre 800 utenti "infettati" del

provider Tiscal (si aggiunga che la mail virale, presumibilmente, era stata ricevuta da un numero molto maggiore di indirizzi e sistemi informatici).

L'appellante deduce che, anche nella denegata ipotesi d'accusa, nel descritto funzionamento, autoreplicante ma non "virale", non sarebbe ravvisabile requisito essenziale del reato 615 ter, costituito dall'accesso al sistema dell'utenza, giacché comunque XXXXX, stante l'effetto autoreplicante automatico, rimaneva ignaro degli indizi informatici raggiunti e dei dati contenuti nelle memorie dei computers che scaricavano il programma.

L'argomento è di particolare rilievo.

La Corte non ritiene che la norma incriminatrice, posta come premesso a tutela del domicilio informatico, possa essere interpretata con tale effetto riduttivo di tutela; la lettera dell'art. 615 ter infatti richiede unicamente l'abusività dell'accesso al sistema, ovvero la permanenza contro lo jus prohibendi del titolare, ma non pretende l'effettiva conoscenza, da parte dell'agente, dei dati protetti.
Avuto riguardo alle specificità dei sistemi informatici e delle trasmissioni telematiche, che consentono la manipolazione e l'uso di un enorme numero di dati senza la diretta interlocuzione con ognuno di essi da parte dell'agente, introdurre in via interpretativa l'ulteriore requisito della conoscenza effettiva dei dati manipolati, a corredo esplicativo della nozione di "accesso abusivo", equivarrebbe ad una sostanziale vanificazione della ratio incriminante.

Nella fattispecie le modalità dell'azione (ovvero la creazione del programma autoreplicante ed il suo "lancio" nel web) erano univocamente dirette ad inviare ed installare occultamente e fraudolentemente il programma, di cui XXXXX ha ammesso la paternità, ad una comunità indiscriminata ed inconsapevole di utenti, usandone i dati personali della rubrica di posta. Ciò appare sufficiente per integrare la nozione di "accesso abusivo" penalmente rilevante, giacché è nel prelievo indesiderato dei dati personali dal domicilio informatico che va individuato il vero bene personalissimo protetto dalla norma, e non tanto nella conoscenza o conoscibilità di quelli da parte del soggetto agente.

In altri termini alla specificità dei sistemi informatici, che consentono l'uso di dati senza la "conoscenza" di essi, come tradizionalmente intesa, da parte dell'operatore, va correlata l'interpretazione della nozione di accesso posta dalla norma incriminante.
Nella prospettazione difensiva dell'appellante altro elemento caratterizzante la fattispecie incriminatrice, e non integrato, è costituito dall'assenza di elusione di misure di sicurezza informatiche, tali non potendo definirsi semplici opzioni di configurazione di un applicativo. In proposito si presentano totalmente condivisibili, ad avviso della Corte, le valutazioni svolte dal giudice di prime cure (pag. 18 della sentenza impugnata), da richiamarsi integralmente.
Come detto il programma Vierika, per potersi installare, modificava occultamente (con il primo script di comandi) le impostazioni di protezione di Internet Explorer; ciò non è posto in discussione dalla difesa, che le qualifica piuttosto come opzioni di configurazione del sistema.
Nella sostanza le "impostazioni di protezione" regolano l'esecuzione automatica di download e contenuti attivi durante la navigazione Internet, permettendo di configurare diversi livelli di protezione, con richiesta o meno di conferma da parte dell'utente e con eventuali barriere automatiche per determinati programmi o contenuti attivi.

Esse quindi non possono che rientrare nella nozione di "misure di sicurezza" a protezione del sistema; misure elementari, facilmente aggirabili, già predisposte nell'applicativo, ma comunque qualificabili misure di protezione, giacché esse attinenti esclusivamente non alla configurazione di Explorer (modalità di fruizione) ma alla maggiore o minore interazione passiva del sistema informatico, connesso al web, dall'esterno verso il suo interno.

Va pertanto confermato il giudizio di sussistenza del reato in esame, condotto nella sentenza impugnata.

La Corte ritiene peraltro fondati i motivi gradati di appello, relativi alla insussistenza delle

aggravanti ritenute -in motivazione, giacché l'imputazione è priva di espressa contestazione ed il dispositivo fa riferimento ad una sola aggravante- dal giudice monocratico del Tribunale. Queste, pur non richiamate attraverso specifica indicazione delle norme di legge violate, sono state valutate contestate in fatto nel riferimento espresso, contenuto nella descrizione della condotta incriminata, "danneggiamento di programmi" ed al "pregiudizio per il corretto funzionamento" degli stessi (integranti le previsioni poste ai nn. 2 e 3 del comma 2 dell'art. 615 ter c.p.).

Invero non è ravvisabile, nelle modalità di installazione e di funzionamento del worm Vierika, in primo luogo alcun "danneggiamento" dei programmi del sistema dell'utente, né alcuna "modificazione" in senso informatico.

Quelli, infatti, anche dopo l'installazione occulta di Vierika, rimanevano perfettamente operativi, come in precedenza, con le stesse caratteristiche di fruizione e di scopi, senza alcuna modificazione di dati, ambiente, interazione, programma; in effetti Vierika si limitava ad usare occultamente i suddetti programmi (in particolare gli applicativi di navigazione web Explorer e di posta elettronica Outlook) ed i dati della rubrica di posta elettronica, senza alcuna modificazione (ovvero diversa quali non era stato progettato; data la duttilità e versatilità funzionale dei programmi applicativi più diffusi, deve invece ritenersi che "alterare" un programma significhi anche manipolarlo in modo che compia azioni non volute dall'utente, ovvero modificarne i parametri di funzionamento, anche secondo opzioni e possibilità previste nel programma stesso, contro la volontà dell'utilizzatore.

Ciò è quanto ha realizzato, diffusamente, il programma Vierika.

Non altrimenti che alterazione è definibile l'azione occulta ed indesiderata di modificazione del registro di di Windows, attraverso i comandi di programma Vierika "HKEY_CURRENT_USER" etc, che modificavano l'home page predefinita del browser, ed abbassando al livello minimo le protezioni; non altrimenti che alterazione di funzionamento sono definibili il comando e l'azione occulte di mass mailing.

Per conseguenza ne deriva compiutamente integrata la fattispecie delineata e punita dall'art. 615 quinquies c.p., e per tale parte va confermata la sentenza di condanna di primo grado.

Per effetto della parziale riforma del giudizio di condanna va rideterminata la pena da infliggersi all'appellante.

Tenuti fermi il riconoscimento delle attenuanti generiche, la sostituzione della pena detentiva ex art. 53 L. 689\81 e la concessione del beneficio della non menzione della condanna, si reputa equo ed adeguato determinare la pena in mesi due di reclusione ed euro 2000 di multa (pena base di mesi tre ed euro 3.000), con pena detentiva sostituita con la pena pecuniaria corrispondente di Euro 2.280 di multa.

Titolo di reato e data di commissione consentono di condonare la pena ex L. 241\06. Nel resto va confermata la sentenza appellata.

PQM

Visto l'art. 605 c.p.p., in parziale riforma della sentenza del Tribunale Monocratico di Bologna in data 21.7.05, dichiara l'appellante XXXXX responsabile del reato di cui all'art. 615 quinquies c.p. e con le già concesse attenuanti generiche determina la pena in mesi due di reclusione ed euro 2.000 di multa, sostituendo la pena detentiva con la corrispondente pena pecuniaria di euro 2.280 di multa, e così complessivamente euro 4.280 di multa, che dichiara interamente condonata ex L. 241\06.

Dichiara non doversi procedere nei confronti dell' appellante XXXXX in ordine al reato di cui all' art. 615 ter c.p., perché, esclusa l'aggravante, lo stesso è improcedibile per difetto di querela.

Conferma nel resto.

Indica in giorni 60 il termine per il deposito della sentenza.

Bologna, 30.01.08

Il Consigliere est.
Dott. Domenico Pasquariello

Il Presidente
Dott. Salvatore Guarino

Depositata in cancelleria il **27.03.2008**