

Il delitto di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art.615quinquies c.p.)

di Telesio Perfetti

Del delitto di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art.615quinquies c.p.)¹

1. Premessa

L'art.615 quinquies c.p. è stato introdotto dall'art.4 della legge 23 Dicembre 1993 n.547², recante *“Modificazioni ed integrazioni delle norme del codice penale e del codice di procedura penale in tema di criminalità informatica”* e trova la sua ratio nell'esigenza di apprestare ai sistemi informatici una tutela penalistica contro il fenomeno (oggi sempre più in aumento) della diffusione in Internet dei cd. *“virus”* o in genere dei cd. *“malware”*³, nella formulazione legislativa indicati quali programmi aventi *“per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento”*.

Non è questa la sede per analizzare la vasta tipologia di programmi maligni attualmente conosciuti. Un accenno è tuttavia indispensabile. Anzitutto i malware, tout court considerati, sono particolari programmi (talora anche semplici da *“scrivere”*) che hanno come scopo precipuo quello di danneggiare un computer (nelle sue parti hardware, ma più spesso in quelle software) ovvero di interromperne, alterarne o rallentarne il funzionamento, ovvero di cancellarne una parte della memoria o ancora di cagionare la perdita (irreversibile o solo temporanea, totale o anche parziale) di dati, informazioni e programmi conservati all'interno di un qualsivoglia sistema informatico. Più specificamente il *“virus”*⁴ è un software che, una volta mandato in esecuzione, è in grado di infettare un P.C. e di autoriprodursi, facendo copie di se stesso, replicandosi senza che l'utilizzatore del sistema contaminato riesca, il più delle volte, a rilevarne l'indesiderata presenza. In genere il virus veniva diffuso tradizionalmente con la consegna di un dischetto (C.D.R., floppy etc.) che lo conteneva al suo interno. Oggi le tecniche di trasmissione si sono però raffinate e nel contempo sono divenute più subdole e di conseguenza meno prevedibili e prevenibili. Tipico è il caso del cd. *“worm”* (letteralm. *“verme”*), malware che non ha bisogno di infettare altri file per diffondersi, perché modifica il sistema operativo della macchina ospite in modo da essere eseguito automaticamente. Esso tenta di replicarsi sfruttando per lo più Internet, cioè la rete, tant'è che viene in genere trasportato attraverso messaggi di posta elettronica, venendo allocato nei cd. *“attachment”* o allegati. L'utente, che o per curiosità (talora attratto dall'oggetto indicato nel messaggio dell'e-mail) o per superficialità clicca su tali allegati, va ad attivare il malware, causando in tal modo danni spesso irreparabili al proprio computer⁵. Un worm si rivela così come un programma particolarmente subdolo e aggressivo, non foss'altro per il fatto che sfrutta i *“bug”* o vulnerabilità dei software di comunicazione, sì da essere eseguito in automatico all'apertura del file residente in allegato, come si è precedentemente detto. Inoltre, una volta eseguito, un worm è in grado non solo di autoreplicarsi come un qualunque virus, ma anche di autospedirsi a tutti gli

¹ *“Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a €10.329”*.

² Tale provvedimento legislativo fu voluto per contrastare quelle che fino ad allora risultarono essere ignote (ma, non per tal motivo, meno insidiose) aggressioni ai diritti e ad altri interessi essenziali della persona umana (riservatezza, libertà morale, diritto di esprimere liberamente il proprio pensiero, onore, autodeterminazione negoziale, patrimonio), nonché ad altri beni giuridicamente rilevanti e meritevoli di protezione penalistica (come la corretta amministrazione della giustizia, l'ordine pubblico ed il regolare funzionamento dei servizi pubblici, la fede pubblica), arretrate tramite l'uso della tecnologia informatica e telematica.

³ Contrazione per *“malicious software”*, letteralm. *“programma malvagio”*.

⁴ Per una precisa e attenta ricognizione delle varie forme di virus più frequentemente ricorrenti, cfr. F.Berghella, *“Guida pratica alle nuove misure di sicurezza per la privacy”*, Maggioli Editore, 2003, p.122 e s.

⁵ Tra i più famosi (nonché pericolosi) worm si annoverano *“Nimda”* (che, entrato in azione una settimana dopo i tragici eventi dell'11 settembre 2001, infettò 8.300.000 computer e provocò danni stimati in circa 650 milioni di dollari), *“Slammer”* (nel 2001), *“Code Red”* (sempre nel 2001) e *“Sasser”* (nel 2003).

indirizzi di posta elettronica trovati nella memoria del P.C. infettato⁶, che così diviene una sorta di strumento involontario per la realizzazione di attività illecite, una sorta di inconsapevole “autore mediato” di reato.

Oltre a virus e worm, tra i programmi maligni è opportuno menzionare gli “spyware”, i “trojan-horse”, le “logic bomb” e i “web-dialer”.

- lo “spyware” è un tipo di programma che raccoglie informazioni riguardanti l'attività on-line di un utente (per es. siti visitati, acquisti eseguiti in rete...). La maliziosità di tale software sta nel fatto che tali informazioni vengono carpite senza che l'utente stesso ne sia informato preventivamente e dunque senza il di lui consenso. Lo spyware poi, una volta acquisiti i dati e le notizie utili, provvederà a inoltrarli ad un data-base gestito quasi sempre da organizzazioni commerciali (in certi casi trattasi di vere e proprie multinazionali ovvero di aziende specializzate in e-commerce), che sfrutteranno quei dati e quelle notizie per trarne profitto. Dunque uno spyware viene realizzato non con il fine di danneggiare un sistema (anzi l'attività di reperimento di informazioni ne presuppone l'integrità), bensì per violare la privacy del cybernauta, in quanto permette alla struttura che gestisce e controlla tali programmi di “profilare” l'utente della rete, id est di conoscerne le abitudini, i gusti e gli interessi di ogni tipo (musicali, artistici, culturali, sessuali etc.). Tali operazioni il più delle volte sono finalizzate all'invio di pubblicità mirata (peraltro non sollecitata o non richiesta e dunque indesiderata, cd. “spamming”). Tuttavia lo spyware può provocare danni collaterali non da poco: può modificare la pagina iniziale del “browser”⁷ ovvero la lista dei “preferiti”. Nei casi più gravi riesce addirittura a rallentare la connessione in Internet ovvero a cagionare tentativi di connessione non richiesti dall'utente ovvero ancora ad alterare il funzionamento del sistema, dal momento che occupa spazi della memoria R.A.M. o della C.P.U. fino a provocarne l'instabilità o il blocco (cd. “crash”), comportandosi così come un vero e proprio virus o worm (anche se diverso nella composizione e nella finalità, che, come detto, non è propriamente quella di danneggiare il sistema sul quale è installato). Trattasi certamente di uno dei codici maligni peggiori, per i tanti motivi suddetti e per il fatto che, come se non bastasse, si installa molto facilmente nel P.C. Quest'ultimo può essere infettato o tramite lo scarico (“download”) di programmi “freeware” (id est gratuiti) oppure semplicemente visitando delle pagine Web disegnate per sfruttare eventuali vulnerabilità del browser, in tal modo consentendo l'esecuzione automatica di applicazioni non sicure. A fronte degli spyware più offensivi ed invasivi, ne esistono altri che vengono eseguiti solo quando si utilizza l'applicazione di cui fanno parte e per mezzo della quale sono stati installati; in siffatti casi la loro esecuzione cessa nel momento in cui l'applicazione stessa viene chiusa. Si ricordi inoltre che un antivirus (programma atto a contrastare l'azione di virus e worm e/o a neutralizzarli), per quanto efficace, non serve contro uno spyware, semplicemente perché quest'ultimo non è un virus. Tuttavia esistono strumenti di difesa appositamente concepiti per rilevare la presenza di spyware nel sistema e per cancellarli.
- “trojan horse”, letteralm. “cavallo di Troia”. E non a caso. In effetti a prima vista potrebbe apparire come un software normale in grado di effettuare una o più operazioni, se non fosse per il fatto che esse sono occulte o meglio diverse da quelle dichiarate. Ergo ci si trova innanzi ad un tipo di malware, le cui funzionalità sono celate all'interno di un programma apparentemente utile o comunque innocuo; è

⁶ In genere un worm per autoinviarsi sfrutta le vulnerabilità dei cd. *client* di posta (per es. Outlook), programmini che servono per la gestione, selezione, archiviazione della posta elettronica in entrata e per agevolare il reperimento degli account quando si tratta di spedire mail.

⁷ Programma che consente la navigazione in Internet. Tra i più comuni si possono ricordare “Internet Explorer” e “Mozilla”.

dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente installa ed esegue anche il codice nascosto. A differenza di virus e worm, il trojan non è capace di porre in essere le procedure necessarie per replicare se stesso. Talora il trojan viene usato dai cracker⁸, i quali lo inseriscono per es. in videogiochi piratati, ma può essere scaricato anche direttamente (e ingenuamente) dall'utente inesperto, in genere durante la visita di siti pornografici o illegali (siti di virus-writer, di hacker, di cracker o in cui si pratica la compravendita o il download gratuito di programmi e giochi di provenienza illecita) ovvero cliccando su file allegati alle mail che pervengono al proprio account (né più né meno come accade per un worm). Un trojan può contenere una qualsivoglia informazione maliziosa e viene spesso utilizzato per installare "keylogger"⁹ o "spyware" all'interno del sistema bersaglio, consentendo all'attacker, che l'ha lanciato, anche il controllo da remoto¹⁰.

- "web-dialer", dall'inglese "to dial", comporre. E' in sostanza un programma di pochi kilobyte (quindi molto semplice e di facile installazione), che crea una connessione ad un'altra rete di calcolatori o semplicemente ad un altro computer tramite la comune linea telefonica o tramite un collegamento I.S.D.N.¹¹ In genere tali programmi sono associati a servizi a valore aggiunto, rectius a tariffazione elevata o speciale. Se esistono dialer legittimi (in quanto richiesti e voluti dall'utente), ne esistono tuttavia di illegali, poiché "manipolano" il sistema, lo alterano, intervengono su di esso in modo illecito, senza consenso dell'utente, a sua insaputa, istradandolo a numeri telefonici ad alto costo. Molti siti Web promettono di fornire gratuitamente loghi e suonerie per telefoni cellulari ovvero canzoni e altri file in formato "mp3", ma anche ricette culinarie, software, film e immagini pornografiche, a patto che il cybernavigatore installi un certo programma, anch'esso offerto gratuitamente. Ma tale programma è in realtà un dialer, che dunque, una volta installato nel sistema, può provocare danni patrimoniali notevoli (per es. bollette telefoniche di svariate migliaia di Euro)¹². Talora i dialer sono contenuti in software Trojan.

⁸ Parola derivata dal verbo anglosassone "to crack", rompere. E' colui che più propriamente può essere considerato il pirata informatico, dacché "spezza", "rompe", "scassina" le misure di sicurezza di un sistema informatico per penetrarvi. In genere agisce per scopi di profitto, talora anche per scopi vandalici e distruttivi. A volte il suo obiettivo è anche quello di sprotteggere ("crackare" come si dice in gergo) un software coperto da copyright e destinato al commercio, al fine di utilizzarlo senza averne il diritto (né per averlo acquistato, né per averne la licenza o altro titolo per l'uso). A differenza dell'hacker propriamente detto, il cracker manifesta nel suo modus operandi l'intento di conseguire un lucro o comunque un profitto.

⁹ Dall'inglese "to log", registrare, annotare o, come altrimenti si dice, "tracciare". Trattasi di un programma malizioso che controlla e salva la sequenza di tasti che viene digitata da un utente, per poi inviarla ad un computer remoto controllato in genere da un hacker. Tali programmi vengono spesso trasportati da trojan o da worm ed hanno in genere lo scopo di intercettare password, codici P.I.N. ad altri codici d'accesso, ivi inclusi i numeri di carte di credito.

¹⁰ In tal senso un trojan può essere utilizzato come mezzo per introdursi in modo occulto nonché illecito nell'altrui sistema, aggirandone le misure di sicurezza predisposte e mantenendovisi invito domino. Ergo si potrebbe in tali casi configurare il delitto di cui all'art.615 ter c.p. (id est "Accesso abusivo ad un sistema informatico o telematico").

¹¹ Acronimo per "Integrated Services Digital Network" e consiste in un servizio di telefonia digitale disponibile su abbonamento nelle aree coperte dal servizio stesso. Nello specifico l'I.S.D.N. è un particolare protocollo (id est insieme di regole che rende possibile una comunicazione on-line), che consente di descrivere l'effettuazione delle chiamate e la relativa terminazione, offrendo peraltro tutta una serie di servizi aggiuntivi all'utente che ne usufruisce (per es. la segnalazione del numero telefonico di chi chiama).

¹² Il dialer, più che per realizzare il delitto di cui all'art.615 quinquies c.p., serve per porre in essere la condotta prevista ex art.640 ter c.p., rubricato come "frode informatica" e introdotto dall'art.10 della l. 547/1993. Quest'ultimo reato è stato modellato sulla falsariga del delitto di "truffa" (art.640 c.p.). Tuttavia tra le due fattispecie criminose v'è una differenza fondamentale concernente il profilo dell'induzione in errore tramite artifici o raggiri, presente nella truffa e non menzionato nel delitto di cui all'art. 640 ter c.p. Orbene nella frode informatica sembrerebbe mancare il cd. "evento intermedio", vale a dire l'atto dispositivo patrimoniale, al quale il soggetto passivo del reato è stato indotto con l'inganno e cioè a causa di un'erronea o falsa rappresentazione della realtà provocata dai raggiri (consistenti nell'arte della dialettica, id est in una serie di ragionamenti intesi a sviare l'attenzione della vittima o ad accattivarsene la fiducia) o dagli artifici (comportamenti tali da far apparire come reale un qualcosa che tale non è ovvero tali da celare la verità e

- “*logic bomb*”, letteralm. “bomba logica”, programma che rimane inerte fino al momento in cui viene innescato da un determinato evento, come per es. una certa data o ricorrenza.

2. Analisi del reato

a) **Soggetto attivo** del reato è “chiunque”, ergo trattasi reato comune.

b) **Presupposto oggettivo**: la nozione di “**sistema**”.

Quanto alla nozione di “sistema”, ci si può rifare alla definizione offerta dalla dottrina dominante e ripresa dalla giurisprudenza a proposito del delitto di cui all’art.615 ter c.p. Ergo per “sistema informatico” devesi intendere <<*una pluralità di apparecchiature destinate a compiere una qualsiasi funzione utile all’uomo, attraverso l’utilizzazione (anche in parte) di tecnologie informatiche. Queste ultime, come si è rilevato in dottrina, sono caratterizzate dalla registrazione (o “memorizzazione”), per mezzo di impulsi elettronici, su supporti adeguati, di dati, cioè di rappresentazioni elementari di un fatto, effettuata attraverso simboli (bit) numerici (“codice”), in combinazioni diverse: tali “dati”, elaborati automaticamente dalla macchina, generano le informazioni costituite “da un insieme più o meno vasto di dati organizzati secondo una logica che consenta loro di attribuire un particolare significato per l’utente” >>¹³. Va aggiunto che mentre ai fini della configurabilità del delitto di cui all’art.615 ter c.p. è necessario che il sistema sia protetto da misure di sicurezza (ergo la forzatura o aggiramento delle stesse è elemento costitutivo del reato), ciò non è invece richiesto per il delitto di cui all’art.615 quinquies c.p., che dunque tutela ogni forma di sistema informatico, protetto o meno.*

c) **Condotte punibili**.

Varie sono le condotte punibili, consistenti nel:

- consegnare, id est dare materialmente un supporto (per es. un C.D.R., un floppy-disk...) contenente un malware;

da nascondere fatti, notizie ed altri dati determinanti per poter prestare un valido e consapevole consenso in un determinato accordo contrattuale etc.). Nella truffa è dunque necessaria l’artificiosa partecipazione della vittima (che dunque reca danno a se stessa), cosa questa non presente nella frode informatica. Tuttavia l’evento intermedio può essere recuperato sol se si pensi alla formulazione della norma: “*chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a se o ad altri un ingiusto profitto con altrui danno, è punito...*”. Pertanto può dirsi che ad essere indotto in errore è non solo, anzi non tanto, l’essere umano, bensì il computer, che viene per l’appunto manipolato o alterato o illecitamente sfruttato per raggiungere l’obbiettivo che il malintenzionato (sia questi un hacker, un cracker o anche solo un disonesto ed avido webmaster o un titolare di un sito web) si era prefissato, vale a dire lo scopo di profitto (proprio o di terzi) con contemporaneo danno dell’utente (profitto e danno sono entrambi eventi finali comuni ai reati de quo, donde truffa e frode informatica sono delitti ad evento naturalistico strettamente inteso e a dolo generico, non già a dolo specifico, come talora erroneamente si ritiene da una parte della dottrina e della giurisprudenza).

Quanto ai rapporti tra art.640 ter e 615 quinquies c.p., v. infra, § 2, p.7.

¹³ V. Cass. Sez.VI Pen. 4 ottobre - 14 dicembre 1999, n.3067, reperibile all’url www.ictlex.net/index.php?p=102. Le disposizioni di cui agli art.615 ter e 615 quinquies c.p. fanno in realtà riferimento a sistemi informatici e “telematici”. Orbene la sopra citata sent. della S.C. ha affermato che la rete telefonica può essere considerata “sistema telematico” ex art.615ter c.p. (ergo anche ax art.615 quinquies), in quanto le linee di tale rete, nell’epoca moderna, utilizzano normalmente le tecnologie informatiche. Infatti la funzione di trasmissione delle comunicazioni si attua con la conversione (codificazione) dei segnali (nel caso fonici) in forma di flusso continuo di cifre (bit) e nel loro trasporto in tale forma all’altro estremo, dove il segnale di origine viene ricostruito (decodificazione) e inoltrato, dopo essere stato registrato in apposite memorie. E’ poi “sistema” anche il cd. centralino, che abilita alla chiamata di determinate utenze e non di altre. Ma v’è di più: linee e centralino costituiscono sistemi informatici in quanto consentono di memorizzare e trattare elettronicamente le informazioni relative ai dati esterni alle conversazioni, come il numero dell’abbonato chiamante e di quello chiamato, il totale degli scatti, la data e l’ora della conversazione, che possono essere stampati su appositi tabulati contenenti il flusso di comunicazioni informatiche o telematiche (espressamente contemplato dall’art.266bis c.p.p.).

- comunicare, id est portare a conoscenza di un soggetto ovvero di un numero determinato di persone le informazioni o le idee alla base del programma maligno, indipendentemente dalle modalità con le quali avviene la comunicazione stessa (direttamente tra persone con lo scambio “fisico” di supporti ovvero on-line, con la trasmissione da un sistema a uno o più sistemi diversi);
- diffondere, id est divulgare, comunicare a più persone indiscriminatamente ovvero a un numero imprecisato di soggetti o di sistemi (si è in presenza sostanzialmente di più comunicazioni¹⁴).

Dalla chiara lettera della norma si può inferire che non costituiscono condotte punibili né la mera creazione, né la mera detenzione di virus. D'altronde se anche tali fatti fossero punibili, si correrebbe il rischio di arretrare troppo la soglia della punibilità¹⁵.

d) Circa l'**oggetto giuridico** o bene protetto dalla norma, si fa in genere riferimento al cd. “*domicilio informatico*”, tant'è che la disposizione de quo è stata collocata proprio all'interno del Titolo relativo ai delitti contro la persona e precisamente nel capo pertinente ai delitti contro l'inviolabilità del domicilio. Per domicilio informatico si vuol indicare <<*l'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art.14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt.614 e 615 c.p.*>>¹⁶. E ciò in quanto il computer rappresenterebbe per ogni persona “*una sorta di propaggine della propria mente e di tutte le sue conoscenze, i ricordi, i segreti che essa custodisce*”¹⁷, una specie di proiezione virtuale del proprio io pensante, un'estensione della dimensione della persona, un luogo in cui sono allocati i dati informatici di ciascuno¹⁸.

Tuttavia in dottrina non sono mancate voci critiche a proposito del bene protetto dalla norma, dacché l'art.615 quinquies c.p., anche per la sua formulazione (si parla infatti di “danneggiamento”), sembra più che altro orientato a tutelare il “patrimonio” informatico, nelle sue componenti hardware e soprattutto software (dati, informazioni e programmi). L'oggetto preminente sarebbe dunque il corretto funzionamento delle tecnologie informatiche, ergo ci si sarebbe aspettati di vedere la norma collocata o subito prima o immediatamente dopo il delitto di cui all'art.635 bis c.p.(danneggiamento informatico), o comunque all'interno del titolo del codice penale concernente i delitti contro il patrimonio¹⁹.

e) Circa l'**elemento soggettivo**, il delitto de quo è delitto (solo) doloso e precisamente a dolo generico, a prescindere dunque dal movente (ludico-vandalico, emulativo, estorsivo, terroristico...), che spinge l'*untore* informatico ad agire, essendo sufficiente la consapevolezza e la volontà di diffondere, comunicare e consegnare il programma e la consapevolezza degli effetti che esso può

¹⁴ In tal senso cfr. G.Pica, “*Diritto penale delle tecnologie informatiche*”, UTET, Torino, 1999, p.98 e s.

¹⁵ Nel senso che creazione e mera detenzione di virus non costituiscano condotte lesive né pericolose per alcun bene giuridico, cfr. P.Galdieri, “*Teoria e pratica nell'interpretazione del reato informatico*”, Giuffré, Milano, 1997, p.161.

¹⁶ Cfr. la relazione al d.d.l. n. 2773, in seguito tradotto per l'appunto nella legge n. 547 del 1993.

Con riferimento specifico al delitto di accesso abusivo, in diverse sent. si è sostenuto che il bene protetto dalla norma sarebbe il domicilio informatico. Ex multis, v. Cass. Sez.III Pen. 31 Luglio 2003, n.32440, reperibile all'url <http://www.eius.it/giurisprudenza/2003/087.asp>, nonché Cass. 3067/1999 cit., laddove si afferma che con l'espressione “domicilio informatico” si vuole indicare lo <<*spazio ideale (ma anche fisico in cui sono contenuti i dati informatici), di pertinenza della persona, al quale estendere la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto (art.14 Cost.)*>>. Sul concetto di domicilio informatico quale luogo anche fisico, cfr. G.Pica, op.cit., p.62, dal momento che i dati informatici, in un certo qual senso, esistono fisicamente sub specie di simboli memorizzati nell'hardware.

¹⁷ Cfr. R.Borruso, in R.Borruso, G.Buonomo, G.Corasanti, G.D'Aietti, “*Profili penali dell'informatica*”, Giuffré, Milano, 1994, p.28.

¹⁸ Cfr. P.Galdieri, op.cit., p.143.

¹⁹ Siffatta interpretazione la si può ritrovare e nel Mantovani (“*Dir.Pen.P.S. I*”, CEDAM, Padova, 1995, p.460) e nel Pica (op.cit., p.109). Secondo quest'ultimo Aut. le attività descritte nell'art.615 quinquies c.p. sarebbero prodromiche al danneggiamento, non tanto alla violazione del domicilio informatico.

produrre (danneggiare o alterare il sistema o comunque arrecare un danno a terzi attraverso l'interruzione del sistema o la cancellazione di dati e informazioni o la cancellazione o alterazione di programmi...) ²⁰. Esclude il dolo l'errore sul fatto che il programma abbia lo scopo o l'effetto di danneggiare dati o sistemi. Una condotta meramente colposa non è punibile ex art.615 quinquies c.p. Si consideri infatti che spesso (per es. nel caso di "worm") i malware circolano con l'ausilio inconsapevole di ignari utenti della rete, a segno che si parla anche di "portatori sani" ²¹ e talora di computer "zombies", ormai non più controllabili dal loro legittimo titolare a causa del fatto che sono stati infettati con un programma maligno, che ne consente il controllo da remoto. Né sarà poi punibile la condotta di chi scambia con altri informazioni sui virus, sulla loro struttura etc., laddove questo scambio sia finalizzato a conoscere i programmi maligni da neutralizzare, onde poter apprestare le opportune difese (cd. "antivirus") ²².

E' necessaria un'ultima precisazione. Sembra alquanto rischioso il riferimento normativo al mero "effetto", anzitutto perché non traspare un'idea di intenzionalità (a differenza dell'espressione "scopo"), indi perché talora conseguenze indesiderate (quali il blocco o "crash" di sistema ovvero l'interruzione temporanea dello stesso ovvero ancora la perdita di taluni file o dati) possono esser cagionate anche da programmi perfettamente leciti ²³. Il rischio sarebbe dunque quello di ricollegare

²⁰ Nel senso che ad integrare il coefficiente minimo di colpevolezza del delitto di cui all'art.615 quinquies c.p. sia sufficiente il dolo generico, v. Trib.Bologna Sez. I Pen., sent. 21 Luglio 2005 (dep. 22 dicembre 2005) reperibile all'url <http://www.penale.it/page.asp?mode=1&IDPag=182>. Il giudice peraltro ha ritenuto irrilevanti ai fini dell'esclusione del dolo le particolari motivazioni addotte dall'imputato (fini di studio e di ricerca) e dal suo difensore (fini ludici), in quanto 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)".

Nel caso di specie (per quanto risulta, il primo concernente il delitto di cui all'art.615 quinquies c.p. ad essere portato all'attenzione dell'autorità giudiziaria), l'agente (riconosciuto poi colpevole del reato ascrittogli) aveva realizzato un worm, denominato "Vierika", costituito da due programmi in grado di alterare una parte dei sistemi informatici aggrediti. Il worm veniva veicolato, come normalmente avviene per questo tipo di malware, con la tecnica dell'attachment (file allegato ad un messaggio di posta elettronica; cfr. § 1, p.1 e s.). L'allegato aveva un'estensione .jpg, tipica dei file contenenti immagini o fotografie. L'utente era portato a credere che nell'allegato (vista l'estensione e visto l'oggetto, indicato come "Vierika is here") fosse presente la fotografia a carattere erotico di una ragazza ("Vierika" per l'appunto). Invece, cliccando sull'allegato, si mandava in esecuzione il primo programma di cui era composto il virus, che aveva quale effetto quello di abbassare al minimo le impostazioni di protezione del browser Internet Explorer e di modificare la homepage dello stesso. Dipoi il secondo programma maligno si attivava una volta che l'ignaro utente si collegava ad Internet, dal momento che veniva automaticamente indirizzato dal browser sulla nuova homepage. E ciò era reso possibile proprio dalla manipolazione dei parametri di sicurezza provocata dal primo programma con conseguente esecuzione del secondo. E quest'ultimo, replicandosi e sfruttando le vulnerabilità del client di posta Outlook (cfr. § 1, p.2, nota 6), si autospediva (sempre via mail, nascosto nell'allegato) agli account presenti in rubrica, venendosi così a produrre un effetto di mass-mailing, molto simile allo spamming, ma più pericoloso, considerata la presenza del virus nell'attachment. E' indubbio che modificare in modo occulto, all'insaputa dell'utente e senza digitazione di appositi comandi da parte sua, l'ordinario modo di funzionare del browser e del client di posta rientra tra gli effetti contemplati nell'art.615 quinquies c.p. Si è infatti in presenza di una alterazione del sistema tale da cagionare un "comportamento anormale" dello stesso.

²¹ Cfr. G.Pica, op.cit., p.106

²² Cfr. G.Pica, op.cit., p.103.

²³ Si pensi a quei programmi di protezione cd. anti-pirateria o anti-crackaggio, che talune software-houses o altre imprese di distribuzione inseriscono all'interno dei supporti contenenti film, giochi, musica, programmi per P.C. etc. Ebbene molti di questi programmi talora hanno causato problemi di compatibilità col sistema (computer, consolle etc.), sul quale i supporti venivano installati per poter essere letti. Correttezza vorrebbe che le aziende di distribuzione di software, cdr, dvd etc. rendessero noto agli acquirenti i rischi che possono derivare da tali protezioni. Laddove fossero tenuti occulti, salva la responsabilità civile per i danni che il sistema dovesse subire, si potrebbe configurare non già il delitto di cui all'art.615 quinquies c.p., ma semmai quello di cui all'art.392 c.p., rubricato come "esercizio arbitrario delle proprie ragioni con violenza sulle cose", laddove l'art.1 della l. 547/1993 ha aggiunto un terzo comma all'art. de quo, stabilendo che si ha violenza sulle cose anche <<allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico>>. A tal riguardo vedasi il caso "Sony/BMG", che ha suscitato una vivace discussione a livello mediatico, nonché a livello dottrinario. Per tutti cfr. C.Giustozzi, "Attenti all'hacker, si chiama Sony/BMG...", reperibile all'url <http://www.interlex.it/copyright/corrado24.htm>. A cura dello stesso Aut. possono anche leggersi "Sony/BMG, virus,

l'evento lesivo all'agente sulla base del mero "*versari in re illicita*", scilicet sulla base del mero rapporto di causalità materiale, senza la benché minima attribuibilità psicologica (nemmeno a titolo di colpa, che peraltro nel delitto de quo non rilevarebbe) all'agente stesso. Ci si troverebbe così di fronte ad un'ipotesi di "responsabilità oggettiva", più o meno occulta²⁴. E ciò con grave violazione dei principi costituzionali in tema di responsabilità penale "personale", ossia "colpevole", laddove la condotta illecita è non solo materialmente, ma anche psicologicamente riconducibile a chi la pone in essere, ergo rimproverabile ed ergo ancora emendabile (combinato disposto dei co. 1 e 3 dell'art.27 Cost.). Solo la persona, che si renda conto del carattere antisociale del comportamento da essa posto in essere, può essere rieducata o risocializzata, poiché la pena (specie se detentiva), in un ordinamento giuridico laico e moderno, proprio alla rieducazione del colpevole deve mirare. Viceversa la sanzione sarebbe sentita come odiosa e ingiustificata costrizione della propria libertà personale senza che vi sia un motivo realmente comprensibile agli occhi del condannato.

f) La **perfezione** del delitto di cui all'art.615quinquies c.p. avviene nel luogo e nel momento in cui venga consegnato, comunicato o diffuso il programma. Trattasi di reato di pericolo o ostativo ovvero di mera condotta²⁵ e non di evento. Ergo il danno al sistema, ai dati o ai programmi non è elemento costitutivo del reato (a differenza del danneggiamento informatico ex art.635 bis c.p.), sebbene resti sul piano della ratio l'esigenza di prevenirlo²⁶. Naturalisticamente configurabile, sembra però non giuridicamente punibile il tentativo.

g) **Rapporti con altri reati.**

Secondo la dottrina maggioritaria, il reato di cui all'art.615quinquies può concorrere con quello di cui all'art.635 bis c.p. Infatti quest'ultimo, a differenza del primo, è reato di evento, ergo deve effettivamente verificarsi la distruzione, il deterioramento etc. previsto dalla disposizione, in quanto tali eventi lesivi sono elementi costitutivi della fattispecie, nel senso che sono necessari al fine del suo perfezionamento. Inoltre è diverso il bene giuridico protetto (il patrimonio nell'art.635 bis e il domicilio informatico, sebbene con le dovute riserve, nell'art.615 quinquies c.p.).

Quanto ai rapporti con l'art.640 ter c.p., in siffatto reato l'alterazione del sistema deve avere come risultato finale il proprio o altrui profitto con altrui danno (accadimento non richiesto ex art.615quinquies). Si è dunque di fronte a delitto di evento, che deve realizzarsi affinché si configuri la fattispecie consumata. Dubbia, quantunque non da escludersi, la configurabilità di un concorso tra codesti reati.

h) Quanto alla **procedibilità**, il delitto di cui all'art.615quinquies c.p. è procedibile d'ufficio.

(dis)informazione" (<http://www.interlex.it/copyright/corrado25.htm>) e "*Sony-BMG e DRM: non finisce qui...*" (<http://www.interlex.it/copyright/corrado27.htm>).

²⁴ In tal senso cfr. P.Galdieri, op.cit.,p.163 e G.Pica, op.cit., p.107. Quanto alle ipotesi di responsabilità oggettiva, rare sì, ma ancora presenti nel nostro c.p. (si pensi alle previsioni degli artt.43, co.3, ovvero 44 e, secondo parte della dottrina, anche degli artt. 82, 83, 116, 117, 584, 586, 588, co.2 e 3), meritano di essere ricordate le parole dell'Antolisei ("*Manuale di diritto penale. Parte generale*", Giuffrè, Milano, 1994, p.331), secondo il quale la responsabilità oggettiva <<è in contrasto con l'odierna coscienza giuridica, la quale reclama imperiosamente la piena realizzazione del principio nessuna pena senza colpa>>. Sulla stessa linea F.Mantovani, "*Diritto penale. Parte generale*", CEDAM, Padova, 1992, p.389: <<Fossile del passato la responsabilità oggettiva, espressa o occulta, contrasta non solo con la moderna coscienza giuridica, ma con la Cost., se si vuole attribuire all'art.27 un significato non vanificante ed anacronistico>>.

²⁵ Il Mantovani ("*Dir.Pen. P.S. I*" cit., p.461) parla di reato "senza offesa".

²⁶ I danni che potrebbero essere originati dai programmi maligni potrebbero concretarsi:

- nel rendere inservibile (anche in modo irreparabile) il sistema nelle parti hardware, sebbene l'ipotesi sia di rara verificaione;
- nella cancellazione (totale o parziale) di dati, informazioni e programmi ovvero nell'alterazione (id est modificazione in pejus) di programmi (mutandone finalità o rendendoli inutilizzabili per taluni scopi);
- nell'interruzione (totale o parziale, definitiva o anche solo temporanea) del funzionamento del sistema ovvero anche solo nel rallentamento dello stesso o nella sospensione di talune operazioni (senza che dati o informazioni vadano perduti).

3. Il virus come strumento per la realizzazione di altre fattispecie criminose

Un'ultima considerazione va fatta in relazione ai crimini che possono essere perpetrati tramite la diffusione in rete di codici maligni. Vista infatti la caratteristica di delitto di pericolo della fattispecie di cui all'art.615 quinquies c.p., essa può presentarsi come prodromica rispetto ad altri reati-fine.

Un esempio può essere costituito dal reato di estorsione ex art. 629 c.p. Infatti può accadere che l'autore, dopo aver realizzato il malware (può trattarsi di uno spyware oppure di un worm), lo invii tramite posta elettronica celato all'interno di un trojan allegato all'e-mail. In tal modo, una volta eseguito, il codice maligno consentirà di controllare da remoto il computer, ovvero un intero sistema (rete Intranet, mainframe etc.), consentendo al virus-writer o comunque a chiunque ne abbia la capacità tecnica e l'interesse, di manipolare programmi e dati, di cancellarli o distruggerli, di rallentare le operazioni, di interromperle etc.²⁷ Tali trojan vengono addirittura affittati o noleggiati (talora venduti) a organizzazioni criminali (vere e proprie "cybermafie"). Il virus dunque come strumento di ricatto per aziende e organizzazioni, le quali sono disposte a versare somme anche molto alte pur di liberarsi dell'indesiderato "ospite".

Inoltre un codice maligno può costituire il mezzo per realizzare i delitti di esercizio privato delle proprie ragioni tramite violenza sulle cose (art.392 c.p., con particolare riferimento al co.3, così come modificato dall'art.1 della l. 547/1993), di violenza privata (art.610 c.p.) e di minaccia (art.612 c.p.), ovvero per forzare o spezzare (nonché aggirare con la tecnica del trojan) le misure di sicurezza poste a presidio di un sistema informatico onde accedervi indebitamente e altrettanto indebitamente permanervi (venendosi così a realizzare la fattispecie criminosa di cui all'art. 615 ter c.p.) ovvero ancora per danneggiare un computer (art.635 bis c.p., come peraltro si è visto).

Quanto alla valenza terroristica di certi attacchi, non bisogna obliare che un malware e soprattutto un worm (a causa della grande facilità di propagazione) può esser utilizzato da organizzazioni criminali per attentare alla sicurezza e al funzionamento di impianti di pubblica utilità (art.420 c.p., co.2, così come modificato dall'art.2 della l. 547/1993) o più in generale per attentare alla sicurezza dei trasporti, soprattutto su rotaia o aerei (art.432 c.p.) o a quella degli impianti di energia elettrica e gas, nonché delle pubbliche comunicazioni telefoniche e telegrafiche (art.433 c.p.). E ciò per l'ovvia ragione che ormai ci si serve proprio di sistemi informatici, protetti e distribuiti in reti Intranet, con tutti i loro terminali, per controllare tali impianti, servizi etc.

²⁷ In tali casi potrebbe configurarsi un concorso tra i delitti di cui agli artt. 615 quinquies, 615 ter aggravato ex co.2, n.3) e 629 c.p., avvinti, qualora se ne ravvisino gli estremi, dal vincolo della continuazione (art.81 cpv. c.p.).