Sentenza Vierika: un commento dell'Avv. Mario Ianulardo

L'Avv. Mario Ianulardo (membro del Consiglio Direttivo del CGT) offre un commento a prima lettura del caso giudiziario del momento: la sentenza della prima condanna di un virus writer italiano, il c.d. "processo Vierika".

Fonte: Punto Informatico
È stata depositata la motivazione della sentenza emessa dal Tribunale di Bologna che ha decretato, nel luglio 2005, la condanna alla pena di mesi sei di reclusione (sostituita ai sensi dell'art.53 L.689/91 con la corrispondente pena pecuniaria di € 6.840 di multa) del primo "virus writer" italiano. Finalmente ora è possibile conoscere quali sono stati gli elementi di prova, acquisiti nel corso dell'istruttoria dibattimentale, che hanno indotto il giudice del Tribunale ad emettere sentenza di condanna nei confronti di C.G. ritenuto l'esclusivo colpevole dei reati di accesso abusivo a un sistema informatico o telematico (art. 615-ter C.P.) e di diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 615 - quinquies C.P.).

Le fonti di prova fornite dalla Polizia Tributaria della Lombardia hanno permesso di accertare la natura e gli effetti che produceva il worm incriminato. Si tratta di 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, 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, e si attiva quando l'utente, collegandosi ad Internet, viene automaticamente indirizzato dal browser sulla nuova home page sopra indicata: l'abbassamento delle protezioni di default di windows ad opera della prima parte del codice, permette l'automatica esecuzione del secondo script contenuto nel documento html.
Come molti altri worm conosciuti, Vierika produce 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" si autoreplichi.

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., aventi nella propria url il nome Vierika http://www.penale.it/stampa.asp?idpag=182 - _edn9#_edn9.

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 file relativi al programma Vierika contenuti nel proprio disco rigido, masterizzandone copie da sottoporre a sequestro sotto il controllo degli agenti.

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

Questi i fatti.

Appare doveroso, tuttavia, in questa sede, porre attenzione all'aspetto caratterizzante l'intera vicenda processuale. Mi riferisco all'aspetto concernente le modalità di acquisizione degli elementi di prova formatisi nel corso dell'istruttoria dibattimentale.
Di non trascurabile importanza l'argomento citato, in quanto è proprio sulla scorta delle prove acquisiste in dibattimento che il giudice decide circa la colpevolezza o meno dell'imputato.

Il contraddittorio tra le parti (P.M. e difesa) si è svolto quasi esclusivamente sul tema della metodologia utilizzata dalla polizia giudiziaria nell'acquisire i mezzi di prova e sulla corrispondenza della metodologia applicata dalla p.g. ai principi dettati in materia penale in tema di formazione ed acquisizione delle prove. Come è intuibile, abbastanza scontato appare l'oggetto dello "scontro" dialettico tra accusa e difesa considerata la non trascurabile circostanza che l'imputato, già nella prima fase delle indagini, in sede di interrogatorio, aveva ammesso di aver creato e diffuso il programma Vierika.

La difesa dell'imputato con reiterati interventi ha posto in discussione la correttezza sia del metodo utilizzato dalla p.g. per estrarre i programmi dal computer dell'indagato, sia il metodo 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) invocando espressamente l'espletamento di una perizia che potesse verificare, sotto un profilo squisitamente tecnico, la correttezza della procedura adottata dalla G. d. F. nonché il risultato degli stessi accertamenti.

Di contrario avviso, invece, il giudicante il quale ha precisato, in sede di motivazione della sentenza, che non si è ritenuto necessario disporre una perizia volta a verificare il funzionamento del programma adducendo, da una parte, che i testi di polizia giudiziaria, escussi in dibattimento, avevano le competenze tecniche necessarie per la decifrazione del codice; dall'altra, ha ritenuto che la difesa non abbia in sostanza contestato i meccanismi di funzionamento del programma, nonostante si sia servita anche della collaborazione di un esperto informatico.

Del resto, si legge testualmente nel provvedimento reso dal giudice: "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".

In buona sostanza il giudice, peritus peritorum, si era già formato il convincimento che l'intera attività d'indagine espletata dalla G. d. F. potesse considerarsi degna di fede.
Infatti, egli aggiunge che "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)".

Si precisa, comunque, che per la prima volta in Italia sono state acquisite in dibattimento le linee guida IACIS, ovvero "International Association of Computer Investigative Specialists", un passaggio importante in attesa di analoghe iniziative nazionali per le best practice in tema di informatica ed indagini.

Riguardo alle argomentazioni difensive, invece, il giudice ha ritenuto che la difesa, pur ribadendo 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", tuttavia non ha documentato "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".

Questo argomento merita una piccola riflessione. Come noto, le indagini e quindi i processi si protraggono per molti anni. La vicenda Vierika, ad esempio, nata all'inizio del 2001, ha visto l'epilogo in primo grado solo alla fine del 2005, a quasi 5 anni di distanza, nonostante le immediate ammissioni dell'imputato che si leggono nella stessa sentenza in commento. Nell'informatica questo periodo è quasi un abisso, la tecnologia evolve rapidamente, come del resto le tecniche di computer forensics e gli stessi tool di acquisizione ed analisi delle tracce informatiche. Difficile, quindi, analizzare i fatti nel giusto contesto temporale, proprio perché non appare agevole ritornare con una sorta di macchina del tempo nel momento delle attività investigative e valutare l'idoneità delle scelte operate. Fondamentale, con il passare del tempo, è porre la lente su quei fatti che non "invecchiano", come la tutela dei diritti degli individui e la dimostrazione di eventuali alterazioni del caso con i dati, anche informatici, acquisiti nel fascicolo.

L'epilogo oramai è noto. L'imputato C.G. è stato riconosciuto colpevole del reato continuato ascrittogli e concesse le attenuanti generiche, condannato alla pena di mesi sei di reclusione, convertiti nella pena pecuniaria in € 6.840,00. Assolto, invece, il coimputato C.S. per non aver commesso il fatto.

Va evidenziato, tuttavia, che auspicabile, invece, sarebbe stato il conferimento dell'incarico peritale (anche da parte della stessa difesa che più volte invocava un perito d'ufficio), sotteso a verificare l'attendibilità o meno del metodo utilizzato dalla polizia giudiziaria e dai tecnici delle società Tiscali s.p.a ed Infostrada s.p.a per acquisire gli elementi probatori.

La vicenda, vale la pena ricordare, ha ad oggetto la valutazione di ipotesi di reati commessi con l'uso di mezzi informatici e telematici. Si parla di software, di bit, di worm, connessioni I.P., di impronte elettroniche.

Si tratta sì di formazione della prova ma non delle prove intese in senso tradizionale bensì di "prove digitali" in una sorta di "metaterritorio" dove sembrerebbe perdere consistenza la naturale propensione dell'uomo di rapportarsi al mondo reale con l'uso dei cinque sensi e del tatto in particolare" (1)

Nel processo si sono affrontati aspetti tecnologici di notevole portata e situazioni tecniche indissolubilmente connesse alla costante ed incessante evoluzione tecnologica. Nuova, infatti, è la materia trattata nonché in costante evoluzione la tecnologia che condiziona enormemente la metodica di acquisizione dei mezzi di prova e, non in ultimo, non vi è ancora giurisprudenza consolidata in ordine alle nuove tipologie dei reati informatici. Ad abundantiam, vale la pena ricordare che in Italia, in particolare, non esiste una "standardizzazione" delle procedure di acquisizione dei mezzi di prova e molto spesso le modalità operative vengono affidate alla professionalità, più o meno sviluppata, degli operatori nonché dei magistrati che autorizzano le operazioni di sequestro ed acquisizione.

Una sentenza molto importante, quindi, per i molti spunti di procedura penale (ed anche di diritto sostanziale) che potrebbero essere approfonditi giuridicamente. Speriamo che questo non rimanga un caso isolato e che altri giudici, con il medesimo entusiasmo tecnico-giuridico, si facciano promotori di altra giurisprudenza sul tema, per fornire quel necessario contributo alla individuazione di una metodica "standard", per quei casi analoghi legati alla formazione della cosiddetta "prova informatica".

Avv. Mario Ianulardo

(1) Cfr. Gerardo Costabile, "Scena criminis, documento informatico e formazione della prova penale", reperibile su www.penale.it

Fonte: Punto Informatico