Prove

Pornografia minorile e *file sharing*: l'influenza della tecnologia informatica sull'asse probatorio

di **Filippo Novario**

Attraverso le cosiddette prove informatiche e la loro valutazione tecnico-giuridica la tecnologia informatica, inevitabilmente sottesa alla commissione di *computer crimes*, influisce sulla prova della colpevolezza dell'imputato e sul ragionamento probatorio del giudice. L'accertamento dei reati di pornografia minorile *online*, soprattutto se perpetrati attraverso la moderna tecnologia del *file sharing*, ne è la dimostrazione.

Emorragia criminale

L'ultimo rapporto del progetto "*Stop-It*", pubblicato dall'organizzazione internazionale indipendente *Save the Children*, mette in evidenza come i casi di pornografia minorile via *Internet* siano in netta crescita (1). Le segnalazioni pervenute all'organizzazione sono state 3106, 10% in più degli anni precedenti, di cui: il 66% riguarda siti *Internet*, il 20% *spam* e *e-mail* non richieste, il 10% tecnologie *peer to peer*, il 2% le *chat* e l'1% le *newsgroup*.

Tra le nuove tecnologie informatiche il *peer to peer*, meglio conosciuto attraverso la sua più comune applicazione, il *file sharing*, fa rilevare il dato più significativo, con una crescita annuale dell'85,4%, portando alla ribalta un problema definito dal diritto sostanziale ma ancora oscuro, data la sua tecnicità, sotto il profilo probatorio e processuale.

La tecnologia del *file sharing*

Il *file sharing* è un sistema *software-hardware*, composto da elaboratori connessi nella rete *Internet* mediante una rete comune, fruibile dai possessori di uno specifico programma, che consente lo scambio di *file* tra i suoi utenti.

La sua struttura è variabile: può ricalcare l'architettura *client-server*, dove un *computer server* condivide e gestisce le sue risorse con i *computer client*; oppure l'architettura *peer to peer*, rete composta da nodi (*computer*) equivalenti che fungono sia da *client* sia da *server* per altri nodi della rete.

La condivisione di *file* è resa possibile dall'installazione di un *software* sul *computer client*, programma applicativo che consente all'utente di: ricercare *file* per criteri *standard* (nome, estensione, grandezza, etc.); scaricare i *file* di interesse, utilizzando l'opzione di *download*, che li copia in una cartella predefinita dal programma o indicata dall'utente; condividere *file* ponendoli in una determinata cartella condivisa oppure nell'*hard disk*. La cartella al cui interno vengono salvati i *file* scaricati normalmente coincide con la cartella di condivisione dei *file*, facendo sì che l'utente condivida automaticamente i *file* prima ancora del loro completo *download*, permettendo una più dinamica fruibilità del sistema.

La tutela sostanziale: art. 600 *ter*, comma 3, *quater* e *quater*-1, c.p.

Dottrina e giurisprudenza (2) riconducono lo scambio di materiale pornografico minorile operato mediante sistemi di *file sharing* alle fattispecie penali previste dagli art. 600 *ter*, comma 3, *quater* e *quater.1* c.p., come introdotte dalla legge sulla tutela dello sfruttamento e della pornografia minorile del 3 ago-

Note:

(1) *http://www.savethechildren. it/2003/download/Stop-It/stop-it_ 2005.pdf*

(2) Cfr. AA.VV., *Elementi di informatica giuridica*, Torino 2006, 290 s.; Cass., sez. III, 8 giugno 2006 n. 23164, in *Cass. Pen.* 2006, 2346 s.; Trib. Lamezia Terme 4 giugno 2007 n. 252, in *Altalex* 2007; Uff. Indagini Preliminari Milano 2 febbraio 2007 n. 230, in *Il merito* 2007, 7-8, 62s., nota A. Sorgato; Trib. Venezia 31 marzo 2005 n. 62, in *Riv. Internet* 2005, 382 s.

sto 1998 n. 269, emanata in adempimento dell'impegno derivante dalla Convenzione di New York del 20 novembre 1989, e dalla l. 6 febbraio 2006, n. 38, che ha dato esecuzione alla decisione quadro 2004/68/ GAI del Consiglio dell'Unione Europea.
L'art. 600 *quater* 1 c.p. estende le disposizioni degli artt. 600 *ter* e 600 *quater* c.p. anche ai casi di pornografia minorile virtuale, dove le immagini di violenza su minori vengono simulate con la creazione di immagini virtuali aventi le fattezze di minori: eventualità plausibile nei sistemi di condivisione di *file*, per la libertà dei contenuti condivisibili.
L'art. 600 *ter*, comma 3, c.p. punisce chi distribuisce, divulga, diffonde o pubblicizza materiale pornografico minorile, anche in via telematica, con un'aggravante per l'ingente quantità. Nel caso del *file sharing* si configura la sola divulgazione e pubblicità di *file* illeciti. Secondo la giurisprudenza, infatti, il sistema di condivisione non compie un trasferimento dei contenuti a determinati soggetti, bensì una messa a disposizione dei contenuti per chiunque possegga uno specifico *software* di *file sharing*, con una loro propagazione ad un numero indeterminato di soggetti (3).
L'art. 600 *quater* c.p. invece punisce chi consapevolmente si procura o detiene materiale pornografico minorile, con l'aggravante in caso di ingente quantità. La fattispecie si configura in tutte le operazioni dei sistemi di *file sharing*: il procurarsi è compatibile con la scelta dei *file* tra quelli condivisi; la detenzione è invece compatibile con la procedura di *download* e di condivisione dei *file*. In entrambi i casi i *file* devono essere nell'immediata disponibilità degli utenti.

La prova della colpevolezza

La prova della colpevolezza per i reati *ex* art. 600 *ter*, *quater* e *quater* 1 c.p. consiste: nell'accertamento positivo dell'elemento oggettivo delle fattispecie di divulgazione, procacciamento o detenzione di immagini pornografiche minorili, anche virtuali; nella prova del nesso causale tra la condotta del soggetto e gli eventi sopraccitati; nell'accertamento positivo dell'elemento soggettivo del reato, consistente nella consapevolezza o nella coscienza e volontà dell'agente, con l'esclusione del dolo eventuale.
L'asse probatorio è costituito da prove scientifiche di tipo informatico, reperibili dagli inquirenti secondo modalità tipiche: sistemi di contrasto, intercettazioni autorizzate, *ex lege* 3 agosto 1998 n. 269, oppure normale attività investigativa *ex* art. 326 c.p.p. Le indagini si articolano in quattro momenti: navigazione su sistemi di *file sharing*, alla ricerca di materiale illecito; acquisizione di flussi di dati corrispondenti all'*IP* oggetto di indagine, numero che identifica univocamente un dispositivo collegato ad una rete informatica; disposizione di sequestri e perquisizioni presso il domicilio fisico del titolare della linea telefonica; analisi dei supporti di memorizzazione rinvenuti, per l'individuazione o la conferma della presenza di *file* a contenuto illecito (4). Risultato delle indagini è il rinvenimento di prove scientifico informatiche di tipo storico, *file*, con le loro caratteristiche tecniche (ora di creazione, utenza, etc.).
La rilevanza delle prove così individuate è particolarmente alta. Se acquisite secondo corrette procedure di *Computer Forensics* (5), risultano da sole idonee a provare l'elemento oggettivo e il nesso causale dei reati suddetti. La presenza di un *file* in una cartella condivisa o di un'azione registrata da un *log* del sistema, *file* su cui avviene la registrazione cronologica delle operazioni, possiede infatti l'attitudine a rappresentare il fatto-reato e la sua dinamica causale.
Le prove informatiche non sono però da sole sufficienti ad assolvere la prova della colpevolezza per quanto riguarda l'individuazione del soggetto agente e l'elemento soggettivo del reato. L'analisi di un *IP* non consente infatti l'individuazione univoca di un soggetto, e le operazioni compiute dai programmi sono spesso frutto di processi informatici automatici e *standard*. Entrambi sono però desumibili, per prove critico-indiziarie, da analisi tecniche compiute su procedure informatiche e da elementi fattuali (6).
La prova della colpevolezza del soggetto agente e dell'elemento soggettivo del reato necessitano dunque di una particolare analisi probatoria, di carattere tecnico-informatico, *in primis* sulle prove informatiche relative all'elemento oggettivo e al nesso causale del reato e, se non sufficiente, una ricerca di ulteriori prove informatiche.

La prova dell'individuazione del soggetto agente

Gli utenti dei sistemi di *file sharing* beneficiano di un anonimato digitale fornito da *IP* dinamici, resta

Note:

(3) Cass., sez. III, 8 giugno 2006 n. 23164, in *Cass. Pen.* 2006, 2346 s.

(4) L. Cuomo, *Siti Internet, pedopornografia e strumenti di contrasto*, in *http://appinter.csm.it/incontri/relaz/15932.pdf.*, 24 s.

(5) Disciplina informatico giuridica nordamericana che consente una corretta acquisizione dei dati attraverso una copia fidefaciente all'originale. Cfr. Ghirardini, Faggioli, *Computer Forensics*, Milano 2007, 45 s.

(6) L. Lupària, *Processo penale e tecnologia informatica*, in *Dir. Internet*, 3, 2008, 224.

però la necessità di un'utenza telefonica per l'accesso al servizio, con la possibilità di risalire ad un luogo fisico dove disporre misure cautelari di tipo informatico forense. Da un'approfondita ricerca dei dati presenti nell'*account* del soggetto indagato, che è l'insieme di strumenti e contenuti attribuiti ad un utente, possono essere rinvenuti elementi su cui fondare prove critico indiziarie per individuare il soggetto agente: la presenza di materiale e carteggi *e-mail* a carattere pedopornografico, accompagnati da elementi personali atti a svelare la vera identità dell'utente, possono avvalorare l'ipotesi dell'accusa.
Un elemento decisivo è però fornito da una componente *software* ulteriore alle prove già rilevate. Gli utenti e i contenuti, al loro ingresso nelle reti di condivisione, vengono identificati mediante l'apposizione automatica di un valore di *hash*, stringa di testo immodificabile che diviene una loro impronta digitale, permettendo di riconoscerli in modo univoco. Un'analisi dei valori di *hash*, di utenti e *file* condivisi, associata alle prove informatiche e fattuali già raccolte, può portare ad una precisa identificazione dell'utenza agente e dei *file* da questa trattati con coscienza e volontà.

La prova dell'elemento soggettivo del reato

Un fenomeno comune nelle reti di *file sharing*, ancora poco conosciuto al diritto, consente una chiara esemplificazione della prova dell'elemento soggettivo del reato: il caso dei *file fake*.
Nel gergo degli utenti di sistemi di *file sharing* è definito *fake* un *file* che possiede caratteristiche diverse dalle aspettative dell'utente che lo vuole scaricare, a causa di errori del sistema *software* o manipolazioni di utenti, poiché corrotto, alterato o con nome o estensione (7) non coerenti con il suo vero contenuto. È anche possibile però che *cyber*criminali condividano contenuti pedopornografici con nomi innocui, quindi *fake*, ma consapevolmente, imponendo la formazione di un particolare asse probatorio informatico focalizzato sulla prova critico indiziaria dell'elemento soggettivo.
Un'analisi delle caratteristiche dei *file* rinvenuti può fornire elementi rilevanti. L'immediata o ritardata cancellazione del *file* illecito può, nel primo caso, palesare la non volontarietà di scaricare un *file* a carattere pedopornografico e, nel secondo caso, rivelare la volontarietà di procacciarlo e detenerlo. Gli accessi al *file* illecito invece, rinvenibili dalle caratteristiche del *file* stesso, oppure dai *log* del sistema operativo, se molteplici ed antecedenti alla sua cancellazione, possono far desumere che il soggetto conoscesse e usufruisse del contenuto del *file*; la mancanza di accessi o un accesso al *file*, immediatamente antecedente alla sua cancellazione, verificabile con l'osservazione incrociata dei *log* del sistema e delle caratteristiche del *file*, possono invece far desumere la non volontarietà del *download*.
Alcune componenti *software*, ulteriori a quelle normalmente analizzate in sede informatico-forense, possono fornire elementi rilevanti e spesso decisivi per la prova dell'elemento soggettivo del reato: ad esempio l'opzione di "anteprima dei *file*" in *download*. Quest'opzione consente di apprezzare il contenuto dei *file* prima del loro completo *download*, il suo utilizzo non necessita di particolari capacità tecnico-informatiche da parte dell'utente, diviene operativa a seguito dell'installazione di un programma di lettura di *file* incompleti e dell'utilizzo, ad opera dell'utente, dell'opzione di immediato *download* di porzioni chiave dei *file*. Da un'analisi dei *log* del programma di lettura è possibile sapere su quali *file* quest'ultimo è stato utilizzato, il momento del suo utilizzo e il numero di visualizzazioni dei *file*. La presenza di un programma di visualizzazione di *file* parziali sul *pc*, e l'evidenza nei *log* del programma di un suo utilizzo sui *file fake* oggetto di indagine in un lasso di tempo antecedente al loro completo *download*, possono evidenziare una consapevole conoscenza del contenuto del *file*.

Nota:

(7) Breve sequenza di caratteri alfanumerici aggiunti dopo il nome del *file* e separati da quest'ultimo da un punto.