|  |  |
| --- | --- |
| S | Brevetto:  On-Line Digital Evidence Management (OLDEM)  Dipartimento di Informatica  *R.M. Capocelli*  Università degli Studi di Salerno  Salerno, 7 agosto 2011 |

# Sommario

Sommario 2

1 Premessa 3

2 Descrizione del problema 3

2.1 La giurisprudenza sul tema 3

La certezza del contenuto e della data. 4

3 Presentazione dell’invenzione 5

3.1 Campo di applicazione 5

3.2 Descrizione generale 6

4 Dettagli tecnici del processo 7

4.1 Open Issues 8

# Premessa

Si intende procedere al deposito brevettuale di un processo messo a punto presso il Dipartimento di Informatica dell’Università di Salerno da un gruppo di ricercatori afferenti al Dipartimento.

Il processo consente l’erogazione di un servizio on-line (fruibile attraverso la rete pubblica Internet) per la certificazione inoppugnabile dei contenuti pubblicati da soggetti terzi attraverso canali di comunicazione on-line (pagine web, chat, ecc.).

# Descrizione del problema

## La giurisprudenza sul tema

La legislazione italiana ha di recente introdotto il reato di stalking o diffamazione a mezzo internet …

“Tra i diritti della personalità facilmente aggredibili, in questa prospettiva, vi è il diritto alla reputazione, minacciabile mediante la diffusione di notizie false o diffamatorie ai danni di un soggetto, attraverso il mezzo di internet, che consente una capillare e rapidissima diffusione dei contenuti in esso pubblicati. …”

*In particolare, per quanto riguarda la diffamazione a mezzo internet e la normativa sulla stampa, la dottrina e la giurisprudenza si sono domandate se tale reato non debba più correttamente essere inquadrato e disciplinato alla stregua di ipotesi particolari, analogamente alla diffamazione a mezzo stampa o a mezzo di trasmissioni radio-televisive. Dapprima ci si è chiesti se si potesse direttamente richiamare la normativa sulla stampa e sulle trasmissioni radio-televisive. L'orientamento prevalso è stato di segno negativo scaturito dall'insormontabile divieto di analogia in malam partem vigente in materia penale .* ***Un chiaro ostacolo all'interpretazione anzidetta è costituito proprio dalla definizione, espressamente dichiarata dalla giurisprudenza dominante insuscettibile di interpretazione estensiva 3, di stampato, data dallo stesso art. 1, l . n. 47 del 1948, che fa riferimento a tutte le riproduzioni tipografiche o comunque ottenute con mezzi meccanici o fisico-chimici; appare evidente l'incompatibilità della suddetta definizione con le modalità di diffusione delle pubblicazioni a mezzo internet, che avvengono attraverso la collocazione di dati ed informazioni trasmessi per via telematica, tramite l'utilizzo della rete telefonica, al server di un cosiddetto provider o webmaster , accessibile a migliaia di utenti contemporaneamente, presso il quale le informazioni restano a disposizione nei diversi siti in modo tale che ciascun interessato può leggerle e conservarle mediante il proprio computer****. Peraltro, alla luce delle pur generiche definizioni contenute nella normativa sovranazionale di riferimento 4, è di tutta evidenza come, in ossequio al principio di stretta legalità, le trasmissioni via internet non possano che ritenersi estranee alle previsioni penali relative alla radio-televisione, poiché esse avvengono con modalità del tutto differenti, e dunque incomparabili, rispetto alle trasmissioni oggetto della regolamentazione operata dalla normativa in esame. Tuttavia, recentemente, uno spiraglio per un'equiparazione di internet agli altri mezzi di comunicazione è stato fornito dalla l. 7 marzo 2001, n. 62 sul diritto d'autore, la quale, se pur ad altri fini, fornisce una definizione di prodotto editoriale che si estende sino a ricomprendere qualsiasi prodotto su supporto cartaceo o su supporto informatico destinato a pubblicazione o diffusione con ogni mezzo anche elettronico. Alcuni giudici di merito 5 hanno affermato che il sito internet deve essere ritenuto prodotto editoriale ai sensi dell'art. 1, l . n. 62 del 2001, in quanto prodotto realizzato su supporto informatico destinato alla diffusione di informazioni con mezzo elettronico attraverso l'immissione nella rete mondiale, accessibile in pratica a chiunque, di una serie di opinioni e informazioni. …*

### La certezza del contenuto e della data.

*Si ponga ad esempio il caso di un soggetto che lamenti l’avvenuta lesione della sua reputazione tramite un articolo diffamatorio “pubblicato” sul web. Dottrina e giurisprudenza, oramai in accordo, affermano che nella nozione di “stampa” di cui all’art. 595, III comma, cp debba essere ricompresso ogni prodotto idoneo alla sua diffusione in una molteplicità di esemplari, con mezzi meccanici o fisico-chimici. Tale determinazione trova già fondamento nell’art. 1. L.8 febbraio 1948, n.47. Analogamente, per “altri mezzi di pubblicità” si intendono, in senso ampio, tutti gli altri mezzi divulgativi, quindi, anche internet [[1]](#footnote-1).*

*Quindi, posto che in astratto è configurabile la diffamazione a mezzo internet, come sarà possibile dare la prova processuale dell’esistenza di uno scritto o filmato o immagine diffamatoria? Non dimentichiamoci che la pagina web incriminata potrebbe essere cancellata dopo poche ore dalla pubblicazione, ma intanto il reato è stato commesso ed il danno prodotto. Basterà produrre e depositare in giudizio una mera copia cartacea della pagina web ovvero le copie di backup della pagina diffamatoria?*

L’art. 2712 c.c. attribuisce piena prova alle rappresentazioni fotografiche, informatiche ed, in genere, ad ogni altra riproduzione meccanica dei fatti e di cose in esse riprodotte, se colui contro il quale sono prodotte non ne disconosce la conformità ai fatti ed alle cose. Le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione. Da ciò va esclusa la qualità di documento, con efficacia probatoria, a una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all’originale e di riferibilità a un determinato momento[[2]](#footnote-2) .

Si impone la necessità di fornire certezza al contenuto del “documento” e dimostrarne la data certa. Tale impellenza viene soddisfatta con una produzione della copia conforme della pagina web, proprio per cristallizzare il contenuto che una certa pagina ha in un momento particolare.

Posto che la pagina web costituisce documento informatico - “rappresentazione informatica di atti e fatti o dati giuridicamente rilevanti” - ai sensi dell’art.1 del d.lgs n. 82/2005 e che, ai sensi all’art. 23, la realizzazione della copia del documento informatico è validamente riprodotta se raccolta in conformità alle regole tecniche vigenti, la copia conforme della pagina web potrà essere eseguita da Notaio (oltre che da un cancelliere, segretario comunale ecc)[[3]](#footnote-3) il quale, innanzi alle peculiarità del documento informatico, adatti ad essa la tipica attività notarile di rilascio di copie autentiche.

La certificazione di conformità del Notaio costituisce il presupposto minimo richiesto dalla giurisprudenza citata e dal successivo d.lgs. n. 82/2005 e può essere resa con copia della pagina web diffamatoria su supporto informatico o su supporto cartaceo.

Per la **copia su supporto informatico** il Notaio dovrà: 1) eseguire la copia di tutte le informazioni visualizzate; 2) apporre l’attestazione di conformità, indicando a) il browser, b) l’ora; c) eventuali certificati di sicurezza; d) l’indirizzo della pagina, comprensivo di URL; 3) apporre la firma digitale a tutti i file ovvero associare tra loro i singoli file, esempio tramite il formato zip, quindi, apporre la firma digitale su quest’ultimo[[4]](#footnote-4).

Per la **copia cartacea** il Notaio non potrà che trasporre un contenuto statico (quindi, a meno che non si voglia ottenere una copia parziale, la copia cartacea non potrà essere utilizzata per assicurarsi la copia di una pagina web con contenuto dinamico; es. filmato). Il Notaio, in tal caso, dovrà indicare: 1) il sito internet; 2) il tipo di browser utilizzato; 3) la data e l’ora in cui la copia viene effettuata; 4) i dati relativi ad eventuali certificati di sicurezza per la verifica dell’identità del sito. Nel caso in cui l’attestazione non rispetti le indicate formalità minime sopra riportate, la copia avrà l’efficacia solo di un principio di prova scritta ai sensi dell’art. 2717 cc.

La Corte di Cassazione con la sentenza n. 2912/94 ha definitivamente chiarito che, ai fini probatori, non basta produrre la mera stampa della pagina web, è necessario depositare copia autenticata nei termini e con le modalità sopra indicate.

Fino ad oggi non era possibile produrre l’evidenza di ciò che altri soggetti pubblicano su internet (contenuti) ed in particolare non era possibile identificare l’origine dei contenuti offensivi.

Con lo stesso procedimento può essere utile poter dimostrare che in un dato istante un certo contenuto (eventualmente protetto dal diritto di autore) è già stato reso disponibile on-line.

Occorre anche considerare che i contenuti di un sito web possono avere un carattere dinamico ed apparire in maniera diversa in funzione di alcuni parametri come ad esempio l’indirizzo di provenienza della richiesta, il tipo di browser utilizzato per visualizzare la risposta, orario, regione di provenienza, username, ecc.

# Presentazione dell’invenzione

## Campo di applicazione

L’invenzione opera nel campo della computer forensics ed in particolare può essere utilizzata per l’acquisizione di evidenze digitali di contenuti pubblicati su internet attraverso un insieme di pagine HTML accessibili per mezzo di un Web Server. Più specificamente è stato disegnato un processo per la realizzazione di uno strumento appartenente alla famiglia dei *Network Forensic Analysis Tool* (NFAT) per produrre copia su supporto informatico dei contenuti di un sito web raggiungibile via rete pubblica (*remote network service*) valida ai fini probatori in vertenze legali.

Computer forensics è una disciplina scientifica che intende fornire supporto e strumenti a valore legale da impiegare nelle indagini da produrre in fase di dibattimento.

Considerando l’estrema volatilità delle informazioni presenti su Internet (possono essere modificate o rimosse in ogni istante) è indispensabile acquisirne una copia a valore legale per provare davanti ad un giudice che tali informazioni sono state rese disponibili su Intenet, configurando, ad esempio, reati come ingiuria a mezzo stampa, diffamazione, violazione del copyright, ecc. In generale chi ha prodotto e pubblicato dei contenuti su Internet è sempre in grado di rimuoverli a suo piacimento e di eliminarne eventuali tracce.

## Descrizione generale

Il processo messo a punto dal Dipartimento di Informatica prevede l’attivazione di un servizio S pubblicamente accessibile tramite internet considerata “terza parte fidata” per la produzione di una “*copia su supporto informatico con valore legale di contenuti pubblicati su Internet*”.

Il servizio ha lo scopo di fornire all’utente che lo richiede l’evidenza legale dell’esistenza di un insieme di contenuti (pagine HTML) su un sito pubblicamente accessibile su internet (tramite una URL ed identificato sia dal nome che dall’indirizzo IP numerico) nell’istante (data e ora) in cui viene effettuata la richiesta.

L’utente U si collega al servizio e specifica il sito W di cui vuole vengano certificati i contenuti pubblicati. Il servizio S effettuerà la connessione al sito W agendo come un *Proxy trasparente* per la successiva navigazione, inoltrando i dati all’utente U dopo aver acquisito una copia della *stream* di dati che sono transitati da e per il sito W. Sarà possibile dimostrare che tale copia sarà una fedele riproduzione dei dati (stream) in quanto rappresenterà il risultato di un processo P (costituito da operazioni matematiche descritte nel seguito) che renderebbe evidente qualsiasi modifica (alterazione, inserimento o cancellazione anche di un solo bit) apportata. In altre parole saranno acquisiti i dati provenienti dal sito W ed in tempo reale saranno prodotte tutte le informazioni atte a garantirne l’integrità (copia conforme) nel tempo. In questo modo gli inventori intendono ricostruire anche per le evidenze acquisite on-line, la proprietà di “*absolute write-blocking*” ben consolidata per evidenze fisiche come un disco di un computer sequestrato dalla PG.

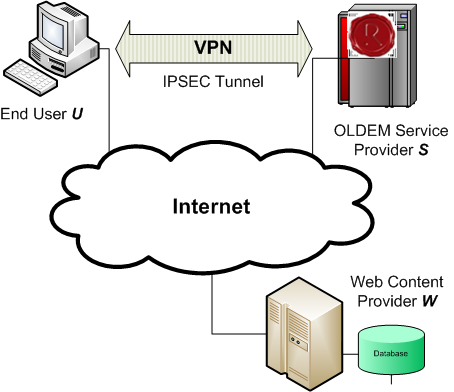
Lo schema è illustrato nella figura seguente:

Figura : Schema degli attori e delle interazioni

Restando ad un alto livello di astrazione il servizio S agisce come un Proxy Trasparente[[5]](#footnote-5) reindirizzando tutto il traffico proveniente dall’utente U verso la destinazione W scelta dall’utente e contemporaneamente rindirizzando tutte le risposte provenienti da W verso l’utente U.

In questo modo l’utente U può navigare il sito target W esattamente come se fosse direttamente connesso ad internet senza l’intermediazione di S.

Agendo come proxy il servizio S potrà acquisire tutti i pacchetti provenienti da U e destinati a W o quelli provenienti da W e destinati a U. Attraverso network utility standard sarà possibile isolare il traffico tra S e W filtrando i valori presenti nei campi degli header IPv4 e TCP. Infatti ogni pacchetto contiene nell’header IPv4 l’indirizzo sorgente e l’indirizzo destinazione (cf Figura 2: struttura dell'header IPv4). Nell’header TCP (cf. Figura 3: struttura dell'header del pacchetto TCP) invece saranno riportate le porte (end-point del servizio) che identificano la stream dati da acquisire.

Il pacchetto TCP rappresenta l’unità informativa di base che il protocollo IP (internet protocol) definisce per lo scambio di informazioni attraverso la rete Internet. Utilizzando il modello ISO/OSI il pacchetto dati TCP è collocato al quarto livello (trasporto) e prescinde quindi dal particolare schema di interconnessione del servizio S alla rete pubblica (router/gateway G).

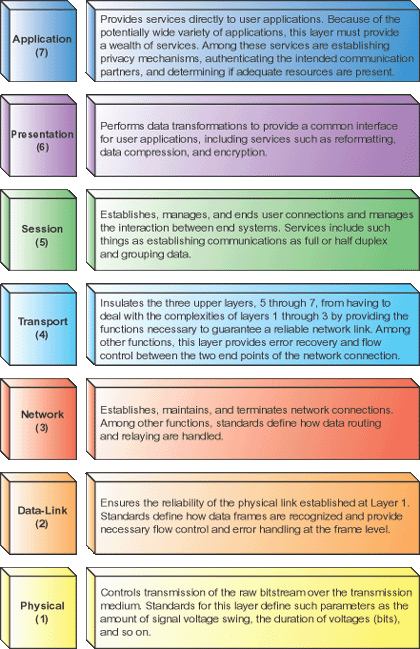
Tutti i pacchetti TCP che nell’header IPv4 (cf figura header TCP e header IPv4) avranno come sorgente o come destinazione l’indirizzo di W saranno catturati (acquisiti localmente) e comunque regolarmente inoltrati alla destinazione originale (al sito W come request o all’utente U come response).

Figura : Scomposizione in livelli dei moduli di rete secondo il modello ISO/OSI

Durante l’intero processo di acquisizione per ogni pacchetto P sarà prodotta una sorta di impronta digitale calcolando il valore di una funzione di hash (SHA256) sul contenuto dell’intero pacchetto P. In generale sarà calcolato il valore della funzione:

Fn = SHA256(Pn+Fn-1)

F0 = è un valore casuale generato dal servizio S.

Quando l’utente U avrà terminato la navigazione, l’ultimo valore prodotto Fx da questo processo sarà utilizzato per il calcolo della firma digitale dell’intera stream, legalmente valida secondo le vigenti norme. A partire dall’ultimo valore della funzione di hash ed il certificato digitale contenente la chiave privata del servizio S sarà calcolata il valore della firma digitale ed il risultato sarà salvato secondo lo standard CADES.

Inoltre sarà apposta una marca temporale rilasciata da una time stamping autority per certificare il tempo (data ed ora) in cui è avvenuta la navigazione registrata nel file raw.

Sono stati resi disponibili anche gli strumenti per verificare l’integrità ex post della stream salvata rispetto al valore finale della firma digitale ed ai valori dei singoli pacchetti (per identificare eventualmente quali hanno causato la difformità).

L’hash corrente ed il pacchetto verranno salvati in un file raw secondo un formato proprietario definito dagli inventori.

Dopo il calcolo della firma verrà prodotto un pacchetto (archivio digitale su supporto magnetico) contenente il risultato di comandi che potranno documentare il corretto funzionamento dei servizi di rete utilizzati da S (whois, ping, traceroute, nslookup, ecc.) al momento dell’acquisizione della stream.

E’ stata inoltre prevista la possibilità, attraverso un plugin da installare presso l’utente, di catturare anche tutto ciò che viene visualizzato nel browser dell’utente U. In questo modo verrà creato un flusso di ritorno attraverso il quale l’utente potrà evidenziare le parti salienti della navigazione che riportano l’evidenza in corso di acquisizione, per semplificare la ricerca evidenziando direttamente nell’indice la natura dell’evidenza.

L’intero pacchetto sarà poi inviato in maniera telematica all’utente U che potrà verificarne l’integrità, la validità della firma digitale ed i valori della dalla marca temporale.

A partire dal file raw, sarà inoltre possibile, attraverso una utility (player) disponibile presso il l’erogatore del servizio S, visualizzare il contenuto dell’intera navigazione estraendo il flusso http e visualizzando i contenuti attraverso un interprete HTML.

# Dettagli tecnici del processo

Proprietà del sistema:

* P1: Insieme al contenuto saranno raccolte tutte le evidenze (indirizzo IP, IP path, autonoumus system, ecc.) atte ad identificare (univocamente) il server dal quale vengono copiati i contenuti. Sebbene sia possibile forgiare un indirizzo IP la sua accessibilità sulla rete pubblica dipende da molteplici fattori che si propagano lentamente attraverso Internet per cui conoscendo l’indirizzo IP è possibile risalire attraverso l’Internet registry al responsabile del gruppo di indirizzi pubblici a cui questo appartiene.
* P2: tutto il traffico sarà catturato / acquisito senza che il provider S (e nessun altra entità) possa avere la possibilità di intevernire modificando il flusso dei dati alterandone i contenuti. Benchè terza parte fidata anche l’erogatore del servizio nell’ambito del processo descritto non potrà produrre dati falsi (alterati).
* P3: Dal flusso catturato deve essere possibile visualizzare i contenuti con strumenti standard (HTML interpreter anche di terze parti)
* P4: La copia digitale dei contenuti avrà valore legale, quindi secondo le leggi vigenti in ogni paese dovrà essere firmata digitalmente in accordo alla procedure previste. In molti casi il formato di firma è già prestabilito per legge (CADES, PADES, ecc.) ed include una marcatura temporale.
* P5: In un qualsiasi tempo successivo all’acquisizione sarà possibile verificare l’integrità del flusso, della firma digitale apposta dal servizio e della marca temporale rilasciata da una time stamping authority.

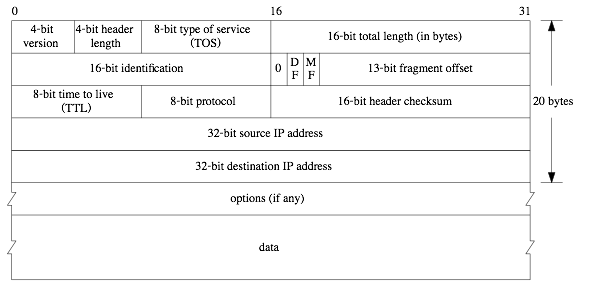


Figura : struttura dell'header IPv4

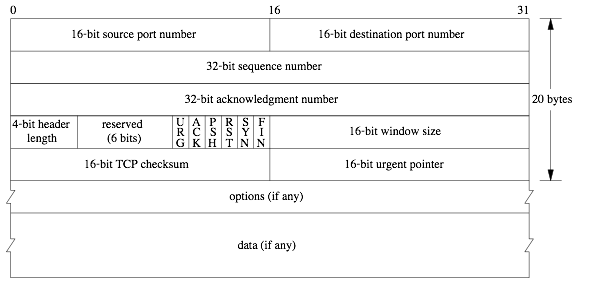


Figura : struttura dell'header del pacchetto TCP



# Open Issues

Come faccio se la connessione è https ?

Dettagli della connessione al proxy se è remoto rispetto all’utente U … è sufficiente avere un VPN?

On-Line Digital Evidence Acquisition

1. Cass. Pen. Sez. V, 17 novembre 2000, RFI, 2001, voce “ingiuria”, n.32 [↑](#footnote-ref-1)
2. Cass. Civ,. Sez. lavoro 16 febbraio 2004, n. 2912 [↑](#footnote-ref-2)
3. Art. 18 del DPR n.445/2000 [↑](#footnote-ref-3)
4. La copia conforme di una pagina web: natura giuridica e modalità operative, in Commissione Studi di Informatica Giuridica 11 maggio 2007, di Arcella e Valia in Consiglio Nazionale del Notariato [↑](#footnote-ref-4)
5. Secondo la definizione comunemente accettata e fornita nella RFC 2616: "*A 'transparent proxy' is a proxy that does not modify the request or response beyond what is required for proxy authentication and identification*" [↑](#footnote-ref-5)