Copia certificata conforme

La copia conforme di una pagina web

di UGO BECHINI 1

La realizzazione della copia conforme di una pagina web deve fare i conti con numerosi potenziali tranelli, alcuni dei quali forse inattesi per molti operatori. Si tenta qui una rassegna, a cavallo del poco decifrabile confine tra informatica e diritto, delle questioni cui dare soluzione onde assicurare la massima giuridica attendibilità della copia, anche in vista di un suo impiego in giudizio.

Sempre più frequentemente, i notai sono richiesti di formare copie conformi di pagine web, allo scopo di fissare in un documento stabile il contenuto che una determinata pagina ha in un dato momento. L'interesse che muove il richiedente può ovviamente essere il più vario, e non ne tenterò qui dunque neppure un parziale repertorio, che rischierebbe di essere ridicolizzato dalla sterminata fantasia che la pratica sa infallibilmente dimostrare.

Non vi sono perplessità di fondo sulla legittimità di una tale operazione 2. La pagina web è sicuramente un documento informatico, secondo la definizione del d.lgs. n. 82/2005 (Codice dell'amministrazione digitale), art. 1: la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti 3. L'esecuzione di copie del documento informatico è prevista all'art. 23: i duplicati,

---

1 Un ringraziamento per i preziosissimi suggerimenti è dovuto ai colleghi notai Enrico Santangelo, Sabrina Chibbaro e Gea Arcella, nonché agli ingegneri Pasquale Starace e Luigi D'Ardia di Notartel s.p.a., società di informatica e telematica del notariato italiano. Errori ed inesattezze, anche sotto il profilo tecnico informatico, restano comunque di mia esclusiva responsabilità.

2 Che compare infatti anche nell'autorevolissimo *Formulario Notarile Commentato* di Gaetano Petrelli (Milano 2001), vol. I, 61.

3 Entrerà in vigore il primo gennaio 2006. Per un primo commento G. Cassano – C. Giurdanella (a cura di), *Commentario al Codice dell'amministrazione digitale*, Milano, 2006; nel frattempo vige la norma (con identico contenuto) del d.P.R. n. 445/2000, sempre all'art. 1.

le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge, se conformi alle vigenti regole tecniche 4.

Il riferimento alle regole tecniche non può sicuramente essere letto come una preclusione all'impiego del supporto tradizionale 5. La legislazione, comprensibilmente, ha sinora concentrato la sua attenzione sulla possibilità di realizzare copie informatiche (di originali informatici o cartacei che siano), lasciando in ombra le copie su carta, ma non si è certo così inteso porre il documento tradizionale in posizione subordinata rispetto a quello elettronico.

A dispetto di quella che potrebbe essere la prima impressione, lo sviluppo della documentazione elettronica porta con sé l'esigenza di far transitare i documenti non solo dalla carta verso il digitale, ma anche a ritroso. Un primo esempio è quello appena accennato: non v'è dubbio che la copia di una pagina web possa realizzarsi anche su supporto informatico, ma è evidente che un documento cartaceo può rivelarsi prezioso in più di un'occasione.

Non mancano altre ipotesi. Se è pacifico, ad esempio, che una procura per vendere un immobile può essere autenticata da un notaio in forma digitale 6 e trasmessa via posta elettronica conservando il suo pieno valore giuridico, è altrettanto pacifico 7 che la procura dovrà essere obbligatoriamente allegata all'atto pubblico di compravendita. Atto pubblico che, secondo le più accreditate opinioni 8, al momento non potrà che avere forma cartacea; anche quando la possibilità di rogare atti pubblici *paperless* sarà definitivamente consolidata nel nostro ordinamento con la risoluzione dei problemi che ancora la ostacolano 9, difficilmente potrà pensarsi di imporre tale modalità alla controparte sprovvista di firma digitale o che semplicemente non desideri utilizzarla in un simile contesto. Occorre dunque (ed occorrerà anche in futuro) eseguire una copia su carta della procura elettronica, operazione resa alquanto complessa dalla natura intrinseca della firma digitale 10.

---

4 Tenore appena diverso aveva l'art. 20 del d.P.R. n. 445/2000 (vedasi alla .nota precedente): i duplicati, le copie, gli estratti del documento informatico, anche se riprodotti su diversi tipi di supporto, sono validi a tutti gli effetti di legge se conformi alle disposizioni del presente testo unico.

5 Volendo muoversi a fil di paradosso, anche la documentazione cartacea ha le sue regole tecniche, e quelle per la dattiloscrittura dettate dall'allegato 1 del d.P.C.M. 3 agosto 1962 sono ad esempio di una meticolosità (e di un livello d'approfondimento tecnico) che non teme confronto.

6 Art. 21 del d.P.R. n. 445/2000, art. 24 del d.lgs. n. 82/2005 (vedasi a nota 2).

7 Art. 51 della legge not. (10 febbraio 1913, n. 89).

8 Si veda per tutti l'attenta indagine di S. Chibbaro, in AA.VV., *Firme elettroniche: questioni ed esperienze di diritto privato* (Milano 2003) pag. 104.

9 Non è pensabile, ad esempio, lasciare all'iniziativa del singolo notaio le modalità di conservazione della raccolta degli originali digitali, considerato tra l'altro che al termine dell'attività del pubblico ufficiale la raccolta deve essere presa in consegna dall'Archivio Notarile, che da quel momento diviene competente per il rilascio delle copie: una qualche standardizzazione delle procedure e dei supporti è indispensabile.

10 In materia resta insostituibile la trattazione di R. Zagami, *Firma digitale e sicurezza giuridica*, Padova 2000. La firma digitale si basa, in ultima analisi, su un equilibrio matematico tra testo e firma, la cui verificabilità si perde con la stampa. Non è

Copia semplice e copia conforme

Nel negare rilevanza processuale ad una copia semplice di pagina web, la Suprema Corte rilevava 11 che "le informazioni tratte da una rete telematica sono per natura volatili e suscettibili di continua trasformazione e, a prescindere dalla ritualità della produzione, va esclusa la qualità di documento in una copia su supporto cartaceo che non risulti essere stata raccolta con garanzie di rispondenza all'originale e di riferibilità a un ben individuato momento".

La copia conforme appare dunque la soluzione del problema 12. Sul piano operativo, alcuni snodi non presentano particolari incertezze. La competenza all'esecuzione della copia spetta (articolo 18 del d.P.R. n. 445/2000) a notaio, cancelliere, segretario comunale, o altro funzionario incaricato dal sindaco. La copia di una pagina web sarà principio di prova per iscritto, ai sensi dell'art. 2717 c.c. 13. Il passaggio più delicato è rappresentato dal contenuto dell'attestazione di conformità 14 eseguita dal Pubblico Ufficiale; a questo argomento sono dedicate le righe che seguono, cui la Cassazione, con il brano appena riportato, regala un'intelligente *road map***.** Si farà innanzitutto riferimento alla copia su carta, riservando poi un apposito paragrafo alle peculiarità della copia in forma digitale.

L'orario

La variabilità nel tempo delle pagine web impone sicuramente che il Pubblico

---

esagerato dire che, una volta stampato, il documento non è più firmato. Per questo problema sono state proposte soluzioni come ad esempio *Paper e-Sign,* ma nessuna è ad oggi uno standard affermato. Sia consentito a questo proposito rinviare a Bernard Reynis ed Ugo Bechini, *La firma digitale transfrontaliera dei notai: una realtà europea*, in *Notariato*, 2004, 6, 573, simultaneamente apparso in lingua francese (*La signature électronique transfrontalière des notaires: une réalité européenne)*, ne *La Semaine Juridique, éd. n. & I.*, 2004 (39) 1447. La soluzione colà proposta dall'autorevole specialista francese (ora anche *incoming President* del notariato transalpino) e da chi scrive, consiste nell'esecuzione della verifica della firma da parte del notaro ricevente; il testo della procura potrà poi essere stampato, con aggiunta di una certificazione di conformità che documenti modalità ed orario della verifica stessa. Il notariato europeo sta attivamente lavorando affinché questa forma di circolazione del documento notarile possa decollare a livello continentale; le firme digitali dei notai italiani sono all'uopo da tempo verificabili presso il sito (non a caso multilingue) *http://ca.notariato.it*.

11 Cassa., sez. lav., 16 febbraio 2004, n. 2912, in *Giur. it.*, 2004, 1355, con nota di R. Bernardoni, *Copia di una pagina web e sua valenza processuale*. Si veda anche il commento di A. Monti, *La stampa di un pagina web non costituisce una prova*, in *Interlex* (*www.interlex.it*) 18 marzo 2004.

12 In tal senso espressamente A. Monti, in chiusura del contributo citato alla nota precedente.

13 Non si versa infatti in nessuna delle ipotesi disciplinate dagli artt. dal 2714 al 2716. Non che queste siano estranee all'area del documento informatico: le copie autentiche digitali degli atti conservati dal Pubblico Ufficiale, ad esempio, fanno fede come l'originale, allo stesso modo del loro equivalente cartaceo. E non si tratta di un'esercitazione teorica: ai soli Registri delle Imprese i notai italiani ne trasmettono ogni anno oltre 700.000.

14 Il documento/copia, qualunque sia l'oggetto ed il supporto utilizzato, deve evidentemente articolarsi nella riproduzione dell'originale ed in una ben distinta attestazione del Pubblico Ufficiale che certifichi la conformità della copia.

Ufficiale indichi con precisione l'orario di esecuzione della copia; trattandosi di una dichiarazione promanante dal Pubblico Ufficiale, avrà pieno valore fidefacente. E' opportuno che l'ora sia sempre ripetuta in formato GMT 15, soprattutto se si considera che siti italiani possono essere tenuti in linea presso macchine collocate in tutt'altra parte del mondo.

L'identificazione della pagina di cui eseguire copia

A prima vista la questione potrebbe apparire peregrina: ogni pagina è identificata da un indirizzo nel ben noto formato del tipo *http://www.ipsoa.it*. In realtà le cose stanno in modo un poco diverso. Sulla Rete le macchine sono contraddistinte da indirizzi numerici, i cosiddetti IP (qualcosa del tipo 86.116.116.232). Quando digitiamo il nome di un sito, il nostro apparecchio interroga automaticamente appositi computers, i cosiddetti server DNS, che si incaricano di "tradurre" l'indirizzo da noi digitato nell'indirizzo IP corrispondente; l'indirizzo numerico viene trasmesso al nostro apparecchio, che può così raggiungere la pagina desiderata. L'architettura complessiva del sistema DNS è estremamente articolata, e pone ai nostri fini più di un problema.

Siti molto frequentati sono spesso attivi simultaneamente su più indirizzi IP: è ad esempio del tutto normale trovare il sito della CNN operativo su otto diversi IP contemporaneamente 16. Non è però detto che l'aggiornamento sia sincronizzato in maniera perfetta. Il che significa che la medesima pagina (in ipotesi: cnn.com) vista da punti diversi della Rete, potrebbe avere contenuti diversi.

Va poi osservato che i server DNS si contano a milioni: forse nove, secondo una stima 17. In linea di massima ogni *provider* ha il suo, ad uso dei propri clienti; il loro livello di sicurezza è, a voler essere particolarmente generosi, variabile. Non è impossibile per un pirata 18 alterare un determinato *server* DNS: tutti gli utenti di quel sistema, digitando (ad esempio) *www.ipsoa.it*, non si troveranno sul sito dell'editore di questa Rivista ma su una pagina creata dal pirata a suo totale piacimento 19.

---

15 Greenwich Mean Time: questo è lo standard universalmente applicato al documento informatico. Anche il sistema di documentazione informatica del notariato italiano utilizza, ovviamente, solo orari GMT, per documentare scadenza del certificato, orario delle operazioni di firma ed orario di emissione della CRL (Certificate Revocation List): una dimostrazione pratica è disponibile presso il sito del Comitato Francoitaliano del Notariato LP, alla pagina *web.tiscali.it/conoge/test*. Il GMT non va confuso con l'orario corrente in Gran Bretagna: anche quando in quel Paese entra in vigore l'ora legale, il GMT resta invariato.

16 Ed accade pure che più macchine condividano un medesimo indirizzo IP.

17 Di Dan Kaminsky, riportata da Joris EVERS, *DNS servers, an Internet Achilles' heel*, in *CNET News.com*, 3 agosto 2005.

18 E' il cosiddetto *DNS poisoning*; si veda più in dettaglio, oltre all'articolo di cui alla nota precedente, C. Bieve, *Poisoned web poses risk to security*, in *New Scientist*, issue 2496, 23 aprile 2005, 25.

19 Si noti che per far ciò non occorre attaccare il sito che si desidera simulare: la deviazione è operata a monte. Se questa tecnica fosse ad esempio utilizzata per creare

Un nuovo potenziale fattore di rischio deriva dalla recente possibilità di utilizzare nella denominazione dei siti anche caratteri non latini. L'apertura verso culture diverse da quella occidentale merita il massimo apprezzamento; purtroppo è pure divenuto tecnicamente possibile 20 creare ad esempio il sito *www.abc.com*, ben distinto da *www.abc.com*, sol che si abbia l'accortezza di usare come "c" la lettera dell'alfabeto cirillico (che corrisponde foneticamente alla nostra "s") anziché quella latina: per il computer sono caratteri diversi anche se tra loro graficamente indistinguibili 21.

Anche senza pensare ad ipotesi dolose, resta il fatto che l'aggiornamento dei dati contenuti nei server DNS non è istantaneo: i ritardi si misurano in ore. E' quindi del tutto normale che per un certo tempo due diversi server DNS "puntino" per la medesima pagina a due diversi indirizzi IP, e quindi a due macchine diverse che possono restituire pagine dal contenuto differente 22. Per ulteriore complicazione, i risultati degli interpelli DNS sono conservati per un certo tempo dal nostro computer: si evita così di riproporre troppo di frequente al sistema le medesime interrogazioni, ma può anche capitare di utilizzare indirizzi non aggiornati.

Per le ragioni cui accennerò al termine di queste righe, non è mia intenzione proporre indicazioni troppo rigide; mi limito ad annotare che l'inserimento nella certificazione di conformità dell'indirizzo IP della pagina consultata sembrerebbe una soluzione semplice ed appropriata a questo genere di problemi. Il dato è facilmente acquisibile: il *browser* Firefox, ad esempio, ha un'apposita estensione, detta ShowIP, che una volta installata visualizza costantemente l'indirizzo IP delle pagine che si visitano. In alternativa si può anche pensare di eseguire una consultazione manuale del *server* DNS 23 ed introdurre poi manualmente nel *browser* 24 l'indirizzo numerico così ottenuto, indicando il tutto nella

---

un clone del sito *www.xxx.it* contenente frasi diffamatorie ai danni di qualcuno, una copia conforme della pagina che ne attribuisse *sic et simpliciter* il contenuto a www.xxx.it conterrebbe un'inesattezza grave: al titolare del sito non potrebbe neppure addebitarsi la mancata predisposizione di adeguate difese, atteso si tratterebbe di un attacco compiuto su macchine interamente fuori dal suo controllo.

20 Si tratta del cosiddetto *Internationalized Domain Name (IDN) homograph spoofing:* si veda in argomento la posizione adottata dall'ICANN il 23 febbraio 2005 (*http://tinyurl.com/cnuz3*). A scopo dimostrativo è stato creato un falso sito www.paypal.com che sfrutta la vulnerabilità descritta nel testo giocando sull'omografia delle "a" cirillica e latina. L'esempio non è stato scelto a caso: Paypal si occupa, come è noto, di trasferimento di fondi. Le due pagine hanno ovviamente indirizzi IP diversi.

21 Il rischio qui è concretamente modesto, anche grazie alle contromisure adottate dai produttori dei *browsers*. Va poi osservato che si rischia concretamente di cadere nella trappola solo laddove si segua un *link*, non quando si compone il nome della pagina desiderata su una tastiera latina. L'ipotesi è però meno inverosimile di quanto appaia a prima vista: immaginiamo che il richiedente inoltri al Pubblico Ufficiale una e-mail contenente la richiesta di copia, e che il destinatario si limiti a cliccare sull'indirizzo contenuto nella e-*mail* anziché ridigitarlo. Non occorre immaginare che il richiedente adoperi malizia: molto semplicemente, può essere stato a sua volta vittima dell'inganno.

22 La corrente (17 settembre 2005) voce *DNS* su *Wikipedia* è sul punto sintetica ed efficace: *not everyone is necessarily seeing the same thing you're seeing (*non è detto che tutti vedano quel che vedi tu*).*

23 E' per lo più sufficiente digitare dalla riga di comando *nslookup*, seguito da uno spazio e dal nome del sito desiderato.

24 Se ad esempio l'interrogazione DNS per *www.notariato.it* ha restituito l'indirizzo

certificazione 25. Vi sono poi indirizzi cui non corrisponde un vero e proprio sito, ma che servono da semplice reindirizzamento verso pagine altrove collocate 26. In tal caso appare consigliabile far constare della circostanza, riportando nella certificazione sia i dati del sito virtuale che quelli del sito effettivo.

Inutile illudersi di esaurire il novero dei tranelli che la tecnologia può riservarci, ma rimane almeno un interrogativo, che apparirà forse bizzarro: come può essere sicuro il Pubblico Ufficiale che la pagina che si accinge a certificare viene davvero da Internet? La questione emerge in relazione ad un paio almeno di situazioni tipiche.

Le pagine web vengono abitualmente archiviate da ogni singolo computer in una porzione della memoria detta *cache*; il rischio è di prendere per attuale una pagina che nel frattempo è stata modificata. La soluzione è fortunatamente assai semplice: procedere al cosiddetto *refresh* della pagina, operazione per la quale tutti i browsers hanno un apposito comando.

Ma vi è un profilo forse meno ovvio. Internet, a rigore, non è propriamente una rete, ma una rete di reti. Moltissimi servizi posseggono risorse proprie, che non appartengono tecnicamente ad Internet. Un esempio. La quasi totalità dei notai italiani dispone di un accesso ad una rete dedicata, detta Rete Unitaria del Notariato (RUN). Dal suo studio, il notaio può accedere indifferentemente al sito interno di servizio (*www.notartel.it*) come a qualunque risorsa esterna (ad esempio: *www.ipsoa.it*) senza alcuna differenza percepibile. L'utente esterno non vede, all'indirizzo *www.notartel.it*, ciò che vede l'utente interno. A voler essere precisi, oggi non vede nulla, ma può benissimo darsi che Notartel s.p.a., che gestisce la RUN, decida di creare allo stesso indirizzo apposite pagine dedicate all'utenza esterna. Il notaio collegato alla RUN che realizzasse, senza nulla precisare, una copia conforme della pagina *www.notartel.it* fornirebbe un'informazione gravemente inesatta, in quanto certificherebbe dati visibili a lui ed ai suoi colleghi ma assenti su Internet, oppure (quel che è peggio) *diversi* da quelli presenti su Internet. Allo stesso modo, può ben capitare che la *homepage* di un *provider* abbia due versioni, una delle quali, più ricca di servizi, riservata ai propri clienti. Non c'è purtroppo un sistema semplice e sicuro per sapere se il sito che stiamo vedendo è una risorsa propria del servizio impiegato o è visibile da Internet. Appare qui altamente raccomandabile indicare almeno quale provider si sta usando.

Una relativa sicurezza sull'identità del sito raggiunto può maturarsi qualora l'accesso avvenga in modalità protetta, il cosiddetto protocollo *https*. I certificati che vengono impiegati in tali frangenti (e visualizzati dai *browsers*) sono però rilasciati da soggetti che non seguono standard di uniforme affidabilità 27: non si

---

IP 217.22.209.194, digitando questi numeri nella casella del browser ove di solito introdurremmo il nome del sito si raggiungerà direttamente il sito stesso.

25 L'accorgimento non funziona però quando più siti sono ospitati presso un solo IP.

26 E' il caso, ad esempio, del sito personale dell'estensore di queste note: www.bechini.net.

27 Per dirla con Matt Blaze *a commercial certification authority protects you from*

tratta dunque di informazioni che si possano acriticamente riprodurre nella dichiarazione di conformità. Si potrà però fare circospetta menzione dell'esistenza del certificato, riportando con attenzione estremi ed autorità emittente.

Se mai ve ne fosse bisogno, va annotato che non può neppure pensarsi di certificare l'assenza di una certa risorsa sulla Rete. Può ben accadere che si tratti di una disfunzione del particolare collegamento in uso.

Il contenuto del documento

Anche qui, la soluzione è apparentemente ovvia: si esegue una stampa, preferibilmente a colori, e se ne certifica la conformità alla pagina originale. Ma di nuovo, le cose non sono così semplici.

Molto probabilmente si ricorderà la vicenda [28] del rapporto USA a proposito del caso Calipari. L'operatore militare USA aveva creduto di cancellare alcune porzioni del documento, di cui non si voleva dare diffusione; in realtà le aveva semplicemente convertite in un testo nero su sfondo nero. A prima vista non si poteva ovviamente leggere alcunché, ma bastava il più banale dei taglia e incolla per trasportare altrove tutto il testo, porzioni oscurate comprese. Lo stesso può accadere con i *files html*, quelli tipici del web, con un'aggravante (se possibile): alcuni *browsers* [29] non mostrano a video i caratteri occultati, e li riproducono invece in fase di stampa [30]. Dinanzi ad una stampa dal contenuto diverso rispetto a quanto è apparso un istante prima sul monitor, il Pubblico Ufficiale sarà verosimilmente a disagio: qual è la soluzione da preferire per una copia conforme corretta? Includere *tout court* porzioni di testo che il navigatore medio non ha visto e non vedrà mai, o rimuovere le parole che si è inteso nascondere ma che nella pagina, bene o male, ci sono? In questi termini (ma vedasi *infra*) la domanda probabilmente non ha risposta: mi par certo, invece, che non abbia senso far dipendere la soluzione dal tipo di browser che si trova casualmente installato sul computer utilizzato dal Pubblico Ufficiale.

Qualcosa di analogo accade per i *links* ipertestuali. Se in un sito si legge ad esempio *Cliccate qui per conoscere un vero criminale*, l'effettivo significato della frase risulta del tutto incomprensibile se non si conosce la destinazione del link stesso: si può andare dalla più neutra delle ovvietà (poniamo che si tratti della foto di Pol Pot) alla satira violenta ma forse talora lecita, alla diffamazione pura, o persino all'autoironia. La pratica del *linking* può avere pesanti implicazioni nel

---

anyone whose money they refuse to take (un'autorità commerciale di certificazione vi protegge solo da coloro il cui denaro l'autorità stessa rifiuta); citazione tratta da Wes KUSSMAUL, *Technological solutions and private sector initiatives*, relazione al ITU/EU (ENISA) Regional Seminar on Cyber Security for CEE, CIS and Baltic States, Riga 25/27 maggio 2005 (in formato pdf: *http://tinyurl.com/93xnj*).

28 Lo scivolone in cui incorsero le forze armate americane venne scoperto da G. Neri il primo maggio 2005 (*http://tinyurl.com/96m2f*).

29 Ad esempio Microsoft Internet Explorer, almeno nelle versioni da me provate.

30 Un semplice esempio è disponibile alla pagina *http://tinyurl.com/co783.*

campo del diritto commerciale ed industriale, soprattutto nelle varianti dette *deep linking* e *framing* 31. La stampata è qui del tutto inutilizzabile, dato che la risorsa verso la quale è operato il link non appare. Neppure appaiono alcune porzioni come ad esempio i cosiddetti *meta-tags*, che possono essere impiegati (anche se con minor efficacia che in passato) per attirare traffico dai motori di ricerca, magari sfruttando abusivamente la popolarità di un marchio concorrente 32.

Ancora. Le pagine *web* possono incorporare elementi extratestuali, fondamentali per l'intelligenza del loro contenuto; immagini, suoni ed anche animazioni, come ad esempio le persino troppo diffuse presentazioni Flash. Talora anche porzioni di testo sono introdotte in pagina come file di immagine, per ottenere particolari effetti grafici. Se una stampata può rendere in maniera lineare un'immagine ed il suo ruolo nel contesto della pagina, altrettanto certo non può dirsi di un'animazione, per non parlare poi degli elementi sonori.

Da ultimo: ogni *browser* ha un suo peculiare comportamento sul piano grafico, che per di più è in qualche misura personalizzabile dall'utente. Nella maggior parte dei casi le variazioni sono irrilevanti, ma alcune pagine sono rese in maniera clamorosamente diversa da *browsers* differenti, nessuno dei quali ha uno status che consenta di attribuire alla sua peculiare risposta grafica un crisma di ufficialità o priorità qualsivoglia. E si potrebbe continuare, discorrendo di *plug-in*, funzioni Java, ActiveX e quant'altro.

Quali conseguenze operative trarne?

---

31 Con il *deep linking* un sito rinvia direttamente ad una pagina interna di un altro sito, anziché alla *homepage*: in tal modo si richiamano risorse altrui senza che l'utente segua il normale percorso all'interno del sito che le contiene. Chi pone gratuitamente in Rete materiale per il quale ha sostenuto un costo, facendo affidamento sul ritorno pubblicitario delle pagine di avvicinamento, ha in effetti più di una ragione per combattere il *deep linking*, che è invece comunemente ammesso quando è diretto verso siti non commerciali. Con il *framing*, il contenuto altrui viene addirittura avvolto nella grafica del sito di partenza, che se ne appropria dunque in modo ancora più evidente. Dettagliata trattazione di queste pratiche, con riferimenti giurisprudenziali, in E. Tosi, *Le responsabilità civili*, in AAVV, *I problemi giuridici di Internet*, Milano 2003, tomo I, 536.

32 Le parole contenute nei *meta-tags* non vengono visualizzate dal browser, ma erano impiegate (e tuttora forse lo sono, ma certamente in misura molto più ridotta) dai motori di ricerca per classificare il contenuto delle pagine, così da poter poi indirizzare gli utenti verso i siti che loro interessano. Ma se la società Advanced Concepts introduceva tra i *meta-tags* del suo sito il nome della concorrente Oppedahl&Larson, il motore di ricerca indirizzava verso la *homepage* di Advanced Concepts anche quanti cercavano il sito di Oppedahl&Larson (il caso è reale, ed ha visto Advanced Concepts sostanzialmente soccombente nel 1997 dinanzi alla *United States District Court* del Colorado; Civil Action Number 97-CV-1592). I motori di ricerca sono oggi più sofisticati, e quindi è scemato l'interesse verso queste pratiche, ma negli anni passati alcuni casi approdarono alle aule di giustizia italiane: Trib. Roma, 18 gennaio 2001, in *Corr. giur.*, 2001, 1087, con nota di G. Cassano, *Meta-tag: il primo caso italiano*; Trib. Milano, 9 febbraio 2002, in *Corr. giur.*, 2002, 1607, con nota di S. Meani, *Possibili tutele contro l'uso distorto di termini corrispondenti a marchi altrui nei meta-tag dei siti web*. Vittime tipiche di queste manipolazioni erano ovviamente i marchi particolarmente noti e desiderati presso il popolo della Rete: non meraviglia quindi che nei repertori di giurisprudenza statunitensi il nome più ricorrente sia quello della Playboy Enterprises Inc.

Buona norma sarà indicare sempre nella certificazione quale browser si è usato (tipo e versione), su quale sistema operativo e, preferibilmente, marca e modello della stampante.

In alcuni dei casi indicati in questo paragrafo (le animazioni Flash sono l'esempio più ovvio), tale precauzione non sarà però sufficiente poiché, qualunque browser si adotti, la semplice stampata non potrà dirsi davvero riproduttiva dell'originale. La soluzione più a portata di mano sembra quella di ricomprendere nella copia anche il codice sorgente [33], che è la pura e semplice sequenza di dati trasmessa dal sito visitato, (per così dire) allo stato grezzo, a monte dell'elaborazione grafica operata dal browser installato sul computer dell'utente. A differenza della normale stampata della pagina, si tratta di un dato obiettivo ed univoco, indipendente dalle prestazioni del sistema funzionante presso il Pubblico Ufficiale, e comprenderà *links, meta-tags* e quant'altro. A sommesso avviso di chi scrive (ma si veda l'ultimo paragrafo) l'inclusione del codice sorgente appare prudenzialmente consigliabile come prassi standard. Non è semplice (ed anche alquanto soggettivo) stabilire se una pagina web contenga elementi suscettibili di dar luogo a riproduzioni a stampa variabili, incomplete o addirittura ingannevoli, e non pare opportuno che una simile valutazione (con correlativa responsabilità, sia detto en passant) sia compiuta dal Pubblico Ufficiale.

Con questo non si saranno sempre esauriti tutti i problemi. Una volta documentato ad esempio che il sito del notariato europeo (*www.cnue.be*) presenta in apertura l'introduzione Flash *www.cnue.be/test.swf*, il richiedente la copia potrà avere interesse a domandare al Pubblico Ufficiale di eseguire anche la copia di quest'ultimo file, senza la quale non si avrebbe alcuna indicazione sull'effettivo contenuto della sezione introduttiva del sito. Trattandosi di un'animazione, la copia non potrà che essere eseguita in forma digitale. L'indicazione dei *files* ulteriori di cui eseguire copia rientrerà, in tutta evidenza, nella esclusiva responsabilità del richiedente.

La copia in formato digitale

Nessun dubbio [34] sulla possibilità di eseguire una copia in forma elettronica; in qualche caso, come s'è visto, è anche l'unica via concretamente praticabile. Il notariato italiano è certamente più che attrezzato in tale prospettiva; basti considerare che i documenti firmati digitalmente dai notai ammontano a circa tre milioni all'anno. La copia dovrà comprendere il file originale, la dichiarazione di conformità in un normale piccolo file di testo, ed una firma digitale che suggelli entrambi. Il problema pratico consiste proprio nell'associare in maniera indissolubile il file originale e la dichiarazione di conformità. In attesa di migliori

33 Ricavabile con estrema semplicità dai migliori *browsers*. In Firefox, ad esempio, è sufficiente digitare Control U.

34 Secondo comma dell'art. 23 del d.lgs. n. 82/2005, già primo comma dell'art. 20 del d.P.R. n. 445/2000 (vedasi a nota 2). Nessuna delle altre fattispecie previste dal prosieguo dell'articolo si applica alla nostra fattispecie.

soluzioni, è probabilmente sufficiente utilizzare un formato noto e diffuso come ad esempio *zip* per creare un unico file, che li comprenda entrambi, cui apporre la firma digitale. Vi sono in prospettiva soluzioni più interessanti, come l'impiego del versatile formato *XML* 35.

Copia o perizia?

L'approccio fin qui seguito presta il fianco ad un'evidente obiezione. L'introduzione nell'attività di copia degli elementi tecnici cui si è fatto cenno rischia di trasformare una semplice attività di documentazione in una sorta di piccola perizia, cui (da un lato) il Pubblico Ufficiale non è qualificato, e che (dall'altro) non ha riscontro nella tradizione. Nel mondo reale ci si basa sulle risultanze dei documenti di identità; il notaio che dichiari che un certo atto è stato stipulato in Sergozzate al Monte, via Mazzini 11, si affiderà ai cartelli stradali e toponomastici. Perché mai, nel caso del web, si dovrebbero imporre al Pubblico Ufficiale ulteriori attività d'indagine?

La mia posizione sul primo punto è in verità molto banale: se si desiderano utilizzare nuovi mezzi, occorre conoscerne il funzionamento. Nelle scuole di notariato si usa ricordare che un tempo la preparazione per l'esame d'accesso alla professione comprendeva anche un'infarinatura sulle caratteristiche chimiche degli inchiostri. Qualunque Pubblico Ufficiale sa distinguere una penna da una matita e sa che la seconda non va impiegata per un atto pubblico: DNS e codici HTML fanno parte dell'ABC del documento informatico in Rete, sono la carta la penna e la matita di oggi. Con una decisiva riserva: la carta ha alle spalle un impiego stabilizzato nei secoli. Dinanzi a realtà così recente e complessa ed in così tumultuosa evoluzione 36, incertezze, prassi oscillanti o divergenti, e persino eventuali rifiuti del Pubblico Ufficiale hanno dalla loro plausibilità e legittimità.

Per quanto concerne la seconda questione, propongo un piccolo esperimento, da eseguirsi su un PC collegato in Rete. Da una finestra a riga di comando (o finestra DOS, o prompt dei comandi) si digiti *nslookup* seguito dall'indirizzo di un sito molto noto, ad esempio quello del New York Times: *nslookup www.nyt.com*. Premuto il tasto invio, il DNS risponde trasmettendoci i dati che ci occorrono ma aggiungendo quasi invariabilmente una precisazione che suona più o meno così: risposta da un server non di fiducia. Il sistema DNS ci sta insomma dicendo: *www.nyt.com* dovrebbe essere da quella parte, ma dato che l'informazione è ricavata da altro server di cui non ci si può fidare, non si assumono responsabilità: potreste trovarvi anche su un sito pirata. Buona navigazione. La stessa precisazione vale per il browser che usiamo tutti i giorni: anche se non ce ne dà avviso, il suo funzionamento dipende da quelle medesime informazioni. Se il

35 In questo senso si è già mosso il notariato spagnolo.

36 Quanti ricordano Gopher? Era forse il servizio più avanzato disponibile su Internet prima del World Wide Web; si accontentava di schermi monocromatici e permetteva di accedere solo a *files* di puro testo, che in sede di copia avrebbero certamente posto problemi più circoscritti! Sembra trascorsa un'era geologica, e sotto alcuni profili è così, ma si tratta di tre lustri appena.

Pubblico Ufficiale dichiarasse senza riserve che una certa pagina è la copia conforme di *www.nyt.com*, si troverebbe paradossalmente a certificare un elemento che è reputato non affidabile da parte dello stesso sistema che lo fornisce.

Nel mondo reale non regnano, è vero, certezze assolute, ma almeno i documenti di identità non recano scritto: il signore della foto forse è Mario Rossi. E non è molto semplice (sempre nel mondo reale) far sì che un notaio sia convinto di trovarsi a Milano mentre invece è a Roma; fargli credere di essere collegato al tal sito mentre invece si trova su un clone piratato è invece, come si è visto, alla portata di un *hacker* ben determinato.

Non va insomma mai sottovalutata la ricchezza del mondo reale, la varietà di risorse culturali ed antropologiche che compongono il quadro all'interno nel quale quotidianamente operiamo in sicurezza 37. Non si deve mai sottovalutare, di conseguenza, il livello d'attenzione che occorre per riprodurre nel mondo dell'informatica, lo standard di certezza cui, anche senza accorgercene, siamo abituati da sempre. Limitarsi a replicare su Internet i gesti del mondo reale significa ridurre drammaticamente il livello di sicurezza e certezza del nostro operato 38.

Non si tratta dunque di attribuire al Pubblico Ufficiale responsabilità e funzioni che non gli competono. Ben al contrario, si tratta di evitare 39 che attribuisca pubblica fede a riproduzioni parziali, soggettive od ingannevoli, ad elementi di cui non ha preso obiettiva conoscenza o, più semplicemente, falsi 40.

Conclusioni operative

Volendo tirare le fila del discorso, la mia posizione (che ovviamente impegna me soltanto) può essere così riassunta. In aggiunta alle indicazioni abituali 41 il

37 Illuminante a questo proposito Wes KUSSMAUL, *Quiet enjoyment: bring security with privacy to your networks and your life*, PKI Press, Weston (Massachusetts, USA) 2004. L'Autore è stato il fondatore di Delphi, il primo Internet *provider* commerciale al mondo. Alle bozze del lavoro di Kussmaul, cui ho avuto accesso grazie alla cortesia dell'Autore, ho ampiamente attinto per la mia relazione *Sicurezza tra mondo reale e virtuale*, presentata al XL Congresso Nazionale del Notariato, Roma 2004.

38 Ciò non vuol dire, naturalmente, che in Rete i pericoli siano sempre maggiori. Come R. Bernardoni (supra, nota 10) e moltissimi altri, proprio non so capacitarmi, ad esempio, del comportamento di quanti si rifiutano di usare la carta di credito sul sito protetto di una grande linea aerea, ma sono pronti a porgere senza batter ciglio la medesima carta di credito al meno affidabile dei venditori di tappeti (con tutto il rispetto per la categoria). La Rete presenta i suoi propri rischi, e non interessa stabilire se siano maggiori o minori di quelli tipici del mondo reale: occorre però analizzarli senza dar nulla per scontato.

39 Nell'interesse di tutti, Pubblico Ufficiale non escluso.

40 Si veda ad esempio il caso descritto a nota 18.

41 Articolo 18 del d.P.R. n. 445/2000: indicazione delle generalità, della qualifica e della sede del Pubblico Ufficiale, certificazione di conformità, numero di fogli impiegati, luogo e data.

Pubblico Ufficiale dovrà certamente indicare l'orario dell'operazione, tipo e versione del browser impiegato, sistema operativo e fornitore d'accesso utilizzato. Trovo inoltre raccomandabile indicare l'indirizzo IP e l'orario (anche) in formato GMT. E' consigliabile (soprattutto laddove gli elementi non testuali abbiano un ruolo determinante) che siano indicati marca e modello della stampante ed infine che la copia ricomprenda il codice sorgente. Qualora il sito sia provvisto di un certificato, se ne potranno riportare gli estremi.

Allo stesso tempo, però, occorre prendere realisticamente atto dell'estrema mutevolezza del quadro di riferimento, che impone di considerare provvisorio ogni risultato. La tecnica è in costante evoluzione: rischi che oggi ci preoccupano saranno presto dimenticati, e forse altri li rimpiazzeranno; il consolidarsi della prassi e del quadro normativo e giurisprudenziale offriranno nuovi punti di riferimento. Ma non v'è solo questo: è ancora in fase di assestamento il nostro modo di atteggiarci nei confronti dell'esperienza, relativamente nuova, di rapporti (anche giuridici) che vivono a cavallo del confine tra realtà fisica e virtuale. Il tempo si farà carico di disegnare i contorni della prassi corretta, e (mi auguro sinceramente) di qualificare come eccessive alcune delle preoccupazioni qui espresse. Per il momento, non mi sembra di sbagliare suggerendo prudenza: accuratezza e ricchezza di dettaglio non nuoceranno di certo, in giudizio od altrove, all'autorevolezza della copia certificata conforme.