2009 Workshop International
on ADR/ODRs
(Alternative / Online Dispute Resolution)
"Construint ponts: marc jurídic i principis"
Barcelona, Espanya, 15 de setembre 2009

Identificazione delle parti ed imputabilità degli atti giuridici nei sistemi ODR.

By Andrea Buti – Italy University of Camerino – ADR Center s.p.a. - email andrea.buti@adrcenter.it

L'utilizzo delle tecnologie della società dell'informazione e dei nuovi media in particolare, se da un lato offre ampie possibilità di creare nuove interazioni umane, nuovi rapporti giuridico-economici e nuove forme di espressione, dall'altro pone interessanti sfide giuridiche connesse al fatto che l'utilizzo di tali strumenti non trova una specifica e puntuale disciplina legale su alcuni aspetti peculiari del modo della rete internet.
L'ODR, non fa eccezione: al pari dei molteplici servizi offerti in via telematica presenta, infatti, delle criticità tipiche del web. In particolare vorrei occuparmi dei problemi connessi all'identificazione dei soggetti coinvolti nell'erogazione e nella fruizione di servizi di composizione on-line delle controversie e dell'imputabilità degli atti giuridici realizzatisi dal primo contatto e sino all'esito finale.

1. Identificazione del provider e dei litiganti

Innanzitutto occorre poter identificare il soggetto che eroga il servizio[1] e verificare la correttezza e veridicità delle informazioni eventualmente rese.
Ove il servizio coinvolga un soggetto che riveste la qualifica di "consumatore" ai sensi dell'art. 2, lett. e) direttiva 2000/31/CE (ossia: qualsiasi persona fisica che agisca a fini che non rientrano nella sua attività commerciale, imprenditoriale o professionale), tale possibilità diventa un obbligo ai sensi dell'art. 10 della medesima direttiva poichè tale norma dispone:
"*1. Oltre agli altri obblighi di informazioni posti dal diritto comunitario, gli Stati membri provvedono affinché, salvo diverso accordo tra le parti diverse da consumatori, il prestatore fornisca in modo chiaro, comprensibile ed inequivocabile, prima dell'inoltro dell'ordine da parte del destinatario del servizio, almeno le seguenti informazioni:*
a) le varie fasi tecniche della conclusione del contratto;
b) se il contratto concluso sarà archiviato dal prestatore e come si potrà accedervi;
c) i mezzi tecnici per individuare e correggere gli errori di inserimento del dati prima di inoltrare l'ordine;
d) le lingue a disposizione per concludere il contratto.
2. Gli Stati membri provvedono affinché, salvo diverso accordo tra parti diverse da consumatori, il

1 Tale termine è utilizzato nell'accezione fornita dalla Direttiva 1998/48/CE, alla quale fa espresso rinvio la Direttiva 2000/31(CE), che di seguito si riporta:
"*2) L'articolo 1 è modificato come segue: a) dopo il punto 1) è inserito il seguente nuovo punto 2)"servizio": qualsiasi servizio della società dell'informazione, vale a dire qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi. Ai fini della presente definizione si intende:*
— "a distanza": un servizio fornito senza la presenza simultanea delle parti;
— "per via elettronica": un servizio inviato all'origine e ricevuto a destinazione mediante attrezzature elettroniche di trattamento (compresa la compressione digitale) e di memorizzazione di dati, e che è interamente trasmesso, inoltrato e ricevuto mediante fili, radio, mezzi ottici od altri mezzi elettromagnetici;
— "a richiesta individuale di un destinatario di servizi": un servizio fornito mediante trasmissione di dati su richiesta individuale"

prestatore indichi gli eventuali codici di condotta pertinenti cui aderisce nonché come accedervi per via elettronica.
3. Le clausole e le condizioni generali del contratto proposte al destinatario devono essere messe a sua disposizione in un modo che gli permetta di memorizzarle e riprodurle."
Tale obbligo, però, non esiste se il soggetto che utilizza il servizio non è un consumatore, ma – nella terminologia utilizzata dalla Direttiva 2000/31/CE – un semplice "destinatario del servizio", ossia una "persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione".
Posto, quindi, che si ricada nell'ipotesi in cui esiste siffatto obbligo informativo, è da notare che come si tratti, pur sempre di informazioni non verificate e destinate – principalmente – ad operare sul piano del consenso, ossia a garanzia di trasparenza e correttezza nei confronti, appunto, della particolare categoria dei "consumatori".
Ma, nel mondo virtuale del web, è essenziale un altro aspetto: poter verifcare cioè che un soggetto che appare come in possesso di certe caratteristiche, le abbia realmente; sarebbe ben possibile, infatti, per un provider crearsi una certa e fittizia identità digitale con la quale offrire tutte le informative di legge: quale garanzia avrebbe però, in questo caso l'utente-consumatore? Uno dei fenomeni più allarmanti, figlio esclusivo della società dell'informazione, infatti, è quello del phishing[2]: un malintenzionato che si spaccia per una banca o un fornitore di un qualsiasi servizio web che, in realtà non è altro che un impostore che cerca di ottenere illegalemente dati personali o credenziali di autenticazione, come numeri di carta di credito, codic PIN o username, per effettuare "furti" su conti correnti bancari.
Insomma quale garanzia che il tale fornitore di ODR sia un soggetto davvero affidabile? E che, prima di tutto, sia proprio chi dice di essere? Il problema, infondo, è lo stesso che affligge il commercio elettronico e che non è stato risolto risolto legalemente, ma dal mercato: non ci sono in effetti troppe garanzie che il tale e-merchant sia davvero affidabile, ma nonostante questo il commercio elettronico mostra un trend in continua crescita. Probabilmente gli utenti iniziano con acquisiti di basso valore per "testare" l'affidabilità del venditore elettronico o verificanoil "feedback" assegnato da altri precedenti acquirenti, come accade per eBay.
Ma, nel caso dell'ODR c'è un problema ulteriore: se un acquisto elettronico non va a buon fine, il soggetto potrà aver perso dei soldi (nel caso di pagamento anticipato) e potrà agire per vie legali, ma il sistema del commercio elettronico, nel suo complesso, non subirà effetti negativi a livello di "immagine" ed affidabilità, poiché molti sono i negozi virtuali, ampia è la concorrenza e, in definitiva... tra molte mele buone, come si dice, una marcia può capitare; nel caso di un servizio ODR, invece, a cagione dell'estrema novità del sistema, si correrebbe davvero il rischio di minare sin dall'inizio la credibilità dell'intero sistema. In altre parole, considerata la delicatezza del servizio reso, viene il dubbio che sia desiderabile utilizzare uno standard superiore.
Individuare quale, non è semplice.
La soluzione tecnicamente preferibile sarebbe senz'altro quella di utilizzare certificati digitali rilasciati da terzi autorizzati dalle Autorità Statali, similmente a quanto accade nell'ambito delle firme elettroniche: i problemi maggori riguardano da un lato la "politica commerciale" e dall'altro l'interoperabilità.
Per l'identificazione dei litiganti valgono sostanzialmente le stesse considerazioni oltre a quelle che seguono.
Per la "certificazione" del sito attraverso il quale vengono offerti servizi ODR, si segnala il servizio reso da Verisign che, attraverso l'utilizzo di una connessione sicura (SSL) consente all'utente di verificare le reali generalità ed identitià del provider. Tale opportunità non è da sottovalutare considerata la crescita sempre più allarmante dei fenomeni di phishing.

2. Le firme elettroniche nell'ODR

2.1. Sotto il primo profilo è da notare come l'uso di firme elettroniche sia in genere limitato. Solo in alcuni settori è invalso l'uso di dispositivi come smart-card[3] o token USB, ad esempio per la

2 Phishing o fishing, letteralmente "andare a pesca" cercare,
3 Secondo dati forniti dal CNIPA (Centro Nazionale per l'Informatica nella Pubblica Informazione) in Europa dovrebbe

sottoscrizione dei bilanci delle società, per alcune operazioni bancarie (home banking) o per il compimento di atti notarili presso gli uffici pubblici che gestiscono iscrizioni o trascrizioni relativi ai diritti su beni immobili. Ammesso e non concesso che un utenza "professionale" (imprese e professionisti - solo alcuni invero -) possano essere in possesso della tecnologia necessaria, è innegabile che la categoria dei "consumatori" resterebbe esclusa dalla possibilità di accedere ai sistemi ODR che utilizzano tale sistema di *strong autenthication* (a meno che non si rivolgano ad associazioni di categoria o sindacati in grado di assisterli).

2.2. Inoltre dal lato delle controversie transfrontaliere (e con ancora maggiori difficoltà per quel che concerne le controversie internazionali con paesi extra UE) si pone il grosso problema dell'interoperabilità tra i diversi sistemi di firma elettronica.

La direttiva 1999/93/CE, peraltro, mira a definire un quadro europeo per le firme elettroniche semplici ed avanzate (in Italia firma digitale): queste ultime utilizzando un sistema PKI[4] con crittografia simmetrica presuppone l'utilizzo di una chiave privata nell'esclusiva disponibilità del titolare della firma e di una parte pubblica rilasciata e resa disponibile da un Certificatore. Tale sistema è attualmente quello tecnologicamente più affidabile considerato che utilizza algoritmi di cifratura (RSA 1024 o 2048 bit,) virtualmente inattaccabili.

Il problema è che tale sistema PKI non è pronto per essere interoperabile con i molteplici dispositivi presenti nei diversi stati (si pensi solo all'Unione Europea). Nonostante si utilizzino certificati digitali creati con un medesimo standard (ad esempio PKCS o X503), sono tutt'ora presenti diverse criticità, sia perchè gli standard sono norme che vanno comunue interpretate ed applicate secondo le peculiarità di ciascun ordinamento, lingua e cultura, sia perché vengono poi in concreto utilizzati *software* diversi e non testati per le diverse piattaforme (magari perché l'operazione non è economicamente conveniente) sia perchè alcuni caratteri tipografici (la dieresi di alcune lingue) potrebbe non essere riconosciuta o generare errori in sistemi in cui non sono solitamente usati.

3. Identificazione e autenticazione

Un altro problema di non poco conto è quello connesso all'identificazione del titolare del dispositivo di firma.

Nella sua versione "semplice", ossia quella definita all'art. 2 n.1 dela Direttiva 1999/93/CE come "*dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici ed utilizzata come metodo di autenticazion*e" essa non è pensata né progettata per identificare un soggetto, ma solo per conseguire una autenticazione a livello di sistema informatico per poter effettuare talune operazioni che richiedono determinati livelli di autorizzazione (credenziali di accesso e/o funzionali).

Per quel che concerne l'identificazione, bisogna quindi far riferimento all'altro tipo di firma elettronica, ossia quella avanzata di cui al n. 2 della citata Direttiva che, infatti la definisce come "*una firma elettronica che soddisfi i seguenti requisiti:*

essere connessa in maniera unica al firmatario;

essere idonea ad identificare il firmatario;

essere creata con mezzi sui quali il firmatario può conservare il proprio controllo esclusivo;

essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati".

Il panorama al riguardo, però, è molto frammentario[5]: ci sono Stati in cui il rilascio del dispositivo di firma digitale può avvenire – con scarsissime certezze circa la reale identità - anche on line a nome del soggetto che sta utilizzando ad esempio una certa carta di credito e Stati, invece, che rilasciano il dispositivo esclusivamente e personalmente al titolare, identificato o identificabile con documenti di identità o in altro modo. Ma nell'ipotesi delle firme elettroniche rilasciate a persone giuridiche la semplice identificazione personale potrebbe non essere sufficiente: sarebbe infatti

circolare qualche milione di firme digitali (quasi 4 milioni solo in Italia), www.cnipa.gov.it

4 Public Key Infrastructure, ossia un sistema in cui un terzo certificatore riconosciuto dall'Autorità Statale rilascia i certificati, consente le verifiche a chiunque e provvede alla relativa gestione.

5 Il rilievo è di D. Gassen e U. Becchini in *Diritto dell'informazione e dell'informatica*, n. 2/2009, p. 349.

necessario che il certificato desse certezza della sussistenza dei necessari poteri di firma e che quindi fosse certificata la posizione, qualifica e funzione del soggetto utilizzatore.
In Italia solo da poco, ad esempio, è stato introdotto il reato di false dichiarazioni al Certificatore, mentre in Giurisprudenza cominciano ad affacciarsi decisioni a tutela dell'identitià digitale: inviare una mail a nome di un altro soggetto integra, infatti, il reato di sostituzione di persona.
E' da segnalare che il notariato europeo (CNUE, www.cnue.be) sta lavorando ad un progetto per la verifica dei certificati *on line* da utilizzare con un qualsiasi *browser* per la navigazione internet al fine di superare gli ostacoli connessi all'utilizzo di diversi sistemi operativi o *software* applicativi. I risultati sono stati illustrati, tra l'altro, alla conferenza *Work on E-Justice*, tenutasi nel 2007 a Bremen (http:www.bmj.bund.de) ed hanno consentito di annoverare il progetto tra quelli di riferimento in un inizativa paneuropea sull'*e-Justice*, volta alla creazione di un portale internet[6].

4. L'imputabilità degli atti

I problemi connessi all'incertezza dei soggetti litiganti generano poi un ulteriore effetto: in mancanza di loro identificazione, a chi dovranno essere imputate le dichiarazioni o manifestazioni di volontà, o le negoziazioni *on line* ?
Poiché i comportamenti e le decisioni umani sono talvolta (per non dire spesso) determinati da valutazioni emozionali o irrazionali oppure sono in qualche misura influenzati da fenomeni psicologici (stress, barriere negoziali, paure, sospetti etc..) potrebbe ben accadere che una delle due parti in un momento successivo alla negoziazione dell'accordo ottenuto con un sevrizio ODR decida da “ripensarci”, magari disconoscendo la precedente manifestazione di volontà.
Se non si è effettuata una previa identificazione dei soggetti, diventa difficile imputare a soggetti determinati le dichiarazioni rese tramite servizi ODR, a meno che non esistano mezzi indiretti.
Tra questi si possono considerare (A) quelle informazioni rese in maniera automatica dai sistemi informatici e (B) la conoscenza di determinati informazioni, dati o circostanze che possono essere note solo ad certo soggetto. Tali mezzi indiretti potrebbero essere idonei anche sotto un profilo probatorio in un eventuale giudizio considerato che potrebbero in ogni caso essere in grado di fondare presunzioni semplici[7] invertendo magari l'onere della prova.
Sotto il primo profilo è infatti da considerare che ogni computer per comunicare con un web server trasferisce informazioni sul tipo di macchina utilizzata, il sistema operativo, il *browser*, il suo indirizzo IP, una serie di riferimenti temporali relativi alle sessioni di connessione: tutti dati che, associati anche all'utenza telefonica, possono fornire elementi indiretti o indizi anche se, in nessun caso potranno provare che tale macchina o utenza telefonica sono state utilizzate da una certa persona fisica. In ambito civile, però, potrebbe farsi anche riferimento alla responsabilità connesse alla custodia del sistema informatico o dell'impianto di telefonia: questo sarà possibile ad esempio nel caso in cui esista una legge specifica che imponga una custode diligenza delle credenziali di autenticazione al fine di scongiurare utilizzi impropri[8] del computer da parte di soggetti non autorizzati, come accade nell'ambito del trattamento dei dati in forza della previsione delle misure di sicurezza previste dalla Direttiva[9] 95/46/CE.

---

6 D. Gassen e U Becchini, *op. cit.,* p. 366.

7 V. art. 2729 c.c. italiano.

8 La Corte dei Conti, ad esempio, ha ritenuto responsabile un impiegato dell'amministrazione tributaria per non aver custodito digilentemente i proprio computer: “*Con atto di citazione, depositato in data 28 luglio 2004, il Procuratore Regionale ha convenuto in giudizio il sig. A.C., dipendente dell'Agenzia delle Entrate, Ufficio di Acireale, ritenendolo responsabile del danno erariale di euro 6.408,06, cagionato al Ministero dell'Economia e delle Finanze, in conseguenza dell'indebito sgravio di imposta operato il 30 novembre 2001 in favore della ditta Alfa, relativo ad imposta sul valore aggiunto, dovuta per l'anno 1994. Dagli atti dell'indagine ispettiva disposta dall'Amministrazione a seguito della rilevazione di anomalie nella effettuazione dello sgravio d'imposta, acquisiti dal magistrato requirente, risulta che la formalità era stata eseguita in assenza dei presupposti richiesti (domanda della ditta interessata e documentazione giustificativa), utilizzando il terminale protetto dalla “password” personale. Lo stesso convenuto, con dichiarazione resa il 29 settembre 2003 all'ispettore, pur negando di essere stato l'autore dello sgravio, ha, tuttavia, ammesso la propria responsabilità, per avere lasciato il terminale attivo, consentendo l'illecita effettuazione dello sgravio*”. Testo integrale disponibile su http://www.corteconti.it/Ricerca-e-1/Gli-Atti-d/cartella/Documenti/Sezione-gi20/Novit--giu/2005/Sentenza-n.390-2005-del-2-marzo-2005.doc_cvt.htm

9 L'art. 17 prevede, infatti che “*Gli Stati membri dispongono che il responsabile del trattamento deve attuare misure*

Anche sotto il profilo fattuale, comunque, la vicenda negoziale *on line* può fornire elementi dirimenti: una sentenza[10] della magistratura amministrativa, ad esempio, può fornire un interessante spunto.
Un ente pubblico, stazione appaltante, all'esito di una gara pubblica per l'esecuzioe di lavori ferroviari comunica con email semplici e senza utilizzare firme elettroniche all'aggudicatario i numeri di serie della carrozze ferroviare su cui effettuare dei lavori di ristrutturazione. Sotto un profilo civile tale comunicazione essendo attinente all'esecuzione degli obblighi contrattuali implica perfezionamento del contratto.
Successivamente la stazione appaltante annulla la gara e contesta di non aver mai concluso alcun contratto adducendo la non imputabilità ad essa delle email: i messaggi di posta elettronica, infatti, in mancanza di firme elettroniche, non possono in alcun modo essere riconducibili alla stazione appaltante. Il Giudice riconosce, però, che i dati comunicati erano dati riservati (numero di serie e caratteristiche delle carrozze su cui operare le lavorazioni) che presumibilmente potevano essere noti solo all'ente. I documenti informatici vengono, pertanto, imputati all'ente pubblico nonostante una speciefica norma imponesse l'uso di firme elettroniche (Codice dell'Amministrazione Digitale D. Lgs. 82/2005).

*tecniche ed organizzative appropriate al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'**accesso non autorizzati**, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete, o da qualsiasi altra forma illecita di trattamento di dati personali*".

10 T.A.R. Puglia, 21 febbraio 2008 n. 562, in http://www.teutas.it/giurisprudenza/tribunale-amministrativo-regionale/322-tar-puglia-sez-lecce-sentenza-n-562-del-21-febbraio-2008.html