

**Collana dell'Istituto per la documentazione giuridica
del Consiglio Nazionale delle Ricerche**
diretta da Nicola Palazzolo (direttore dell'IDG)

Serie «Studi e documenti», n. 2

Consiglio Scientifico dell'Istituto e della Collana

Onofrio Fanelli (*presidente*)
Bruno Caruso, Pierangelo Catalano
Costantino Ciampi (*responsabile attività editoriali*)
Maurizio Fioravanti, Mario Jori, Paola Mariani
Pietro Mercatali, Mario Ragona, Pierluigi Spinosa

Redazione

Istituto per la documentazione giuridica
del Consiglio Nazionale delle Ricerche
Via Panciatichi, 56/16
50127 FIRENZE
Tel.: 055-43995
Fax: 055-4221637
E-mail: collana@idg.fi.cnr.it
URL: <http://www.idg.fi.cnr.it/>

Amministrazione

Edizioni Scientifiche Italiane
Via Chiatamone, 7
80121 NAPOLI
Tel.: 081-7645443 *pbx*
Fax: 081-7646477
e-mail: info@esispa.com
URL: <http://www.esispa.com>

Istituto per la documentazione giuridica
del Consiglio Nazionale delle Ricerche

DOCUMENTO INFORMATICO FIRMA DIGITALE E COMMERCIO ELETTRONICO

a cura di
VITO RIZZO



Edizioni Scientifiche Italiane

Atti del Convegno
**«Documento informatico,
firma digitale e commercio elettronico»**
Camerino, 29-30 ottobre 1999

UNIVERSITÀ DEGLI STUDI DI CAMERINO
Scuola di Specializzazione in Diritto Civile
Centro Interdipartimentale in Diritto Civile Costituzionale

CONSIGLIO NAZIONALE DELLE RICERCHE
Istituto per la documentazione giuridica di Firenze

Con la collaborazione ed il contributo di:

Centro di Teoria dell'interpretazione "Emilio Betti"
Dottorato di ricerca in Diritto Civile Costituzionale
Istituto di diritto privato
Facoltà di giurisprudenza

Segreteria organizzativa del Convegno: Maria Concetta De Vivo (Univ. Camerino)
Revisione editoriale dei testi: Manola Cherubini (IDG-CNR, Firenze)
Editing e impaginazione: Simona Binazzi (IDG-CNR, Firenze)

Rizzo, Vito (a cura di)
Documento informatico, firma digitale e commercio elettronico
Collana: IDG, Serie «Studi e documenti», n. 2
Napoli, Edizioni Scientifiche Italiane, 2000
pp. 288; 24 cm
ISBN 88-495-0196-X

© 2000 by Edizioni Scientifiche Italiane s.p.a.
80121 Napoli, via Chiatamone 7
00185 Roma, via dei Taurini 27

Internet: www.esispa.com
E-mail: info@esispa.com

I diritti di traduzione, riproduzione e adattamento, totale o parziale
e con qualsiasi mezzo (compresi i microfilm e le copie fotostatiche),
sono riservati per tutti i Paesi.

INDICE

Introduzione e saluti

IGNAZIO BUTI, <i>Introduzione e saluti</i>	9
VITO RIZZO, <i>Presentazione del Convegno</i>	11
NICOLA PALAZZOLO, <i>Introduzione e saluti</i>	15

I Sessione

Presiede: VITTORIO FROSINI

VITTORIO FROSINI, <i>Apertura dei lavori</i>	19
ANTONELLO BUSFITO, <i>Internet e commercio elettronico: profili introduttivi</i>	21
PASQUALE COSTANZO, <i>Profili costituzionalistici del commercio elettronico</i>	29
COSIMANTINO CIAMPI, <i>E-commerce: normativa e organismi internazionali</i>	43
DONATO LIMONE, <i>Commercio elettronico. analisi della situazione italiana e comunitaria</i>	71
CARIO SARZANA DI SANI'IPPOLITO, <i>Le attività illecite nell'ambito del commercio elettronico. Aspetti penalistici e criminologici</i>	81

II Sessione

Presiede: NICOLA PALAZZOLO

MANLIO CAMMARATA, <i>Documenti informatici la smaterializzazione della scrittura</i>	95
ANDREA MONTI, <i>La crittografia è un'arma? Il difficile bilanciamento fra diritti individuali e interessi pubblici</i>	101
ENRICO MACCARONE, <i>Chiavi biometriche (Art. 1, lett. g, D.P.R. n. 513 del 1997)</i>	111
RAIMONDO ZAGAMI, <i>Valore giuridico della firma digitale e conclusione telematica del contratto</i>	117
ANTONIO CILLI, <i>Nuove forme di commercio: violazioni ed accertamenti</i>	135

III Sessione

Presiede: PIETRO PERLINGHIERI

RICCARDO ACCIAI, <i>La tutela dei dati personali: la privacy e l'e-commerce</i>	161
ALBERTO MARA GAMBINO, <i>Commercio elettronico e tutela del consumatore</i>	177
FRANCESCO CARDARELLI, <i>Funzioni e poteri pubblicistici in materia di commercio elettronico</i>	189
GIANLUIGI CIACCI, <i>Strumenti di pagamento on-line e l'e-cash</i>	203
UMBERTO RAPETTO, Ugo Poggi, <i>Profilo tributario delle vendite on-line di beni e di servizi</i>	217

MARIA CONCETTA DI VIVO, <i>Commercio elettronico. una breve guida alle risorse in Rete</i>	237
PILIRO PERLINGIERI, <i>Intervento conclusivo - Documento Informatico, firma digitale e commercio elettronico</i>	261
Interventi selezionati	
Fulvio Sarzana Di Sant'Ippolito, <i>L'arbitrato nelle reti telematiche e il commercio elettronico: un rapido strumento di risoluzione delle controversie sorte nella «Rete delle reti»</i>	271
MARIO CAMMARATA, <i>La cifratura e il sistema digitale del notariato</i>	281
RAIMONDO ZAGAMI, <i>L'atto pubblico notarile e il servizio digitale dei notai</i>	283
MASSIMILIANO MINERVA, <i>Alcuni concetti relativi ai sistemi di firma digitale</i>	285

INTRODUZIONE E SALUTI

Introduzione e saluti del Magnifico Rettore dell'Università degli studi di Camerino

IGNAZIO BUTI

Sono molto lieto di aprire questo importante convegno che mi consente di rivedere molti vecchi amici dell'Università e miei personali. In particolare, voglio ringraziare gli organizzatori di questo incontro, che sono il prof. Vito Rizzo, Direttore della Scuola di specializzazione in diritto civile, ed il prof. Nicola Palazzolo Direttore dell'Istituto per la Documentazione Giuridica del CNR di Firenze.

Un saluto anche a coloro che sono collegati con noi in videoconferenza presso la sede dell'Ente Nazionale Previdenza ed Assistenza Consulenti del lavoro, con il quale stiamo avendo una proficua collaborazione da oltre un anno, con l'esperimento di un primo anno in comune delle Facoltà di Architettura di Ascoli; di Scienze matematiche e fisiche e Scienze naturali. Il buon successo finora ottenuto spero sarà un buon viatico per il futuro.

Un saluto anche agli ascoltatori di Radio radicale, collegati con noi via Internet.

Non mi resta che augurare a tutti voi buon lavoro e un felice soggiorno a Camerino.

Presentazione del Convegno

VITO RIZZO¹

Dopo il saluto del Rettore, che ringrazio per la sua presenza e per aver voluto sempre appoggiare nelle varie sedi questa iniziativa convegnistica, consentendone così la realizzazione, rivolgo anch'io un caloroso benvenuto ed un cordialissimo saluto a tutti i presenti; permettetemi, inoltre, di esprimere un ringraziamento particolare ai relatori che animeranno le giornate di questo Convegno e che hanno accolto con vero entusiasmo il nostro invito a riflettere insieme su un tema di così viva attualità ed ai Presidenti delle tre sessioni in cui il Convegno si articola, proff. Vittorio Frosini, Nicola Palazzolo, Pietro Perlingieri, che ci onorano con la loro presenza.

È per me un piacere ricordare, ancora una volta, e sottolineare che questa iniziativa si colloca nel solco di un'ormai collaudata tradizione e di una felicemente sperimentata collaborazione scientifica tra Scuola di specializzazione in diritto civile dell'Università di Camerino e Istituto per la documentazione giuridica di Firenze del CNR.

Essa palesemente si collega, rappresentandone un'ideale continuazione, con il Convegno su "Diritto e tecnologie dell'informazione" tenuto a Camerino nell'ottobre del 1996 e organizzato dalle due Istituzioni (i cui atti hanno trovato pubblicazione nel volume dallo stesso titolo).

Concludemmo quell'esperienza con il proposito di non lasciar inaridire e morire questa forma di collaborazione, che d'altra parte risaliva ancora più indietro nel tempo, agli albori (se così possiamo dire) dell'informatizzazione della scienza giuridica in Italia, ma di mantenerla vitale e di arricchirla sempre più con nuove iniziative. Trova così chiarimento l'*humus* che ha rappresentato l'elemento generativo e vitale di questo Convegno.

Tre anni fa ci siamo occupati di una tematica più generale proponendoci, da un lato, di fare una verifica delle possibilità operative che le nuove tecnologie dell'informazione aprono al giurista e, dall'altro, di fare una riflessione sui delicati problemi giuridici che l'impiego di queste tecnologie ha suscitato.

¹ rizzo@camscrv.unicam.it

Oggi il tema della riflessione si è **maggiormente circoscritto e definito** e ci è stato suggerito, se non imposto, **dalla pressione dei tempi e degli eventi.**

La nostra società è sempre più **società dell'informazione** ed il commercio elettronico, come è stato **suggestivamente sottolineato**, è la società dell'informazione realizzata **nella pratica.** La tumultuosa e rapida diffusione delle reti telematiche e, in **specie, della Rete delle reti - Internet** - inevitabilmente ed inesorabilmente **assegnerà una posizione di assoluta centralità a questa nuova forma di commercio ed alle problematiche ad essa connesse.**

Ancora una volta la società, in tutte le sue componenti, è chiamata a raccogliere la sfida dei tempi. Ancora una volta il giurista, pur se in una posizione mediata, riflessa, sollecitata dalla preventiva evoluzione di altre scienze, è chiamato ad interrogarsi sulla ricaduta di questa evoluzione nell'ambito della propria scienza, dei propri strumenti, delle proprie tecniche, e a proporre, questa volta più direttamente come protagonista, le soluzioni giuridiche più adeguate ai nuovi ed emergenti problemi.

Va preso, comunque, definitivamente atto che le nuove forme di commercio e di negoziazione impongono, ed imporranno sempre più, seri elementi di meditazione non soltanto al civilista, inteso in senso ampio, ma anche al costituzionalista, al penalista, all'amministrativista, al tributarista, all'internazionalista, al cultore del diritto comunitario ecc., richiedendo ad ognuno lo sforzo di un adeguamento, di un aggiornamento delle abituali categorie, se non della creazione di nuove categorie.

Si avverte l'esigenza, e con ciò si fanno emergere le singole tracce che vanno a comporre l'intelaiatura del presente convegno, di una normativa oltre e più che nazionale, visto il carattere transfrontaliero e globalizzante del fenomeno, comunitaria e internazionale, dell'eventuale avvento di nuovi organismi che possano operare in questa più vasta dimensione, si da creare un clima di fiducia degli operatori commerciali, da un lato, e dei consumatori, dall'altro, indispensabile per lo sviluppo del commercio elettronico.

In questo contesto vanno colte e sottolineate le nuove possibilità di sviluppo che si aprono a livello commerciale, a livello imprenditoriale (non soltanto nei confronti della grande, ma anche della piccola impresa), a livello occupazionale, la sollecitazione ad un più ampio (e possibilmente corretto) operare della concorrenza.

Va altresì sottolineato che il commercio elettronico rivoluziona la tradizionale relazione consumatore-distributore-produttore: se da un lato vanno segnalati i notevoli vantaggi di cui il consumatore potrebbe beneficiare (tra questi: un più agevole accesso al mercato, una più vasta gamma di scelte, più immediate e complete informazioni, prezzi potenzialmente inferiori), non vanno, da altro lato, sottaciuti i rischi che queste moderne tecnologie indubbiamente accentuano, se non addirittura creano *ex novo*, richiedendo nuove forme di protezione del consumatore.

Si è già accennato al fatto che per agevolare lo sviluppo del commercio elettronico si deve creare un clima di fiducia da parte dei soggetti che ne sono i protagonisti; ciò appare possibile soltanto attraverso l'introduzione di meccanismi idonei a garantire la sicurezza degli scambi e delle transazioni: trovano in ciò spiegazione l'uso di tecnologie di crittazione, la recente normativa in materia di valore giuridico del documento informatico e della firma digitale in merito, in particolare, ai problemi dell'imputazione, dell'integrità e della prova del documento (ampio spazio è stato riservato a questi aspetti), oltre che l'impiego di altre forme di tutela che possono operare, a questo fine, a livello penale, nei confronti dei nuovi crimini informatici.

In considerazione del mezzo impiegato assumono particolare rilievo il problema della tutela della *privacy* e dell'uso dei dati personali, il problema della tutela del diritto d'autore. Per lo sviluppo del commercio elettronico sono altresì indispensabili sistemi di pagamento elettronico di agevole impiego, efficaci e sicuri ed un contesto fiscale certo, trasparente, prevedibile e neutrale.

Si è così soltanto fatto cenno alle principali problematiche che saranno molto più diffusamente e molto meglio analizzate dai singoli relatori, nella speranza di aver lasciato intravedere, con una rapida visione d'insieme, le singole trame del presente Convegno, il filo conduttore che le lega, l'idea di fondo che ne è alla base e le anima.

Consentitemi, in chiusura, di esprimere la speranza che anche questo nostro Convegno possa dare un contributo ai fini di una sempre più ampia informazione e familiarizzazione con queste nuove forme di negoziazione e di commercio, quanto meno nei loro aspetti più prettamente giuridici, che rappresenta un passaggio ineliminabile per un loro sempre più diffuso e crescente impiego nella società di oggi. La società dell'infor-

mazione che si evolve esige, infatti, una formazione continua al fine di usufruire al meglio delle *chances* che essa offre.

Lascio ora la parola al prof. Palazzolo, direttore dell'Istituto per la documentazione giuridica di Firenze, che ringrazio per la proficua e per noi sicuramente preziosa collaborazione con l'Istituto che egli dirige e per la sua presenza, ancora una volta, qui a Camerino, che io voglio interpretare, spero me lo permetta, come segno di particolare e viva amicizia. Ringrazio con lui il dott. Costantino Ciampi, testimone e protagonista, anch'egli, di questa lunga amicizia che ha contribuito, con la sua esperienza, alla definizione delle linee del Convegno. Lascio la parola al prof. Palazzolo non senza aver ringraziato, però, anche la dott.ssa Concetta De Vivo per la sua fondamentale collaborazione ai fini dell'organizzazione del Convegno.

Introduzione e saluti del Direttore dell'Istituto per la documentazione giuridica del CNR di Firenze

NICOLA PALAZZOLO¹

Il mio, a differenza di quello del prof. Vito Rizzo che mi ha preceduto, sarà poco più che un saluto. In realtà lui è entrato, nonostante abbia detto il contrario, *in medias res*, ha costruito la trama di questo convegno.

Mi limiterò a dire che sono sempre contento di venire a Camerino perché ritrovo questo clima di amicizia già sperimentato anche in occasioni diverse, quando partecipo, essendo romanista, a convegni specifici di diritto romano, che, quindi, potrebbero definirsi di tutt'altro genere rispetto agli incontri di questo tipo, in cui ci si ritrova comunque e sempre in qualità di giuristi.

Già il convegno del 1996 aveva gettato le basi, mettendo in evidenza alcuni punti chiave, come risulta dagli Atti pubblicati a cura dell'IDG, per un discorso che oggi continua con contenuti più ricchi e specializzati. In qualità di direttore dell'IDG mi sono impegnato alla pubblicazione anche degli Atti di questo convegno, che saranno inseriti in una collana nata da poco per i tipi dell'ESI di Napoli.

Non entrerò nel merito del Convegno. Devo dire che questi incontri periodici di Camerino hanno per me una grande importanza, specialmente in un momento come questo, dove a livello di discipline universitarie si sta cercando di chiarire i contenuti dell'informatica giuridica, da un lato, e del diritto dell'informatica dall'altro. Questi convegni cercano appunto di puntualizzare e quindi di vedere le reciproche interazioni e distinzioni fra l'uno e l'altro aspetto di una medesima realtà, che, a livello scientifico prima e didattico dopo, vanno individuate, distinte e separate. Questi convegni hanno un ruolo importante per far capire ai giuristi, a chi insegna nelle facoltà giuridiche, i contenuti dell'informatica giuridica e del diritto dell'informatica. Oggi, sotto queste definizioni spesso vengono confuse assieme cose diverse ed è questo il motivo per cui queste discipline non riescono ancora a trovare un'adeguata collocazione a livello didattico-disciplinare; vediamo che, mentre nella realtà gli aspetti

¹ Palazzolo@idg.fi.cnr.it

sottolineati dal prof. Vito Rizzo, e tutto il convegno lo metterà in luce, diventano sempre più importanti, stentiamo a renderli importanti a livello di didattica universitaria. Questa è la cosa che in questo momento mi sta più a cuore, non tanto e non solo, in quanto Direttore dell'IDG, ma come docente impegnato nella didattica, così come tanti di voi.

Riuscire oggi ad individuare i confini e gli ambiti delle discipline consentirà di fare un notevole passo avanti nella direzione di una migliore collocazione sia dell'informatica giuridica, cioè dell'applicazione dell'informatica all'attività del giurista in tutte le sue applicazioni, sia del diritto dell'informatica, cioè della valutazione giuridica che viene data di questo grosso fenomeno in crescita. Devo dire che su quest'ultimo punto le reazioni sono abbastanza chiare, perché, mentre relativamente all'informatica giuridica c'è magari una reazione latente del giurista che ne capisce poco però non vuol mostrarlo, per il diritto dell'informatica la reazione è spesso esplicita. Durante la seduta finale (e qui c'è il prof. Frosini che presiede la seduta) del Convegno organizzato dall'IDG, che si è tenuto il mese scorso a Firenze, dedicata all'insegnamento dell'informatica giuridica e del diritto dell'informatica, è emerso come in ambito universitario le reazioni fossero esplicitamente negative. Molti illustri docenti, presidi di facoltà giuridiche, sostenevano che il Diritto dell'informatica non avendo un'autonoma fisionomia, non può avere autonomia didattica. Credo che un convegno come questo, con le relazioni preannunciate, dimostri proprio il contrario e cioè che questa materia ha un contenuto autonomo, del tutto diverso dai contenuti delle discipline del diritto positivo, e proprio per questo deve avere una sua collocazione e un suo ruolo.

Concludo con l'auspicio che queste giornate siano un ulteriore passo verso i chiarimenti che ho accennato e che siano promosse anche altre iniziative, intermedie, che fungano da filo rosso tra i grossi convegni.

Grazie.

I SESSIONE

Presiede: Vittorio Frosini

Apertura dei lavori del Presidente della I Sessione

VITTORIO FROSINI

Illustri colleghi, Direttori della Scuola di specializzazione in Diritto Civile e dell'Istituto per la documentazione giuridica, signori colleghi, signore e signori vi sono due motivi perché io esprima il mio sentito ringraziamento per avermi chiamato a partecipare a questo congresso.

Il primo è che proprio qui, nell'Università di Camerino, undici anni orsono, nei giorni 11 e 12 novembre 1988, io venni a presiedere il 1° convegno dell'Associazione Nazionale dei Docenti di Informatica Giuridica, che l'amico Donato Limone ed io avevamo programmato per la sua costituzione.

La Facoltà giuridica di Camerino fu infatti la prima e allora unica tra le facoltà italiane ad istituire la cattedra della disciplina, dopo di allora si sono verificati grandi progressi nel campo tecnologico e notevoli sviluppi in quello giuridico, come questo congresso è chiamato a documentare.

L'associazione ANDIG tenne altri convegni e diede opera per la pubblicazione di una collana di studi, ma la sua incidenza sui programmi didattici delle facoltà giuridiche è stata resa inefficace dall'inerzia al riguardo delle stesse facoltà, salvo qualche eccezione.

L'Italia rimane perciò alla periferia della cultura universitaria europea in questo settore ed è merito di questa Università di Camerino di dimostrare, ancora una volta, la sua capacità di richiamo sui grandi temi culturali, come in altre occasioni a cui ho avuto io stesso la fortuna di partecipare, quali il convegno sul pensiero di Emilio Betti, ricordato dal collega e amico Vito Rizzo, e il congresso internazionale di Storia dei Parlamenti anch'esso qui tenuto.

Questo è il primo motivo.

L'altro motivo per il quale mi sia consentito di esprimere un mio vivo compiacimento è che all'Università di Camerino in questa circostanza è associato l'Istituto per la documentazione giuridica di Firenze, del quale io ho seguito il cammino in ascesa dal lontano anno 1972, quando venni eletto al Consiglio Nazionale delle Ricerche e al quale da allora ho prestatato, in varie forme, la mia collaborazione.

La mia partecipazione all'attività dell'Istituto fiorentino è stata per me resa grata anche da ragioni affettive, per i rapporti di amicizia personale che mi legano al Direttore, prof. Nicola Palazzolo, a cui mi accomunano antichi ricordi di vita catanese, e al Direttore della rivista "Informatica e Diritto", Costantino Ciampi, con il quale ho condiviso in questi anni le esperienze di vita della rivista. E consentite che io rivolga anche un personale indirizzo di saluto al collega con cui siamo stati insieme nella facoltà di giurisprudenza della Sapienza di Roma, prof. Pietro Perlingieri.

E, infine, mi sia consentito di aggiungere anche un terzo motivo di compiacimento per la presenza fra i relatori a questo convegno di illustri amici di antica data e di miei antichi allievi dei corsi di dottorato di ricerca tenuti nell'Istituto romano che io ho diretto fino a due anni fa.

Per un vecchio professore, come io sono, che ha vissuto quasi tutta la sua esistenza nell'Università, a cominciare dai remoti anni della Scuola Normale di Pisa, in cui fui ammesso nel 1939 e dove tutt'oggi mi trovo, questi motivi suscitano nell'animo profonde risonanze. Grazie. Adesso daremo inizio ai lavori, per i quali seguirò l'ordine di successione indicato nel programma.

Internet e commercio elettronico: profili introduttivi

ANTONELLO Busetto¹

Internet non è più solo uno strumento di comunicazione e si sta trasformando in uno strumento essenziale per l'attività delle aziende.

Così come sarebbe impensabile che un'impresa non avesse accesso alla rete elettrica ed ai servizi connessi, altrettanto indispensabile è oggi la rete Internet e le sue applicazioni.

L'Italia è in ritardo da questo punto di vista e deve rapidamente recuperare terreno nei confronti dei Paesi più avanzati, facendo in modo che tutte le imprese possano cogliere le opportunità della Società dell'Informazione, creando una sensibilità collettiva maggiormente orientata verso l'innovazione e le nuove tecnologie.

La crescita di una cultura diffusa e la presenza di un ambiente sociale favorevole sono stati elementi decisivi per la crescita dei distretti industriali. Oggi occorre creare le medesime condizioni per lo sviluppo di una cultura dell'innovazione che consenta di poter contare su di un diffuso contesto sociale, che nei settori molto innovativi costituisce elemento fondamentale nelle decisioni di investimento.

Il sistema Paese sarà in grado di fare un vero salto di qualità se anche studenti, lavoratori e famiglie riusciranno a superare il *gap* culturale verso l'uso dell'informatica e della telematica.

Investire in innovazione e formazione è il più importante investimento che dobbiamo fare alle soglie del 2000.

Il differente contesto economico esistente tra Europa e Stati Uniti (Paese di riferimento su queste tematiche in termini di spesa, di investimenti in nuove tecnologie, nonché in termini di sviluppo di Internet e del Commercio Elettronico) si può attribuire alla minore diffusione delle tecnologie informatiche e di telecomunicazione, accompagnata da un insufficiente sviluppo infrastrutturale, e dall'altra parte a motivi di tipo culturale, anche se la scarsa propensione delle aziende ad investire in in-

¹ busetto@minindustria.it

novazione ha contribuito a rallentare lo sviluppo del mercato, sia in termini di domanda sia in termini di offerta di soluzioni e di applicazioni.

Dove stanno andando gli Stati Uniti? Secondo le previsioni del Dipartimento del Commercio Americano entro il 2006 metà della forza lavoro americana sarà impegnata **direttamente o indirettamente nell'industria delle Tecnologie dell'Informazione (IT)** (come produzione che come usi finali di prodotti e servizi). Basta questo dato a darci una dimensione di quali enormi cambiamenti **avverranno nelle economie**, e nelle società a seguito del processo di **globalizzazione**. Per capire qual è il **punto di partenza per l'Italia**, dobbiamo considerare che, includendo anche il settore delle comunicazioni, la nostra forza lavoro ICT è oggi solo il 5% del totale.

Se facciamo ulteriori confronti con gli Stati Uniti emergono chiaramente sia i ritardi sia le opportunità di sviluppo. Il peso del settore ICT sul PIL, che nel nostro Paese è appena del 4%, in America supera l'8% (gli Stati Uniti erano al 4% nel 1977), contribuendo per il 35% alla crescita economica reale del Paese. Questo aspetto ha immediati riflessi sul fronte occupazionale, dove politiche **aggressive orientate all'innovazione** hanno contribuito notevolmente alla **riduzione del tasso di disoccupazione negli USA**, che oggi viaggia su valori fisiologici, proprio grazie al contributo del settore in parola (intorno al 4%).

Tuttavia nonostante le opportunità esistenti, così come in Italia esiste un deficit di offerta di figure professionali di circa 30.000 unità nel settore ICT, negli Stati Uniti sono circa 350.000 le posizioni vacanti, a conferma di come la richiesta del mercato sia in forte aumento.

Appare allora chiaro come le dinamiche in corso **non consentono indecisioni e ritardi** e coloro che riusciranno per primi a conquistare il mercato elettronico se ne avvantaggeranno in misura crescente a discapito dei concorrenti, che perderanno terreno rapidamente ed in modo difficilmente recuperabile: **sarà la Rete stessa**, man mano che si estende, a rafforzare le posizioni di coloro che vi partecipano.

I rischi, molto rilevanti per il nostro tessuto produttivo, vanno valutati in termini di:

- trasformazione dell'economia italiana in economia di nicchia oppure di assemblaggio e distribuzione subordinata alle aree forti dell'Europa;

- **trasferimento all'estero delle** funzioni strategiche ed ad alto contenuto innovativo;
- **riduzione della base occupazionale nei settori tradizionali**, dove l'automazione e la delocalizzazione comportano una riduzione dell'impiego di manodopera non compensata dalle opportunità di lavoro nei settori più innovativi.

Il recupero del *gap* tecnologico rappresenta pertanto una **necessità assoluta** per il nostro Paese, ma non solo rispetto ai settori più **avanzati**. Anche il **consolidamento delle posizioni competitive** nei settori più tradizionali richiede, per potersi differenziare dai beni a ridotto costo provenienti dai paesi emergenti, un intenso processo di rinnovamento accompagnato da un **aumento della capacità produttiva** sui segmenti a maggiore valore aggiunto e dal **rafforzamento** del sistema dei servizi avanzati come quelli finanziari, di *marketing*, ecc.

Questa operazione di **riposizionamento competitivo** del sistema produttivo nazionale impone un **adeguamento** che coinvolge pertanto non solo il sistema delle imprese, ma anche il riassetto del sistema finanziario, la riorganizzazione dei servizi e la creazione di diverse e più efficienti istituzioni economiche e le nuove tecnologie dell'informazione e della comunicazione potranno dare un valido contributo al processo virtuoso di crescita del prodotto, della produttività e dell'occupazione, svolgendo un ruolo trainante e catalizzatore di intere filiere produttive.

Alla luce di queste considerazioni è possibile, quindi, collocare la **partecipazione dell'Italia al mercato globale** in un quadro più completo, in cui il nostro Sistema-Paese giocherà le proprie carte per rimanere nel gruppo dei paesi più avanzati, per consolidare le posizioni di mercato raggiunte in questi anni e per svolgere un ruolo determinante nel rafforzamento della competitività europea sullo scenario internazionale. Un'adeguata attenzione alla modernizzazione consentirà di collocarsi su un sentiero di crescita stabile e consistente e di creare anche nuove opportunità di impiego.

L'economia italiana, all'interno di tale contesto, punterà molto sulla grande flessibilità e capacità di **adattamento a livello microeconomico** delle Piccole e Medie Imprese: un **patrimonio industriale** molto rilevante, che assorbe oltre il 78% della forza lavoro e che ha mostrato negli ultimi anni una notevole capacità nel creare **nuova occupazione**, posizionandosi sui segmenti più dinamici all'interno dei **settori tradizionali** e sviluppando

un sistema di adeguamento tecnologico che utilizza canali alternativi a quelli della ricerca e sviluppo istituzionalizzati.

Ciò consentirà di raggiungere le finalità che il Governo si pone nel perseguire il suo disegno per lo sviluppo della Società dell'Informazione: insieme alla crescita della competitività delle imprese, la diffusione della cultura informatica, la modernizzazione, la trasparenza e l'efficienza della P.A., la tutela del mercato e la difesa dei consumatori.

In questo contesto il ruolo della politica per rilanciare lo sviluppo economico e dare tono al nostro sistema industriale si è orientato sui seguenti obiettivi:

- abbassamento dei costi di sistema attraverso una nuova regolazione dei mercati ed una liberalizzazione per creare nuova capacità competitiva e nuovi *business*;
- rin vigorimento del mercato dei capitali per garantire un adeguato sostegno finanziario ai progetti imprenditoriali, sia per via di regolamentazione e attraverso misure fiscali orientate alla capitalizzazione, sia attraverso un atteggiamento del sistema del credito più attento alle esigenze del sistema produttivo;
- rafforzamento della competitività del contesto ambientale in cui operano le imprese. Il decentramento e la semplificazione in materia di politica industriale spostano verso il territorio ampi margini di autonomia di governo dell'intervento pubblico a sostegno dello sviluppo industriale.
- sviluppo dell'innovazione come condizione essenziale per il consolidamento competitivo del nostro sistema all'interno dei nuovi scenari internazionali.

Altri stimoli al mercato verranno dalle iniziative della Pubblica Amministrazione Centrale e Periferica in tema di semplificazione delle procedure e di informatizzazione, ai quali si cominciano ad affiancare applicazioni e servizi per i cittadini e per le imprese, realizzati attraverso le reti telematiche, ed, anche se alcuni disagi e problemi si verificano nella fase di *start-up*, evidenti sono i benefici che deriveranno dalla rivoluzione in atto.

Nel corso degli ultimi anni il Governo ha lavorato per garantire un ambiente più favorevole al raggiungimento di questi obiettivi e i provvedimenti più significativi in questa direzione sono stati:

- la liberalizzazione del settore delle telecomunicazioni e l'istituzione dell'Autorità di settore, che hanno consentito l'entrata sul mercato di nuovi soggetti;
- la liberalizzazione del commercio in linea con lo sviluppo del Commercio Elettronico che, con le sue caratteristiche di trasversalità in tutti i settori produttivi, contribuisce ad una libera ridistribuzione delle funzioni, delle categorie di prodotti, delle organizzazioni;
- l'informatizzazione della Pubblica Amministrazione e l'avvio della Rete Unitaria, su cui il Governo sta investendo ingenti risorse finanziarie e che rappresenta un grande progetto di modernizzazione dello Stato;
- l'emanazione della legge di semplificazione dei procedimenti amministrativi ed in particolare le norme riguardanti la validità ai fini legali del documento informatico e della firma digitale ed i relativi provvedimenti di attuazione;
- l'istituzione presso la Presidenza del Consiglio dei Ministri del *Forum* per la Società dell'Informazione come luogo non solo di coordinamento delle iniziative delle Amministrazioni, ma anche di proposta;
- le misure a sostegno delle imprese del settore dei servizi, dell'informatica e delle telecomunicazioni e l'estensione dell'ammissibilità ai benefici delle leggi di incentivazione per gli investimenti in beni immateriali ed in particolare per quelli relativi alle tecnologie dell'informazione e della comunicazione (leggi 488/92, 341/95 e 266/97), per le quali nel solo 1998 sono stati erogati incentivi per circa 1.000 MLD;
- le politiche di settore ed in particolare, anche a seguito della liberalizzazione del commercio, quelle per lo sviluppo del Commercio Elettronico con l'istituzione dell'Osservatorio Permanente.

Queste politiche hanno già prodotto alcuni significativi risultati e, nonostante i ritardi, si cominciano a notare segnali di miglioramento sempre più incoraggianti. La crescita del mercato IT, che nel '97 era stata del 6,1% e nel '98 dell'8,5%, si dovrebbe attestare quest'anno su valori superiori al 10% e livelli di crescita ancora maggiore verranno raggiunti nel mercato del *software* e dei servizi (+11,6% - dato del primo semestre '99

su primo semestre '98) ed in quello dei *personal computers* (+18,3% - primo semestre '99 su primo semestre '98).

Un segnale di come stia crescendo l'interesse per le nuove tecnologie viene poi dal mercato mobiliare, dove il nuovo listino di Piazza Affari "Nuovo Mercato", riservato alle aziende ad alto potenziale di crescita, è recentemente decollato in Italia nell'ambito di un circuito europeo al quale partecipano le borse di Francoforte, Parigi, Amsterdam e Bruxelles e dove sono quotate oltre 100 società.

Anche in questo caso l'Italia (come l'Europa) deve registrare un certo ritardo, essendo per il momento quotate solo poche aziende (tra le quali *Opengate* che è stata recentemente premiata in occasione della sessione inaugurale del Premio per il Commercio Elettronico italiano istituito dal Ministero dell'Industria in occasione di SMAU), ma promette di offrire ad imprese innovative e dinamiche, operanti in settori ad alta tecnologia, un canale di accesso al capitale di rischio in grado di rispondere alle loro esigenze di sviluppo.

Ciò dovrebbe contribuire a migliorare uno dei fattori critici del nostro sistema economico, dove la grande carenza di un'adeguata finanza d'impresa non consente di sfruttare le grandi opportunità imprenditoriali che si sono aperte negli ultimi anni. La debolezza del mercato azionario e l'inadeguatezza del rapporto tra banche ed impresa sono alla base della sfasatura tra il processo di animazione, allargamento e rafforzamento del mercato azionario e le esigenze di sviluppo e consolidamento del sistema imprenditoriale nazionale.

Un altro chiaro indice dell'evoluzione del mercato è la possibilità, ormai offerta da numerosi *providers*, di accedere gratuitamente ad Internet, a dimostrazione dello spostamento dell'attenzione degli operatori su aspetti che coinvolgono direttamente gli interessi e l'operatività delle aziende ed offrono alle aziende medesime e agli altri soggetti coinvolti ben più importanti occasioni di *business* rispetto al servizio di accesso.

All'interno della strategia a favore delle attività produttive il Governo pone grande attenzione alle Piccole e Medie Imprese, riconoscendo a questo segmento della struttura produttiva un ruolo fondamentale nel garantire la competitività del sistema e lo sviluppo economico; e sul piano concreto la disponibilità verso i problemi delle PMI si è tradotta: nell'inserimento in finanziaria di una serie di provvedimenti per lo sviluppo e la diffusione del Commercio Elettronico che recepiscono alcune

esigenze del sistema produttivo, incentivando le iniziative cantierabili e premiando i risultati.

Il nuovo contesto competitivo, al quale dovranno adattarsi le imprese, si basa su un mercato globale in cui qualsiasi impresa può raggiungere un qualunque utente e ogni consumatore può rivolgersi a qualunque impresa nel mondo. Anche i nuovi entrati hanno le stesse possibilità di chi è sul mercato da tempo e le possibilità di *business* si estendono ad un numero di aspiranti illimitato, con un tasso di "ricambio" molto elevato (ogni 4 secondi nasce un nuovo sito Internet). Nascono nuove modalità di fare *business* e le abitudini commerciali tradizionali diventano obsolete. Sugli aspetti infrastrutturali e tecnologici prevalgono gli aspetti organizzativi e di servizio.

Ormai le tecnologie consentono di concludere contratti *on-line* con fornitori e clienti garantendo riservatezza, autenticità, integrità e non ripudio e la validità e rilevanza a tutti gli effetti di legge degli atti, dati e documenti informatici, così come la loro archiviazione e trasmissione, secondo il dettato della legge 59/97, consentono di dare valore giuridico alle transazioni via Internet.

Fare del commercio elettronico tra imprese è tuttavia cosa ben diversa dalla semplice realizzazione di un sito *Web* e di un catalogo elettronico: significa partecipare ad un nuovo mercato con leggi economiche nuove. Le imprese che operano in Rete devono essere in grado di gestire la catena del valore in modo integrato. Acquisti, magazzino, produzione, contabilità, finanza, vendite ed aspetti logistici andranno considerati in un'unica piattaforma operativa che consideri le diverse attività come processi da gestire in tempo reale e con un elevato grado di interazione. Bisognerà agire non tanto sul *front-end* nei riguardi delle interfacce esterne (clienti e fornitori) quanto per realizzare un'integrazione di tali interfacce con il *back-office* aziendale.

Sarà allora necessario prevedere punti di riferimento e di orientamento che offrano una prima informazione operativa ed una guida alla risoluzione dei problemi organizzativi, insieme con l'accesso ad un parco di fornitori di servizi che conformino la loro attività ad un codice di autoregolamentazione e di qualità, tale da generare fiducia da parte del piccolo e medio imprenditore.

Si tratta in definitiva di promuovere l'offerta di modelli di sviluppo e piattaforme standardizzate, indirizzando la domanda verso soluzioni de-

finite rivolte alle diverse tipologie di impresa per classi di fatturato e di addetti, per ambiti settoriali e per realtà territoriale e distrettuali.

È questa l'impostazione che seguiremo nei Collegati alla Finanziaria per definire le modalità di accesso agli strumenti di incentivazione specificamente previsti per il Commercio Elettronico.

L'attività di orientamento sarà portata avanti insieme alle Associazioni delle imprese e dovrà operare come "portale" dedicato al mondo industriale attraverso specifiche strutture operative e *call-centers* telematici che diano indicazioni sulle tecnologie *hardware* e *software* e sui servizi necessari (certificazione, di TLC, bancari, di logistica, ecc.) nonché sulle attività di organizzazione e di formazione. Le soluzioni messe a punto saranno opportunamente pubblicizzate attraverso un piano di comunicazione e di sensibilizzazione e saranno integrate dalla partecipazione di operatori esterni attraverso Accordi di Programma e Convenzioni che allargheranno le opzioni e la fattibilità delle realizzazioni.

Vorrei concludere dicendo che, anche se le considerazioni effettuate ci consentono di guardare al futuro con grande ottimismo, la velocità o la lentezza, con cui le nostre imprese sapranno riprogettare l'azienda in chiave di innovazione investendo in organizzazione e risorse umane, saranno decisive ai fini della loro capacità competitiva.

L'innovazione rappresenta la vera scommessa per il nostro sistema produttivo e le tecnologie dell'informazione e della comunicazione potranno dare un contributo decisivo al processo di crescita e di modernizzazione del Paese.

Profili costituzionalistici del commercio elettronico

PASQUALE COSTANZO¹

SOMMARIO: 1. Premessa - 2. Commercio elettronico e libertà di comunicazione - 3. Commercio elettronico e libertà d'informazione - 4. Commercio elettronico e riservatezza personale - 5. Commercio elettronico e libertà economica - 6. Alcune conclusioni.

1. PREMESSA

La trattazione dei profili costituzionalistici di un certo tema giuridico corre spesso (apparentemente) il rischio di risultare un'esercitazione tanto elegante quanto astratta. Rischio tanto più grande allorché il tema prescelto vanti sistemazioni risalenti in essenziali branche del diritto come il diritto civile o il diritto commerciale. Potrebbe essere proprio il caso del commercio elettronico, di cui sarebbe lecito pensare (se ci si passa il bisticcio di parole) che, per quanto sia "elettronico", sempre "commercio" resta, vale a dire, nella sua sostanza, l'esercizio a scopo di lucro di un'attività che ha per fine lo scambio di beni contro denaro.

Non so quindi se la mia trattazione sarà elegante: lascio ovviamente agli autorevoli uditori giudicare. La mia vera preoccupazione è però che almeno essa non risulti astratta.

A questo scopo vorrei subito ritornare sulla definizione di commercio che ho fornito qualche istante fa e notare come essa in realtà vada troppo stretta (e sia al limite fuorviante con riguardo) alla fenomenologia che si è ormai concordi nell'ascrivere al commercio elettronico.

In questo senso, dunque, se è vero che si verte in ogni caso nell'ambito di un'attività economica, ciò che sconsiglia - anche al costituzionalista - di abbandonarsi a discorsi abbastanza scontati è proprio la particolare configurazione del commercio elettronico.

A differenza del commercio tradizionale, infatti, nel commercio elettronico occorre tenere nel massimo conto principalmente tre fattori.

¹ costituz@unige.it

Il primo fattore è costituito dal mezzo peculiare che permette ed anzi ha dato, com'è noto, origine a questa particolare forma di commercio. Il secondo fattore è rappresentato dai protagonisti, che, anche rispetto a forme più aggiornate di commercio, assumono, da un lato, ruoli abbastanza inediti, e non si esauriscono, dall'altro, nei soli soggetti stipulanti l'atto di commercio. Il terzo è dato sicuramente dalla "vocazione" internazionale di questa particolare forma di commercio.

Tutto ciò, come subito vedremo, contribuisce a creare un quadro piuttosto complesso, nel quale, se l'intuitivo punto di partenza è offerto dalle disposizioni in materia di libertà d'iniziativa economica contenute nella Costituzione (pur se nella particolare "curvatura" impressa loro dalla normativa comunitaria), si rivela però anche indispensabile procedere secondo prospettive in parte o completamente nuove.

Un approccio peraltro al quale è assai sconsigliabile mostrarsi refrattari, se è vero che persino normative recenti e innovative come quelle sulla tutela del consumatore o sui contratti a distanza e la stessa disciplina della *privacy* si sono trovate notevolmente "spiazzate" di fronte alla realtà fenomenica del cosiddetto cyberspazio.

2. COMMERCIO ELETTRONICO E LIBERTÀ DI COMUNICAZIONE

Scendendo più nel dettaglio e guardando al primo dei fattori citati poc'anzi, si può innanzi tutto rilevare come le varie attività che vanno a comporre il "commercio elettronico" risultino, a differenza di quanto accade per il commercio tradizionale (almeno quello svolto in appositi locali), veicolate o agevolate da uno strumento comunicativo (in ciò condividendo per vero qualche tratto caratteristico, ad esempio, delle televendite, ma anche, a ben vedere, delle vendite per corrispondenza).

Da questo punto di vista occorre, dunque, far riferimento in via preliminare allo scenario delle telecomunicazioni. Più semplicemente, il particolare contesto del commercio elettronico ci obbliga a fare i conti con una problematica peculiare, cosicché, per esempio, mentre per il banchetto di frutta al mercato rionale il rapporto conformativo coincide con il rapporto regolativo con la pubblica autorità (sia che si consideri la licenza di commercio, sia che si pensi alla concessione per l'uso dello spazio pubblico), nel caso del commercio elettronico anche il rapporto instaurato con il soggetto che gestisce la rete telecomunicativa viene a co-

stituire un fattore conformante e imprescindibile dell'attività economica svolta.

Ma su quest'ultimo aspetto non mancheremo di ritornare più avanti. Si tratta ora piuttosto di rammentare cose abbastanza note e, in particolare, come il settore delle telecomunicazioni abbia conosciuto, sotto l'impulso della normativa comunitaria, un'evoluzione e taluni sconvolgimenti di rilevante portata e, ciò che qui maggiormente interessa, di forte impatto sul piano costituzionalistico.

Non mi riferisco, si badi bene, semplicemente all'emarginazione più o meno consistente che l'art. 43 della Costituzione può aver subito per effetto dell'irrompere nell'ordinamento interno del principio comunitario della concorrenza, così che antichi monopoli hanno perduto, anche nel settore telecomunicativo, la loro legittimazione, ma soprattutto ai riflessi che questo stesso fenomeno ha prodotto sull'esercizio della libertà comunicativa garantita dall'art. 15 della Costituzione.

È infatti possibile sostenere che il nuovo quadro liberalizzato non solo abbia dato nuova consistenza a diritti di natura economica, ma che abbia dato anche piena visibilità ad una serie di posizioni soggettive degli utenti che il vecchio sistema monopolistico (improntato a logiche amministrative) aveva in qualche modo emarginato.

Si tratta, in primo luogo, della possibilità di ragionare chiaramente di un diritto di accedere alla rete telecomunicativa, da concepirsi nel nostro caso anche come una sorta di diritto-madre rispetto a quello eventualmente da riconoscersi in ordine alla connessione ad Internet. Né ad una simile ricostruzione pare opporsi la circostanza che la disciplina costituzionale sembri preoccuparsi più delle modalità della comunicazione che della disponibilità del *medium*. Infatti, anche a non voler aderire alla suggestiva ipotesi per cui il prodursi sempre più accelerato di fenomeni di convergenza multimediale sia di per sé idoneo ad operare una diversa dislocazione dei principi costituzionali (particolarmente visibile nella normativa di liberalizzazione), nel senso cioè che l'accesso alle reti telecomunicative verrebbe comunque ora a fruire di quella libertà di utilizzo del mezzo che è esplicitamente statuita nell'art. 21 della Costituzione, mi pare che sia già possibile trarre da quelle modalità (conferendo cioè portata sostanziale ai termini della libertà e della sicurezza) il pregiudiziale postulato della libertà di accesso al mezzo telecomunicativo.

Se pure in via accessoria rispetto a questo principale diritto, si evidenziano poi altre situazioni soggettive protette, come quella derivante, oltreché dalla segretezza delle comunicazioni, anche dall'obbligo per gli operatori di mantenere un atteggiamento di neutralità rispetto ai contenuti veicolati nella Rete, nel tempo stesso che (come esplicitato dall'art. 3 del d. lgs. 13 maggio 1998, n. 171) incombe al fornitore di un servizio di telecomunicazioni informare gli utenti circa la sussistenza di situazioni che permettano di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei.

In questo stesso ordine di idee può collocarsi ancora il diritto alla sicurezza dei dati personali (previsto dall'art. 2 dello stesso d. lgs. n. 171 del 1998), che comporta che il fornitore di un servizio di telecomunicazioni accessibile al pubblico debba prendere le misure tecniche ed organizzative previste dalla normativa sulla *privacy* per salvaguardare la sicurezza del servizio e dei dati personali, da adottare (quando la sicurezza del servizio o dei dati personali richiede anche misure che riguardano la Rete), congiuntamente con il fornitore della rete pubblica di telecomunicazioni.

Tutti profili, questi, che sicuramente hanno a che fare anche con il commercio elettronico, in cui non tutte le attività si configurano come attività assistite da un regime di pubblicità, ma dove anzi la presenza e l'efficacia di sistemi di protezione costituiscono la condizione pregiudiziale del loro stesso dispiegarsi.

Comunque sia, e in via di estrema sintesi, sembrerebbe di poter convenire, in base ai dati fin qui raccolti, sulla configurazione dell'atto di commercio elettronico fondamentalmente come atto di comunicazione, con il conseguente dispiegarsi nei suoi confronti della corrispondente specifica tutela costituzionale.

3. COMMERCIO ELETTRONICO E LIBERTÀ D'INFORMAZIONE

Ci si potrebbe però ancora chiedere se l'attitudine a reclamare essenziali garanzie costituzionali, da parte dell'atto di commercio elettronico, possa cogliersi non soltanto nel *medium*, ma altresì nel messaggio, specie quando esso assuma le sembianze di un'informazione diramata per l'intero cyberspazio, non diversamente da una qualsiasi altra manifesta-

zione di pensiero. Un aspetto, questo, che riguarda soprattutto quella parte del commercio elettronico che attiene all'attività pubblicitaria.

Purtroppo, non soccorrono qui le medesime certezze viste poc'anzi, in quanto, anche rispetto alla pubblicità in Rete, non possono non riproporsi i dilemmi che caratterizzano in generale l'inquadramento teorico dell'attività pubblicitaria, oscillante tra la stretta inerenza all'esercizio dell'iniziativa economica e l'assorbimento nella libertà di manifestazione del pensiero o della libertà d'informazione.

Tuttavia, com'è noto, non parrebbe quest'ultimo almeno il pensiero della Corte costituzionale, che ha ritenuto la pubblicità commerciale ontologicamente estranea alla libertà garantita nell'art. 21 della Costituzione, reputandola essenzialmente «una componente delle attività delle imprese, come tale assistita dalle garanzie di cui all'art. 41 Cost., e assoggettabile, in ipotesi, alle limitazioni ivi previste ai commi 2° e 3°».

Certo non ci sfugge come la Corte europea dei diritti dell'uomo sia pervenuta da ultimo ad un diverso approdo, ritenendo applicabile alla pubblicità commerciale l'art. 10 della Convenzione in materia di libertà di manifestazione del pensiero. Ma, a parte che questa giurisprudenza presenta ancora aporie importanti (dovute evidentemente alla stessa compromissoria formulazione dell'art. 10), occorre anche notare che, a seguire la tesi dell'inquadramento nei «rapporti civili», risulterebbe di difficile giustificazione, a fronte dell'ineludibile divieto costituzionale di limitazione dell'utilizzo dei mezzi informativi in ragione dei contenuti concreti, qualsiasi disciplina di contingentamento delle quote di pubblicità propria della logica dell'*antitrust*.

Analogamente, se si dovesse privilegiare l'aspetto del pensiero su quello dell'impresa, risulterebbe assai più difficile portare a coerenza tutti quanti i molteplici limiti sostanziali e di metodo che circoscrivono l'attività pubblicitaria e che non mette conto in questa sede richiamare, pur nella consapevolezza che essi valgono anche per Internet.

Per altro verso, tuttavia, questa comunanza di problematiche tra pubblicità tradizionale e pubblicità in Rete non deve impedire di cogliere gli aspetti che fanno della pubblicità internetiana un fenomeno con caratteristiche assolutamente peculiari.

L'informazione commerciale in Rete tende infatti a presentarsi, assai più che per il commercio tradizionale, e comunque in un senso del tutto specifico, come una componente essenziale dell'attività d'impresa, dato

che è naturale che chi accede a qualche mercato virtuale per effettuare un acquisto desideri anche ottenere informazioni in misura considerevolmente più ampia e dettagliata di quanto accada quando la merce può essere direttamente apprezzata, valutata e soppesata su di un banco vendita esposto al pubblico oppure controllata e magari provata presso un'esposizione commerciale.

In quest'ottica, allora, in una sorta di eterogenesi dei fini, l'offerta di informazioni cessa di essere soltanto una necessità economica di chi propone l'acquisto, ma assurge a vera e propria pretesa del consumatore, configurabile legittimamente nei termini di un diritto, così come previsto nel d. lgs. 22 maggio 1999, n. 185 (di attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza).

Ma questa stessa situazione non manca nemmeno di qualche aspetto paradossale, poiché mentre si ragiona di specifici diritti informativi dei consumatori *on-line*, le caratteristiche interattive del mezzo risultano suscettibili di mettere a repentaglio altri aspetti legati sia alla libertà (si pensi alle forme di pubblicità indesiderata), sia, particolarmente per quanto riguarda la più generale attività di *marketing*, alla riservatezza dei suoi destinatari.

A quest'ultimo proposito, anzi, Internet consente di realizzare uno degli obiettivi più ambiziosi della moderna tecnica in tema di ricerche del mercato, vale a dire l'identificazione personale del potenziale cliente, laddove anche l'attività pubblicitaria più avanzata si arresta invece sulla soglia del tipo, per così dire, aggregato di clientela finale e della classificazione dei consumatori in fasce con caratteristiche più o meno omogenee. Ma un *marketing* così personalizzato non può prescindere, se vuole essere efficace, specie in una rete aperta, dall'allestimento di basi di dati accessibili in linea in modo da stabilire in tempo reale delle correlazioni tra ogni genere di dati. Laddove la raccolta di dati non avviene soltanto mediante la collaborazione (per lo più inconsapevole) dell'utente che richiede informazioni tramite qualche *form*, ma con la semplice navigazione sul *Web*, i cui passaggi sono registrati su un *log* del *server* che ospita il sito visitato, per non parlare delle operazioni vere e proprie di stipula del contratto e del pagamento.

Infatti, anche se, a séguito dell'adozione sempre più massiccia come mezzo di pagamento di carte elettroniche di vario tipo anche per acquisti

di beni e di servizi di costo contenuto, il consumatore ha già in parte abdicato al beneficio dell'anonimato, per gli acquisti in Rete la perdita dell'anonimato non costituisce più una scelta operata a fronte della praticità del mezzo di pagamento, ma una necessità ed anzi un requisito obbligatorio della transazione commerciale. Sono anzi la stessa serietà e sicurezza della transazione ad esigere che l'atto di commercio intervenga tra due entità certe e identificate.

Ciò però realizza ancora una volta a favore del venditore una sorta di plusvalore, consistente nella registrazione dei dati del cliente e delle sue propensioni di acquisto, tale anzi che nessun sondaggio di mercato riuscirebbe ad ottenere in maniera così precisa e affidabile.

4. COMMERCIO ELETTRONICO E RISERVATEZZA PERSONALE

La riservatezza individuale si rivela, dunque, un tema critico, sia che si consideri l'atto di commercio elettronico come un atto di comunicazione, sia che lo si configuri, con maggior attenzione al contenuto di questa, come un atto d'informazione.

Si capisce allora perché l'atto di commercio elettronico susciti apprensioni e riserve che l'ordinario atto di commercio non solleva o produce solo in una misura molto marginale. Il particolare contesto nel quale l'atto si compie, dove possiamo aver disseminato numerose tracce del nostro passaggio, e la particolare potenza di intreccio di tutti questi dati da parte della tecnologia utilizzata comporta infatti un'elevazione inaudita della soglia di rischio per la riservatezza personale.

Si tratta, del resto, di una problematica sulla quale si gioca verosimilmente il destino del commercio elettronico o quanto meno la possibilità di un suo decollo significativo e per la quale, com'è noto, si vanno allestendo risposte diverse e anche contrastanti, al di qua e al di là dell'Atlantico.

Ma altri sicuramente approfondiranno con maggior competenza e autorevolezza questa problematica nel corso del convegno.

Al costituzionalista spetta essenzialmente di sottolineare ancora una volta come l'aspetto della riservatezza costituisca un fattore determinante dello *status libertatis* delle persone.

Anche se il concetto di riservatezza è quello per cui maggiormente si sconta la mancanza di riferimenti testuali nella Carta repubblicana, dove

la nozione ottiene al massimo di essere collegata esplicitamente solo a quella di domicilio, ciò non significa che ne debba essere accreditata una valenza, per così dire, soltanto proprietaria, incentrata cioè sulla relazione dominicale o territoriale con determinati luoghi come l'abitazione o l'ufficio.

La riservatezza di cui si controverte oggi attiene invece al più ampio diritto di escludere l'altrui conoscenza con riferimento al dispiegarsi della personalità umana in se stessa considerata. Ciò che sembra trovare migliore considerazione e tutela non semplicemente nell'art. 14, che garantisce l'inviolabilità del domicilio, ma in via sistematica a partire dall'art. 2 della Costituzione che sancisce il riconoscimento e la garanzia dei diritti dell'uomo non solo come partecipe del consorzio sociale, ma anche e pregiudizialmente come "singolo" ed esige che, per lo svolgimento della sua personalità siano apprestati i più adeguati meccanismi di garanzia e rimossi tutti i fattori di impedimento e di condizionamento, fino al riferimento che l'art. 41 fa alla tutela della libertà umana come limite dell'iniziativa economica privata: uno specifico limite, questo, che (sia che alluda alle libertà civili ed economiche, sia alla stessa libertà politica) non mi pare abbia costituito almeno fino a tempi recenti oggetto di soverchia attenzione.

5. COMMERCIO ELETTRONICO E LIBERTÀ ECONOMICA

Il commercio elettronico chiama finalmente in causa le garanzie costituzionali legate alla libertà d'iniziativa economica.

Iniziativa economica suscettibile qui di una duplice considerazione: A) quella, già accennata all'inizio, riguardante gli atti di commercio attinenti alle infrastrutture e ai servizi di telecomunicazione, e B) quella concernente le attività commerciali veicolate in Rete.

A) Ma, mentre riguardo al primo aspetto occorre confrontarsi essenzialmente con la complessa disciplina emanata a vari livelli prevalentemente per fare fronte ad adempimenti di origine internazionale e comunitaria, tesa ad affermare, anche in questo particolare settore, le regole del mercato aperto e della concorrenza (si è peraltro già ricordata la dislocazione di valori costituzionali operata da tale vicenda e comunque l'affievolimento della stessa posizione sovrana dell'ordinamento nel par-

ticolare settore), il secondo aspetto presenta, a nostro modo di vedere, una pluralità di approcci possibili.

B) Si tratta, infatti, di considerare il rapporto degli operatori commerciali in Rete: a) con gli operatori telecomunicativi, b) con gli operatori di commercio non elettronico; c) con la Pubblica Amministrazione; d) con gli utenti consumatori.

a) Ora, per quanto riguarda il problema dell'accesso alla Rete da parte degli operatori commerciali, mi pare che non ci siano problemi particolari, essendo tenuti gli operatori telecomunicativi ad offrire in via di principio il servizio in maniera generalizzata; è, se mai, il problema della responsabilità per le attività svolte in Rete a sollevare qualche discussione, non potendosi in via assoluta escludere un coinvolgimento, ad esempio, del fornitore di spazio *Web* (per solito coincidente con il fornitore di accesso ad Internet) in forme di responsabilità per le attività svolte in Rete, sempre che, in ossequio al principio costituzionale della responsabilità personale, se ne possa individuare, anche soltanto a livello omissivo, un qualche criterio d'imputabilità.

b) Per quanto riguarda il secondo dei piani dianzi menzionati, posto che nei confronti di chi intende offrire un servizio in linea dovrebbero valere le medesime regole applicabili agli stessi servizi nel commercio tradizionale (quindi requisiti soggettivi, se richiesti, iscrizione alla camera di commercio ecc.), dal punto di vista costituzionalistico, si dovrebbe escludere che l'atto di commercio elettronico possa essere assoggettato ad oneri o controlli ulteriori rispetto a quelli eventualmente presenti nel commercio tradizionale per servizi di uguale specie, a meno che non siano razionalmente richiesti dalla specificità del mezzo comunicativo utilizzato.

In questo senso, dunque, occorrerebbe riflettere sul disposto dell'art. 1, comma 6, lett. a), punto 5), della legge n. 249 del 1997, emanato con tutta evidenza da un legislatore ancora inconsapevole della realtà del commercio elettronico, che assoggetta all'obbligo dell'iscrizione nel registro degli operatori di comunicazione, oltretutto le imprese fornitrici di servizi telematici e telecomunicativi, anche l'editoria elettronica e digitale.

Ma il profilo dell'eguaglianza di trattamento chiama in causa anche un'altra questione d'interesse costituzionalistico, che non a caso il convegno si ripropone di affrontare, vale a dire quella della fiscalità in Internet. È, infatti, innegabile che l'atto di commercio rappresenti un indice plau-

sibile per individuare, da un lato, un'occasione di arricchimento da parte di chi effettua vendite in Rete e, dall'altro, una manifestazione di capacità economica, da parte di chi effettua l'acquisto. Si tratta allora di far valere, anche sotto questo particolare profilo, la regola dell'eguaglianza di fronte all'imposizione tributaria, anche se, com'è noto, esiste una forte propensione a prevedere forme di esenzione e di alleggerimento del carico tributario sulle transazioni in Rete al fine di non frenare lo sviluppo del commercio elettronico in un momento in cui i massimi sforzi devono essere rivolti allo stimolo ed all'incentivazione dell'applicazione, che inizia solo ora a suscitare un primo interesse nei cittadini, negli operatori commerciali, nelle imprese.

Occorre però dire che una simile propensione dovrebbe manifestarsi in forme del tutto eccezionali e non eccedenti il carattere della provvisorietà, se non si vuole che venga compromesso il principio di eguale trattamento con grave turbamento delle stesse regole della concorrenza, laddove pare di poter condividere l'idea che incomba piuttosto nell'Amministrazione finanziaria trovare il giusto equilibrio per coniugare le esigenze di regolazione fiscale del settore e di tutela dell'interesse erariale con le esigenze degli operatori rivolte alla rimozione degli ostacoli burocratici che si frappongono allo sviluppo del commercio elettronico ed alla semplificazione degli adempimenti.

c) È, del resto, noto, attraverso gli studi di settore e attraverso le dichiarazioni dei diretti interessati, come uno dei fattori di freno allo sviluppo delle attività d'impresa nel nostro Paese sia costituito dall'insoddisfacente funzionamento della Pubblica Amministrazione, allorché le imprese costituite o costituenti debbano in qualche modo farsi presenti presso i pubblici poteri per l'assolvimento di obblighi, l'accesso alle informazioni e, quando ancora consentito, per l'erogazione di sovvenzioni e contributi.

È però anche opinione accreditata che il coinvolgimento pieno dell'amministrazione nella rete del commercio elettronico potrebbe funzionare da acceleratore dei processi di crescita, specie grazie alla dematerializzazione delle procedure amministrative (si è già iniziato con le dichiarazioni dei redditi, ma le cose da fare, soprattutto nel campo dei servizi alle imprese, restano ancora molte), alla pratica della consulenza *online*, all'allestimento di efficienti banche dati di carattere legislativo e am-

ministrativo e l'integrazione tra i sistemi informativi delle varie amministrazioni del sistema bancario e delle aziende fornitrici di servizi.

Né, ai fini dell'ottemperanza ai valori costituzionali del buon andamento e dell'imparzialità dell'amministrazione, potrebbe trascurarsi l'efficacia in termini di trasparenza e moralizzazione del ricorso a procedure informatizzate in Rete per l'approvvigionamento della Pubblica Amministrazione e di particolare interesse sarebbero, ad esempio, le iniziative finalizzate alla realizzazione di sistemi per la gestione telematica delle gare d'appalto.

d) Ma una medesima logica e tensione civile deve alimentare anche la relazione Pubblica Amministrazione-cittadino consumatore.

Si tratta, come è stato rilevato in un recente documento ufficiale, di uno degli aspetti più qualificanti della cosiddetta "democrazia elettronica": quello cioè che attiene a nuovi rapporti delle pubbliche amministrazioni con il cittadino e che ha implicazioni con il commercio elettronico soprattutto di carattere metodologico, attraverso le pratiche e le procedure che prevedono l'utilizzo di tecniche e tecnologie normalmente utilizzate per il commercio elettronico più "tradizionale", come il documento informatico, la firma elettronica, i pagamenti elettronici, per la semplificazione e lo snellimento dei molteplici rapporti con gli amministrati.

Ma, restando sull'ultimo dei quattro piani sopra indicati, ossia nell'ottica dei consumatori, accanto alle garanzie già accennate a favore del libero sviluppo imprenditoriale, non si possono ovviamente sottacere i limiti che l'art. 41 Cost. appone all'iniziativa economica privata e di cui si è già fatto cenno parlando del rispetto della libertà umana, ma a cui occorre ancora aggiungere il rispetto della sicurezza e della dignità dell'uomo.

Direi che è soprattutto in questo quadro che trovano legittimazione le varie normative che tendono a inquadrare in maniera rigorosa, sottraendola alla pura logica del profitto, la commercializzazione di determinati prodotti. Rischio, questo, che appare amplificato nel quadro del commercio elettronico dove la possibilità dell'instaurarsi di mercati (come dire?) alternativi è grandemente favorita.

Ma anche per l'ordinaria attività di commercio non vanno sottovalutate le cautele a favore del consumatore: cautele che già in qualche modo trovano concretezza nella normativa di tutela del consumatore a livello contrattuale e a cui sarebbe impensabile sottrarre il commercio elettronico.

co, e delle quali anzi occorre verificare la reale efficacia in un ambiente ancora più gravido di rischi per il cliente-utente. A tal proposito, ritorno a ribadire l'importanza del diritto d'informazione: aggiungerei ora "in senso sostanziale", vale a dire come "diritto di comprensione", da misurarsi sulla facilità di movimento e di leggibilità all'interno del sito.

6. ALCUNE CONCLUSIONI

Ma il commercio elettronico, se presenta nuovi problemi relativamente alla riservatezza delle informazioni personali, alla sicurezza delle transazioni finanziarie, e, aggiungiamo pure, alla garanzia di qualità del prodotto, presenta altresì per il consumatore nuove opportunità e vantaggi, nella possibilità di confronto e scelta di produttori, prodotti e prezzi diversi e nell'annullamento del fattore distanza, che possono portare considerevoli benefici.

Da un punto di vista ancor più generale, non si dovrebbero poi ancora trascurare le potenzialità del commercio elettronico al fine di costituire i consumatori in una specie di contropotere capace di mettere le aziende in concorrenza tra loro per soddisfare le esigenze del consumo.

Anche se per il momento solo a livello ottativo, alcune delle esigenze qui rappresentate sono rinvenibili nell'art. 21 d. lgs. 31 marzo 1998, n. 11, che impegna il Ministero dell'industria, del commercio e dell'artigianato, a promuovere l'introduzione e l'uso del commercio elettronico con azioni volte, tra l'altro, a tutelare gli interessi dei consumatori, nonché a favorire l'uso di strumenti e tecniche di gestione di qualità, volte a garantire l'affidabilità degli operatori e ad accrescere la fiducia del consumatore, anche attraverso accordi con associazioni rappresentative dei consumatori, laddove occorre anche non dimenticare che, sul piano delle competenze, tale Ministero (che ha anche istituito un Osservatorio permanente per il Commercio Elettronico) non risulta l'unica struttura di governo interessata, dovendosi fare riferimento anche alla Presidenza del Consiglio dei Ministri per quanto riguarda la proprietà intellettuale (al competente Dipartimento della Presidenza), al Ministero del commercio estero per gli aspetti transfrontalieri del fenomeno in esame, nonché evidentemente alle *authority* cui spettano, direttamente od indirettamente, competenze regolative e di controllo su aspetti toccati dal cosiddetto *e-commerce*.

E proprio su quest'ultimo accenno è forse possibile effettuare qualche notazione conclusiva concernente il ruolo che dovrebbe spettare ad una disciplina del settore. Disciplina che, atteso il terzo dei fattori caratteristici del commercio elettronico accennato all'inizio, e cioè la sua vocazione internazionale, nonché la tendenza alla rapida obsolescenza delle regole giuridiche autoritative a fronte dell'accelerato sviluppo della tecnologia, dovrebbe, da un lato, fare affidamento sulla creazioni di regole stipulate ed accettate a livello internazionale, e, dall'altro, appoggiarsi possibilmente su forme di autoregolamentazione dei soggetti operanti nel settore (come, del resto, auspicato anche da recenti prese di posizione a livello mondiale e comunitario).

Ma, ancora una volta, può allora apprezzarsi la presenza di un quadro costituzionale eterointegrato dalla prospettiva comunitaria, al quale non è pensabile che il commercio elettronico possa essere ritenuto estraneo. Un quadro, dunque, in cui il mercato risulti regolato non semplicemente dalle sue dinamiche interne, ma astretto da vincoli di compatibilità rispetto ai principi supremi della Costituzione nazionale e agli obiettivi da reputarsi ormai anch'essi di valore costituzionale dell'integrazione comunitaria fissati dall'art. 2 del Trattato, come l'occupazione, la protezione sociale, l'ambiente, la qualità della vita, la coesione economico-sociale e la solidarietà.

E-commerce: **normativa e organismi internazionali**

COSTANTINO CIAMPI¹

SOMMARIO: 1. *Introduzione* - 2. *Definizione e tipologia del Commercio elettronico* - 3. *Normative tecniche e giuridiche per il Commercio elettronico* - 3.1. *Premessa* - 3.2. *Protezione dei consumatori* - 3.3. *Protezione del diritto d'autore* - 3.4. *Sicurezza delle transazioni* - 3.5. *Contratti per via elettronica* - 3.6. *Standards tecnici* - 4. *Considerazioni conclusive* - 5 *Appendice: 18 diapositive.*

1. INTRODUZIONE

La mia relazione intende analizzare l'interesse e l'attività (anche normativa: a livello giuridico e tecnico) che diversi organismi internazionali (sia globali che regionali) stanno dedicando, da alcuni anni (o in qualche caso da pochi mesi), al tema del "commercio elettronico" (*e-commerce*, *e-business*, per gli anglofoni), cioè - come abbiamo già sentito nelle precedenti relazioni - al tema delle transazioni commerciali su reti telematiche.

Questi organismi sono molto numerosi, com'è possibile vedere dalle due diapositive che ho preparato (*cf.* § 5. *Appendice: Diapositive 2 e 3*), ed hanno "mandati" parecchio diversi fra loro. Ne ho enumerati 14 a livello globale e 6 a livello regionale, limitandomi a quegli organismi che hanno svolto finora un'azione più incisiva.

L'elenco della Diapositiva 2 raccoglie una tipologia variegata di enti che va: da organizzazioni del settore bancario (WB e BIS) ad organismi di coordinamento sovranazionale nel settore delle poste e delle telecomunicazioni (UPU e ITU); da organismi di coordinamento generale nel settore della conoscenza, della cultura, della scienza, e della proprietà intellettuale (UNESCO, WIPO-OMPI) ad organizzazioni specifiche nel settore del commercio e dei traffici su scala globale (WTO-OMC, UNCITRAL, ecc.).

A livello regionale (cioè di porzioni geograficamente limitate nel mondo) (*cf.* Diapositiva 3) troviamo organizzazioni che si occupano della cooperazione e dello sviluppo economico tra le nazioni ad econo-

¹ c ciampi@idg fi cur it

mia avanzata, come l'OCSE-OECD, che non ha poteri regolamentari cogenti nei confronti dei 29 Paesi che ne fanno parte, o - al contrario - organismi sovranazionali come l'Unione Europea, che con la sua azione e i suoi poteri di normazione, derivanti dai Trattati istitutivi, incide fortemente ogni giorno sugli ordinamenti giuridici dei 15 Paesi membri.

Naturalmente in questo mio intervento, per ovvie ragioni di tempo, esaminerò soltanto l'azione di alcune organizzazioni internazionali, e di questi organismi citerò solo le principali linee direttrici nei confronti del tema emergente di nostro interesse.

Le ragioni del crescente interesse delle organizzazioni internazionali per l'*e-commerce* è facilmente comprensibile.

La comunicazione elettronica e il commercio elettronico su scala mondiale stanno acquistando sempre maggiore importanza e costituiranno uno dei fattori chiave per lo sviluppo globale della società dell'informazione.

In effetti, in pochi decenni e con rapidità impensabile all'origine del fenomeno, si è passati dall'economia rurale e dalle contrattazioni con stretta di mano, nelle fiere e mercati delle nostre piazze, alle transazioni multi-miliardarie tra persone che non si conoscono direttamente e che si scambiano documenti e consenso attraverso le tecnologie del documento telematico e della firma digitale.

Le stime del volume globale di affari toccato dal commercio elettronico sono le più varie. Le più prudenti (*gr.* Diapositiva 4) parlano di circa 100 miliardi di dollari nel 1999 con un tasso di crescita pari al 100% annuo che, se mantenuto costante, porteranno ad oltre 1.500 miliardi di dollari il valore delle contrattazioni su reti telematiche di qui a quattro anni (stime meno prudenti parlano addirittura di 3.000 miliardi di dollari).

Per valutare le conseguenze indotte dal nuovo paradigma dell'economia elettronica, basta sfogliare quotidiani e riviste (anche non specializzate) e soprattutto navigare sulla Rete. L'economia mondiale è ormai realmente avviata verso la globalizzazione dei mercati: fenomeni che accadono in un Paese hanno implicazioni a migliaia di chilometri di distanza.

Sono molteplici i fattori di tipo economico, culturale e politico-legislativo che hanno influenzato, e continueranno a influenzare,

l'adozione e la penetrazione delle nuove tecnologie nelle prassi commerciali delle diverse aree del mondo e dei singoli Paesi.

Qui, nella diapositiva, ne sono elencati alcuni:

- la liberalizzazione normativa,
- la capacità di adattamento culturale,
- il Prodotto Interno Lordo (PIL),
- la penetrazione di Internet e
- il relativo tasso di crescita degli accessi alla Rete.

L'influenza della legislazione sullo sviluppo del commercio elettronico costituirà oggetto specifico della seconda parte del mio intervento. Qui converrà esaminare brevemente alcune cifre relative alla penetrazione di Internet a livello mondiale.

Si osservino le cifre presentate nel diagramma (*cf.* Diapositiva 5). Su oltre 171 milioni di persone collegate nel mondo ad Internet (la stima si riferisce al maggio di quest'anno), gli Stati Uniti e il Canada coprono quasi 97 milioni di accessi per una percentuale del 56,6%, contro 40 milioni di utenti europei, che rappresentano appena il 23,4% del totale.

Anche questo secondo diagramma (*cf.* Diapositiva 6) mette in evidenza il *gap* che divide l'Europa e, in particolare l'Italia, dagli Stati Uniti: negli USA il 37% della popolazione utilizza Internet, cioè più di 1 americano su tre utilizza normalmente la Rete, mentre in Italia solo il 2,7 % della popolazione, per un totale di circa 1.500.000 di individui, usa sporadicamente la Rete. Migliore la situazione in Francia con l'8% della popolazione che utilizza Internet e soprattutto nel Regno Unito dove si raggiungono punte del 15% di utilizzo, rapportate all'intera popolazione.

L'ultimo diagramma di questo gruppo di diapositive (*cf.* Diapositiva 7) mette a raffronto la penetrazione di Internet rispetto alla penetrazione di altri strumenti tecnologici della moderna società dell'informazione, quali gli apparecchi di telefonia mobile e la televisione via cavo che concorrono con le reti telematiche allo sviluppo del commercio elettronico. Su una popolazione mondiale stimata in 6 miliardi di persone alla fine di quest'anno esistono 500 milioni di telefoni cellulari, contro meno di 200 milioni di stazioni collegate con Internet e 140 milioni di televisioni via cavo. La proiezione di questi dati tra 4 anni, nell'anno 2003, prevede su una popolazione mondiale di 7 miliardi di individui 1 miliardo e 200 mi-

lioni di telefoni cellulari, oltre 800 milioni di PC collegati con Internet e 350 milioni di televisioni via cavo.

Oltre al governo americano, decisamente impegnato a favorire e a finanziare lo sviluppo dell'economia elettronica e di Internet (si leggano in proposito il rapporto dell'amministrazione Clinton dal titolo "*A Framework for Global Electronic Commerce*" e l'ultimo rapporto del Dipartimento del Commercio Statunitense del giugno 1999, intitolato "*The Emerging Digital Economy II*"; il primo rapporto era dell'aprile 1998), numerosi Paesi stanno studiando e finanziando iniziative per promuovere e regolamentare l'utilizzo delle reti per le transazioni commerciali e comunicative in ambito pubblico e privato (cfr. Diapositiva 8).

Di particolare interesse è il secondo rapporto preparato da AGB, una federazione delle più importanti associazioni informatiche e telematiche nel mondo, presentato a Parigi nel *Forum* dell'OCSE svoltosi due settimane fa, che è intitolato "*A Global Action Plan for Electronic Commerce*" (cfr. Diapositiva 9).

Il denso rapporto, di oltre 85 pagine, scritto congiuntamente dalle maggiori associazioni di settore, presenta un "interessante Decalogo di principi fondamentali" indirizzato ai Governi membri dell'OCSE. Questi principi sono indicati come punti chiave per lo sviluppo equilibrato del commercio elettronico.

Particolarmente condivisibile è l'ultimo punto nel quale s'insiste sulla necessità che i Governi e il settore privato aumentino la fiducia dei cittadini nell'infrastruttura globale dell'informazione con un'azione congiunta perseguita attraverso il sistema educativo, l'innovazione tecnologica, la sicurezza delle reti, l'adozione di codici di autodisciplina e di adeguati meccanismi di risoluzione delle controversie.

Certamente dove non c'è sicurezza negli scambi e fiducia negli operatori che vi partecipano, il mercato - secondo l'antica saggezza - non può durare e non può prosperare.

L'Unione Europea, proprio tenendo conto di queste esigenze e dell'urgenza di controllare e dirigere in qualche modo il fenomeno della globalizzazione dell'economia elettronica, ha da tempo costituito una commissione con il compito di definire una politica di interventi volti a favorire lo sviluppo del commercio elettronico, soprattutto nelle piccole e medie imprese.

Com'è indicato nel grafico proiettato (*cf.* Diapositiva 10), gli interventi sono molteplici e articolati: essi vanno dall'introduzione di norme volte a favorire la libera circolazione delle merci e dei servizi sulle reti, alla politica di liberalizzazione delle telecomunicazioni e di protezione dei consumatori, e infine alle misure di prevenzione di fenomeni di criminalità, così facili a diffondersi per via elettronica.

Va sottolineato che per un equilibrato sviluppo del settore sono estremamente rilevanti gli aspetti legati:

- alla sicurezza delle transazioni,
- alla definizione degli *standards* internazionali, e
- all'impegno del legislatore nel definire chiaramente le regole e le modalità di relazione tra i soggetti coinvolti nelle attività di commercio elettronico.

Questi aspetti sembrano essere i prerequisiti essenziali per lo sviluppo dell'economia elettronica in Europa.

L'Unione Europea molto tempestivamente sin dal 1997/98 si è preoccupata di definire² e regolare i servizi della società dell'informazione in una direttiva poco conosciuta, la n. 48 del 20 luglio 1998, che modifica la precedente direttiva n. 34 dello stesso anno. Con questa direttiva si pone a carico degli Stati membri l'obbligo di notificare all'Unione tutte le future normative nazionali che si applicheranno ai servizi della società dell'informazione.

Recentemente, inoltre, nell'ambito del *Quinto Programma Quadro (1998-2002)* la Commissione europea ha lanciato un programma specifico di ricerca e di sviluppo tecnologico intitolato "La società dell'informazione di facile uso" finanziato con 3.600 milioni di euro, nel quale si intersecano molti progetti che hanno una qualche relazione con le tematiche del commercio elettronico.

² "Qualsiasi servizio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi". I principi essenziali della direttiva sono quelli della validità della normativa del "Paese d'origine" del prestatore di servizi, del mutuo riconoscimento, dell'assenza di autorizzazione preventiva. Sono previsti requisiti di trasparenza e obblighi specifici d'informazione; si obbligano gli Stati a promuovere codici di condotta, si prevede la composizione stragiudiziale delle controversie "anche per vie elettroniche adeguate". In materia di tutela del consumatore, si applica (ma con alcune riserve) il principio cosiddetto "del Paese d'origine".

2. DEFINIZIONE E TIPOLOGIA DEL COMMERCIO ELETTRONICO

Secondo la definizione espressa in un documento comunitario³ (cfr. Diapositiva 11), il commercio elettronico consiste nello svolgimento di attività commerciali e di transazioni per via elettronica e comprende attività diverse, quali:

- la commercializzazione di beni e servizi;
- la distribuzione *on-line* di contenuti digitali (musica, libri, *software*, ecc.);
- le operazioni finanziarie e di borsa;
- gli appalti pubblici ed altre procedure transattive della Pubblica Amministrazione, sempre effettuate per via telematica.

Il commercio elettronico non si esaurisce quindi nei trasferimenti elettronici dei fondi e dei documenti (questi sono solo uno degli elementi chiave per lo sviluppo delle transazioni commerciali su Rete), ma comprende anche le altre fasi del rapporto transattivo: dalla fase di ricerca ed individuazione dell'interlocutore a quella di trattativa e negoziazione; da quella degli adempimenti e delle scritture formali a quella dei pagamenti e della consegna fisica o elettronica del bene o servizio acquisito.

Possono distinguersi quattro diverse categorie di commercio elettronico:

- da operatore commerciale a operatore commerciale (*business to business*): è il caso dell'impresa che usa la Rete per inviare ordini ai propri fornitori, ricevere fatture, effettuare pagamenti; è già utilizzato da anni, in particolare attraverso l'EDI sulle reti private;
- da operatori commerciali a consumatori (*business to consumer*): corrisponde alla vendita elettronica al minuto ed ha avuto una grande espansione grazie al servizio *Web* di Internet;
- da operatori commerciali alle amministrazioni pubbliche (*business to administration*): copre tutti i tipi di transazioni elettroniche tra imprese e Pubblica Amministrazione; per esempio,

³ Comunicazione della Commissione Europea al Parlamento, al Consiglio, al Comitato economico e sociale e al Comitato delle regioni, COM (97) 157, "Un'iniziativa europea in materia di commercio elettronico".

negli Stati Uniti, le richieste di forniture pubbliche vengono pubblicizzate su Internet, e le imprese possono rispondere per via elettronica;

- da consumatori alle amministrazioni pubbliche (*consumer to administration*): è ancora all'inizio, ma potrà avere una forte espansione, in particolare nel nostro Paese quando verrà realizzata la Rete Unitaria della Pubblica Amministrazione, instaurando un rapporto diretto tra P.A. e cittadino.

Tra le varie aree di applicazione del commercio e delle transazioni elettroniche, è particolarmente rilevante quella relativa ai rapporti tra la Pubblica Amministrazione e le aziende, da una parte, e i cittadini, dall'altra. Quest'ultimo ambito, in realtà più attinente alle tematiche della cosiddetta "democrazia elettronica" e ai rapporti innovativi delle pubbliche amministrazioni coi cittadini, ha collegamenti con il commercio elettronico limitatamente alle pratiche e alle procedure che prevedono l'impiego di tecniche e tecnologie generalmente utilizzate per il commercio elettronico in senso proprio: come il documento informatico, la firma digitale (o elettronica), i pagamenti elettronici. Ma questa area è in forte espansione soprattutto in quei Paesi, come l'Italia, dove i pubblici poteri hanno investito ingenti risorse nelle infrastrutture di reti pubbliche per migliorare i servizi al cittadino e lo scambio di informazioni tra le amministrazioni.

3. NORMATIVE TECNICHE E GIURIDICHE PER IL COMMERCIO ELETTRONICO

3.1. Premessa

Anche se già oggi esistono le premesse, sia giuridiche (in parte) sia tecnologiche, affinché l'impiego dei servizi *on-line* tra imprese, individui (consumatori) e pubbliche amministrazioni si estenda gradualmente alla maggior parte dei rapporti tra questi soggetti, le operazioni di commercio elettronico non sono però attualmente disciplinate in modo specifico e completo.

Esistono, infatti, ampi spazi d'indeterminazione e di libertà per numerosi aspetti della materia (tra cui quello fiscale e quello della tutela dei dati personali), per i quali occorre individuare soluzioni giuridiche che

rendano compatibili le transazioni telematiche con la disciplina del commercio tradizionale, suscitando la fiducia degli utenti sia pubblici che privati. La natura stessa del commercio elettronico richiede poi un approccio che oltrepassi i confini nazionali e sappia particolarmente bilanciare i vari interessi, pubblici e privati, emergenti nel settore.

Con riguardo al quadro internazionale, le linee d'intervento più recenti sono state tracciate nella Conferenza ministeriale di Ottawa dell'OCSE (nell'ottobre 1998) sul tema "Un mondo senza frontiere: concretizzare il potenziale del commercio elettronico mondiale"⁴. La Conferenza si è conclusa con tre specifiche Dichiarazioni, relative a:

- protezione della vita privata sulle reti telematiche;
- protezione dei consumatori nel contesto del commercio elettronico;
- autenticazione per il commercio elettronico.

Il primo di questi aspetti è ora al centro dell'attenzione in una serrata trattativa tra l'Unione Europea e gli Stati Uniti riguardo alla tutela da garantire ai dati personali che viaggiano tra i due continenti. La direttiva europea (Direttiva 97/66/CE) prevede lo scambio dei dati solo con i Paesi che garantiscono un adeguato livello di protezione. La discussione con gli Stati Uniti è fondamentale perché destinata ad orientare le determinazioni verso gli altri Paesi. In gioco sembra esserci non solo uno scontro tra lo statalismo europeo e il liberismo americano (basti pensare che nel corso del 1998 gli Stati federali hanno promulgato ben 758 leggi in materia di *privacy*), ma qualcosa di più in termini di libertà e di sviluppo, per cui deve potersi contare su una base giuridica forte.

Più recentemente l'OCSE ha organizzato a Parigi il 12 e 13 ottobre di quest'anno, cioè appena due settimane fa, un *Forum* internazionale sul commercio elettronico, i cui atti sono consultabili su Internet, all'indirizzo indicato nella Diapositiva (*cf.* Diapositiva 12). Alla Conferenza hanno partecipato oltre ai rappresentanti dei vari Governi nazionali, anche i rappresentanti di tutte le organizzazioni sovranazionali (elencate nelle prime diapositive) che hanno interesse allo sviluppo e alla regolamentazione del commercio elettronico.

⁴ Le conclusioni della Conferenza, svoltasi ad Ottawa dal 7 al 9 ottobre 1998, sono pubblicate anche in allegato alla Relazione 1998 dell'Ufficio del Garante per la protezione dei dati.

Dai vari interventi alla Conferenza OCSE di Parigi può essere ricavato un quadro d'insieme di tutti i problemi giuridici sul tappeto nell'ambito del commercio elettronico e degli organismi che stanno lavorando alla loro risoluzione. Questo quadro d'insieme è rappresentato, in forma sintetica, nella Diapositiva che vedete proiettata.

Cito, a titolo di esempio, il problema dei «nomi di dominio», per la cui regolamentazione è di importanza fondamentale il lavoro svolto in seno all'OMPI (WIPO) che ha prodotto una Raccomandazione indirizzata all'ICANN, cioè all'organismo di Internet deputato ad assegnare i «nomi di dominio» (cioè gli indirizzi in chiaro dei siti *Web*), che sono spesso fonte di controversie giudiziarie.

3.2. Protezione dei consumatori

Un incentivo allo sviluppo del settore viene ora dalla Direttiva 97/7/CE, del 20 maggio 1997, sulla tutela dei consumatori in materia di contratti a distanza e dal suo integrale recepimento col d. lgs. 22 maggio 1999, n. 185⁵ e dalla Proposta di direttiva europea sul commercio elettronico (COM (99) 0427, nella versione modificata a seguito degli emendamenti approvati dal Parlamento europeo), che esamineremo più avanti (*cf.* Diapositiva 13).

Per ciò che attiene in particolare alla protezione dei consumatori, questa proposta di direttiva prevede una serie di misure che rafforzeranno la tutela del consumatore e aumenteranno la sua fiducia nei nuovi servizi in Europa.

In particolare:

- essa farà diminuire i rischi di attività illegale su Internet in Europa attraverso effettivi controlli delle autorità nazionali alla fonte stessa delle attività (nello Stato membro in cui risiede l'impresa interessata) e responsabilizzerà le autorità nazionali rispetto al loro obbligo di tutelare l'interesse generale non solo all'interno delle proprie frontiere, ma in tutta la Comunità e nell'interesse dei cittadini degli altri Stati membri;

⁵ Il decreto si applica naturalmente, come già previsto dalla direttiva, ai contratti tra fornitori e consumatori, stipulati utilizzando una o più tecniche di comunicazione a distanza, nell'ambito di un sistema di vendita o prestazione di servizi organizzati dagli stessi fornitori. Esso tutela il consumatore per tre aspetti fondamentali: sotto il profilo dell'informazione, del recesso e delle «garanzie ulteriori» rispetto a quelle previste dalla Direttiva europea.

- essa impone agli operatori obblighi di informazione e di trasparenza, indispensabili perché i consumatori possano prendere decisioni ponderate;
- essa offre alcune nuove garanzie nelle relazioni contrattuali, come l'obbligo di mettere a disposizione degli utenti mezzi che gli consentano di correggere errori di manipolazione, o il chiarimento del momento in cui un contratto *on-line* viene concluso e la necessità per il fornitore di inviare una ricevuta di ritorno;
- essa, infine, garantisce migliori mezzi di ricorso incoraggiando i codici di autodisciplina e rendendo possibile l'uso *on-line* di meccanismi extragiudiziali di composizione delle vertenze (conciliazioni, arbitraggi), facilitando ricorsi giurisdizionali rapidi ed efficaci e istituendo punti di contatto negli Stati membri per assistere i consumatori.

Anche l'OCSE è attiva in questo settore. Sta completando il suo lavoro sulle *Guidelines for Consumer Protection in the Context of Electronic Commerce*, che si prevede saranno pronte entro la fine di quest'anno.

3.3. Protezione del diritto d'autore

Il diritto d'autore, com'è noto, è il frutto di una sorta di monopolio riconosciuto da un ordinamento giuridico. All'autore di un'opera viene conferito il diritto esclusivo di utilizzazione dell'oggetto della proprietà - il prodotto dell'ingegno e dell'intelletto - e quindi il diritto di impedirne l'uso non consentito da parte di terzi, per un predeterminato periodo di tempo.

La protezione del diritto d'autore, in passato, è stata resa possibile da due presupposti: la *materializzazione* del prodotto su supporti fisici (per lo più cartacei) e la tutela dell'opera all'interno di una *specificata organizzazione territoriale*, ove essa esiste nella sua materialità.

Entrambi questi presupposti divengono sempre più evanescenti con il progresso tecnologico sviluppatosi negli ultimi decenni e con l'affermarsi della società dell'informazione: la tecnologia attuale permette a chiunque sia di dematerializzare l'opera con costi ridottissimi, rendendola quindi priva del suo supporto materiale, sia di trasmetterla e diffonderla senza vincoli posti da limiti territoriali e da confini di sovranità.

È questa una delle nuove ricchezze del mondo contemporaneo, misurabile non più in tonnellate d'acciaio o in merci prodotte, ma in *bit* (per parafrasare Negroponte). Ma è proprio questa ricchezza che costituisce la causa dell'impoverimento della possibilità di tutela del diritto d'autore e del monopolio che esso involge.

Paradossalmente, proprio nel momento in cui l'autore avrebbe potuto sfruttare nel modo più completo il prodotto del proprio ingegno, quest'obiettivo sfugge perché proprio la globalizzazione dell'informazione e l'eliminazione della componente territoriale rendono impossibile garantire e proteggere il diritto.

Non è ancora del tutto chiaro come questa crisi possa essere superata. Certamente la sua protezione non potrà più essere quella organizzata e fissata in passato. Ma, di fronte a questo problema, si manifestano, come osserva un esperto giurista del settore, Paolo Auteri, parafrasando Umberto Eco, due atteggiamenti antitetici: quello degli "Integrati" e quello degli "Apocalittici".

Secondo i primi, è sufficiente adeguare l'istituto alla nuova realtà, in modo da garantire con nuovi mezzi tecnici e giuridici la protezione del titolare del diritto. Secondo gli "Apocalittici", invece, è necessario ripensare il diritto d'autore dalle sue fondamenta, non essendo possibile mantenere in vigore un istituto sorto in una situazione storica, giuridica, tecnologica e culturale totalmente diversa da quella attuale.

Quel che è certo è che la protezione del diritto d'autore in Internet costituisce uno dei temi più dibattuti e fonte di ormai numerosissime controversie giudiziarie.

A livello dell'Unione Europea, tra gli anni 1988 e 1995, sono stati pubblicati vari Libri Verdi su questi argomenti, tra cui:

- *Il diritto d'autore e le sfide tecnologiche: problemi di diritto d'autore, che richiedono un'azione immediata*, Bruxelles, 7 giugno 1988
- *Il diritto d'autore e i diritti connessi nella società dell'informazione*, Bruxelles, 9 luglio 1995.

Molte sono le direttive che si sono occupate del diritto d'autore, per lo più integrando e rafforzando le normative internazionali in materia (cfr. Diapositiva 14). Ricordo in particolare:

- la direttiva 250/91, recepita in Italia con d. lgs. n. 518/1992, con la quale è stata introdotta un'apposita tutela per il *software*, parificandolo all'opera letteraria;
- e la direttiva 9/96, recepita in Italia con d. lgs. 6 maggio 1999, n. 169, con la quale è stata introdotta una specifica autonoma protezione per gli autori delle banche dati.

Recentemente, in data 10 febbraio 1999, il Parlamento europeo si è pronunciato a favore della proposta di direttiva sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (Documento 599PC0250).

Si richiama l'attenzione sui diversi "Considerando", che affrontano il problema della distribuzione delle opere su Rete, della loro identificazione e dei modelli di consumo *on line* di materiale protetto.

3.4. Sicurezza delle transazioni

Su questo punto centrale non mi soffermo molto perché immagino sarà oggetto di altri interventi nel corso di questo Convegno.

Ricorderò soltanto che il 13 maggio 1998, su iniziativa di Martin Bangemann e di Mario Monti, allora Commissari responsabili rispettivamente per le telecomunicazioni e per il mercato unico, la Commissione europea ha avanzato una proposta di direttiva che istituisce un quadro giuridico per l'uso delle firme elettroniche (*cfr.* Diapositiva 15). Il Parlamento si è già pronunciato in prima lettura il 6 maggio scorso e appena qualche giorno fa in seconda lettura.

Gli elementi principali della proposta di direttiva attengono a:

- i requisiti essenziali per i servizi di certificazione delle firme elettroniche;
- la responsabilità dei fornitori di servizi di certificazione;
- l'equiparazione della validità giuridica delle firme elettroniche certificate rispetto a quelle autografe;
- un quadro neutrale dal punto di vista tecnologico rispetto alla tecnologia utilizzata per apporre firme elettroniche;
- il campo d'applicazione della direttiva che non si applica ai gruppi chiusi di utenti, quali le intranet aziendali o i sistemi bancari;

- l'assenza di un regime autorizzativo per i servizi di certificazione;
- la dimensione internazionale del problema: per agevolare il commercio elettronico su scala mondiale, la proposta include meccanismi per la cooperazione con i Paesi terzi in materia di reciproco riconoscimento dei certificati, sulla base di accordi bilaterali e multilaterali.

Il quadro d'insieme che ne deriva è che questa proposta di direttiva è meno rigida e più liberale del quadro normativo ormai vigente in Italia in tema di firma digitale. La regolamentazione della firma digitale in Italia, com'è noto, è stata costruita dal nostro legislatore attraverso un procedimento legislativo complesso, il cui elemento principale è il D.P.R. 10 novembre 1997, n. 513, che ha riconosciuto validità giuridica all'uso delle tecnologie informatiche e telematiche per formare, archiviare e trasmettere documenti, al quale hanno fatto seguito il D.P.C.M. 8 febbraio 1999 recante il Regolamento tecnico e la Circolare AIPA n. 22 del 26 luglio 1999, contenente disposizioni circa le modalità di iscrizione nell'albo dei certificatori.

Probabilmente quando la direttiva sarà approvata definitivamente ed entrerà in vigore il nostro legislatore, che insieme alla Germania era stato tra i primi a recepire l'innovazione tecnologica nel proprio sistema economico-giuridico con il riconoscimento delle firme digitali, dovrà riadattare la propria legislazione per armonizzarla con la normativa europea. Peraltro, bisogna dire che il nostro legislatore si era opportunamente cautelato, prevedendo la possibilità, ogni due anni, di modificare il *Regolamento tecnico* secondo le «esigenze dettate dall'evoluzione delle conoscenze scientifiche e tecnologiche».

3.5. Contratti per via elettronica

Sull'argomento della contrattazione per via elettronica esiste fondamentalmente una *Proposta di direttiva europea sul commercio elettronico* (COM (99) 0427, nella versione modificata a seguito degli emendamenti approvati dal Parlamento europeo) (*cf.* Diapositiva 16).

La Proposta di direttiva instaura un quadro giuridico per i servizi della società dell'informazione indicati, richiamando la definizione di cui alla Direttiva 83/189/CE (così come modificata dalla Direttiva 98/48/CE). In questa direttiva i nuovi servizi vengono definiti come "qualsiasi servi-

zio prestato normalmente dietro retribuzione, a distanza, per via elettronica e a richiesta individuale di un destinatario di servizi”.

I principi essenziali della proposta sono quelli: della validità della normativa del “Paese d’origine” del prestatore di servizi; del mutuo riconoscimento; dell’assenza di autorizzazione preventiva. Sono previsti requisiti di trasparenza e obblighi specifici d’informazione; si obbligano gli Stati a promuovere codici di autodisciplina; si prevede la composizione stragiudiziale delle controversie “anche per vie elettroniche adeguate”. In materia di tutela del consumatore, si applica (ma con alcune riserve) il principio cosiddetto “del Paese d’origine”⁶.

⁶ Nella proposta di direttiva vengono in particolare esaminate 5 questioni fondamentali

1) *Il luogo di stabilimento dei fornitori di servizi della società dell’informazione*

La proposta permette di eliminare l’attuale incertezza giuridica in materia, dando una definizione del luogo di stabilimento conforme ai principi enunciati nel trattato e nella giurisprudenza della Corte di giustizia il che è fondamentale per il regolare funzionamento del mercato unico. Essa vieta poi procedure di autorizzazione specifiche ai servizi della società dell’informazione e fissa, riguardo le informazioni, i requisiti che il fornitore deve soddisfare per garantire la trasparenza delle sue attività.

2) *Le comunicazioni commerciali (pubblicità, marketing diretto, ecc.)*

La comunicazione commerciale è un altro aspetto essenziale della maggior parte dei servizi di commercio elettronico. Occorre precisare e agevolare l’uso. La proposta definisce dunque la nozione di “comunicazione commerciale” e fissa, in proposito, requisiti di trasparenza per guadagnare la fiducia dei consumatori e incoraggiare pratiche commerciali leali. Per consentire ai consumatori rapide reazioni in caso di ingerenze dannose, la proposta impone che le comunicazioni commerciali per via elettronica siano chiaramente identificate e che, per quanto riguarda le professioni regolamentate (come gli avvocati), le legislazioni nazionali relative alla comunicazione commerciale permettano la prestazione di servizi *on-line*, nel rispetto delle norme deontologiche. A tal fine, le organizzazioni professionali dovranno elaborare appositi codici di condotta.

3) *La conclusione di contratti on-line*

Il commercio elettronico non potrà veramente svilupparsi se sarà difficile concludere contratti *on-line* per requisiti di tipo formale, non adeguati a questo tipo di ambiente. Gli Stati membri devono rivedere la loro legislazione in questo senso. La proposta, precisando il momento in cui viene concluso - in alcuni casi - il contratto, permette anche di eliminare talune incertezze giuridiche, lasciando intatta la libertà contrattuale.

4) *La responsabilità degli intermediari.*

È generalmente ammesso che, per facilitare il commercio elettronico, vada precisata la responsabilità dei fornitori di servizi *on-line* riguardo la trasmissione e lo stoccaggio di informazioni appartenenti a terzi (tali fornitori agiscono allora da “intermediari”). Per eliminare l’attuale incertezza giuridica e ottenere approcci coerenti da parte degli Stati membri, la proposta prevede una deroga se i fornitori effettuano un “semplice trasporto” e limita la loro responsabilità riguardo ad altre attività “di intermediario”. Nella ricerca di un prudente equilibrio tra gli interessi in gioco, viene incoraggiata la cooperazione tra le parti e limitato il rischio di attività *on-line* illecite.

5) *L’attuazione delle normative*

Anziché elaborare nuove norme, la Commissione cerca l’attuazione effettiva delle norme comunitarie e delle legislazioni nazionali vigenti. Consolidandone i relativi meccanismi, essa favori-

Con il moltiplicarsi delle transazioni commerciali svolte con i nuovi mezzi tecnologici senza limiti di frontiere, è divenuto difficile definire la giurisdizione di una controversia, quando sorgono problemi tra compratore e fornitore. Sorgono, infatti, due questioni fondamentali.

- Qual è il giudice competente a conoscere della controversia?
- Qual è la legge che il giudice dovrà applicare?

Chiara perciò la necessità di adattare al nuovo scenario tecnologico la vecchia convenzione di Bruxelles del 1968, che disciplinava la competenza giudiziaria in campo commerciale e civile. Per questo, la Commissione europea ha presentato una nuova proposta di aggiornamento dell'accordo, che introduce norme uniformi e al passo con i tempi, per definire la competenza giudiziaria in campo commerciale e civile, cercando di semplificare e accelerare l'esecuzione delle decisioni. Il Consiglio dell'Unione ha iniziato, alla fine del 1997, a lavorare alla revisione della convenzione di Bruxelles per allinearne le disposizioni su quelle della convenzione di Lugano. Il 27 maggio 1999 il Consiglio è pervenuto, pronunciandosi all'unanimità, ad un accordo politico sulle disposizioni sostanziali. La proposta di regolamento adottata il 14 luglio u.s. dalla Commissione tra propria in l'arghissima misura il testo di questo accordo politico [doc. COM(99)348].

La Commissione ha inoltre deciso di organizzare nei prossimi giorni, il 4 e 5 novembre a Bruxelles, un'audizione sul tema "Commercio elettronico: competenza giudiziaria e legge d'applicazione", al fine di consentire a tutti coloro che operano nel settore del commercio elettronico, e in particolare alle varie categorie di operatori economici e di consumatori (senza dimenticare i legislatori, le autorità di regolamentazione e altri gruppi interessati) di esprimere la propria opinione.

sce l'istituzione di un vero mercato interno – fondato sulla fiducia reciproca tra gli Stati membri. A questo scopo, essa incoraggia l'elaborazione di codici di condotta su scala comunitaria, stimola la cooperazione amministrativa tra gli Stati membri e facilita l'attuazione di altri sistemi efficaci di composizione delle controversie a livello transnazionale. Per ragioni analoghe, la proposta prevede l'obbligo per gli Stati membri di istituire un sistema di ricorso giurisdizionale rapido ed efficace, adeguato all'ambiente *on-line*.

3.6. *Standards tecnici*

Accanto alla normativa giuridica di cui abbiamo finora discusso, un ruolo preponderante per lo sviluppo del commercio elettronico assume anche la normativa tecnica, emanata dagli organismi internazionali di normalizzazione (cfr. Diapositiva 17).

Lo *standard* più conosciuto finora nell'ambito delle transazioni commerciali su Rete è stato l'EDI (*Electronic Data Interchange*) che è divenuto anche norma ISO col numero identificativo 9735; in tempi più recenti si è aggiunto il protocollo SET (*Secure Electronic Transaction*) per i pagamenti elettronici.

Attualmente, sono allo studio nuovi *standards* che accompagnano l'evoluzione della tecnologia *Web* di Internet, verso la seconda generazione.

Conformemente a questa tendenza, l'organismo delle Nazioni Unite per i servizi commerciali e il commercio elettronico (UN/CEFACT) e l'Organizzazione per la promozione delle informazioni strutturate (OASIS) hanno avviato i lavori in vista di stabilire norme valide a livello mondiale per le specifiche commerciali della tecnologia XML (*eXtensible Mark-up Language* - Linguaggio di marcatura estensibile).

Le due organizzazioni hanno stabilito un gruppo di lavoro per l'applicazione della tecnologia XML nel commercio elettronico, al fine di elaborare un quadro tecnico che consentirà un approccio compatibile allo scambio dei dati elettronici.

In effetti, la tecnologia XML figura tra le più importanti tecnologie emergenti per le comunicazioni globali su Internet, poiché consente lo scambio dei cosiddetti dati "intelligenti", pronti ad essere analizzati, selezionati, formattati e personalizzati.

L'idea è che la combinazione di un trattamento più efficiente, di una ricerca più accurata e di *links* più flessibili potrebbe rivoluzionare il modo di fare affari sul *Web* e contribuire, nel lungo termine, alla crescita del commercio elettronico su scala mondiale.

L'esigenza di nuovi *standards* più sicuri è sentita anche nel settore della cifratura dei dati e delle chiavi asimmetriche assegnate ai soggetti che intendono firmare in forma digitale i loro documenti, nonché in quello delle chiavi biometriche, per l'identificazione dei soggetti che operano in Rete.

4. CONSIDERAZIONI CONCLUSIVE

Mi avvio rapidamente alla conclusione (*gr.* Diapositiva 18).

Nel corso del mio intervento ho evidenziato l'enorme portata delle nuove tecnologie e ho mostrato che tutti i programmi dei Paesi tecnologicamente più avanzati, d'oltreoceano ed europei, i *summit* e le conferenze dei più vari organismi internazionali - dall'Unione Europea all'Organizzazione per la cooperazione e lo sviluppo economico (OCSE-OECD); dall'Organizzazione mondiale per il commercio (OMC-WTO) all'Organizzazione internazionale di standardizzazione (ISO) - sottolineano il ruolo decisivo affidato ai poteri pubblici in questo settore, cui spettano funzioni normative, di promozione e realizzazione di progetti in aree ritenute prioritarie, di standardizzazione tecnologica.

Una prima considerazione da fare è che, in presenza di un panorama tecnologico e normativo radicalmente mutato, appaiono oggi del tutto inadeguati gli approcci settoriali via via seguiti nell'affrontare questa materia. S'impone ormai una visione d'insieme dei vari problemi ad esso attinenti e delle loro reciproche relazioni, in un processo continuo di confronto e di osmosi tra i poteri pubblici e strati sempre più ampi della società: la tutela della *privacy* e il problema della sicurezza (dei dati e delle informazioni, degli archivi, dei sistemi informatici e delle reti di telecomunicazioni); la proprietà intellettuale dei dati e delle informazioni in circolazione e il commercio elettronico; i documenti elettronici e la fiscalità per l'acquisizione di beni e servizi informatici e telematici; l'integrazione *computer-tv* e le nuove tecnologie cosiddette "pulite", tutti questi problemi, dunque, devono esserli ripensati con un approccio globale.

In altre parole, bisogna rendersi conto, a tutti i livelli, che siamo entrati definitivamente nella "società dell'informazione". Da parte mia, penso che essa non si sostituisca alla società industriale o alla società dei servizi, ma che ne costituisca il nuovo stadio di sviluppo, una nuova forma incentrata sull'"immateriale" e di cui l'informazione, sotto tutte le sue forme, ne sarà - a un tempo - il cuore e il sistema nervoso.

L'ingresso nel ciber spazio è ricco di potenzialità sia economiche che culturali. Questa evoluzione fluidifica i mercati in termini di facilità di scambi, di pratiche sociali, ma anche in termini di facilità di accesso alla formazione e alla cultura.

Bisogna accettare di entrare in questo nuovo spazio e d'integrarsi: Internet (o quello che diventerà questa Rete universale) non è buona o cattiva in sé, solo l'uso che se ne farà ci permetterà di giudicare.

L'ingresso nel cibernazio non potrà essere che positivo, purché non sia fonte di nuove esclusioni (si pensi alla nota contrapposizione tra "info-ricchi" "info-poveri") o d'una forma di omologazione culturale.

Se il mercato diviene globale, i costumi non lo sono ancora; di qui una tensione, forte e costante, tra la spinta verso l'omologazione dei comportamenti, delle abitudini di consumo e dei modi di vita, da un lato, e dall'altro, il bisogno d'identità, di solidarietà, di qualità della vita, la cultura che si oppone a questa quasi "deteritorializzazione" creata dalla realtà virtuale.

In questa ricerca di equilibrio e di sviluppo armonioso, la comunità internazionale e i poteri pubblici nazionali non devono lasciare che a giocare siano le sole forze di mercato, devono invece impegnarsi collettivamente nello sviluppo della società dell'informazione per promuovere la libertà di scambio e di espressione, l'accesso al sapere e la solidarietà.

5. APPENDICE

Diapositiva 1

*Forum delle opportunità
della digitale
comunicazione elettronica*

Cambrino, 29-30 ottobre 1999

**Electronic
Commerce**

Normativa
e organismi
internazionali

*Costantino Ciampi
IDG/CNR, Firenze*

"Progress is
impossible without
change, and those
who cannot
change their minds
cannot change
anything"
George Bernard Shaw

Diapositiva 2

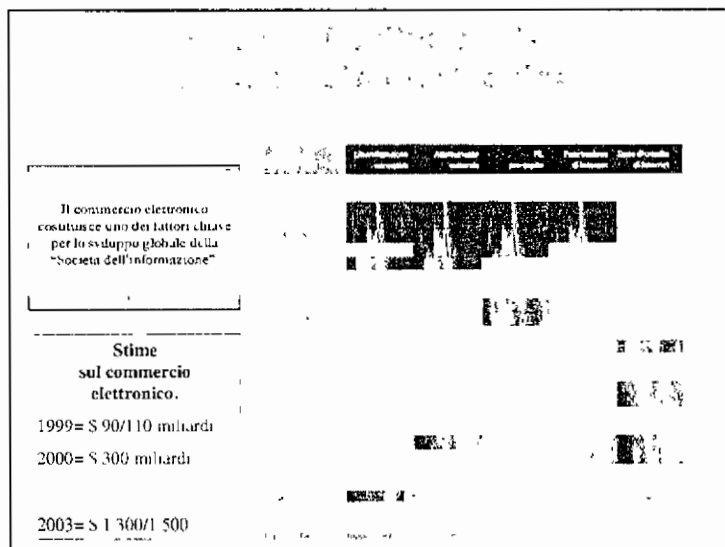
E-Commerce e Organismi Internazionali
(a livello mondiale)

- **BIS** - Bank for International Settlements
- **IEC** - International Electronic Commerce Commission
- **ILO** - International Labour Organization
- **ISO** - International Standard Organisation
- **ITU** - International Telecommunication Union
- **UN-CEFACT / UN/ECE** - United Nations Agencies
- **UNCITRAL** - UN Commission on International Trade Law
- **UNCTAD** - UN Conference on Trade and Development
- **UNESCO** - UN Educational, Scientific and Cultural Organization
- **UPU** - Universal Postal Union
- **WB** - The World Bank
- **WCO** - World Customs Organization
- **WIPO** - World Intellectual Property Organization
- **WTO** - World Trade Organization

Diapositiva 3

E-Commerce e Organismi Internazionali (a livello regionale)

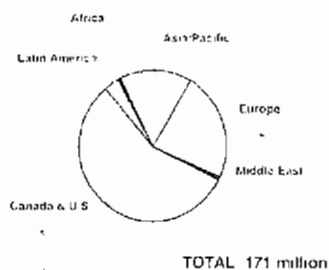
- APEC - Asian Pacific Economic Cooperation
- CoE - Council of Europe
- EFTA - European Free Trade Association
- EU - European Union
- FTAA - Free Trade Area of the Americas
- OECD - Organisation for Economic Co-operation and Development

Diapositiva 4

Diapositiva 5

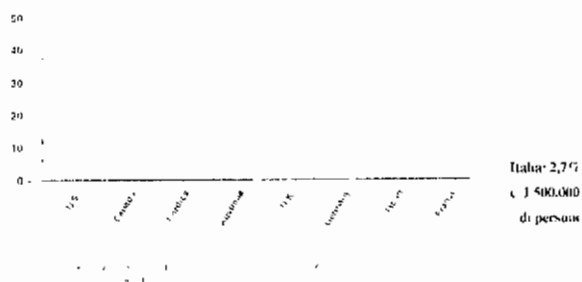
**Numero di persone che accedono
ad Internet, per area geografica**

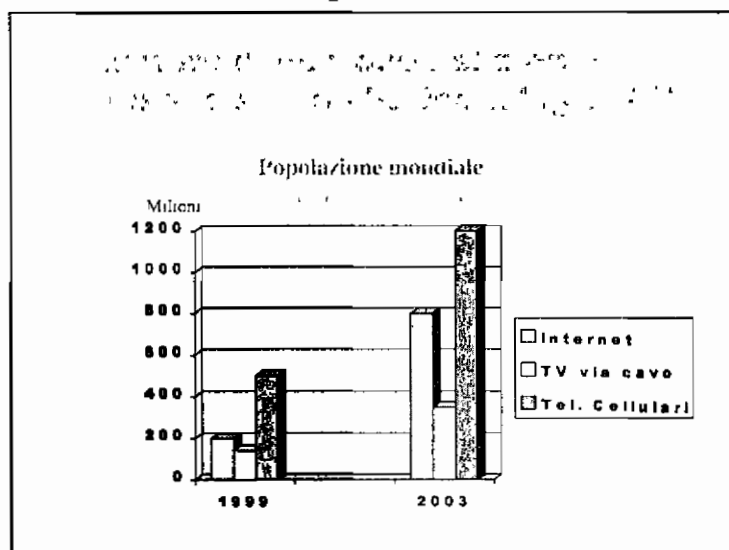
Figure 1.1
Number of People with Internet Access, by Region
May 1999
(millions)

**Diapositiva 6**

**Percentuale della popolazione che
accede ad Internet, per nazione**

Figure 1.2
Percent of the Population with Internet Access
at Home or at Work
1998



Diapositiva 7**Diapositiva 8**

La politica di Clinton e Gore nel Piano per l'era
della informazione dell'economia globale

Clinton - Gore

**A Framework for Global
Electronic Commerce**

1998

US - Commerce Dpt

**The Emerging Digital
Economy II**

June 1999

AGB

Alliance for global Business

**A Global Action Plan
for Electronic Commerce**

Prepared by Business with
Recommendations for Governments

2nd edition, October 1999



Diapositiva 9



AGB- Alliance for Global Business

A Global Action Plan for Electronic Commerce, 88 p.

10 Principi chiave

1 This development of electronic commerce should be led primarily by the private sector in response to market forces

2 Participation in electronic commerce should be pursued through an open and fair competitive market

3 Government intervention, when required, should promote a stable, international legal environment, allow a fair allocation of scarce resources and protect public interest. Such intervention should be no more than is essential and should be clear, transparent, objective, non-discriminatory, proportional, flexible, and technologically neutral

4 Mechanisms for private sector input and involvement in policy making should be promoted and widely used in all countries and international fora

5 Electronic commerce is global in nature. Government policies that affect it should be internationally coordinated and compatible and should facilitate interoperability within an international, voluntary and consensus based environment for standards setting

6 Transactions conducted using electronic commerce should receive neutral tax treatment in comparison to transactions using non electronic means. Taxation of electronic commerce should be consistent with established, internationally accepted practices, and administered in the least burdensome manner

7 Regulation of the underlying telecommunication infrastructure, when necessary, should enable users to compete globally in an open and fair market. As competition develops, regulation should be phased out and there should be a greater reliance on competition law

8 The protection of users, in particular with regard to privacy, confidentiality, anonymity and content control should be pursued through policies driven by choice, individual empowerment, industry led solutions. It will be in accordance with applicable laws

9 Business should make available to consumers and, where appropriate, business users the means to exercise choice with respect to privacy, confidentiality, content control and, under appropriate circumstances, anonymity

10 A high level of trust in the Global Information Infrastructure-Global Information Society (GII-GIS) should be pursued by mutual agreement, education, further technological innovations to enhance security and reliability, adoption of adequate dispute resolution mechanisms, and private sector self-regulation

Diapositiva 10

Iniziativa dell'Unione Europea nel settore del Commercio elettronico

Infrastruttura, crittografia
Pieno accesso al Mercato Unico
Sviluppo globale

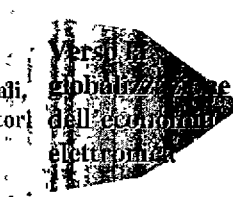
Codici di condotta/autorregolanti
P.A. & Commercio elettronico
Pubblico confronto

Liberizzazione delle Telecom & ITC
Gestione di Internet & futuro
Interoperabilità, R&D
Progetto Pilota

Legislazione

Prassi commerciali,
Protezz. consumatori

Accesso & tecnologia



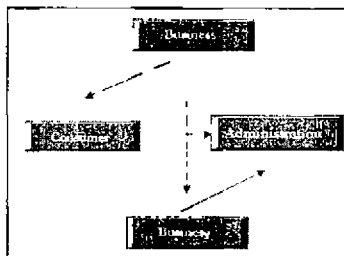
Diapositiva 11

Definizione e Tipologia del Commercio elettronico

E-commerce = svolgimento di attività commerciali e di transazioni per via elettronica

- commercializzazione di beni e servizi
- distribuzione on-line di contenuti digitali
- gestione finanziaria e di banca
- supply public ed altre procedure transattive col pubblico e con i cittadini

- Business-Business
- Business-Consumer
- Business-Administration
- Consumer-Administration



Diapositiva 12

Problemi giuridici del EC e Organizzazioni internazionali

Contesto del Lavoro dell'OCSE sul Commercio elettronico - Luglio 12-13 ottobre 1999

- | | |
|--|---|
| • Protezione dei dati/Privacy | • Direttiva UE in vigore Ott/98 |
| • Regime fiscale | • WTO 'duty free Internet' Convenzione modello OCSE |
| • Sicurezza nelle transazioni | • Proposta di Direttiva UE sulla firma elettronica (26 ottobre 1999) |
| • Diritto d'autore | • Proposta di Direttiva UE sul diritto d'autore nella società dell'informazione (maggio 1999) - Direttiva 96/9/CE sulle banche dati - WIPO - WTO Trips Agreement 1995 |
| • Contratti per via elettronica
(filippo responsabile compliance dell'EC) | • Proposta di Direttiva UE sul commercio elettronico (6 maggio 1999) |
| • Contenuti nocivi e illegali | • Auto regolamentazione di aziende proposta (1999/0276) |
| • Nomi di dominio | • WIPO Internet Report (1999) Risposta al Libro verde (1996) |
| • Pagamenti elettronici | • Aggiornamento della Raccomandazione |
| • Protezione dei consumatori | • Risoluzione UE estensione dei diritti (28/6/99) Contratti a distanza (20/6/97) Draft Guidelines for Consumer Protection (OCSE 1999) |

Diapositiva 13

Problemi giuridici del EC &
Organizzazioni internazionali

**Protezione
dei consumatori**

- **Direttiva 97/7/CE del 20 maggio 1997** riguardante la protezione dei consumatori in materia di contratti a distanza
- **Proposta di direttiva UE** sul commercio elettronico del 18 novembre 1998 (con emendamenti approvati dal Parlamento europeo nel maggio 1999)
- **Draft Guidelines for Consumer Protection in the Context of Electronic Commerce**, OCSE (novembre 1999)

Diapositiva 14

Problemi giuridici del EC &
Organizzazioni internazionali

**Protezione
del diritto d'autore**

- **Proposta di Direttiva CE** sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione - approvata dal Parlamento europeo il 10.2.99
- **WTO TRIPs (Trade related Aspects of Intellectual Property Rights) Agreement**, 199X
- **WIPO/OMPI - Rapporto finale sulla procedura di assegnazione dei Nomi di Dominio** - 30 aprile 1999
- **WIPO/OMPI - Conferenza internazionale sul commercio elettronico e la proprietà intellettuale** - Ginevra, 14-16 settembre 1999

Diapositiva 15

PROPOSTA DI DIRETTIVA
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

Sicurezza delle transazioni

- Proposta di direttiva UE [COM(98)297 Del. 98/0191 COD] relativa a regole comuni sulle firme elettroniche presentata alla Commissione il 13 maggio 1998 (con emendamenti approvati dal Parlamento Europeo in prima lettura nel gennaio 1999 e in seconda lettura nell'ottobre 1999)

Diapositiva 16

PROPOSTA DI DIRETTIVA
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

Contratti per via elettronica

- Convenzione di Bruxelles (1968)
- *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, 1996 (rev. 1998)
- Proposta di direttiva UE [COM(99)0427] sul commercio elettronico del 18 novembre 1998 (con emendamenti approvati dal Parlamento Europeo nel maggio 1999)
- Proposta di Regolamento UE che modifica la convenzione di Bruxelles 1968 [doc. COM(99)348]
- Audizione presso la Commissione il 4 e 5 nov. 1999 sul tema "Commercio elettronico: competenza giurisdizionale e legge d'applicazione"

Diapositiva 17

Problemi giuridici e di EC 2
Organizzazioni internazionali

Standards tecnici

- **Standard E.D.I. (Electronic Data Interchange)** - UN/EDIFACT e ISO 9735
- Standards nei pagamenti - **Secure Electronic Transaction (SET) Protocol**
- **Uso di XML (eXtensible Markup Language)** nel commercio elettronico - XML/EDI
- **Uso di ECML (Electronic Commerce Modeling Language)**, vers. 1.0
- Nuovi standards per la cifratura dei documenti e per l'apposizione di firme digitali
- Standards per la marcatura di opere protette usufruibili in rete o scaricabili dalla rete
- Chiavi "biometriche" per l'identificazione degli operatori in rete

Diapositiva 18

Problemi giuridici e di EC 2
Organizzazioni internazionali

Considerazioni conclusive

- Approccio globale e non settoriale ai problemi della Società dell'informazione
- L'informazione (bene "immatériale") come cuore e sistema nervoso della nuova società
- Il cibernazio è ricco di potenzialità economiche e culturali
 - **Rischi in agguato**
 - nuove esclusioni (*info-ricchi / info-poveri*)
 - omologazione culturale
- Ruolo fondamentale della comunità internazionale e dei poteri pubblici per un armonioso sviluppo della società dell'informazione che voglia rispettare l'identità culturale dei popoli

Commercio elettronico: analisi della situazione italiana e comunitaria

DONATO LIMONE

Anziché leggere una vera e propria relazione, mi limiterò a seguire con voi alcune diapositive, che saranno proiettate, riguardanti la normativa comunitaria e nazionale in tema di commercio elettronico.

I vari testi normativi, emessi a partire dall'anno 1998 fino ad oggi, hanno costituito nel loro insieme il presupposto necessario per la formulazione della proposta di direttiva sul commercio elettronico, che prenderemo in esame.

In particolare mi riferisco a tutti quei testi, quali la Comunicazione della Commissione al Consiglio, al Parlamento, al Comitato economico e sociale, relativa ad un'iniziativa europea in materia di commercio elettronico e a tutta una serie di pareri e proposte di direttive e/o direttive in materia di tutela dei dati personali, di tutela dei consumatori, di sviluppo tecnologico, di Internet sicuro, di vendita a distanza di servizi finanziari ai consumatori, di firme elettroniche.

Andando ad esaminare ora le fonti di riferimento relative alla situazione italiana, dobbiamo sicuramente citare:

- l'art. 21 del decreto n. 114 del 1998, in cui sono definite una serie di azioni con cui il Ministero dell'Industria, del Commercio e dell'Artigianato promuove l'introduzione all'uso del commercio elettronico;
- in materia di firma digitale la legge n. 59 del 1997, il D.P.R. 513/97, il decreto sulle norme tecniche emesso in data 8 febbraio 1999 e le circolari AIPA per l'iscrizione nell'elenco dei certificatori;
- altre normative importanti, perché relative alla firma digitale e al principio della validità giuridica dei documenti informatici, ovvero il D.P.R. n. 428 del 1998 in materia di protocollo informatico nelle pubbliche amministrazioni, l'art. 2 della legge n. 191 del 1998 in materia di carta d'identità elettronica, l'art. 4 della stessa legge sul telelavoro nella Pubblica Amministrazione, il D.P.R. n. 70 del 1999, che regola la stessa materia, e il D.P.C.M. rela-

tivo alla carta d'identità elettronica, approvato dal Consiglio dei Ministri proprio pochi giorni fa;

- una serie di decreti in corso di formazione, di cui ovviamente dò appena notizia, relativamente a:
 - ◆ le norme tecniche per la carta d'identità elettronica;
 - ◆ le norme tecniche per il protocollo informatico;
 - ◆ le norme tecniche per la formazione e la conservazione dei documenti informatici delle pubbliche amministrazioni, in adempimento al D.P.R. n. 513 del 1997 (che non riguarda solo la firma digitale);
 - ◆ la formazione e la conservazione dei documenti informatici relativi agli adempimenti fiscali (cioè alla tenuta delle scritture fiscali, contabili e quant'altro);
 - ◆ gli appalti pubblici di forniture e servizi di informatica ai sensi della legge n. 59 del 1997 (in un articolo è prevista anche la possibilità di effettuare appalti in modo totalmente telematico tramite la firma digitale);
 - ◆ il regolamento in materia di documenti informatici dell'amministrazione giudiziaria, di cui si è discusso pochi giorni fa in sede AIPA e che permetterà di gestire i documenti, i procedimenti e il processo servendosi della firma digitale, ai sensi del D.P.R. n. 513/97;
 - ◆ il decreto legislativo, più volte richiamato, sulla tutela giuridica delle banche dati;
 - ◆ il decreto legislativo n. 185 del 1999 di attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza;
 - ◆ la legge sulla tutela dei dati;
 - ◆ il D.P.R. sulle misure minime di sicurezza dei dati personali;
 - ◆ la legge n. 249 del 1997 sull'istituzione dell'autorità garante delle comunicazioni;
 - ◆ il D.P.R. n. 318 del 1997 in attuazione di due direttive importanti: la 387 e la 388 del 1990 in materia di liberalizzazione delle reti e dei servizi di telecomunicazione;

- ◆ ed altri documenti ampiamente illustrati in precedenza dal prof. Costantino Ciampi.

Avere ben presente questo quadro complessivo delle fonti è necessario per capire come si sta procedendo nel settore del commercio elettronico e non solo.

Se ci atteniamo ad alcune indicazioni e principi stabiliti dalla Comunicazione della Commissione in data 21 gennaio 1998 e poi andiamo a vedere quanto è stato prodotto dall'Unione Europea relativamente al commercio elettronico, possiamo subito notare che vi sono delle differenze notevolissime, che vanno a creare una serie di problemi.

Sicuramente il principio della globalizzazione sta alla base delle iniziative comunitarie in materia di commercio elettronico. Senza dubbio esiste uno stretto rapporto fra Internet e commercio elettronico, inteso quest'ultimo sia in forma diretta (cioè tutta la filiera automatizzata completa, dagli ordini *on-line* alla fruizione, ai pagamenti), che in forma indiretta (ordini e pagamenti elettronici, completati poi dalla consegna delle merci ordinate, l'offerta elettronica di servizi, le cosiddette transazioni commerciali immateriali).

Chiaramente l'iniziativa comunitaria dovrà considerare l'introduzione dell'EURO nell'ambito del commercio elettronico, che rappresenta un'opportunità, ma anche un vincolo ed esiste sicuramente un problema di regolamentazione a livello internazionale, sul quale il prof. Ciampi ha già richiamato l'attenzione.

L'Unione Europea deve quindi dialogare a livello internazionale sulla società dell'informazione con posizioni chiaramente definite; la criminalità informatica è una minaccia sia per la società dell'informazione che per il commercio elettronico.

Altri principi che devono essere garantiti dall'iniziativa comunitaria sono costituiti dall'accesso al mercato globale (infrastrutture, tecnologie e servizi), dall'ottimizzazione degli effetti della liberalizzazione delle telecomunicazioni, dall'interoperabilità in un contesto concorrenziale, dalla normalizzazione e standardizzazione delle transazioni per sostenere lo sviluppo del commercio elettronico anche con costi inferiori, e, infine, dalla cooperazione industriale internazionale per lo sviluppo di sistemi aperti e flessibili.

La Comunicazione del 1998 definì un quadro regolatore molto ampio, di cui alcuni elementi erano: la creazione di un clima di fiducia attraverso un sistema di sicurezza, la verifica della firma digitale, la trasmissione sicura di ordinazioni, informazioni e documenti, la comunicazione sicura di dati personali, le transazioni sicure di beni immateriali, la tutela dei segreti industriali, la protezione dei diritti d'autore.

Ancora, nel quadro regolatore si è cercato di garantire un accesso completo al mercato unico (il quadro regolatore costituisce, infatti, un terreno comune di dialogo e confronto fra Stati Uniti, OCSE, VTO, ecc.) e di garantire la sicurezza, la riservatezza e il concetto di protezione dei dati, che trasversalmente tocca questo problema.

Il concetto di protezione dei dati, in particolare, viene considerato da questa Comunicazione, che trova la sua base nella Direttiva, sotto i seguenti profili:

- l'integrità ed autenticità del messaggio elettronico;
- il carattere personale e confidenziale del messaggio stesso;
- l'accettazione del messaggio come mezzo di prova;
- la preclusione del misconoscimento da parte del destinatario;
- il riconoscimento giuridico di terzi fiduciari per la certificazione di firme digitali (le cosiddette autorità di certificazione che nel nostro ordinamento si chiamano certificatori);
- la centralità della firma digitale per il commercio elettronico come fondamento della fiducia del sistema di sicurezza (nella direttiva non avremo più traccia della firma digitale, salvo solo in due punti dei Considerando per poi sparire dal testo).

L'iniziativa comunitaria, sempre relativamente al quadro regolatore, deve garantire:

- un'adeguata protezione dei diritti di proprietà intellettuale dei servizi ad accesso condizionato: in molti casi, infatti, il contenuto della proprietà intellettuale rappresenta la maggior parte del valore dato di un servizio elettronico;
- un contesto fiscale chiaro e neutrale: la fiscalità nel commercio elettronico svolgerà una funzione fondamentale, al fine di evitare sia una doppia imposizione, sia una distorsione nell'ambito della concorrenza.

Il contesto commerciale favorevole è legato alla diffusione dei sistemi DAI, alla sensibilizzazione e alla conquista della fiducia dei consumatori, alle imprese che devono adottare delle prassi ottimali e alle pubbliche amministrazioni, che possono giocare un ruolo molto forte almeno per alcuni settori attinenti ad esempio alla fiscalità, alle dogane e alla sicurezza sociale.

Il commercio elettronico viene visto nella Comunicazione come servizio per il cittadino, l'istruzione e la formazione, nei vari livelli, come fondamentali allo sviluppo del commercio elettronico.

Passiamo ora ad alcuni aspetti giuridici relativi alla Direttiva.

Anzitutto il principio dello spazio interno senza frontiere chiaramente giustifica il commercio elettronico quale fonte di occupazione, innovazione, competitività e crescita delle imprese.

Il diritto comunitario deve garantire un'integrazione giuridica, al fine di creare le condizioni ottimali per lo sviluppo del commercio elettronico.

Nei servizi della società dell'informazione sono compresi anche quelli prestati a distanza per via elettronica, l'eliminazione delle barriere per garantire la certezza del diritto e la fiducia dei consumatori.

Il commercio elettronico deve rispettare le norme in materia di tutela dei dati personali, non si introducono regole speciali di diritto internazionale privato sui conflitti di leggi e giurisdizioni, i servizi della società dell'informazione devono essere sottoposti soltanto alla normativa dello Stato membro nel quale il prestatore è stabilito.

Il luogo di stabilimento del prestatore è determinato in base alla giurisprudenza della Corte di giustizia della CE; nel caso di società che forniscono servizi tramite Internet, il luogo di stabilimento non è dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, nel caso di più sedi di uno stesso fornitore lo Stato membro competente è quello in cui questi ha il centro di attività; devono essere, quindi, previsti meccanismi di cooperazione tra Stati nel caso in cui sia difficile determinare lo Stato di competenza.

Passiamo ora ad affrontare alcune considerazioni di carattere generale sulla direttiva.

Sicuramente rispetto ai testi precedenti alla Comunicazione ed in generale a tutta l'impostazione precedente, la Direttiva tratta del commer-

cio elettronico in modo non sistematico, affrontando solo alcuni degli aspetti giuridici relativi, senza neppure definire il commercio elettronico stesso, cosa non grave, ma che quantomeno sarebbe stata utile.

La Direttiva stabilisce il principio della validità dell'ordinamento d'origine per quanto riguarda il prestatore dei servizi e d'altra parte la validità dell'ordinamento del Paese di riferimento dei consumatori per quanto riguarda questi ultimi. Vi è uno scarto normativo molto forte fra questi due tipi di approccio, uno riferito al prestatore e l'altro al consumatore, e la direttiva lo scarica tranquillamente sui Paesi membri, creando grossi problemi.

Noi avremo due problemi relativi all'armonizzazione: sotto il profilo orizzontale a livello comunitario, la direttiva dovrà integrare tutte le altre direttive già emanate o in fase di emanazione che hanno a che fare con il commercio elettronico. Secondariamente i Paesi membri dovranno a loro volta armonizzare la normativa interna al diritto comunitario.

Evidentemente vi sarà una disparità di recepimento notevole, ad esempio in materia di tutela dei consumatori, che creerà grossi problemi proprio alla circolazione senza barriere del commercio elettronico.

Questo è senz'altro uno degli aspetti preoccupanti di questa Direttiva, che, pur necessariamente leggera, non deve però peccare di leggerezza.

Altro aspetto problematico è quello relativo alla definizione dei servizi della società dell'informazione. Le direttive in questa materia, già richiamate dal prof. Ciampi, dovrebbero chiarire quali sono questi servizi, altrimenti avremo deroghe ed esclusioni in campo applicativo e una disarticolazione nell'intervento comunitario, oltre che nazionale.

Sicuramente la costituzione di una rete transfrontaliera di agenzie di protezione dei destinatari dei prestatori introduce la possibilità di risolvere le controversie anche tramite canali telematici di assistenza, senza precludere il diritto di ricorrere all'autorità giudiziaria.

Esaminando però da vicino alcuni articoli, abbiamo rilevato la necessità di un'armonizzazione in materia, anche se ho grandi dubbi su tale capacità sotto il profilo giuridico-tecnico da parte del Parlamento italiano.

Nell'ultima edizione della Direttiva viene chiarito meglio il discorso dell'assenza di autorizzazioni preventive, l'articolo stabilisce infatti che l'accesso ai servizi dell'informazione non deve essere condizionato da

autorizzazioni o da altri requisiti che lo subordinino a decisioni, provvedimenti o comportamenti particolari di un'autorità. Restano salvi i sistemi di autorizzazione che non riguardano i servizi della società dell'informazione.

Anche qui, più di una volta, si fanno salvi gli obblighi derivanti dalla direttiva 97/7/CE. Si rinvia, quindi, semplicisticamente al legislatore nazionale e si stabilisce il principio di consentire ai destinatari e alle autorità un accesso facile, diretto e permanente ad una serie di informazioni, meglio articolate nell'ultimo testo; esse devono riguardare i dati anagrafici del prestatore, il suo indirizzo, le modalità di contatto rapido, l'indirizzo di posta elettronica, l'iscrizione nel registro del commercio, se l'attività è soggetta ad autorizzazione, i dati relativi alle professioni, l'attività soggetta ad IVA e l'indicazione precisa ed inequivocabile dei prezzi, delle clausole, delle condizioni essenziali e dei costi supplementari; inoltre altre informazioni, che è possibile aggiungere, sono la validità delle offerte, i tempi di consegna previsti (questi dati non sono inclusi in quest'ultimo testo, è una proposta di modifica ulteriore), le condizioni generali di assicurazione, le condizioni generali dell'accordo contrattuale, la sicurezza dei prodotti (per esempio, nel caso di *software*, licenze, limite di diffusione, tempi per lo scaricamento dalla Rete e quant'altro).

Va aggiunto che, come richiamato precedentemente anche dal prof. Costanzo, nel commercio elettronico è necessario tenere distinta la pubblicità dalle forme di commercializzazione e per i destinatari questa distinzione deve essere chiara.

La comunicazione commerciale deve rispettare alcune condizioni di base: l'identificabilità della comunicazione commerciale come tale, l'identificabilità della persona fisica e giuridica per conto della quale la stessa viene effettuata, l'identificabilità delle offerte promozionali autorizzate (ribassi, premi, omaggi, ecc.), la presentazione chiara e precisa delle condizioni di accesso alle offerte promozionali, l'identificabilità certa di concorso o giochi autorizzati e la chiarezza delle relative condizioni.

Nel caso della comunicazione commerciale non sollecitata, il problema riguarda proprio come le informazioni commerciali e pubblicitarie si presentano in Rete: esiste il curioso sistema di obbligare il destinatario ad inserire in qualche registro a livello comunitario la propria indicazione di

non desiderare questo tipo di informazioni, cosicché fino a che egli non ne avrà preso coscienza, sarà costretto a subirle.

Di conseguenza è necessario definire bene questo sistema di costruzione di registri e relativi filtri a livello comunitario o, quanto meno, a livello nazionale.

Altre considerazioni vanno aggiunte relativamente ai codici di condotta, strumento per agevolare lo sviluppo del commercio, ponendo meno vincoli: nell'ultimo testo è stato fatto opportuno riferimento ad un intervento della Commissione, affinché con la procedura, di cui all'art. 23 della Direttiva, fosse possibile intervenire e precisare le informazioni che tutti i codici di condotta dovrebbero prevedere.

In materia di disciplina dei contratti per via elettronica si stabiliscono e si confermano i principi generali sulla validità e l'efficacia dei contratti così stipulati e non si capisce in base a quale principio siano poi sottoscritti in modo certo e sicuro.

Per quanto riguarda il momento della conclusione del contratto, anche qui si fa riferimento ad un meccanismo che, dal punto di vista astratto, risulta logico, ovvero quello degli avvisi di ricevimento da parte dei due soggetti, in modo tale che il contratto si completi e quindi si concluda, tuttavia si potevano inserire, almeno tra le varie possibilità, la firma digitale o la validazione temporale di ricevute elettroniche.

È, infine, problematica anche la questione delle responsabilità dei prestatori intermediari, per cui gli Stati membri devono imporre ai prestatori un obbligo generale di sorveglianza sulle informazioni che trasmettono e memorizzano e tutti escludono chiaramente la responsabilità del prestatore che ha già definito e messo in Rete un set di informazioni, su cui non sa se interverranno in qualche modo intermediari ad apporre modifiche.

Confermo il principio della composizione extragiudiziale delle controversie, che indubbiamente può risultare agevolata in via telematica, senza escludere la possibilità del ricorso giurisdizionale, ma snellendo indubbiamente molte delle conflittualità che possono scaturire nell'ambito del commercio elettronico.

Infine la cooperazione tra autorità è importante e può essere svolta anche in via telematica, su tutte quelle materie che sono state qui configurate, rispetto a specifici aspetti giuridici e permettendo un maggior

monitoraggio e un più puntuale intervento da parte delle diverse autorità stesse.

Concludo manifestando la mia preoccupazione riguardo alle modalità e capacità di armonizzazione necessarie sia a livello comunitario che nazionale. Preoccupazione rafforzata dal fatto che addirittura nel testo si fa riferimento a terminologie quali "cliccare su icone" e non ad altre un po' più serie come la firma digitale, i sistemi certi di pagamento, di trasferimento di ordini, di offerte e di comunicazione, in particolare la Direttiva ignora tutto il problema della sicurezza sulle reti, quasi che la Rete fosse un casuale e semplice strumento di sviluppo del commercio elettronico.

Le attività illecite nell'ambito del commercio elettronico. Aspetti penalistici e criminologici

CARLO SARZANA DI S. IPPOLITO

La mia attuale relazione prende spunto dalla proposta di direttiva del Parlamento Europeo e del Consiglio, relativa a taluni aspetti giuridici del commercio elettronico, presentata dalla Commissione, nell'ultima versione conosciuta, e intende trattare alcuni argomenti connessi.

Il primo riguarda la protezione dei dati personali e della vita privata con riferimento sia alla legge 31 dicembre 1996, n. 675, sia al d. lgs. 13 maggio 1998, n. 171 (tutela della vita privata nel settore delle telecomunicazioni).

Il secondo argomento riguarda la firma digitale ed il documento informatico con particolare riguardo ai relativi profili penalistici (D.P.R. 10 novembre 1997, n. 513).

Il terzo argomento riguarda la natura dei contratti a distanza (d. lgs. 22 maggio 1999, n. 185): più precisamente, alcuni aspetti penalistici della regolamentazione.

In ordine al primo tema, ricordo che l'art. 36 legge n. 675 del 1996 (omessa adozione di misure necessarie alla sicurezza dei dati), con riferimento all'art. 15 della stessa legge, prevede delle sanzioni penali non lievi per la omissione di tali misure. A questo riguardo, rileva incidentalmente che, dopo un sotterraneo e prolungato braccio di ferro tra AIPA e Garante per la protezione dei dati, finalmente nel luglio scorso ha visto la luce il regolamento recante norme per l'individuazione delle misure minime di sicurezza (D.P.R. 28 luglio 1999, n. 318) per cui può dirsi che, ad oggi, il regime sanzionatorio è effettivo. Non posso non ricordare che il citato articolo 36 è stato oggetto di penetranti critiche. Il primo comma prevede per l'ipotesi dolosa la reclusione sino ad un anno; il secondo comma dell'articolo in questione stabilisce che, se il fatto è commesso per colpa, si applica lo stesso la detenzione sino ad un anno. Vi è quindi un'equiparazione totale *quoad poenam* tra l'ipotesi dolosa non aggravata di cui al primo comma e l'ipotesi colposa prevista dal secondo comma. A parte il fatto che questa anomalia, rafforza sempre più l'idea che "la gatta

frettolosa fa i gattini ciechi", la dottrina¹ ha puntualmente osservato che la risposta sanzionatoria in questo caso è inspiegabilmente appiattita in "violazione dei principi costituzionali di ragionevolezza e colpevolezza".

Altro argomento interessante è quello relativo alle chiamate telefoniche indesiderate, che presenta qualche analogia con l'invio di *e-mail* indesiderate in tema di posta elettronica (*spamming*).

L'art. 12 della Direttiva comunitaria 97/166/CE sulla tutela della vita privata nel Settore delle telecomunicazioni recita «... l'uso dei sistemi automatizzati di chiamata senza intervento di un operatore, di dispositivi automatici di chiamata o di *telefax* o di *telecopier* per scopi di invio di materiale pubblicitario può essere consentito soltanto nei confronti degli abbonati che hanno dato preventivamente il loro consenso».

Il legislatore italiano ha trasposto tale direttiva nel diritto interno con il citato d. lgs. n. 171 del 1998, il cui art. 10 stabilisce testualmente al primo comma, copiando praticamente l'art. 13 della direttiva:

«Art. 10 - Chiamate indesiderate

1. L'uso di un sistema automatizzato di chiamata senza intervento di un operatore o del *telefax* per scopi di invio di materiale pubblicitario o di vendita diretta, ovvero per il compimento di ricerche di mercato o di comunicazione commerciale interattiva, è consentito con il consenso espresso dell'abbonato.

2. Le chiamate per le finalità di cui al comma 1, effettuate con mezzi diversi da quelli ivi indicati sono consentite ai sensi degli articoli 11 e 12 della legge».

La violazione della norma sopracitata è sanzionata pesantemente in quanto il successivo art. 11 stabilisce che in tal caso «restano ferme [sic] le sanzioni di cui all'art. 35 della legge n. 675/96» (reclusione sino a due anni o da tre mesi a due anni per le ipotesi dolose, reclusione sino ad un anno per l'ipotesi colposa).

Le pene previste per i fatti di cui all'art. 35, appaiono irragionevolmente pesanti se comparate ad un'ipotesi più grave, quella delle molestie telefoniche, prevista dall'art. 660 c.p., considerata tuttavia come semplice contravvenzione e punita con l'arresto sino a sei mesi o con l'ammenda sino ad un milione. Il decreto dimentica di indicare, poi, come sia possi-

¹ P. Veneziani, *Ben guardati protetti e tecniche di tutela penale*, in Riv. trim. dir. pen. econ., 1997, p. 12

bile preventivamente accertarsi che il soggetto non desideri ricevere chiamate indesiderate del genere di quelle indicate nell'art. 10. Negli altri Paesi (USA, UK, Francia, ecc.) esistono appositi elenchi denominati dal loro colore, *Orange book*, nei quali si iscrivono coloro che non desiderano ricevere chiamate di un certo tipo o l'invio, trattandosi di *telex*, di certo materiale.

A proposito di tutela dei dati personali e di ciò che può accadere nell'ambito internazionale, desidero citare un episodio, in un certo senso divertente, del quale sono stato protagonista di recente e che riguarda il sistema di intercettazione denominato in codice *Echelon* e di cui ho parlato in altra sede, oggetto di un interessante studio della STOA².

Nel corso di una riunione del Gruppo di lavoro sulla sicurezza dell'informazione e della vita privata, creato in seno al Comitato PIIC dell'OCSE del maggio 1998, ho richiamato l'attenzione dei delegati proprio sul problema di *Echelon*. La riunione era presieduta da un australiano, appartenente, quindi ad un Paese facente parte dell'accordo UK-USA, il quale, nonostante che altri delegati avessero dichiarato il loro interesse all'argomento, ha lasciato cadere la questione.

² L'Organizzazione Scientific and Technological Options Assessment (STOA), organo tecnico del Parlamento Europeo, ha pubblicato, il 19 gennaio 1998, un interessante studio dal titolo *An appraisal of technologies of Political Control*. Gli obiettivi del rapporto erano molteplici e, cioè: a) fornire ai membri del Parlamento Europeo una guida in ordine ai recenti sviluppi nelle tecnologie del controllo politico; b) identificare, analizzare e descrivere lo stato dell'arte nell'ambito dei più salienti sviluppi della tecnologia; c) presentare ai membri del P.E. un rendiconto dei *trends* correnti, sia in Europa che nel mondo; d) sviluppare raccomandazioni in ordine alle politiche che regolano le strategie per il management ed il controllo. Il rapporto è diviso in sette sezioni, una delle quali, la terza, è intitolata "Sviluppi nelle tecnologie della sorveglianza, ivi inclusa l'emergenza delle nuove forme delle reti di intercettazione delle comunicazioni locali, nazionali ed internazionali e la creazione di strumenti per il riconoscimento e la localizzazione degli individui". Nell'ambito di questo capitolo è collocato il paragrafo intitolato "Reti di intercettazione nazionale ed internazionale delle telecomunicazioni", nel quale si rivela che in Europa tutta la posta elettronica, le comunicazioni telefoniche o quelle via fax sono intercettate sistematicamente dalla *National Security Agency*. Le informazioni intercettate sono trasferite, dopo essere raccolte in un centro inglese, via satellite a Fort Meade nel Maryland. Il sistema si chiama in codice *Echelon* ed è parte del cosiddetto sistema UK-USA, ma, al contrario dei sistemi di spionaggio sviluppati durante la guerra fredda, in via principale ha scopi non militari. *Echelon*, secondo il citato documento, raccoglie un'enorme massa di comunicazioni e tira fuori ciò che è importante, s'intende per i proprietari del sistema, usando sistemi di intelligenza artificiale come *Memex* per la ricerca mediante parole chiave. I *partners* degli USA in questo sistema, la cui costituzione risale al 1948, sono il Regno Unito, il Canada, la Nuova Zelanda e l'Australia, molto attivi nell'espletamento dei servizi di raccolta delle informazioni.

Nel leggere il verbale della riunione, mi sono accorto che non vi era alcun accenno al mio non breve intervento e, alla successiva riunione, ho chiesto le opportune spiegazioni. Il Segretariato è stato quindi costretto a modificare il verbale, inserendo sbrigativamente le seguenti frasi «pr. 14 a) *As the general issue of privacy, the Italian delegation proposed that the working party might consider addressing the issue of the Echelon interception system*». Inutile dire che inoltre, io, al ritorno in Italia, sono stato garbatamente informato che alcuni membri del Gruppo non avevano gradito né il mio intervento né le mie successive precisazioni. In séguito, ha avuto qualche difficoltà a seguire i lavori del Gruppo a causa - guarda caso - di difficoltà di bilancio del Ministero degli esteri, finanziatore delle mie missioni all'OCSE.

Lo STOA, tuttavia, ha continuato ad indagare, pubblicando nel settembre scorso (1999), un secondo e documentato studio molto imbarazzante per i Paesi coinvolti. Siccome, poi, io avevo rilasciato alcune interviste a proposito di Echelon, il Garante per la protezione dei dati è stato chiamato in causa e, a quanto ha affermato la stampa, avrebbe preso posizione contro il sistema, tanto che alcuni giornali, con la solito esagerazione, si sono spinti ad affermare «Rodotà scende in guerra contro gli USA»!

Dal canto suo, il Governo italiano dell'epoca ha deciso, come si dice a Roma, "di dormire da piedi" e, infatti, il Presidente del Consiglio Prodi, bersagliato di interrogazioni da parte di vari parlamentari, nella seduta della Camera del 24 aprile 1998 ha dichiarato testualmente «Né la Presidenza del Consiglio né i ministri interpellati sono a conoscenza dell'esistenza di questo sistema di intercettazione ...». Occorre continuare?

Un argomento collegato a quello delle misure di protezione dei dati e delle informazioni, molto vivo anche nell'ambito delle imprese private che agiscono nel campo del commercio elettronico, è quello relativo all'uso della crittografia.

Esiste al riguardo un equivoco che rasenta l'ipocrisia e che io più volte ho richiamato in sede internazionale. Cioè, da un lato si invitano, anche a livello governativo, le organizzazioni private a dotarsi di sistemi sicuri per proteggere le informazioni e si cita in prima linea l'uso della crittografia. Dall'altro lato, e cioè da parte dei governi e del personale del *law enforcement*, si sostiene che in ogni caso l'uso dei sistemi deve consenti-

re, nel caso di illeciti, la possibilità di decrittazione. In realtà su Internet sono disponibili sistemi crittografici a chiave robusta, come il famoso PGO (*Pretty Good Privacy*), che le forze dell'ordine sembra non riescano a decrittare.

Passo ora ad accennare ad alcuni problemi penalistici collegati all'uso della firma digitale³.

Rilevo anzitutto che la dottrina (vedi Borruso) afferma esplicitamente che nell'atto formato da un computer, la sottoscrizione non può avere altro valore che quello di un'assunzione di responsabilità circa la congruità delle procedure previste per il suo funzionamento. Devo dire peraltro che, già prima dell'emanazione del D.P.R. n. 513 del 1997, la dottrina si era prospettata i problemi pratici collegati all'introduzione della firma digitale. Così il maggior studioso in materia, Raimondo Zagami, in un articolo dal titolo «Firma digitale, crittografia, validità del documento elettronico» (in *Dir. inf.*, 1, 1996), affermava che erano da analizzare gli aspetti penalistici di un sistema basato sulle firme digitali, verificando i limiti di applicabilità della normativa sui crimini informatici, specialmente per quanto riguardava la fattispecie di falsificazione di chiavi private e firme digitali e gli attentati ai sistemi informatici e telematici compiuti dalle autorità certificatrici: inoltre, a proposito di rischi collegati all'uso della firma digitale, rilevava che sussistevano sempre i rischi di sottrazione delle chiavi private e di inganni e frodi a danno e da parte delle autorità certificanti.

Peraltro, in un successivo articolo (*La firma digitale dei soggetti privati nel regolamento concernente atti, documenti e contratti in forma elettronica*, in *Dir. inf.*, 6, 1997) l'autore prospettava l'ipotesi di chiavi digitali false, ponendosi, però, da un punto esclusivamente civilistico. In effetti esistono i riflessi penalistici collegati all'utilizzo abusivo delle chiavi private da parte di persona diversa dal titolare: in questo caso, cioè nell'uso di una chiave privata da parte di chi non è legittimo proprietario, si verificherebbe forse un'usurpazione dell'identità della persona e potrebbe essere applicabile l'art. 494 c.p. (sostituzione di persona), ove sussistessero gli altri elementi previsti dalla norma. Lo stesso autore sostiene che l'appropriazione di firme digitali altrui può derivare, oltre che dalla sottrazione di una chiave privata (furto?, appropriazione indebita?), anche

³ L'argomento trattato è parte dei paragrafi 3 e 4 del capitolo sesto del volume *Profili giuridici del commercio via Internet*, Giuffrè, Milano, 1999, p. 128 ss.

dalla creazione di una nuova copia di chiavi e della loro falsa certificazione, derivante dal dolo o dalla negligenza di un certificatore. Sempre secondo il citato autore, l'uso abusivo di una chiave privata altrui ripropone, almeno in parte, gli stessi problemi derivanti da una sottoscrizione (su carta) apocrifa.

L'ultima ipotesi, rileva sempre l'autore, è quella dell'uso di una chiave associata ad un nome falso in quanto inesistente (la cosiddetta contraffazione per invenzione contrapposta a quella per usurpazione), che può derivare dall'uso abusivo di una chiave privata del cerificatore o dall'emissione (con dolo o con colpa) di falsi certificati da parte di quest'ufficio (conclusione del contratto sotto falso nome).

Ritengo che nei casi sopra indicati potrebbe probabilmente applicarsi l'art. 485 c.p. (falsità in scrittura privata). Per chi fa uso di chiave privata sottratta potrebbero applicarsi le altre norme in tema di difesa del patrimonio (truffa, ricettazione, ecc.) e chi fa uso di scritture informatiche false, in quanto la sottoscrizione è falsa, potrebbe essere incriminato ai sensi dell'art. 489 c.p. (uso di atto falso).

Secondo la dottrina (PARODI, *Il documento informatico nel sistema normativo penale*, in *Dir. pen. e proc.*, 3, 1998), coordinando gli articoli del Regolamento relativi alla firma digitale con gli articoli 485 c.p. (falsità in scrittura privata) e 491bis c.p., ne deriverebbe una rilevanza penale per comportamenti verificatisi nel corso di rapporti privati destinati ad articolarsi e concludersi mediante strumenti informatici e che siano diretti a compromettere l'autenticità dei documenti stessi e ciò:

1. sia nel caso in cui un soggetto «formi un documento informatico falso utilizzando surrettiziamente chiavi o altri mezzi per ricondurre il documento stesso ad un soggetto che non ne è stato l'autore»;

2. sia che alteri un documento informatico effettivamente esistente ed autentico nella sua sottoscrizione, intervenendo sul contenuto del medesimo o aggiungendo parti non originariamente presenti.

Sempre secondo l'autore citato, l'ipotesi di cui all'art. 486 c.p. (falsità in foglio firmato in bianco, atto privato), esaminata in questo nuovo quadro, fornirebbe rilevanti prospettive di indagine con riguardo agli incarichi fiduciari di "gestione finanziaria".

Un argomento rilevante ai fini penalistici è quello relativo all'inquadramento della qualità dei soggetti certificatori ed alla natura della loro attività.

Dico subito che, per ragioni di politica criminale e di efficace prevenzione ed accertamento dei reati commessi mediante l'utilizzo di sistemi informatici, sarebbe stato forse opportuno sanzionare in qualche modo l'utilizzo delle chiavi asimmetriche di cifratura al di fuori della procedura stabilita dall'art. 8, comma 1, D.P.R. n. 513 del 1997.

Il regolamento citato precisa i requisiti che deve possedere il certificatore incluso nell'elenco pubblico tenuto dall'AIPA (v. comma 3 del citato art. 8)⁴.

Non può negarsi che sul certificatore incombono obblighi e doveri di grande rilevanza e cioè (v. art. 9):

- identificare il richiedente;
- rilasciare e rendere pubblico il certificato;
- specificare, su richiesta dell'istante e con il consenso del terzo interessato, la sussistenza dei poteri di rappresentanza, ecc.;
- attenersi alle regole tecniche di cui all'art. 3;
- informare i richiedenti, in modo compiuto e chiaro, sulle procedure di certificazione;
- attenersi alle misure minime di sicurezza per il trattamento dei dati personali emanate ai sensi dell'art. 15, comma 2, l. n. 675 del 1996, ecc.

Inoltre, il certificatore dovrebbe anche specificare, ai sensi dell'art. 12, comma 2, la data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico redatto in conformità delle disposizioni, ecc.

⁴ Nella G.U. del 15 aprile 1999, n. 97, è stato pubblicato il Decreto del Presidente del Consiglio dei Ministri 8 febbraio 1999 riguardante le regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la registrazione e la validazione, anche temporale, dei documenti informatici ai sensi dell'art. 3, comma 1, D.P.R. 10 novembre 1997, n. 513. L'art. 3, comma 1, del citato decreto, stabilisce che le firme digitali certificate ai sensi dell'art. 8, comma 4, D.P.R. n. 513 del 1997 (e cioè la procedura di certificazione svolta da un certificatore operante sulla base di licenza o autorizzazione rilasciata da altro Stato membro dell'Unione Europea o nello spazio economico europeo, sulla base di equivalenti requisiti) sono considerate equivalenti a quelle generate in conformità con le regole tecniche stabilite nel decreto citato. L'art. 8 riguarda la conservazione delle chiavi; in esso si prevede il divieto della duplicazione della chiave privata o dei depositi che la contengono e si pongono particolari obblighi a carico del titolare delle chiavi.

Ora, proprio ai fini dell'applicazione delle norme in tema di falsificazione, sarebbe forse stato opportuno che il regolamento citato avesse definito chiaramente la natura dell'attività svolta dai certificatori privati: ciò ai sensi degli artt. 347, 348 e 349 c.p.⁵, nonché, in ordine all'eventuale applicazione degli articoli del codice penale in tema di falsità personale (494, 4995, 496 c.p.), non lasciando tali compiti alla dottrina e all'interprete.

Non può negarsi che la definizione del certificato, data dall'articolo 1, lett. *m*, non aiuta nell'inquadramento dogmatico-penalistico del soggetto. Rileva lo Zagami (op. cit.), esaminando la figura dei certificatori e criticando l'insufficienza del regolamento al riguardo, «... sembra che con la scelta della forma della s.p.a. si sia inteso istituire un sistema di certificazione con soggetti imprenditori operanti in regime di libera concorrenza». E, tuttavia, il certificato ha, tra l'altro, un'importante funzione di natura pubblicistica, inteso il termine nel senso ampio, per quanto riguarda l'accertamento dello stato di capacità legale e naturale del richiedente (v. art. 9, lett. *z*), mentre il certificatore ha l'obbligo di procedere tempestivamente alla revoca o alla sospensione del certificato in presenza anche di soli sospetti su abusi e falsificazioni.

Allora potrebbe forse sostenersi, tenendo presenti i caratteri dell'attività oggettivamente esercitata e ritenendo che si tratti di un pubblico servizio, che ai certificatori dovrebbe applicarsi l'art. 358 c.p. e riconoscere loro la qualità di «persona incaricata di un pubblico servizio». In ultima analisi, potrebbe anche esaminarsi la possibilità del riconoscimento della qualità di persone esercenti un servizio di pubblica necessità, ma occorrerebbe allora stabilire che l'attività di certificazione privata dovrebbe essere vietata a tutti coloro che non seguono, prima dello svolgimento dell'attività, la procedura stabilita dall'art. 8, comma 3, e dichiarare esplicitamente che l'attività di certificazione digitale integra un servizio riconosciuto da parte della P.A. come di pubblica necessità.

Un altro argomento, che mi sembra degno di considerazione, è quello relativo alla protezione dei consumatori in tema di contratti a distanza.

Anche qui la tecnica usata dal legislatore italiano suscita perplessità.

⁵ 347: obbligo di riferire la notizia del reato, 348: assicurazione delle fonti di prova, 349: identificazione della persona nei cui confronti vengono svolte indagini e di altra persona

Le ipotesi previste dal citato art. 10 d. lgs. n. 171 del 1998 sembrano sovrapponibili a quelle di cui all'art. 10 d. lgs. n. 185 del 1999, intitolato «Limiti all'impiego di talune tecniche di comunicazione a distanza», che recita:

«1. L'impiego da parte di un fornitore del telefono, della posta elettronica, di sistemi automatizzati di chiamata senza l'intervento di un operatore o di fax, richiede il consenso preventivo del consumatore.

2. Tecniche di comunicazione a distanza diverse da quelle di cui al comma 1, qualora consentano una comunicazione individuale, possono essere impiegate dal fornitore se il consumatore non si dichiara esplicitamente contrario».

Posto quindi che le ipotesi previste dal citato art. 10 d. lgs. n. 171 del 1998 sembrano sovrapponibili in larga misura a quelle di cui all'art. 10 d. lgs. n. 185 del 1999, va osservato che nel primo caso è prevista una sanzione penale e nel secondo caso una sanzione amministrativa. Dovrebbe quindi applicarsi l'art. 9 legge 24 novembre 1981, n. 680 (Modifiche al sistema penale), che prevede il principio di specialità, secondo cui «quando uno stesso fatto è punito da una disposizione penale e da una disposizione che prevede una sanzione amministrativa, ovvero da una pluralità di disposizioni che prevedano sanzioni amministrative, si applica la disposizione speciale», richiamandosi quindi espressamente il principio di cui all'art. 15 del codice penale⁶.

Tuttavia è la stessa legge n. 185 a risolvere il problema, giacché esiste nell'art. 12, che prevede la sanzione, l'inciso «fatta salva l'applicazione della legge penale qualora il fatto costituisce reato». Tale riferimento è però di difficile interpretazione: si potrebbe ritenere che ai fatti che integrano insieme le ipotesi previste dall'art. 10 d. lgs. n. 171 e quello previsto dall'art. 10 d. lgs. n. 185 si applichi la (sola) sanzione penale, mentre alle ipotesi residuali si applicherebbero le sole sanzioni amministrative.

È ora da osservare un'apparente incongruenza legislativa in tema di vendite all'asta telematica. L'art. 2, comma 1, lett. e, d. lgs. n. 185, esclude dal campo di applicazione della legge i «contratti conclusi in occasioni di una vendita all'asta», ripetendo pedissequamente quanto previsto dall'art.

⁶ «Articolo 15 - *Materia regolata da più leggi penali o da più disposizioni della medesima legge penale.* 1. Quando più leggi penali o più disposizioni della medesima legge penale regolano la stessa materia, la legge o la disposizione di legge speciale deroga alla legge o alla disposizione di legge generale, salvo che sia altrimenti stabilito».

3, comma 1, della Direttiva 97/7/CE riguardante la protezione dei consumatori in materia di contratti a distanza.

Sembrerebbe quindi che le vendite all'asta telematiche, pur essendo escluse dall'ambito di applicazione della normativa in tema di contratto a distanza, siano riconosciute come valide nell'ordinamento giuridico italiano ed invece tali aste sono esplicitamente vietate dalla legge, giacché il d. lgs. 31 marzo 1998, n. 114 (Riforma della disciplina relativa al settore del commercio) afferma, all'art. 18, comma 5, che «le operazioni di vendita all'asta realizzate per mezzo della televisione, o di altri mezzi di comunicazione sono vietate» e la violazione di tale divieto è punita con pesanti sanzioni amministrative ai sensi dell'art. 22 della stessa legge.

La dottrina⁷ sostiene che ai contratti a distanza si applica anche, in via collaterale, la disciplina stabilita dal D.P.R. n. 513 del 1997 e relative norme di attuazione. In particolare, dovrebbe applicarsi l'art. 18, comma 1, d. lgs. n. 114 del 1998, che prevede la comunicazione dell'attività al Comune nel quale l'esercente ha la residenza, se persona fisica, o la sede legale. Inoltre, alle vendite a distanza si applicano anche, in base al comma 7 dell'art. 10, le disposizioni di cui al d. lgs. 15 gennaio 1992, n. 50, in tema di contratti negoziati fuori dai locali commerciali, richiamato quest'ultimo dall'art. 15 d. lgs. n. 185 del 1999, che prevede, all'art. 11, sanzioni amministrative, della stessa entità peraltro di quelle previste dall'art. 12.

Il groviglio di disposizioni si risolve ove si tenga presente la norma di chiusura prevista dall'art. 15 d. lgs. n. 185, secondo cui nel concorso di norme si applicano le disposizioni più favorevoli per il consumatore contenute nel decreto citato: ciò sino all'emanazione di un testo unico di coordinamento.

Le ipotesi di illecito sanzionato in via amministrativa riguardano anzitutto le norme di cui agli artt. 3, 4, 6, 9 e 10 e cioè:

1. violazioni del dovere di informazione del consumatore (art. 3);
2. violazioni del diritto per il consumatore di ricevere le conferme scritte delle informazioni (art. 4);
3. violazione della disposizione in tema di esecuzione del contratto (art. 6);

⁷ Comandè, in Guida al diritto, 17 luglio 1999, p. 23

4. violazione del divieto di forniture non richieste (art. 9);

5. violazione dei limiti all'utilizzo di talune tecniche di comunicazione a distanza (art. 10).

Alle previsioni di cui sopra si aggiungono le ipotesi del fornitore che ostacola l'esercizio del diritto di recesso da parte del consumatore secondo le modalità di cui all'art. 5 ovvero non rimborsa al consumatore la somma da questi eventualmente pagata.

La sanzione amministrativa va da L. 1 milione a L. 10 milioni: nei casi di particolare gravità o di recidiva, i limiti del minimo e del massimo della sanzione sono raddoppiati.

L'entrata in vigore del regime sanzionatorio, secondo le previsioni del comma 3 dell'art. 15 della legge, è fissato al 19 ottobre 1999, applicandosi nel frattempo le disposizioni di cui all'art. 11 d. lgs. n. 50 del 1992, che prevede peraltro le stesse sanzioni: quindi in pratica non dovrebbero sorgere questioni di diritto intertemporale.

La dottrina⁸ sostiene che l'ampio richiamo alle modalità di esecuzione del diritto di recesso, effettuato dall'art. 12 d. lgs. n. 185, consente di ritenere che qualunque violazione, anche formale, delle prescrizioni dell'art. 5 faccia scattare il regime sanzionatorio.

L'art. 12 d. lgs. n. 185 inizia con l'inciso «fatta salva l'applicazione della legge penale»: il riferimento è a possibili delitti quali la truffa (art. 640 c.p.), la frode in commercio (art. 433 c.p.), l'insolvenza fraudolenta (art. 641 c.p.), ecc.

La dottrina⁹ si è prospettata il caso in cui il fornitore, dopo il regolare esercizio da parte del consumatore del diritto di recesso, non restituisca le somme percepite nei termini indicati dal comma 7 dell'art. 5 (30 giorni) ed ha concluso avanzando l'ipotesi che in questo caso potrebbe sussistere il delitto di appropriazione indebita (art. 646 c.p.), che si verifica allorché «il soggetto, per procurare a sé o ad altri un ingiusto profitto, si appropria il denaro o la cosa mobile altrui di cui abbia, a qualsiasi titolo, il possesso».

Credo che occorra esaminare caso per caso ed accertare se esiste nella fattispecie il dolo specifico previsto dall'art. 646 e se il semplice ritardo nella restituzione possa configurare il delitto in questione.

⁸ Forlenza, in *Guida al diritto*, 17 luglio 1999, n. 28, p. 31 ss

⁹ Forlenza, cit

Secondo la dottrina prevalente¹⁰, qualora il possessore non adempie l'obbligo di restituire la cosa, il reato sussiste se egli oppone alla richiesta un rifiuto immotivato e pretestuoso, oppure nega di averla ricevuta o comunque si comporti in modo da dimostrare la volontà di continuare a tenere la cosa medesima per un tempo infinito.

Concludo ora rilevando che il commercio elettronico avrà effetti e ripercussioni sociali e giuridiche di enorme rilevanza. Occorrerà, però, anche in questo caso, arginare in qualche modo l'occupazione del mercato da parte di grosse concentrazioni di imprese e studiare qualche forma di legge *antitrust* per assicurare un equilibrio nella concorrenza. La figura del *cyber squatting*, cioè della creazione di siti artificiali, fatti al solo scopo di estorcere denaro ai titolari legittimi di marchi o denominazioni, dovrà essere severamente repressa a livello nazionale ed internazionale mediante appositi accordi bilaterali o multilaterali. Le Camere di commercio internazionali potrebbero svolgere opera preziosa per la formulazione di appositi codici di condotta per i consumatori e le imprese, in modo da ridurre al minimo i rischi derivanti da comportamenti illeciti o sleali in questo settore.

¹⁰ Antolisei, *Manuale di diritto penale*, Milano, 1986, parte speciale, I, p. 283

II SESSIONE

Presiede: Nicola Palazzolo

Documenti informatici: la smaterializzazione della scrittura

MANLIO CAMMARATA¹

Si è detto che il documento informatico “valido e rilevante a tutti gli effetti di legge”, introdotto dal secondo comma dell’articolo 15 della legge n. 59 del 1997, determinerà una vera rivoluzione nella Pubblica Amministrazione e nei rapporti tra privati.

Se questa previsione sia vera, lo capiremo tra qualche tempo, quando si saranno potute misurare le resistenze e le vischiosità della burocrazia e gli effetti del ritardo culturale del nostro Paese nel campo delle tecnologie dell’informazione.

Ma, senza dubbio, il documento informatico determinerà una rivoluzione ancora più profonda nell’ordinamento giuridico e nella scienza del diritto, perché introduce un’innovazione i cui effetti non sono misurabili: un cambiamento radicale nella concezione e nell’uso del “documento”, così come lo conosciamo da alcune migliaia di anni, nella sua natura di *res signata*, cioè di una “cosa” che riporta dei segni, delle informazioni.

Infatti il documento informatico è “immateriale”. Qualsiasi tentativo di “materializzarlo”, come cercherò di dimostrare in questo intervento, è destinato a fallire o a riportarlo nell’ambito della *res* e quindi delle regole tradizionali.

La “smaterializzazione”, o “dematerializzazione”, di realtà materiali non è una novità assoluta: basti pensare alle transazioni finanziarie che avvengono da anni in tutto il mondo, spostando enormi quantità di denaro senza che passi di mano una sola banconota, una sola moneta. E tutto questo attraverso “documenti informatici”, appunto, anche se non rispondenti ai requisiti della nostra normativa.

Per comprendere meglio i termini del problema, può essere utile ritornare con la memoria a non molti anni fa, quando i giuristi cercavano di spiegare al colto e all’inclita che non si poteva parlare di “furto di *software*” nel caso di copie abusive di programmi, per il fatto che la vittima

¹ m.cammarata@interlex.it

dell'atto illecito non veniva spossessata dell'oggetto, proprio perché il *software* non è un "oggetto", una *res*.

Nel nostro ordinamento ci sono due definizioni, diverse e contraddittorie, del documento informatico. La prima, in ordine di tempo, è quella dell'art. 491^{bis} c.p., introdotto dalla l. 23 dicembre 1993, n. 547: «... per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli». La definizione è confermata dal comma aggiunto all'art. 621: «è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi».

Dunque il documento informatico, secondo il codice penale, è un "supporto", una *res* che "contiene" qualcosa.

Invece il D.P.R. 10 novembre 1997, n. 513, che detta le norme fondamentali della nostra materia, recita all'art. 1:

«Definizioni. 1. Ai fini del presente regolamento s'intende: a) per documento informatico, la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti».

Che cosa è una "rappresentazione informatica"? Tutti ormai sanno che si tratta di una sequenza di *bit*, che, elaborata da un sistema informatico, può essere resa visibile su uno schermo o stampata sulla carta.

Per capire se questa definizione è compatibile con la precedente, dobbiamo porre due domande: 1) il *bit* è una *res*?; 2) che relazione c'è tra il *bit* e il supporto?

Alla prima domanda la risposta è: no, senza dubbio. Il *bit* è costituito dalla "variazione di uno stato elettrico, magnetico o ottico". Un *bit* esiste perché, in un certo punto di un circuito elettrico, si verifica una tensione diversa da quella presente un attimo prima, o in una certa zona di un supporto magnetico c'è una carica diversa da quella della zona precedente, o ancora un determinato punto di un supporto ottico presenta una riflettanza diversa da quella del punto che gli è vicino.

Non si può toccare un *bit*, prenderlo in mano e nemmeno vederlo al microscopio: quello che si vede, ingrandendo la superficie di un CD, è soltanto un "buco", cioè un segno "interpretabile come *bit* soltanto all'interno di un sistema informatico". A rigor di logica, il *bit* è semplice-

mente un "simbolo" o un'unità di misura, potremmo dire addirittura un'astrazione.

Dunque il documento informatico è una sequenza di simboli, il cui significato non è interpretabile dall'uomo se non attraverso una macchina che li trasforma in "segni".

Per rispondere alla seconda domanda dobbiamo considerare un altro aspetto. Qualsiasi sequenza di *bit* può essere duplicata, spedita e ricevuta senza la minima alterazione. Uno scritto, un'immagine, un suono trasformati in sequenza *bit* possono essere riprodotti in un numero illimitato di esemplari e trasmessi a qualsiasi distanza senza che sia possibile distinguere l'originale dai suoi duplicati. Di fatto una sequenza di *bit* è un numero: sempre lo stesso, per quante volte lo si riproduca o lo si spedisca all'altro capo del mondo. Di più: non è in alcun modo possibile distinguere tra il primo esemplare e i suoi duplicati, essi sono tutti assolutamente identici, dal primo all'ultimo.

Il documento informatico è una sequenza di *bit*, che rappresentano il contenuto del documento, ai quali si aggiungono altri *bit*, che costituiscono la firma digitale, in un'altra sequenza che collega univocamente il contenuto del documento e il suo firmatario. Si tratta, per usare la definizione del D.P.C.M. 8 febbraio 1999, di due "evidenze informatiche". Anche se le due evidenze - firma e documento - vengono separate, non si perde la reciproca correlazione, verificabile con alcune operazioni matematiche.

Tutto questo consente di separare il documento e la firma dal supporto iniziale e passarli su altri supporti, senza che venga meno la riferibilità della firma al contenuto, e quindi la natura del documento. Un supporto ci deve essere (al limite, l'etere, se il documento viene radiotrasmesso), perché i *bit* costituiscono pur sempre una variazione di stato fisico. Ma "il supporto è indifferente per l'esistenza del documento".

Cerchiamo di capire meglio con un esempio. Prendiamo un dischetto sul quale sia registrato un documento informatico e lo inseriamo nel computer, visualizziamo il documento sullo schermo e attiviamo il programma che, collegandosi automaticamente al sito del certificatore, verifica la firma digitale attraverso la chiave pubblica del firmatario. Queste operazioni ci permettono di constatare che il dischetto contiene realmente un documento informatico "valido e rilevante a tutti gli effetti di legge".

Ora prendiamo il dischetto e lo distruggiamo. Per il codice penale abbiamo distrutto un documento informatico, perché l'art. 491bis dice che per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria, ecc.

Ma si dà il caso che del dischetto appena distrutto esista un duplicato. Inserendo il duplicato nel *computer* possiamo constatare che si tratta dello stesso documento di prima, valido e rilevante a tutti gli effetti di legge, come risulta dalla verifica della firma digitale.

Non basta. Perché il documento potrebbe esserci stato inviato da un amico, e quindi questi ne avrà un esemplare. Oppure potremmo averlo inviato a un altro amico, e questi ne avrà quindi un duplicato. Quindi la distruzione del supporto non comporta necessariamente la distruzione del documento, perché il supporto è solo un "accidente" - sia pure indispensabile - del documento stesso. In questo modo cade tutto l'impianto del documento informatico nella concezione della legge n. 547 del 1993.

Possiamo considerare un altro aspetto. Quello che vediamo sullo schermo non è il documento informatico in sé, ma la rappresentazione del suo contenuto, accompagnata dall'indicazione che si tratta di un documento provvisto di firma digitale e, se abbiamo compiuto l'operazione di verifica, che il documento è autentico. Volendo, possiamo visualizzare la firma digitale, ma ci troviamo di fronte a una sequenza di simboli che per noi è priva di qualsiasi significato.

Ora stampiamo il documento sulla carta, con tutta la sequenza di segni grafici che costituiscono la firma digitale. Questo è un documento informatico? No, è un pezzo di carta che può essere certificato come conforme a un documento informatico da un pubblico ufficiale che verifichi la corrispondenza del contenuto e l'autenticità della firma.

Dunque, nel momento preciso in cui un documento informatico si "concretizza", perde la propria natura di documento informatico. Esso è tale solo se la firma digitale è verificabile attraverso il *computer*, quindi deve avere la natura immateriale "dell'evidenza informatica", che il D.P.C.M. 8 febbraio 1999 definisce come «una sequenza di simboli binari che può essere elaborata da una procedura informatica».

Tutto questo non può non comportare un ripensamento di molti concetti consolidati nell'ordinamento giuridico. Un solo esempio: l'impossibilità di distinguere l'originale dai suoi duplicati significa, in pratica, che di un documento possono esistere *n* originali, ugualmente validi

e rilevanti a tutti gli effetti di legge. In pratica non esiste più il concetto di documento "originale" (distinto dal duplicato e dalla copia) e non esiste neanche il concetto di "copia informatica", dal momento che essa è indistinguibile dall'originale.

Dunque tutti gli atti che oggi è necessario consegnare o esibire in originale, non possono essere usati nella forma di documenti informatici. La cambiale informatica, allo stato attuale della normativa, è impossibile, perché essa potrebbe essere presentata all'incasso per un numero infinito di volte. Eppure, nel giorno in cui una buona parte delle transazioni finanziarie tra privati avvenisse con lo scambio di documenti provvisti di firma digitale, la cambiale informatica potrebbe essere molto utile (un altro esempio di documento che oggi non può che essere cartaceo è la procura speciale).

Dunque occorre non tanto rivedere le vecchie regole, quanto inventare regole completamente nuove per una realtà ancora tutta da scoprire. È una sfida senza precedenti per il mondo del diritto.

La crittografia è un'arma? Il difficile bilanciamento fra diritti individuali e interessi pubblici

ANDREA MONTI¹

SOMMARIO: 1. Premessa - 2. Alcune definizioni - Gli ambiti di applicazione - 3.1. La tutela della proprietà intellettuale - 3.2. I contratti on-line - La sicurezza nazionale.

1. PREMESSA

Questo intervento poco avrà di giuridico e molto di politico, perché su una materia così delicata come la regolamentazione della crittografia il legislatore ha certamente “saltato un passaggio”. Nel senso che si è immediatamente proiettato² ad affrontare una serie di questioni tecniche³, ma non ha compiuto una scelta di fondo: quella di stabilire un quadro di riferimento organico che tenesse conto sia degli aspetti di rango costituzionale, sia di quelli legati all’impatto sul sistema normativo ordinario.

Esposto sinteticamente il punto di partenza del ragionamento, prima di procedere oltre, e per inquadrare correttamente i termini del problema, si rende necessaria un’altrettanto sintetica ma importante definizione terminologica.

L’esiguità degli spazi a disposizione impone di dare per scontata una conoscenza - peraltro ormai diffusa - dei fondamenti sul funzionamento della crittografia e di limitarsi a ricordare che con questo termine si intende quella branca della matematica che studia i sistemi per rendere non comprensibile un messaggio a chiunque non sia in possesso della chiave per “svelare l’arcano”.

¹ lawfirm@andreamonti.net

² probabilmente, sulla spinta del regime dell’emergenza che caratterizza ora mai la produzione normativa in ambito informatico.

³ Come per esempio l’introduzione della firma digitale e delle relative norme tecniche, il regolamento sulle misure minime di sicurezza per la legge sui dati personali (che contribuisce ad elevare la crittografia ad un rango estremamente elevato nell’ambito delle problematiche giuridiche).

2. ALCUNE DEFINIZIONI

Dato un testo in chiaro, cioè il testo comunemente intelligibile, si chiama **cifratura** l'operazione che lo trasforma in testo in cifra, cioè in una sequenza di simboli, intelligibile **esclusivamente a chi ne possiede** l'algoritmo decifrante (la chiave).

L'operazione inversa, cioè la traduzione del testo in cifra in testo in chiaro tramite l'applicazione della chiave, si chiama **decifratura**.

L'operazione, invece, con la quale si **risale dal testo in cifra al testo in chiaro**, senza avere la chiave⁴ si chiama **crittanalisi**.

Un altro elemento fondamentale è la distinzione fra crittografia a chiave simmetrica e crittografia a chiave asimmetrica (o pubblica).

La crittografia, come la conosciamo dai tempi di Cesare e prima ancora da quelli degli antichi greci⁵, è definita a chiave **simmetrica** perché la stessa chiave pone il testo in chiaro in testo in cifra e viceversa.

Al contrario, la crittografia a chiave pubblica - nata negli anni '70⁶ - è un nuovo sistema studiato esplicitamente per la trasmissione dei dati su canali insicuri mediante un doppio sistema di chiavi. La prima (chiave pubblica) viene usata per cifrare, e una volta che ciò è stato fatto è impossibile decifrare il messaggio a meno di non avere la seconda (chiave privata).

Dal che si capisce perché si chiama **crittografia asimmetrica**: le due chiavi sono assolutamente indistinguibili rispetto alla funzione nel senso che - date due chiavi A e B - se cifriamo con A, decifriamo con B o viceversa⁷. Ma una volta impiegate una, soltanto l'altra consentirà di decifrare il messaggio.

Un'altra importante questione terminologica riguarda i concetti di *Key Recovery* e *Key Escrow*.

⁴ Quindi utilizzando una serie di sistemi di attacco, che vanno dal cosiddetto "attacco a forza bruta" ad una serie di tecniche molto più complesse sotto il profilo matematico.

⁵ Il testo più completo ed autorevole sulla storia della crittografia rimane ancora D. Kahn, *The Codebreakers*, New York 1967-1996.

⁶ Peraltro c'è anche un'interessante querelle sull'effettiva paternità dell'invenzione, perché sembra che in realtà l'elaborazione di questo algoritmo, non sia americana ma sia inglese - i biografi ci daranno la risposta.

⁷ Vedi ampiamente sul punto C. Giustozzi, A. Monti, E. Zimuel, *Segreti, spie, codici criptati*, Milano 1999.

Il *Key Recovery* è un sistema che consente il recupero della chiave⁸ necessaria per decifrare il messaggio anche ad un soggetto diverso da quello che lo ha originariamente cifrato. Questa tecnologia si rivela particolarmente utile in tutti quegli ambiti - come quello aziendale, per esempio - dove non è possibile che circolino informazioni con modalità che le rendono (potenzialmente) inintelligibili al loro legittimo titolare⁹.

Il *Key Escrow* è un concetto diverso di natura più giuridica che tecnica, perché implica la consegna volontaria ad una terza parte fidata della chiave (o di parte di essa) che consente la decifrazione¹⁰.

Qui anticipo già quello che dirò successivamente, e cioè che questo è uno dei problemi fondamentali sui quali poi si dibatte quando si deve andare a parlare dei limiti in cui consentire l'utilizzo della crittografia a livello diffuso.

Key Escrow e *Key Recovery* sono di fatto il problema centrale sul quale si sta combattendo una battaglia silenziosa, ma non per questo meno cruenta.

3. GLI AMBITI DI APPLICAZIONE

Fino a pochissimi anni fa, fino al 1997, oserei dire, si è trascorso il tempo pensando alla crittografia come ad una cosa da spie o da diplomatici e quindi tutto sommato confinata così in un ambiente abbastanza ristretto.

Le cose oggi non stanno più in questo modo e la crittografia è applicata in maniera talmente ampia da andare a toccare dei settori che normalmente non avremmo mai nemmeno pensato di associare a questa tecnologia.

3.1. La tutela della proprietà intellettuale

In questo settore la digitalizzazione delle opere dell'ingegno sta ponendo grossi problemi in termini di repressione dei fenomeni di duplicazione abusiva e di utilizzo illecito di servizi. Se le soluzioni tecniche che

⁸ Quindi vale sia in ambito di crittografia a chiave simmetrica, sia a chiave pubblica

⁹ Anche questo è un terreno molto insidioso. Da un lato, è ormai un dato acquisito dal legislatore e dalla giurisprudenza che non è lecito utilizzare sistemi di monitoraggio a distanza delle attività dei lavoratori.

¹⁰ Cfr W. Diffie, S. Landau, *Privacy on the line*, Boston 1998.

si stanno affermando sono tutte orientate all'impiego di "sigilli crittografici" in grado di distinguere la copia dall'originale o di inibire l'alterazione dell'opera, quelle giuridiche sono al limite della costituzionalità. Non si può pensare altrimenti quando si sente proporre di sanzionare penalmente addirittura il semplice scambio di informazioni tecniche relative agli algoritmi di cifratura e agli apparati di decifratura¹¹.

3.2. I contratti *on-line*

Un'altra problematica rilevante è quella della stipulazione dei contratti per via telematica.

Da un lato, la firma digitale introdotta dalla legge Bassanini - quando funzionerà - consentirà di stipulare anche contratti a forma vincolata dotati di efficacia piena. Ma è anche vero che rimane non pienamente risolto il problema della tutela e dell'imputabilità della manifestazione di volontà di un soggetto che comunica in Rete e che è un discorso che prescinde dalla firma digitale¹². Ciò vale in modo particolare per un altro ampio settore che non è regolato necessariamente dalla normativa sulla firma digitale. Si tratta dei contratti a forma libera, che possono essere validamente stipulati, proprio perché non ci sono requisiti formali stringenti posti dalla legge, anche mediante scambi di manifestazioni di volontà a distanza purché la manifestazione di volontà sia attribuibile, imputabile al soggetto che l'ha formata.

In questo senso la crittografia, anche non facente parte della costruzione normativa di cui al D.P.R. 513/97, ha un suo ruolo importante, perché in questo caso non stiamo parlando di firma digitale e di documento informatico, ma dell'attribuzione di valore giuridico ad una manifestazione di volontà. Cioè di un sistema che in qualche modo può sostituire l'identificazione personale diretta.

Quando due persone si trovano una di fronte all'altra si riconoscono somaticamente, e più in generale secondo una serie di criteri, grazie ai quali è possibile riferire univocamente le reciproche manifestazioni di volontà. Se viene meno questa prossimità fisica, c'è bisogno di un qual-

¹¹ I° quanto previsto dal ddl C.4953, a proposito del quale vale al pena di ricordare le considerazioni critiche mosse dall'associazione ALCEI (http://www.alcei.it/sequestri/9903_dnautore_sequestri.htm)

¹² Vedi sul punto A. Monti, *l'olontà, dichiarazione e responsabilità nella comunicazione elettronica interattiva*, in *Il commercio elettronico* a cura di W. G. Scott, Fano, 1999.

cosa che la possa sostituire, recuperando un affidamento altrimenti perduto per sempre. È a questo punto che l'impiego dei sistemi di crittografia a chiave pubblica (non necessariamente coerenti con il sistema del D.P.R. 513/97) può rivelarsi decisivo, nel momento in cui consente di riferire in modo univoco il contenuto non alterabile della manifestazione di volontà ad un soggetto.

3.3. La sicurezza nazionale

Al vertice di questa piramide di valori ci sono sicuramente gli interessi superiori dello Stato, che, per alcuni, si pongono in opposizione frontale con la tutela dei diritti individuali. A tal proposito, uno degli argomenti più utilizzati per invocare limitazioni nell'utilizzo della crittografia è quello che vede in limiti e divieti l'unico sistema per contenere lo strapotere della grande criminalità organizzata. Che diversamente si troverebbe in una sorta di universo parallelo di comunicazioni totalmente impenetrabile ai sistemi tradizionali. La scelta fondamentale da compiere, si dice, quindi, è quella fra crittografia forte e crittografia debole.

Sì, perché non esiste una sola crittografia, ma tante. La crittografia in sé è soltanto un'idea che poi deve essere applicata concretamente in base alle scelte politiche e normative del momento. Ecco dunque il primo nodo da sciogliere: vogliamo una crittografia debole, cioè una crittografia abbastanza robusta ma non tanto da resistere ad "attacchi" di una certa potenza, oppure vogliamo una crittografia forte? Vogliamo una fortezza inespugnabile o una casa (ma quanto?) sufficientemente protetta che però alla prima raffica di vento viene giù?

L'Italia è fortemente in ritardo su questo dibattito politico, ecco perché dicevo che il legislatore si è preoccupato più di aspetti tecnici, ma non ha dato sufficiente spazio ad un dibattito molto più ampio, come invece è accaduto oltre confine.

Gli Stati Uniti, al contrario, si sono occupati di questo problema da moltissimo tempo e per ovvi motivi¹³, ma con una normativa particolarmente schizofrenica. Perché se all'interno del patrio suolo è assolutamente legittimo per qualsiasi cittadino americano utilizzare crittografia

¹³ essendo il Paese nel quale all'inizio del secolo la crittografia è letteralmente fiorita con la creazione della Black Chamber che di fatto fu l'antesignana dell'attuale National Security Agency, cioè del più grande apparato di ricerca e sviluppo in materia di sicurezza e di crittografia e di crittoanalisi.

forte (anche quella teoricamente inviolabile), nel momento in cui si passa all'estero questo discorso cambia radicalmente e non è possibile esportare dagli Stati Uniti della crittografia veramente forte. Anche se questi vincoli sono stati molto allentati nel corso degli ultimi anni, si deve considerare che fino al '96 la crittografia esportabile era di robustezza veramente scarsa. Inoltre per garantirsi che l'applicazione di questi divieti di esportazione fosse effettivamente messa in pratica è stato predisposto un sistema normativo che ha equiparato le tecnologie di cifratura alle munizioni da guerra. Questo perché esportare armi verso paesi "nemici" - e dunque pure "macchine cifranti" - è un reato gravissimo negli Stati Uniti.

Poi è anche vero - per esempio - che siccome nessuno vieta di esportare libri, succede sistematicamente che i codici sorgenti di programmi di crittografia venissero stampati in un libro e poi spediti all'estero¹⁴. D'altra parte credo ci si troverebbe in enormi difficoltà nel dover spiegare ad un giudice statunitense le ragioni del divieto di esportazione di un testo, specie a fronte della forte tradizione di tutela della libertà di espressione che si è sviluppata in questo Paese.

Un altro esempio abbastanza interessante è quello della Francia che è stata protagonista a oltre duecento anni dalla prima, di una nuova rivoluzione.

Questo Paese per anni ha avuto un regime assolutamente draconiano sull'utilizzo della crittografia a scopo privato, che era praticamente vietata per qualsiasi cosa. Salvo poi¹⁵ annunciare una rivoluzione copernicana della politica di settore, che nel giro di pochissimo tempo è passata da un regime proibizionista ad un sistema estremamente elastico che va verso ulteriori allentamenti delle maglie normative.

Vediamo ora che cosa è successo in Italia.

Sarà curioso per voi sapere che forse la prima applicazione normativa della crittografia risale al 1924, quando un Regio Decreto impediva ai

¹⁴ In particolare c'è una società americana che produce la versione commerciale di uno dei più noti software di crittografia attuale disponibili sul mercato e per uso personale gratuitamente, che fa esattamente in questo modo: realizza la versione americana, stampa i codici li manda in Olanda o in Svizzera, i codici vengono acquisiti con uno scanner e poi il programma viene ricompilato e reso disponibile con la sigla I accanto al nome, che identifica la versione, in un modo del tutto lecito.

¹⁵ La stampa ha attribuito questa decisione al così detto scandalo Echelon, cioè della presa di coscienza a livello planetario, dell'esistenza di un network di intercettazioni gestito dai paesi di lingua anglosassone.

professori di tenere il registro di classe con dei segni crittografici, evidentemente per ottemperare ad un dovere di trasparenza in caso di controlli.

Ma escludendo questo antico precedente, si potrebbe pensare che la crittografia in Italia non sia stata oggetto di attenzione normativa se non con il D.P.R. 513/97.

Non è vero, perché se leggete le norme in materia dell'esercizio di attività di radioamatore (può sembrare un settore totalmente scollegato da quello di cui stiamo parlando), scoprirete che ai radioamatori è assolutamente vietato parlare in codice. Devono assolutamente comunicare in chiaro, non solo, non possono nemmeno parlare in lingua straniera, hanno un parco di cinque lingue che possono utilizzare e nessun'altra.

La domanda spontanea è: come fanno ad accorgersene se invece di parlare italiano, spagnolo, tedesco, inglese, francese e russo parlano in cinese o polacco?

Risposta: ci vuole un organismo di controllo e la polizia postale è nata per questo. La cosiddetta *escopost* era l'organo di polizia che doveva sovrintendere al controllo dei radioamatori e chi ha un minimo di esperienza nel settore sa che negli anni '70 chi aveva questa passione è stato oggetto di vere e proprie "persecuzioni".

Da quanto sopra emerge chiaramente che il Legislatore italiano ha storicamente orientato in senso repressivo la regolamentazione dei sistemi di protezione delle comunicazioni.

La cosa strana, invece, facendo un salto di venti anni in avanti, è che quando si è passati all'Internet nessuno si è sconvolto dell'impiego così diffuso della crittografia negli ambiti più disparati (commercio elettronico, transazioni *on-line*, ecc.).

Questo è il segnale più evidente della schizofrenia normativa che anima il legislatore, quello stesso legislatore che addirittura, sempre in materia di protezione delle comunicazioni, sottopone l'allevamento dei colombi viaggiatori al controllo della polizia militare.

Sta di fatto che Legislatore e Stato si rendono perfettamente conto che sistemi di comunicazione liberamente disponibili e fuori dal controllo possono essere chiaramente utilizzati dalla grande criminalità o a scopo terroristico.

Anche se su questo permettetemi di avanzare qualche dubbio, se è vero che fino al 1994 negli Stati Uniti non si è verificato un solo caso, in cui un'indagine di polizia sia stata messa in nulla dall'impiego da parte dei delinquenti di strumenti crittografici¹⁶.

Magari la situazione sarà anche cambiata nel frattempo, però è abbastanza indicativo che nel Paese che ha, sicuramente, il più alto tasso di evoluzione tecnologica nel settore specifico, la criminalità organizzata non abbia mai utilizzato, almeno fino al '94, sistemi di questo tipo in modo tale da inficiare le attività di immagine della polizia.

Tutto questo credo che dovrebbe farci riflettere, perché tuttora in Italia il livello del dibattito, e qui vengo a riprendere l'inizio del mio discorso, vede replicare in modo anche abbastanza settario e apodittico i due grandi apparati concettuali e ideologici che si sono scontrati in America.

Da un lato ci sono quelli che io ho chiamato *national security advocate*, secondo i quali se le persone utilizzassero crittografia debole sarebbe più facile svolgere indagini, diversamente, si creerebbero grossi problemi.

Dall'altro c'è il *privacy guardian party*, che invece rivendica il diritto all'anonimato assoluto, il diritto a rivelarsi selettivamente al mondo.

Ora ai primi è abbastanza semplice obiettare che quand'anche lo Stato vietasse certe forme di crittografia o consentisse soltanto l'impiego di sistemi a crittografia debole, la grossa criminalità non avrebbe nessun problema ad "affittare" un matematico bulgaro per farsi fare un programma *ad hoc* anche al di fuori dei limiti imposti dalla legge.

Non mi sembra, appunto, che l'esistenza di norme che vietano certi comportamenti sia un limite per la criminalità.

C'è anche da dire che imporre per legge una crittografia debole equivarrebbe a chiedere alle persone di non installare porte blindate troppo resistenti nelle case, perché se un domani si dovesse aver bisogno di fare un'irruzione di emergenza per un qualsiasi motivo, non sarebbe possibile entrare.

Anche qui è abbastanza chiaro che in attesa di un'eventualità che potrebbe non accadere mai, schiere di malintenzionati vi avranno già svuotato la casa più e più volte. Perché voi - in pieno adempimento di una

¹⁶ Cfr. B. Schneier, D. Banisar, *The Electronic Privacy Paper*, 1997 J. Wiley & Son

norma così discutibile - avrete sistematicamente installato una porta sempre più debole.

D'altro canto, agli strenui sostenitori della riservatezza a tutti i costi c'è anche da dire che è antistorico pensare che lo Stato non possa dotarsi degli strumenti più avanzati per reprimere forme di criminalità sempre più pericolose.

Allora come si cava il ragno dal buco?

Anche qui credo che la soluzione in realtà sia già nelle cose, come dimostra in parte l'esperienza degli Stati Uniti.

Non è ovviamente l'unica soluzione possibile - e non è questo il migliore dei mondi possibili - però è una proposta che potrebbe funzionare.

I cittadini americani hanno la possibilità di utilizzare crittografia forte per uso civile, ma è anche vero che lo Stato americano si è dotato del più imponente apparato di cifratura e crittanalisi, cioè la *National Security Agency*. Cioè a dire: libertà, diritto del cittadino di tutelare la propria riservatezza, ma diritto dello Stato di dotarsi degli strumenti che consentono di violare tecnicamente questo tipo di protezioni (posto che ci riescano), nel caso in cui questo sia necessario.

Ma non a scopo preventivo, perché questo è il nodo della questione. Finché le regole saranno quelle che sono, le indagini preventive non sono ammesse; il nostro, fino a prova contraria, è un diritto penale del fatto, non della condotta, né tantomeno dell'atteggiamento interiore.

E allora se rimane fermo - e non vedo come sia possibile il contrario - il principio della materialità della condotta illecita e quindi della necessità di un fatto di reato, perché poi si possa attivare un'indagine di polizia non posso accettare in una prospettiva costituzionale¹⁷ che possano esistere degli strumenti che preventivamente indeboliscono i diritti dei cittadini.

Anche perché la Storia ci ha insegnato che quello che è stato possibile (ed è tuttora possibile) fare distortendo l'applicazione di strumenti investigativi.

Allora a questo punto è inutile pensare a delle norme formali sganciate dalla realtà dei fatti, sganciate da un dibattito ampio, che consenta

¹⁷ Perché a questo punto non siamo più nemmeno parlando né di interessi individuali né di interessi dello Stato.

di costruire quelle salde strutture d'assieme sulle quali poi erigere un apparato normativo - ancorché articolato - sicuramente coerente.

È su questo auspicio che io concludo questa mia relazione e vi ringrazio.

Chiavi biometriche (Art. 1, lett. g, D.P.R. n. 513 del 1997)

ENRICO MACCARONE¹

In tema di firma digitale e documento informatico è singolare osservare come il mondo del diritto si sia attivato per disciplinare un fenomeno prima del suo nascere o, quanto meno, prima del suo diffondersi, e non - come ordinariamente avviene - per regolamentare un fenomeno o un istituto già consolidato nella pratica.

Non è logicamente possibile regolamentare una materia dai forti riferimenti tecnologici se non dopo avere operato precise scelte di campo, più o meno necessitate, all'interno dello scenario tecnologico di riferimento.

Nel caso del D.P.R. n. 513 del 1997 tali scelte sono state relativamente semplici per ciò che riguarda lo *standard* di generazione della firma digitale, essendosi già da tempo affermato in campo internazionale lo *standard* derivante dalle applicazioni delle chiavi asimmetriche di cifratura; meno semplici, e ne vedremo i motivi, le scelte relative all'infrastruttura di firma (la cosiddetta PKI - *Public Key Infrastructure*) ed alla regolamentazione degli enti preposti all'attività di certificazione.

Il metodo migliore per affrontare le tematiche che ci interessano, e più in particolare le tematiche collegate alle tecnologie di firma digitale a chiave pubblica, è indubbiamente quello di elencare in via preventiva - anche se per sommi capi - tutti i passaggi necessari per una corretta e valida utilizzazione del sistema.

Tali passaggi possono essere così semplificati:

1)- *fase preparatoria*:

- acquisizione di un *software* per la generazione della coppia di chiavi;
- generazione della coppia di chiavi;
- individuazione, per sua natura casuale, della chiave pubblica e della chiave privata;

¹ emaccarone@notariato.it

- **secretazione e conservazione della chiave privata su adeguato e sicuro supporto;**
- **invio della chiave pubblica al certificatore;**
- **ottenimento del certificato e sua archiviazione;**
- **pubblicazione del certificato presso il certificatore.**

II)- *fase gestionale*:

- **mantenimento in vita di tutti i presupposti soggettivi ed oggettivi per la validità del certificato;**
- *idem*, per mantenere l'inviolabilità delle chiavi personali.

III)- *utilizzazione*:

- **formazione del documento informatico;**
- **procedura di *hashing* e generazione firma digitale;**
- **apposizione marca temporale;**
- **conservazione, invio e archiviazione del documento informatico;**
- **gestione dell'archivio dei documenti.**

Il processo così definito rispecchia sia logicamente sia strutturalmente l'impianto del D.P.R. n. 513 del 1997 e, in particolare, la sequenza delle definizioni enunciate in seno al suo art. 1, una sequenza la cui logica viene apparentemente interrotta dalla definizione di "chiave biometrica" riportata al punto 1.g).

Ma a ben guardare tale collocazione non è frutto del caso, bensì di una precisa scelta strategica che vale la pena di approfondire, tesa ad evitare l'equivoco (dimostratosi abbastanza frequente) di ritenere sufficiente l'utilizzazione delle sole chiavi biometriche per lo sblocco delle chiavi di firma e la conseguente generazione di firme digitali. Un equivoco evidenziatosi sia durante i lavori preparatori al D.P.R. n. 513 del 1997, sia durante lo svolgimento dei numerosi convegni che nel corso degli ultimi due anni si sono svolti in più sedi sullo stesso D.P.R., e cioè l'equivoco di ritenere che l'apposizione della firma digitale possa esser fatta utilizzando come chiave di sblocco la sola impronta biometrica o, peggio ancora, utilizzando quale chiave di cifratura la "stringa" fornita dalla chiave biometrica.

Il processo di generazione della firma digitale è ovviamente collegato ad un'espressione di volontà del sottoscrittore e trova il proprio momento culminante e giuridicamente rilevante nella conferma di voler sottoscrivere, conferma fornita allo strumento informatico attraverso l'immissione di una serie di informazioni: tipicamente dalla digitazione di una *password* e, ove previsto, dall'immissione di ulteriori informazioni o di una o più chiavi biometriche.

L'impianto del D.P.R. n. 513 del 1997 e delle Regole Tecniche ad esso afferenti escludono di fatto che in generale tale processo possa dipendere esclusivamente dall'immissione di una o più chiavi biometriche, e ciò non tanto per motivazioni tecniche (di fatto inesistenti) quanto per precisi motivi giuridici strettamente collegati al "consenso" ed ai modi di formazione di esso.

La scienza ha nel tempo individuato almeno quattro elementi, tutti singolarmente individualizzanti, utili per distinguere un individuo da un altro:

- il "soma", corrispondente alla contemporanea rilevazione dei tratti del volto e della distribuzione del calore sullo stesso;
- l'impronta della retina;
- l'impronta digitale;
- l'impronta vocale.

Il primo ed il secondo sono ad oggi gli elementi di maggiore affidabilità; minore affidabilità viene riconosciuta al terzo ed al quarto, poiché (anche se raramente) replicabili o duplicabili in natura, nel senso che uno di tali elementi può essere presente contemporaneamente in più soggetti.

Rilevare il "soma" di un soggetto è operazione complessa, che ad oggi può essere svolta solo utilizzando tecnologie ad alto costo.

Ben più semplice ed economica è l'operazione di rilevamento delle altre tre impronte, oggi resa possibile da apparecchiature e programmi relativamente di basso costo, addirittura capaci (per il rilevamento dell'impronta digitale e della retina) di rilevare se la fonte dell'impronta è viva, se al suo interno vi sono circolazione sanguigna e conseguente calore.

Un'impronta - qualunque essa sia - viene rilevata in modo meccanico, nel senso che il soggetto da identificare non deve compiere alcuna particolare attività se non quella di poggiare un dito su un apparecchio, o guardare un punto fisso, o emettere un suono vocale.

Ma quale consenso può ragionevolmente farsi derivare dal guardare un punto fisso o compiere un'altra delle attività meccaniche ora dette? Certamente nessuno.

Ma vi è di più.

Se esaminiamo da vicino il modo di riconoscimento di una chiave biometrica, ci rendiamo subito conto del fatto che per consentire le necessarie elaborazioni, e quindi per la sua stessa esistenza, essa ha necessità di venire memorizzata anche temporaneamente su un qualsiasi supporto informatico: una volta rilevata, l'impronta viene collazionata con altra impronta precedentemente acquisita e solo in caso di raffronto positivo avviene il riconoscimento, la conferma di avvio del processo richiesto.

Il dovere archiviare un'impronta di riferimento - anche se per millisecondi - all'interno di un qualsiasi sistema informativo la rende per ciò stesso insicura, poiché si tratta pur sempre di informazione per sua natura duplicabile (non ha importanza se con tecniche semplici o sofisticate) e quindi in grado di annullare sul nascere il mantenimento del segreto collegato alla conservazione ed all'uso della chiave privata.

Peggio ancora se la rappresentazione informatica di tale impronta viene archiviata all'interno di un *database*.

Non è quindi un caso se nel D.P.R. n. 513 del 1997, parlando di chiavi biometriche, si faccia esclusivo riferimento a meccanismi di sicurezza ed in particolare a metodi di verifica dell'identità, ben stando attenti a non cadere nel tranello della genericità e ad evitare che dall'uso di chiavi biometriche possa farsi discendere una qualsiasi manifestazione di volontà.

Tutto ciò non esclude, però, che delle chiavi biometriche possa farsi uso per attivare processi serializzati o ripetitivi di generazione della firma digitale (es. la sottoscrizione di un alto numero di mandati di pagamento, o di lettere circolari): in tal senso «... si applica alle firme apposte con procedura automatica, purché l'attivazione della procedura sia chiaramente riconducibile alla volontà del sottoscrittore» e sempre a condizio-

ne che «... prima di procedere alla generazione della firma, il dispositivo di firma deve procedere all'identificazione del titolare» (art. 10 Regole Tecniche).

In conclusione: la firma digitale viene generata scatenando un processo che, utilizzando la chiave privata del titolare, conservata all'interno di un dispositivo di firma, rende disponibile tale chiave soltanto dopo avere identificato il titolare (anche a mezzo di chiave biometrica, nei limiti suddetti) e verificato la sua volontà di sottoscrivere (non verificabile, per i motivi suddetti e fatte salve le eccezioni ex art. 10 Regole Tecniche, attraverso la semplice immissione di una chiave biometrica)

Di tutto ciò, infine, abbiamo conferma diretta dalla lettura delle regole tecniche dettate con D.P.C.M. 8 febbraio 1999, che all'art. 8 dispongono la conservazione delle «... informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave», ed al successivo art. 10 ribadiscono la necessaria riconducibilità della sottoscrizione ad un'espressa manifestazione di volontà del sottoscrittore stesso.

Che la rilevazione di una chiave biometrica non possa essere considerata espressione di volontà è stato già sottolineato; a norma del richiamato art. 10 delle regole tecniche essa può invece essere considerata come ottima metodica per procedere all'identificazione del titolare (art. 10, comma 4), come strumento cioè di sicurezza così come descritto dall'art. 1, lett. g), D.P.R. n. 513 del 1997.

È appena il caso di sottolineare, per ultimo, che i dati biometrici "camminano" con il loro "titolare", vengono da esso portati e non conservati. Ammetterne la possibilità di separazione dal titolare e quindi la conservabilità porterebbe all'assurda conseguenza di una macabra ed impossibile previsione legislativa: quando non utilizzato, il dito (o la retina, o altro) va staccato dal corpo del titolare e conservato in luogo sicuro.

Valore giuridico della firma digitale e conclusione telematica del contratto

RAIMONDO ZAGAMI¹

SOMMARIO: 1. *La firma digitale quale fonte di certezze giuridiche* - 2. *Il ruolo delle terze parti fidate nel sistema della firma digitale* - 3. *A) La scrittura privata informatica - Intervento della terza parte fidata per la certificazione delle chiavi* - 4. *Segue: uso ed abuso della chiave privata* - 5. *B) La scrittura privata informatica autenticata - Intervento della terza parte fidata per la certificazione delle firme* - 6. *Segue: atti pubblici notarili.*

1. LA FIRMA DIGITALE QUALE FONTE DI CERTEZZE GIURIDICHE

La firma digitale è una tecnologia matematico-informatica che si propone di realizzare nel documento informatico le stesse funzioni tradizionalmente soddisfatte dalla sottoscrizione nel documento cartaceo. Norma eminente in tal senso è l'art. 10 comma 2 del D.P.R. n. 513/1997, secondo cui «L'apposizione o l'associazione della firma digitale al documento informatico *equivale alla sottoscrizione* prevista per gli atti e documenti in forma scritta su supporto cartaceo». Tale "equivalenza" è da riferirsi solo alle *funzioni* della sottoscrizione (indicativa, dichiarativa e probatoria), ma non anche ai suoi *requisiti*, i quali sono invece profondamente diversi tra sottoscrizione cartacea e firma digitale.

L'"equivalenza" tra firma digitale e sottoscrizione cartacea conduce di conseguenza all'attribuzione al documento informatico della stessa efficacia probatoria tradizionalmente riconosciuta al documento cartaceo nelle sue varie forme. E così l'art. 5 comma 1 del D.P.R. n. 513/1997 stabilisce che «Il documento informatico, sottoscritto con firma digitale ai sensi dell'articolo 10, ha efficacia di scrittura privata ai sensi dell'articolo 2702 del codice civile»; l'art. 16 comma 1 dello stesso D.P.R., che «Si ha per riconosciuta, ai sensi dell'articolo 2703 del codice civile, la firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato»; non vi è ancora alcun riconosci-

¹ rzagami@notariato.it

mento legislativo dell'atto pubblico notarile "originale" in forma informatica.

Dal punto di vista della tecnologia, una firma digitale è un codice informatico più o meno lungo (circa 100 caratteri), risultato dell'applicazione di un procedimento di cifratura asimmetrico (algoritmo) e di una chiave privata ad un documento informatico. La verifica dell'autenticità di una firma digitale si effettua applicando lo stesso algoritmo di cifratura asimmetrico, unitamente alla chiave pubblica correlata alla chiave privata originariamente utilizzata per la firma. Si usano, infatti, coppie di chiavi di cifratura, formate da una chiave privata con cui si appone la firma e da una correlata chiave pubblica con cui si verificano le firme già apposte.

La firma digitale, a seguito della verifica, offre soltanto due (relative) certezze: in primo luogo, che la firma è stata calcolata impiegando la chiave privata corrispondente a quella pubblica utilizzata per la verifica; in secondo luogo, che il documento informatico firmato non è stato modificato dal momento del calcolo della firma stessa (*integrità*). Scrivo "relative" certezze, perché è noto che la sicurezza di una firma digitale dipende dalla robustezza del sottostante sistema di cifratura e, dunque, non è *impossibile* falsificare una firma, bensì solo *estremamente difficile*, richiedendosi straordinarie capacità di calcolo e lunghissimi tempi di elaborazione. La sicurezza di un procedimento di cifratura è, peraltro, direttamente proporzionale alla lunghezza delle chiavi utilizzate.

Di per sé la verifica di una firma digitale non è in grado di offrire alcuna risultanza probatoria riguardo *all'identità* del soggetto sottoscrittore (la provenienza del documento). La correlazione tra chiave pubblica e chiave privata è, infatti, soltanto di tipo matematico. Diversamente, una sottoscrizione cartacea, eventualmente a seguito di verifica, consente di stabilire un collegamento immediato e diretto tra sottoscrizione stessa e soggetto sottoscrittore.

La sottoscrizione cartacea è un dato somatico e personale, che risulta in un segno diverso per ogni soggetto che l'appone. La firma digitale, invece, non è un dato somatico, in quanto risulta dall'applicazione di un dato informatico (la chiave privata), un mezzo tecnico astrattamente utilizzabile da chiunque, in modo del tutto analogo ad un sigillo. L'analogia con un sigillo è ancora più pregnante qualora si consideri che la chiave privata è memorizzata in un dispositivo di firma che, presumibilmente,

consisterà in una carta dotata di memoria e microprocessore (*smart card*). Proprio per sottolineare questa peculiarità e differenza, nel breve dibattito che ha preceduto l'emanazione del D.P.R. n. 513/1997 si è sostenuta l'opportunità di parlare di "sigillo informatico", piuttosto che di "firma digitale" (MICCOLI). Pertanto, firme digitali apposte da soggetti diversi sullo stesso documento, utilizzando la stessa chiave e lo stesso algoritmo, non sono tra loro tecnicamente distinguibili.

Il problema è, dunque, quello di stabilire un legame tra la firma digitale apposta ed il soggetto firmatario; tra il documento informatico ed il suo autore. In altri termini, determinare il soggetto autore della firma digitale a seguito della sua verifica.

2. IL RUOLO DELLE TERZE PARTI FIDATE NEL SISTEMA DELLA FIRMA DIGITALE

Il pieno collegamento soggettivo tra la firma digitale ed il soggetto firmatario si realizza con l'intervento di una terza parte fidata ed imparziale in due distinte fasi.

A) In primo luogo, occorre stabilire un legame tra la coppia di chiavi ed un'identità soggettiva. Questo legame può essere posto solo mediante l'intervento della terza parte fidata che *certifica* la titolarità della coppia di chiavi in capo ad un determinato soggetto *previamente* identificato (art. 9 comma 2 lett. a D.P.R. n. 513/1997).

In realtà, tale certificazione può riferirsi solo alla chiave pubblica e non anche a quella privata, dato che la prima è di per sé correlata alla seconda. Non è quindi necessario, ai fini delle risultanze della firma digitale, che il certificatore conosca la chiave privata.

La certificazione della chiave pubblica è contenuta in un documento informatico definito come certificato, a sua volta firmato digitalmente dalla parte emittente. Il certificato è emesso preliminarmente ed è poi valido per una moltitudine successiva ed indeterminata di firme, salvo una sua cessazione di validità (scadenza, sospensione o revoca).

La terza parte fidata che certifica le chiavi, secondo la scelta normativa italiana, è un soggetto che deve rivestire la forma di società per azioni e deve rispondere a stringenti requisiti per essere iscritto in un apposito elenco pubblico tenuto dall'AIPA (art. 8 D.P.R. n. 513/1997).

La verifica di una firma digitale compiuta con una chiave pubblica certificata consente di ottenere un'identità soggettiva cui ricollegare la chiave stessa e dunque la firma. Si può così affermare con (relativa) certezza che la firma digitale verificata sia stata apposta con la chiave privata di titolarità del soggetto che risulta dal relativo certificato.

Si badi bene, con la certificazione della chiave non si ha la certezza che Tizio, titolare della chiave come risulta dal certificato, ha apposto la firma utilizzando la correlata chiave privata; bensì soltanto che la firma stessa è stata apposta utilizzando la chiave privata di titolarità di Tizio. Tecnicamente non si può conoscere l'autore della firma, ma solo il soggetto titolare della chiave. Resta incerto se la chiave privata sia stata utilizzata realmente da Tizio nell'apporre la firma o se, invece, non sia stata utilizzata concretamente da Caio.

Si ribadisce, infatti, che la chiave privata è un dato informatico, uno strumento tecnico, contenuto in una *smart card*, utilizzabile astrattamente da chiunque. Una firma digitale non essendo un dato somatico è sempre uguale (se apposta con la stessa chiave e sullo stesso documento) e, quindi, correttamente (matematicamente) verificabile, anche se apposta da soggetti diversi.

Così, nello scambio di dichiarazioni telematiche, il destinatario - oppure chi verifica un documento *ex post* - non può avere la certezza che la firma digitale che riceve, ancorché verificata con un certificato valido (non scaduto e non revocato o sospeso), sia stata effettivamente apposta dal titolare della chiave.

Le regole tecniche approvate con D.P.C.M. 8 febbraio 1999 stabiliscono che «il dispositivo di firma deve procedere all'identificazione del titolare» (art. 10 comma 4), negando così l'uso della chiave ad una persona diversa. Presumibilmente si tratterà di una *smart card* protetta da un codice segreto come un PIN o una *password*. Questo codice non è inattaccabile; inoltre, è concepibile una cessione volontaria della chiave ad altri, con la comunicazione del codice, oppure una sua decifrazione mediante attacco al cifrario.

Si sostiene che le tecniche di riconoscimento biometriche, basate sulle caratteristiche fisiche della persona (ad es. impronte digitali, impronta della retina, codice genetico, ecc.), sarebbero in grado di attribuire alla firma digitale quella caratteristica di somaticità e personalità che le manca, avvicinandola (o parificandola) alla sottoscrizione cartacea. Il D.P.R.

n. 513/1997 definisce il concetto di "chiave biometrica" (art. 1 lett. g) e rinvia, poi, alle regole tecniche per disciplinare l'eventuale uso (art. 3 comma 3). Le regole tecniche emanate non contengono però ancora espliciti riferimenti all'impiego di tecniche di riconoscimento biometriche; nell'art. 8 comma 4 lett. b si parla piuttosto di «informazioni di abilitazione all'uso della chiave privata».

L'eventuale impiego dei dati biometrici quale strumento per l'accesso alla chiave privata, non renderebbe, comunque, "personale" o "somatica" la firma digitale, nel senso di come tale requisito si intende per la sottoscrizione.

I dati biometrici, come anche i PIN e le *passwords*, hanno la stessa funzione di strumento di controllo per l'accesso ai sistemi informatici (*simple authentication* secondo la raccomandazione ITU X.509), nel caso specifico per limitare l'uso del mezzo tecnico (cioè la chiave); e si contrappongono alla firma digitale che consente di creare documenti di cui sia possibile verificare *ex post* integrità e provenienza (*strong authentication* secondo la raccomandazione ITU X.509). Di per sé, il dato biometrico non consente di stabilire alcun legame tra un soggetto ed un documento, dato che non dipende dal contenuto del documento, ed è riutilizzabile.

I sistemi di riconoscimento biometrici presuppongono una digitalizzazione del dato fisico oggetto di esame e la sua archiviazione per servire quale termine di confronto al momento della richiesta di accesso. Non può quindi essere escluso il rischio di sottrazioni, falsificazioni, abusi ed in generale di aggiramenti del sistema di riconoscimento biometrico o di decifrazione della chiave. Con una metafora, la situazione è analoga alla conservazione di un sigillo (la chiave) in una cassaforte apribile con un codice segreto, che può essere rappresentato da un semplice PIN o da un insieme di numeri più complessi (la rappresentazione digitale del dato biometrico di riferimento). Al contrario, una sottoscrizione tradizionale, pur con tutte le difficoltà ed incertezze di accertamento, è un segno grafico che è concettualmente ed intrinsecamente diverso per ogni soggetto.

Pur riconoscendo l'elevatissimo grado di sicurezza dei sistemi di riconoscimento biometrici, resta il fatto che concettualmente non sono in grado di fornire alla firma digitale quel carattere di somaticità e personalità che le manca.

B) Occorre, quindi, risolvere questo secondo problema del legame tra la firma digitale concretamente apposta ed un'identità soggettiva.

L'unico sistema per stabilire un **legame (relativamente)** certo tra la firma digitale concretamente apposta e l'**identità soggettiva** del reale firmatario è, ancora una volta, l'intervento certificatorio di una terza parte fidata.

Essenzialmente, questa terza parte fidata assiste di persona alla concreta apposizione (generazione) della firma sul documento informatico e ne certifica il fatto, previa identificazione soggettiva del firmatario, con l'emissione di apposita certificazione a sua volta firmata digitalmente. Per cui, a seguito della successiva verifica, si potrà avere la (relativa) certezza dell'autore della firma e non soltanto del titolare della chiave.

Questo tipo di certificato è definito dalle *Digital Signature Guidelines* dell'*American Bar Association* (1996) e dal *Digital Signature Act* dello Utah (1995-1996), come *Transactional certificate* (o anche *attesting certificate*, o *notarial certificate*) per contrapporlo ai certificati prima esaminati (che, invece, collegano la chiave pubblica al soggetto), definiti come *Identifying certificates* (certificati di identità). Rispetto ai certificati d'identità, i certificati di attestazione devono essere emessi dopo la relativa firma digitale, hanno un contenuto diverso e, per loro natura, sono certificati riferibili ad un singolo atto (mentre un *identity certificate* si riferisce ad un numero indefinito di futuri atti); non hanno un *operational period*, cioè non hanno inizio, né fine di validità; non rileva neanche la revoca o sospensione, dato che si basano su una singola (o più transazioni) e non su un periodo di tempo di validità.

La normativa italiana sulla firma digitale accoglie sostanzialmente la figura del *Transactional certificate* e la inquadra nell'ordinamento preesistente configurandola come un'autenticazione di firma, ed assegnandone la responsabilità primariamente al notaio, quale terza parte fidata ed imparziale.

Ai sensi dell'art. 16 del D.P.R. n. 513/1997, il notaio garantisce la reale identità della parte che sottoscrive con firma digitale utilizzando la chiave privata (funzione propria del *Transactional certificate*); inoltre, indaga la volontà del sottoscrittore, realizzando la cosiddetta funzione di adeguamento; ed, infine, esegue il controllo di legalità e di conformità all'ordinamento giuridico dell'atto autenticato.

Negli Stati Uniti, in coincidenza con l'introduzione di queste nuove tecnologie, si è avvertita la necessità di istituire la nuova figura professionale del cosiddetto *Cybernotary*, delineata ufficialmente in una Risoluzione

dell'*American Bar Association* del 2 agosto 1994 e, poi, successivamente implementata per la prima volta nello Stato della Florida con legge del 30 maggio 1997. Il *cybernotary* innesta in un ordinamento di *common law* una funzione notarile propria del notariato di tipo latino, avendo egli il compito non solo di certificare l'apposizione della firma digitale, ma anche di assicurare la legalità dei documenti destinati all'estero (*authentication*), affinché essi non siano respinti dall'ordinamento destinatario, costituendo, pertanto, un ponte tra due tradizioni giuridiche.

A questo punto, si tratta di accertare quale efficacia probatoria possiede il documento informatico con firma digitale, a seconda che si sia realizzato l'intervento della terza parte fidata solo nella prima fase (certificazione della chiave), od anche nella seconda fase (autenticazione della firma).

3. A) LA SCRITTURA PRIVATA INFORMATICA - INTERVENTO DELLA TERZA PARTE FIDATA PER LA CERTIFICAZIONE DELLE CHIAVI

Il documento informatico con firma digitale verificabile con una chiave pubblica certificata ha l'efficacia probatoria di scrittura privata ai sensi dell'art. 2702 c.c. (art. 5 comma 1 D.P.R. n. 513/1997).

L'attribuzione dell'efficacia di scrittura privata al documento informatico comporta la possibilità di compiere in tale forma gli atti per i quali è richiesta la forma scritta *ad substantiam* (art. 1325 n. 4 c.c.) o *ad probationem* (art. 2725 c.c.). In tal modo il legislatore ha ritenuto che il documento informatico con firma digitale soddisfi gli scopi perseguiti con l'imposizione di una forma vincolata: a) *ponderatezza*, cioè richiamare l'attenzione delle parti sull'importanza dell'atto che si accingono a compiere; b) *documentazione*, cioè produzione di un documento idoneo a fissare nel tempo il compimento dell'atto al fine di maggiore certezza (funzione probatoria) e di conoscibilità (strumenti pubblicitari) tra le parti e per i terzi.

Poiché il documento informatico (art. 1 lett. a D.P.R. n. 513/1997) è idoneo ad essere rappresentato non solo per testi, ma anche immagini, filmati, suoni ed in generale qualunque informazione digitalizzabile, ne deriva la configurabilità di *scritture private non testuali*. In perfetta applicazione del regolamento non si può negare che costituisca scrittura privata ex art. 5 comma 1 e soddisfi così letteralmente e sostanzialmente i requi-

siti richiesti dall'art. 1350 c.c., un **documento informatico**, (eventualmente anche autenticabile *ex art.* 16), **recante la registrazione digitale audio e video** (completabile pure con elementi testuali) della conclusione di un **negozio** (da trascrivere mediante indicizzazione non automatica del contenuto). Nuove prospettive si aprono anche per la forma del testamento, per cui, accanto a quello olografo, potrebbe così assumere valore quello nuncupativo.

Secondo il D.P.R. n. 513/1997, affinché per il documento informatico si realizzi l'efficacia probatoria della scrittura privata, è sufficiente l'intervento della terza parte fidata solo nella prima fase (certificazione delle chiavi) e non è richiesto l'intervento della terza parte fidata anche nella seconda fase (autenticazione della firma).

Attribuire al documento informatico l'efficacia probatoria di scrittura privata comporta che «fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta» (art. 2702 c.c., richiamato anche dall'art. 5 comma 1).

In caso di riconoscimento (*rectius* mancato disconoscimento entro i termini), la scrittura privata informatica forma piena prova. Se la scrittura è disconosciuta, può essere attivato il giudizio di verifica (artt. 216 ss. c.p.c.), in cui l'onere della prova spetta a chi ha prodotto la scrittura informatica, il quale si limiterà a tal scopo ad esibire la relativa chiave pubblica certificata ed a richiedere la verifica tecnica della firma; l'esito positivo del giudizio di verifica porta alla stessa efficacia probatoria ottenibile con il riconoscimento (piena prova).

Circa l'ammissibilità del disconoscimento, della verifica e della querela di falso per il documento informatico sorgono pochi dubbi, dato l'espresso rinvio operato ai relativi istituti. Si è posto, invece, il problema se l'oggetto della prova nella *verificazione giudiziale* consiste nell'individuazione del reale *autore* della firma (colui che ha utilizzato il dispositivo), oppure più semplicemente nell'individuazione del *soggetto titolare del certificato*. In quest'ultimo senso gli orientamenti prevalenti, dato che diversamente si porrebbe a carico di chi produce la scrittura un onere probatorio **eccessivamente gravoso** e contro i principi. La titolarità di una firma digitale comporterebbe dunque di per sé una presunzione di responsabilità.

Una volta che (a seguito di riconoscimento o verifica) la scrittura privata informatica acquisisce efficacia di piena prova, tale efficacia può essere contestata solo tramite il procedimento di *querela di falso* (artt. 221 ss. c.p.c.). In esso l'onere della prova spetta a colui che risulta sottoscrittore (art. 221 comma 2 c.p.c.), determinandosi così un'inversione rispetto al momento in cui la scrittura è prodotta (prima del riconoscimento o della verifica).

L'oggetto del giudizio di querela di falso per la firma digitale consiste nello stabilire chi sia l'effettivo soggetto (autore) che ha apposto la firma utilizzando la chiave. Non si tratta, dunque di provare la "falsità" della firma (come differente da un preteso modello somatico), dato che la firma generata sullo stesso documento con la stessa chiave è indistinguibile, anche se la chiave è utilizzata da soggetti diversi dal titolare; bensì l'"abuso" nell'utilizzo della relativa chiave privata. A colui che è risultato titolare della chiave (a seguito della verifica) spetta il difficile onere di provare il contrario, utilizzando ogni mezzo. È controverso se possa essere proposta la querela di falso indipendentemente dalla verifica della scrittura.

Alla luce di quanto fin qui detto, risulta che l'efficacia della scrittura privata informatica diviene in realtà diversa e superiore rispetto all'efficacia probatoria della scrittura privata cartacea come delineata nell'art. 2702 c.c. Infatti, il giudizio di verifica di una firma digitale sarebbe concretamente un procedimento rapidissimo ed automatico, che potrebbe ugualmente e facilmente compiere chiunque, ottenendo riscontri oggettivi senza alcuna complicata indagine grafologica. Pertanto, in realtà, la scrittura privata informatica sottoscritta con una firma digitale verificabile attraverso un valido certificato, avrebbe in sostanza, sempre e comunque, «l'efficacia di piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta». Riconoscimento e disconoscimento/verifica sarebbero dunque, sostanzialmente irrilevanti e non più necessari. E, a differenza della tradizionale scrittura privata cartacea, si determinerebbe così sostanzialmente fin dall'inizio quell'inversione dell'onere della prova che pone a carico del titolare della firma l'onere di provarne la falsità - abuso della chiave privata.

Queste gravi conclusioni discendono, in ultima analisi, dal fatto che, secondo il D.P.R. n. 513/1997, l'efficacia probatoria (di piena prova)

della scrittura privata informatica deriva semplicemente dalla verifica di una firma digitale tramite una chiave pubblica certificata. In altri termini, secondo lo schema qui prospettato, l'efficacia probatoria è riconducibile ad un intervento della terza parte fidata solo nella prima fase (certificazione della chiave), non essendo richiesta, ai fini probatori della scrittura privata, anche una certificazione nella seconda fase dell'apposizione della firma (autenticazione), ritenendosi sufficiente garanzia l'"identificazione" del soggetto operata dal dispositivo di firma (art. 10 comma 4), unitamente all'identificazione preliminare operata dal certificatore in sede di emissione del certificato (art. 9 comma 2 D.P.R. n. 513/1997).

Resta, pertanto, incerto il soggetto che ha realmente apposto la sottoscrizione, utilizzando materialmente il dispositivo di firma. L'unica certezza che una tale firma offre, come si è detto, consiste nel fatto che sia stata apposta una firma utilizzando una chiave di titolarità di un certo soggetto, senza però poter sapere se la firma stessa sia stata realmente apposta del titolare risultante dal certificato.

Non potendo tecnicamente risultare alcuna prova circa il soggetto reale autore della sottoscrizione, l'unico sistema per attribuire efficacia probatoria a tali firme è ricorrere a dei *meccanismi presuntivi di responsabilità* in capo al titolare della chiave come risulta dal certificato. Dalla verifica di una firma digitale non risulterebbe dunque l'autore di essa, bensì più correttamente soltanto il soggetto che è responsabile per la firma apposta. Dalla titolarità di un certificato deriverebbe una presunzione di provenienza delle firme digitali con esso verificabili in capo al titolare medesimo.

Il problema è accertare se tale presunzione di provenienza (responsabilità) ammetta - ed in che misura - una prova contraria da parte del titolare della chiave certificata, per potersi sottrarre alla responsabilità derivante da una firma a lui riconducibile, ma da lui non realmente apposta. Lo strumento giuridico per contestare la sostanziale presunzione di provenienza (apposizione) della firma in capo al titolare del certificato, sembra essere, come si è detto, la querela di falso, con un difficile onere probatorio a carico dell'attore.

Un meccanismo presuntivo di questo tipo, con la possibilità espressa della prova contraria, è ad esempio previsto dal *Digital Signature Act* dello Utah.

4. SEGUE: USO ED ABUSO DELLA CHIAVE PRIVATA

Concretamente, la generazione della firma da parte di persona diversa al titolare della chiave può verificarsi in vari modi. Ad es. lo smarrimento del dispositivo di firma ed il suo utilizzo abusivo (prima della revoca), rottura del cifrario ed individuazione della chiave privata da parte di un crittoanalista, aggiramento dei sistemi di riconoscimento biometrici, falsa certificazione (nel 1999 non sono più considerate sicure le chiavi di lunghezza non superiore a 512 *bits*). Un tale comportamento è facilmente concepibile quando la *smart card* è protetta da un semplice codice, ma, come si è detto, non è del tutto escludibile anche in presenza di sistemi di riconoscimento biometrici.

Va, comunque, subito precisato che l'utilizzo di una chiave privata dopo la perdita di validità del relativo certificato, a seguito di scadenza, sospensione o revoca, «equivale a mancata sottoscrizione» (art. 10 comma 5 D.P.R. n. 513/199). Il problema si pone, pertanto, solo per le firma digitali apposte durante il periodo di validità del certificato (*operational period*). Ad es. il dispositivo di firma smarrito che è utilizzato da un impostore, prima della richiesta e pubblicazione della revoca da parte del certificatore.

Per la soluzione di questo problema occorre procedere alla ricerca di una ragionevole soluzione che soddisfi in modo equilibrato i diversi interessi coinvolti, nel rispetto del più generale quadro normativo dell'ordinamento italiano, tenendo in considerazione i seguenti fattori:

- a) che il reale autore della firma potrebbe non essere identificabile (ad es. contrattazione telematica);
- b) che il terzo, dalla verifica del certificato valido, ripone un affidamento che merita di essere tutelato e che la sua buona fede dovrebbe essere presunta;
- c) che il titolare della chiave certificata è tenuto a rispettare dei comportamenti di diligenza nella sua custodia;
- d) che il titolare della chiave certificata è entrato volontariamente (con il contratto di certificazione) in un sistema di cui era in grado di valutare anticipatamente i rischi e le responsabilità;
- e) che il titolare potrebbe aver autorizzato altri ad usare la sua chiave.

La querela di falso, attivata secondo le modalità prima esposte, potrebbe essere bloccata dalla prova da parte del terzo affidatario incolpevole, che l'uso abusivo della chiave è stato determinato da un comportamento negligente del titolare, producendosi gli effetti della *rappresentanza apparente* imputabile. In tal senso, applicando i principi alla firma digitale, si potrebbe affermare che l'onere di dimostrare l'apparenza è assolto dal terzo semplicemente esibendo la firma digitale, e quindi, che il titolare della chiave deve dimostrare la reale situazione contraria all'apparenza. Inoltre, l'apparenza non rileva se il terzo conosceva o avrebbe potuto conoscere con la normale diligenza che la firma è stata apposta da persona diversa dal titolare o eccedendo l'autorizzazione; la buona fede del terzo si presume.

Se è dichiarata la falsità, entra in gioco un profilo risarcitorio nei confronti del terzo che ha riposto un affidamento. Infatti, il titolare della chiave, ai sensi dell'art. 9 D.P.R. n. 513/1997, è tenuto al risarcimento dei danni cagionati dall'uso della chiave. In base a tale norma dovrebbe spettare a suo carico l'onere di provare di aver adottato tutte le «misure organizzative e tecniche idonee ad evitare danno ad altri» (ad es. la cura nella custodia della chiave).

Per quanto riguarda l'utente, nella valutazione di una sua eventuale responsabilità, si dovrà tener conto degli obblighi a suo carico, consistenti nella conservazione della chiave e del dispositivo con la massima diligenza; conservazione delle informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave; richiesta immediata della revoca delle certificazioni relative alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi (art. 8 comma 4 reg. tec.); nonché divieto di duplicare la chiave privata o i dispositivi che la contengono (art. 8 comma 2 reg. tec.).

Si discute se la norma dell'art. 9, comma 1, debba applicarsi al solo certificatore, oppure anche all'utente. La disposizione sembrerebbe applicabile anche agli utenti, dato che l'art. 8 comma 1 (applicabile soltanto agli utenti e non ai certificatori) presenta una formulazione in parte identica all'art. 9 comma 1 in questione. Il comma 2 dell'art. 9 è, invece, testualmente, applicabile solo ai certificatori e non anche agli utenti. La rubrica dell'art. 9 parla, inoltre, di «obblighi dell'utente e del certificatore».

Sembra trattarsi, in sostanza, di una tipizzazione della fattispecie di «responsabilità per l'esercizio di attività pericolose» prevista dall'art. 2050

c.c., come si desume anche dalla relazione ufficiale al D.P.R. n. 513/1997, che riporta anche esempi riferiti al solo utente, come l'abuso da parte di altri in mancanza di tempestiva revoca.

Al terzo, che ha riposto un affidamento, secondo i principi generali, spetterà fornire la prova del danno ricevuto e del nesso di causalità tra attività ed evento. Egli potrebbe anche fornire la prova che il titolare della chiave abbia omesso colposamente di effettuare la revoca della chiave stessa, essendo a conoscenza della sua compromissione o dell'uso abusivo.

Tuttavia, se il terzo conosceva (o era in grado di conoscere) che l'utilizzatore era persona diversa dal titolare, si verifica un'interruzione del nesso di causalità, ed il titolare non può più essere ritenuto responsabile. L'art. 1227 comma 2 c.c. (richiamato dall'art. 2056 c.c.), stabilisce, infatti, che «il risarcimento non è dovuto per i danni che il creditore avrebbe potuto evitare usando l'ordinaria diligenza». La prova della mala fede o della colpa del terzo danneggiato, secondo i principi generali, spetta al titolare della chiave (danneggiante), una volta che il danneggiato stesso abbia provato il nesso di causalità.

In definitiva, secondo la ricostruzione esposta, si potrebbe realizzare una dissociazione tra gli effetti dell'atto e gli eventuali obblighi risarcitori. I primi, potrebbero essere eliminati a seguito della querela di falso; i secondi, a tutela dell'affidamento dei terzi, sussisterebbero indipendentemente dall'efficacia della firma. Per la diffusione del sistema diventano indispensabili adeguati contrappesi assicurativi a garanzia dei titolari delle chiavi, analogamente a quanto accade oggi per le carte di credito.

Peraltro, le ipotesi in cui una chiave privata è utilizzata da un soggetto diverso dal suo titolare non sempre danno luogo ad abusi, contrastabili con la querela di falso, ma possono anche prospettare fattispecie meritevoli di tutela.

Si pensi alle ipotesi in cui la *smart card* è volontariamente consegnata, insieme al codice di abilitazione, ad altra persona per essere utilizzata. In tal caso è dubbio se possa parlarsi di rappresentanza diretta, essendo difficile un inquadramento nella categoria tradizionale della spendita del nome (*contemplatio domini*). La particolarità è che, in tal caso, Caio non solo agisce *in nome* e per conto di Tizio; ma agisce *con il nome* di Tizio, eventualmente senza nemmeno fare risultare il proprio nome Caio: vi è la spendita del nome del solo rappresentato, ma non anche del nome del

rappresentate; manca la cosiddetta **dichiarazione di procura** (incarico rappresentativo).

Allora ci si deve chiedere se esiste spazio per una nuova nozione di *contemplatio domini* valida per l'ambito informatico che possa rispondere alle nuove esigenze e che non richieda necessariamente la dichiarazione di procura (menzione dell'incarico rappresentativo), realizzando nello stesso tempo la *ratio* a base della spendita del nome. Infatti, quando Caio utilizza la chiave di Tizio, spendendo (soltanto) il nome di quest'ultimo, non vi possono essere dubbi in capo al terzo che l'atto sia riferibile al rappresentato (Tizio), piuttosto che al rappresentante (Caio), del quale ultimo potrebbe ignorare anche il nome.

Nell'ambito del documento informatico sono realizzabili comportamenti e fattispecie che non erano prima nemmeno concepibili. Nell'ambito cartaceo è inconcepibile che Caio firmi con il nome di Tizio apponendo una firma che non è tecnicamente distinguibile da quella che avrebbe potuto apporre lo stesso Tizio. Questa, invece, è proprio la fattispecie in questione, facilmente realizzabile con la firma digitale, proprio in relazione a quella sua precisata caratteristica di "sigillo" informatico.

Qualora si accetti la tesi della rappresentanza diretta come sopra, la diversa e speculare ipotesi in cui l'uso della chiave altrui è compiuto senza previa autorizzazione, potrebbe essere inquadrata sotto la categoria della falsa rappresentanza, come tale suscettibile di ratifica (art. 1399 c.c.). Con riferimento alla documentazione cartacea, è stato scritto che «La sottoscrizione apocrifa [apposta da persona diversa da quella risultante dal nome sottoscritto] non è altro che una *contemplatio* non autorizzata, e produce i medesimi effetti di ogni altra spendita del nome: il diritto potestativo del contemplato alla ratifica dell'atto. Il *falsus procurator* e l'usurpatore del nome altrui si presentano come ipotesi omologhe di difetto di potere: il negozio concluso da un soggetto diverso da chi appare come titolare, presenta il requisito negativo del difetto di un potere rappresentativo» (ORLANDI).

Per fondare la responsabilità del titolare della chiave nei confronti del terzo non sembra, comunque, applicabile l'art. 1398 c.c., il quale stabilisce una responsabilità non del rappresentato (nel nostro caso il titolare della chiave), bensì del falso rappresentante, il quale potrebbe essere, nel caso in esame, non identificabile (si pensi ad es. alle contrattazioni telematiche a distanza).

5. B) LA SCRITTURA PRIVATA INFORMATICA AUTENTICATA - INTERVENTO DELLA TERZA PARTE FIDATA PER LA CERTIFICAZIONE DELLE FIRME

In una prospettiva di **simmetria** tra documentazione cartacea ed informatica, l'efficacia probatoria della scrittura privata informatica autenticata è quella stessa stabilita per la sottoscrizione autenticata su carta dall'art. 2703 c.c. La disposizione dell'art. 16 comma 1 del D.P.R. n. 513/1997 riproduce in modo sostanzialmente identico il contenuto dell'art. 2703 c.c., e nello stesso tempo vi rinvia espressamente. La firma digitale, la cui apposizione è autenticata dal notaio o da altro pubblico ufficiale autorizzato «si ha per riconosciuta» (art. 16 comma 1 ed art. 2703 comma 1 c.c.) e, pertanto, ai sensi dell'art. 2702 c.c., farà piena prova della provenienza delle dichiarazioni da chi ha sottoscritto il documento informatico, anche se colui contro il quale è prodotto non riconosce la sottoscrizione, salvo l'esperibilità della querela di falso.

Sotto questo punto di vista, alla luce di quanto detto prima, le differenze tra firma digitale autenticata e non autenticata, si affievoliscono. Infatti, come si è visto, anche la firma digitale non autenticata in realtà acquisterebbe l'efficacia di far piena prova (fino a querela di falso) a seguito di un giudizio di **verificazione** del tutto formale, oggettivo ed immediatamente risolvibile mediante l'esibizione di una chiave pubblica certificata. D'altra parte, anche per la firma digitale autenticata occorrerebbe procedere ugualmente ad una verifica della firma digitale apposta dal pubblico ufficiale.

L'autentica o la verifica giudiziale sono, comunque, indispensabili per l'ottenimento di un titolo per le modifiche dei registri di pubblicità legale (ad es. Registro delle imprese e Registri immobiliari). Inoltre, si ribadisce che l'intervento della terza parte fidata in sede di autentica ex art. 16 è l'unico strumento che fornisce la garanzia della reale identità del sottoscrittore, cioè che la firma digitale sia stata apposta spontaneamente e coscientemente dall'effettivo titolare della chiave pubblica utilizzabile per la verifica e non da altri. Inoltre, il notaio indaga la volontà del sottoscrittore ed esegue il controllo di legalità.

L'art. 16 del Regolamento, riproducendo in parte l'art. 2703 c.c., prescrive che «l'autenticazione della firma digitale consiste nell'attestazione, da parte del pubblico ufficiale, che la firma digitale è stata apposta in sua presenza [art. 72 l. not.] dal titolare, **previo accertamento della sua iden-**

tà personale, della validità della chiave utilizzata e del fatto che il documento sottoscritto risponde alla volontà della parte [art. 47 comma 3 l. not.] e non è in contrasto con l'ordinamento giuridico ai sensi dell'articolo 28, primo comma, numero 1°, della legge 16 febbraio 1913, n. 89» (legge notarile).

In presenza di un'autenticazione *ex art. 16* l'ipotesi che la firma sia stata apposta da un soggetto diverso dal titolare della chiave, può essere fatta valere con la querela di falso. Allo stesso modo, può essere fatta valere la falsità della firma digitale del pubblico ufficiale autenticante.

I poteri del pubblico ufficiale autenticante andrebbero dimostrati attraverso un certificato particolare della sua chiave pubblica, denominato certificato d'attribuzione, emesso e gestito in modo diverso e più sicuro dei certificati ordinari d'identità. Ai sensi dell'art. 17 comma 3 del D.P.R. n. 513/1997, «le chiavi pubbliche dei pubblici ufficiali non appartenenti alla Pubblica Amministrazione sono certificate e pubblicate autonomamente in conformità alle leggi ed ai regolamenti che definiscono l'uso delle firme autografe nell'ambito dei rispettivi ordinamenti giuridici».

6. SEGUE: ATTI PUBBLICI NOTARILI

Un intervento del notaio in questa seconda fase (apposizione della firma) potrebbe essere volto alla produzione di un atto pubblico notarile. Il D.P.R. n. 513/1997 non prevede, ma nemmeno esclude, la redazione di un atto pubblico notarile *originale* in forma informatica, come è invece espresso per la scrittura privata (art. 5 comma 1).

In attesa di un intervento normativo chiarificatore, si è, pertanto, sostenuta l'ammissibilità in base al regolamento di un atto pubblico notarile in forma informatica (PETRELLI, MICCOLI, ANDRINI), adducendo vari argomenti. La legge Bassanini (e non il D.P.R. n. 513/1997) avrebbe abrogato parzialmente le norme della legge notarile - e tutte le altre norme - incompatibili con la documentazione informatica. Nel D.P.R. n. 513/1997 non è stata riproposta la disposizione dell'art. 1 comma 2 del primo progetto di legge del settembre 1996, che escludeva espressamente gli originali degli atti pubblici notarili. Diverse norme prevedono già atti pubblici in forma informatica, come ad es. l'art. 491 *bis* c.p., il quale prevede una fattispecie di falso applicabile agli atti pubblici; l'art. 3 del d. lgs. 12 febbraio 1993, n. 39, relativo alla documentazione amministrativa; e

lo stesso art. 15 comma 2 della l. n. 59/1997, relativamente agli atti amministrativi. Le formalità richieste per l'atto pubblico notarile non sarebbero incompatibili con il tipo di documentazione informatica e, comunque, parziali e letterali incompatibilità sarebbero superate da un'interpretazione evolutiva delle norme.

Al contrario, l'esclusione di un atto pubblico notarile esclusivamente in forma informatica potrebbe sostenersi con i seguenti argomenti. In primo luogo, perché, mentre è stato richiamato l'art. 2702 c.c. per la scrittura privata, ed è stato quasi esattamente riprodotto l'art. 2703 c.c. (scrittura privata autenticata), non è posta alcuna norma che tratti degli atti pubblici notarili (*ubi lex voluit duxit; ubi noluit tacuit*). In tal modo, resterebbero pienamente applicabili tutte le formalità richieste dalla legge notarile (l. n. 89/1913) e dalla l. n. 15/1968, le quali sono ancora parzialmente incompatibili con una documentazione informatica (d'altra parte il regolamento non aveva, comunque, la forza di legge per effettuare modifiche in tal senso). Inoltre, la scelta di escludere gli atti pubblici notarili avrebbe anche una sua intrinseca ragionevolezza, dato che potrebbe essere stata probabilmente determinata dal fatto di non voler estendere una tecnologia ancora nuova ed inapplicata, e pertanto "rischiosa", ad un documento che, possedendo un'efficacia probatoria privilegiata (art. 2700 c.c.), rappresenta il massimo rigore formale del nostro ordinamento, ed in quanto tale è richiesto come forma minima per atti ritenuti dal legislatore di rilevante importanza patrimoniale e personale.

D'altra parte, per la conclusione degli atti notarili, l'utilità della firma digitale è minore, dato che essi non potrebbero comunque essere conclusi telematicamente, poiché, a differenza delle scritture private autenticate, è richiesta la contestuale presenza di tutte le parti (e degli eventuali testimoni e fidefacienti) davanti al notaio per la lettura e sottoscrizione. L'utilità si ripresenta quando occorre duplicare o trasmettere telematicamente il documento pubblico già concluso. In tal senso, il D.P.R. n. 513/1997 viene in aiuto, poiché, anche a voler negare la stipulabilità di un atto pubblico notarile *originale* in forma informatica, si prevede la copia informatica di un atto pubblico che fa fede come l'originale su carta (art. 6 comma 2).

In conclusione, tutti i problemi giuridici fin qui esposti non sorgerebbero e non meriterebbero ulteriori approfondimenti se si volesse circo-

scrivere l'operatività della firma digitale a settori limitati e specifici (ad es. pubbliche amministrazioni e grandi aziende). Ma se l'intenzione è quella di estendere questo sistema alla generalità dei cittadini, per compiere la cosiddetta "rivoluzione epocale del documento informatico", non si può prescindere dal ricercare equilibrate soluzioni giuridiche che garantiscano tutte le parti coinvolte.

Nuove forme di commercio: violazioni ed accertamenti

ANTONIO CILLI¹

SOMMARIO: *Premessa - 1. Internet e la rivoluzione del commercio - 2. Il pagamento su Internet con le carte di credito - 3. La giurisprudenza sulle truffe con le carte di credito - 4. I rischi derivanti dal pagamento on-line - 5. Notizie dai gruppi di discussione su Internet - 6. I canali di discussione in tempo reale - 7. Le difficoltà di accertamento delle violazioni - 8. Nota bibliografica - 9. Appendice: 17 diapositive*

PREMESSA

Il Decreto legislativo 114/98 (denominato “Bersani”, dal nome del ministro proponente), pubblicato sulla Gazzetta Ufficiale n. 80/L del 24 aprile 1998, contiene la riforma della disciplina relativa al settore del commercio.

Prevede alcune riforme sostanziali sull'esercizio delle attività commerciali. In particolare si prefigge di perseguire le seguenti finalità: l'efficienza, la modernizzazione e lo sviluppo della rete distributiva, nonché l'evoluzione tecnologica dell'offerta.

La novità più interessante per il nostro settore è certamente il riconoscimento normativo, dettato all'art. 21, del “commercio elettronico”. La norma prevede che il Ministero dell'industria, del commercio e dell'artigianato promuova l'introduzione e l'uso del commercio elettronico con azioni volte a:

- a) sostenere una crescita equilibrata del mercato elettronico;
- b) tutelare gli interessi dei consumatori;
- c) promuovere lo sviluppo di campagne di informazione ed apprendimento per operatori del settore ed operatori del servizio;

¹ cilli@bmpe.unich.it Docente di informatica presso la facoltà di Economia ambientale dell'Università “G. d'Annunzio” di Chieti. Consulente della Procura di Pescara per le violazioni informatiche e di informatica giuridica. Coautore del testo “Il commercio elettronico” ed. Utet 1999.

- d) predisporre azioni specifiche finalizzate a migliorare la competitività globale delle imprese, con particolare riferimento alle piccole e alle medie, attraverso l'utilizzo del commercio elettronico;
- e) favorire l'uso di strumenti e tecniche di gestione di qualità volte a garantire l'affidabilità degli operatori e ad accrescere la fiducia del consumatore;
- f) garantire la partecipazione italiana al processo di cooperazione e negoziazione europea ed intenzionale per lo sviluppo del commercio elettronico.

In questo senso sono previste convenzioni e accordi di programma tra il Ministero dell'Industria e soggetti pubblici o privati, nonché con associazioni rappresentative delle imprese e dei consumatori.

Prima di fare previsioni ed esaminare i risvolti dell'avvento del "commercio elettronico" è bene guardare lo stato della tecnologia rispetto alle correnti attività commerciali. Sarà utile conoscere l'iter delle violazioni, fino ad ora compiute, per adottare tutti gli accorgimenti tecnici idonei a limitare l'entità del fenomeno.

1. INTERNET E LA RIVOLUZIONE DEL COMMERCIO

Sempre più navigatori di Internet sono attratti - per facilità e celerità dell'operazione - dal fare *shopping* in Rete.

L'opportunità di incontrarsi nei mercati virtuali della Rete ha eliminato le barriere che separavano le imprese dai consumatori ed i venditori dagli acquirenti. Esistono già varie tipologie di beni acquistabili attraverso la Rete: si possono distinguere i beni immateriali - *software* e servizi informativi - da quelli materiali che invece possono essere ordinati tramite i dispositivi elettronici ma che si avvalgono poi di un sistema misto per l'ottenimento del prodotto. Come avviene un acquisto da Internet?

Si comincia dal compilare una *form* con i propri dati e l'indicazione del prodotto desiderato e si finisce con lo scegliere la forma di pagamento più idonea. Sono molti quelli che scelgono di pagare *on-line*: la sola fatica è quella di leggere e trascrivere i numeri.

C'è da dire, però, che coloro che hanno avuto spiacevoli sorprese a riguardo, ci pensano più volte prima di abbandonarsi al piacere di fare l'operazione senza alzarsi dalla propria poltrona.

Ma cominciamo con l'analizzare la validità di un contratto concluso "xxxtramite" la Rete: l'elemento essenziale è la fiducia tra le parti, così che il cliente invia l'ordine, aspettandosi di ricevere dal fornitore l'esatto quantitativo di prodotto ordinato.

Se le parti rispettassero gli accordi, non ci sarebbe sistema più pratico per spostare le attività commerciali nelle reti telematiche! Ma cosa accade quando, per esempio, il quantitativo di merce ordinato non corrisponde a quello ricevuto? Come può l'acquirente dimostrare qual era il quantitativo realmente richiesto? E che dire del venditore per quanto riguarda l'onere della prova sulla qualità e sul prezzo pattuito?

Analizziamo solo alcune operazioni commerciali concluse via *e-mail* e a mezzo *browser*.

È dato per scontato che un contratto concluso tramite Internet o attraverso qualsiasi rete telematica, è prima di ogni altra considerazione un "contratto". Questa affermazione non è così banale come potrebbe apparire dalla semplice lettura. Con questo chiarimento, anche in presenza di diverse legislazioni il contratto produce sempre degli effetti.

2. IL PAGAMENTO SU INTERNET CON LE CARTE DI CREDITO

Vediamo ora di approfondire il fenomeno italiano del pagamento su Internet tramite le carte di credito (American Express, Carta Si, Mastercard, Visa) che rispondono sicuramente all'esigenza di celerità dell'operazione. È il caso di indicare che da qualche anno si sta diffondendo il fenomeno della moneta virtuale *e-money*, considerata la terza generazione dei mezzi di pagamento su Internet. Questo argomento richiede una trattazione a parte per poter considerare il valore giuridico della moneta elettronica.

Indipendentemente dall'esperienza personale, il pagamento tramite l'uso diretto di una carta di credito presenta il problema "rischio" per una serie di circostanze. L'utilizzo di carte di credito senza numero di codice (PIN) è certamente un pericolo concreto. Ma cosa avviene in caso di pirateria e soprattutto chi ne paga le conseguenze?

In questo caso il commerciante non può essere sicuro che il mandante sia effettivamente il titolare della carta, a meno che non vengano utilizzati sistemi di autenticazione riconosciuti validi dalle parti. Diversa è la situazione in caso di smarrimento o furto di carte di credito, utilizzate

poi illecitamente da altre persone. Nonostante la sicurezza che molti sistemi offrono nel criptare i dati trasmessi, il pericolo della pirateria informatica non è da sottovalutare.

Per questo motivo si è fatto ricorso alla nuova figura degli "intermediari elettronici", cioè a un terzo soggetto che, ricevendo l'incarico dall'acquirente, gestisce il pagamento al venditore dopo aver consentito la verifica del suo mandatario.

Il D.P.R. 513/97 (che ha recepito la "Bassanini1") all'art. 14 introduce il "pagamento informatico", cioè il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati secondo le regole tecniche che dovevano essere emanate entro novembre 1998. Il regolamento che attendiamo dovrebbe essere risolutivo anche per i problemi di sicurezza dei dati previsti dall'art. 15 della legge 675/96 - legge sulla tutela dei dati personali - che però ha già partorito il D.P.R. 318/99 in G.U. 14-09/1999 "individuazione delle misure minime di sicurezza". Il citato Regolamento, da una prima lettura, oltre a non fornire indicazioni di carattere "tecnico" e quindi direttamente applicabile, non può essere esaustivo a giudicare dall'entità dei complessivi 10 articoli che lo compongono.

3. LA GIURISPRUDENZA SULLE TRUFFE CON LE CARTE DI CREDITO

Non abbiamo ancora pronunce giurisprudenziali rilevanti sui nuovi casi di violazione attraverso i sistemi elettronici. Possiamo però esaminare alcuni aspetti tipici delle violazioni, attraverso l'utilizzo delle carte di credito tradizionali.

Il Tribunale di Milano nel febbraio del 1994, ha condannato un negoziante per aver omesso di verificare la corrispondenza della firma dell'acquirente dal documento di riconoscimento alla carta di credito. Nella sentenza pubblicata in "Nuova Giurisprudenza Civile, 1995, I, 179" è stata riconosciuta sia la violazione degli obblighi contrattuali che la violazione del principio del *neminem laedere* esteso anche ai rapporti di credito.

Sempre il Tribunale di Milano nel novembre 1992 aveva ritenuto responsabile un negoziante per aver, in un breve lasso di tempo, accettato carte di credito rubate non richiedendo l'autorizzazione dell'emittente,

poiché le singole operazioni non superavano il limite giornaliero di spesa consentita.

Il Tribunale di Pescara nell'ottobre del 1994 ha ritenuto che il reato di possesso e acquisizione di carte di credito di provenienza illecita, previsto dall'art. 12 della L. 197/91, è un reato di pericolo - per la cui consumazione non è richiesta l'effettiva lesione del bene giuridico - e non si richiede che il profitto venga conseguito.

La stessa violazione commessa attraverso la Rete non cambia l'imputazione del reato, ma sicuramente il giudice si troverà di fronte ad accertamenti che possono andare oltre la sua competenza territoriale con tempi ben più lunghi per la definizione del procedimento.

4. I RISCHI DERIVANTI DAL PAGAMENTO ON-LINE

Quando si verifica la pirateria attraverso i sistemi e le reti informatiche la giurisprudenza fa fatica a consolidare i principi appena esposti.

D'altronde, se con l'utilizzo di una carta di credito si può denunciare l'esercente per aver omesso il controllo tra la firma sulla tessera e quella sul documento d'identità, il discorso non è ancora applicabile ad un pagamento in Rete privo di sistemi di sicurezza (ad oggi non obbligatori) e in mancanza dell'uso della firma digitale, introdotta dal citato Regolamento - D.P.R. 513/97 - ma non applicabile per mancanza di ulteriore regolamento tecnico, oltre che di applicazione di quello già emanato.

Passerà alla storia la rivoluzione della carta stampata e delle firme non più apposte con penna e inchiostro, ma rischiamo di far scrivere sui libri di storia che, dopo tanta attesa, c'è stato un periodo d'inerzia per cominciare ad usare i nuovi strumenti tecnologici.

Non dobbiamo illuderci che, con questa normativa, la rivoluzione possa dare i suoi effetti in tempi brevi.

Ma dopo aver raggiunto questo traguardo, tra i primi in Europa, possiamo guardare un attimo al passato. Gli anni 1996-98 sono stati molto importanti per il riconoscimento legislativo dell'evoluzione tecnologica e dell'avvento della rete telematica Internet. Grazie anche alle riforme in tema di semplificazione amministrativa la legge Bassanini, n. 59/97 ha stabilito che: «gli atti, dati e documenti formati dalla Pubblica Amministrazione e dai privati con strumenti informatici o telematici, i contratti stipulati nelle medesime forme, nonché la loro archiviazione e transmis-

sione con strumenti informatici sono validi e rilevanti a tutti gli effetti di legge».

Fino ad ottobre '98 la sperimentazione della firma digitale è stata attivata solo in 5 città italiane: Bologna, Modena, Torino, Siena, Pesaro. Eppure le riforme in atto, come quella del commercio elettronico, facevano presagire un interesse collettivo per l'applicazione delle tecnologie di firma digitale nei diversi settori commerciali. Ad esempio, le Pubbliche Amministrazioni dovrebbero cercare nuove forme di collaborazione con le imprese per produrre più servizi ai cittadini.

Il bisogno di questa collaborazione e la ricerca di regole comuni, non è certo solo il problema italiano. L'Unione Europea sta seguendo tutti gli sviluppi tecnologici e in tema di firma digitale ha pubblicato sulla gazzetta del 6 aprile 1999 un parere del Comitato delle regioni in merito alla «Proposta di direttiva del Parlamento europeo e del Consiglio relativa a regolamenti sulle firme elettroniche». Negli obiettivi della proposta si legge che, anche se in molte situazioni è possibile reperire soluzioni soddisfacenti..... malgrado le firme digitali realizzate tramite tecniche crittografiche siano attualmente considerate un importante tipo di firma elettronica, il quadro di regolamentazione europeo deve essere sufficientemente flessibile da includere altre tecniche che possono essere impiegate per garantire l'autenticazione. I problemi non mancheranno, alcuni appaiono prevedibili e quindi evitabili, ma in corso d'opera si dovranno adottare sicuramente tutti gli accorgimenti necessari per consentire lo sviluppo e la fiducia nelle nuove tecnologie da parte di tutti i cittadini.

Ulteriore pericolo, da approfondire con la propria Banca è che alcune carte, utilizzate per più pagamenti che non superano singolarmente il tetto massimo di spesa, obbligano il proprio Istituto a versare tutte le somme - superando il proprio *plafond* mensile - ai Servizi Interbancari che gestiscono le carte. Né potrebbe derivare l'obbligo per il cliente di rimborsare conseguentemente la propria Banca. Non a caso alcune pagine informative, diffuse anche via Internet contengono l'avvertenza "Sconsigliamo l'utilizzo in chiaro del vostro numero di carta su Internet", oppure "I sistemi di sicurezza attualmente in uso non sono pienamente riconosciuti dai circuiti internazionali visa e mastercard/eurocard". La seguente informativa è consultabile al seguente indirizzo Internet: <http://www.cartasi.it/java/istruzioni.html>.

Tornando al discorso rischio del commercio elettronico, in prevalenza legato alla forma di pagamento, la soluzione - almeno per il momento - si deve ricercare nella lettura dei *contratti* stipulati per l'acquisto della propria carta di credito. Il plurale all'affermazione "contratti" non è fortuito, perché esistono almeno 3 contratti: il contratto tra venditore e consumatore, il contratto tra emittente e titolare della carta e il contratto tra emittente e commerciante. Quest'ultimo contratto offre all'Istituto di Credito la possibilità di accreditare dal conto del commerciante anche le eventuali somme contestate dal cliente. Non si tratta dunque di inventare modelli nuovi di rapporti contrattuali o particolari forme di sicurezza nei rapporti commerciali *on-line*. La prevenzione, e soprattutto la chiarezza del contratto, possono evitare spiacevoli sorprese o l'insorgere di un contenzioso con inutili perdite di tempo e denaro.

5. NOTIZIE DAI GRUPPI DI DISCUSSIONE SU INTERNET

Esistono decine di migliaia di gruppi di discussione, sparsi nel mondo, presenti su Internet. Dal 1994 è stata introdotta in Italia la gerarchia *it*, che raccoglie quasi trecento gruppi in lingua italiana. È possibile accedere a questi gruppi, anche in assenza di *software* specifico. Con un *browser* potete cercare l'indirizzo del tipo: <http://www.mailgate.org/mailgate/index.html> ed accedere direttamente ai gruppi di discussioni italiani.

Per esempio nei gruppi *it.discussioni.consumatori.tutela* o *it.discussioni.consumatori.rete* si discutono spesso delle truffe o dei nuovi raggiri perpetrati a danno degli utenti ignari dei rischi delle transazioni in Rete.

Riportiamo di seguito alcuni messaggi per capire il tono delle discussioni:

Subject: Truffe con PagoBancomat - Soldi facili subito!

Date: Wed, 15 Apr. xxxx

* Newsgroups: it.discussioni.consumatori.tutela

* From: xxxxxxxx@iol.it

* Subject: Truffe con PagoBancomat - Soldi facili subito!

Questa vicenda è vera, purtroppo!

Mi arriva a casa l'estratto conto della mia banca (importa quale?), sul quale campeg-

gia nelle informazioni alla clientela il seguente messaggio che riproto integralmente.

Si sono verificate negli ultimi mesi truffe a danno di utilizzatori di sportelli bancomat durante l'operazione di prelievo contante. I malviventi impediscono, con abili manipolazioni, la restituzione della carta al legittimo titolare convincendolo, offrendo la loro collaborazione, a digitare di nuovo il codice segreto in loro presenza. I malviventi riescono in seguito a recuperare le carte dallo sportello bancomat e, conoscendo il codice segreto, effettuando prelievi contante o acquisti POS.

"Per evitare prelievi fraudolenti, occorre prestare la massima attenzione nell'uso e custodia della propria carta evitando di digitare il codice segreto in presenza di estranei.

Nel caso la carta non venisse restituita o si accorgesse di comportamenti anomali, è necessario bloccarla al numero verde 167-822056 o contattare la propria dipendenza.

Ecco, questo è l'avvertimento, ma quanto è attuabile??? Quante volte usiamo il pagobancomat su terminali POS e digitiamo il codice nel mezzo di supermercati o altri esercizi commerciali e di ristorazione, tanto per dire ben tre esempi? Quando sono stati annotati il codice segreto e i riferimenti bancari (ben in vista sul dorso della carta), sono sufficienti per clonare carte bancomat? Mi direte "serve anche il know-how, bisogna sapere cosa scrivere e come scriverlo", ma davvero è un problema?

La storia vera di una mia collega di lavoro è semplicemente questa. martedì 7 aprile si accorge di essere priva del suo fidato bancomat, alla cosa non dà peso, avendolo scordato a casa più volte in passato e quindi credendolo al sicuro. Al venerdì le viene comunicato che il suo conto è in rosso e la tessera bancomat è stata trattenuta da un terminale di prelievo contante. Cade dalle nuvole e scopre che da giovedì 9 fino al momento del ritiro da parte della macchinetta per ben quattro volte è stato prelevato contante e pure effettuati acquisti di una certa consistenza che farebbero pensare a spese del supermercato per entità e le venti-sessanta lire conclusive dell'importo. La mia collega, pur essendo talvolta distratta, è una persona affidabile e mi fido di lei quando dice che potrebbe aver lasciato il tesserino su una macchina di prelievo contante, ma non ha la più pallida idea di come abbiano ottenuto il codice segreto. Una delle ipotesi che abbiamo fatto è che la tessera sia stata raccolta martedì e dopo un paio di giorni sia arrivata in mano ai soliti ignoti che hanno sovrascritto un loro codice segreto su quello originale - ipotesi maledettamente realistica - oppure il bancomat fosse tatocco e abbiano attraverso un falso specchio ritratto la tessera e osservato la digitazione del codice segreto.

Alcuni mesi fa, ormai sono passati degli anni, una banda molto bene organizzata aveva predisposto un "copybancomat" in cui un sottile pannello della misura e aspetto "giusti" veniva sovrapposto al pannello di inserimento della tessera, registrava la traccia magnetica e filmava con una spy-camera il codice segreto. Sarebbe l'unica spiegazione che mi convince, visto che permette la clonazione delle carte, con prelievi garantiti anche al confronto-firma. Per contrastare queste truffe servirebbe un innalzamento del livello di diffidenza nell'uso delle carte sia da parte degli utenti che da parte degli esercenti, non mi scandalizzerei se qualcuno mi chiedesse anche la carta d'identità.

Vengono anche in mente che il tesserino sia stato raccolto e usato - in ultima ipotesi - da personale competente di una qualche banca, solo per il fatto che hanno già "per lavoro" la possibilità di accedere ad apparecchi e archivi usati per codificare le stesse

carte. Mi rendo conto che è come dare dei ladri alla polizia e non è mia intenzione offendere nessuna delle categorie citate, ma essere bancari o poliziotti non può essere automaticamente considerato una patente di onestà e limpidezza

Ragà, state accorti. Se la mia banca mi avvisa che "da alcuni mesi" si stanno verificando questi episodi non si tratta del caso isolato, presumo quindi che ci sia una vera e propria organizzazione che segue questo ramo di attività a delinquere, e forse il sistema migliore per bloccarli subito è tenere sul conto una liquidità minima!!

Perdere in tre giorni mesi e mesi di risparmi. Grazie no!

* Newsgroups: it.discussioni consumatori tutela

* From: xxxx@tin.it

* Subject: Re. Truffe con PagoBancomat - Soldi facili subito!

Il 16 Aprile, xxxx@nowhere.com ha scritto: 3.000.000 in contanti (limite massimo di prelievo mensile con un bancomat... ma ci vorrebbero almeno SEI giorni per riuscire a prelevare 3 milioni!!!!!!) Sicuro??

Una volta lessi su una rivista che le macchine Bancomat non aggiornano in tempo reale il database della banca emittente (se fai prelievi da istituti diversi dal tuo). Addirittura si parlava di aggiornamenti fatti alle 8 di mattina, ma su questo non ci credo molto. Comunque, se è vero che gli aggiornamenti non sono in tempo reale, sarebbe possibile fregare i 3 milioni in poche ore.

Anni fa fu scoperta una truffa basata proprio su questi tempi e su info prelevate da Internet -)

* Newsgroups: it.diritto

* From: xxxxx@tin.it

* Subject: USO ABUSIVO DI CARTA DI CREDITO. RIMEDI?

* Date: 20 Apr xxxx

Ciao a tutti. Leggendo l'ultimo estratto conto della mia Carta Si ho purtroppo constatato che alcune società o soggetti sconosciuti con strani nomi inglesi hanno ottenuto degli accrediti attraverso transazioni su Internet che ovviamente non ho mai fatto.

Si tratta di non elevati importi, per fortuna, con operazioni in dollari. Ho subito protestato con il mio gestore il quale, dopo mille controlli e discussioni, ha detto che provvederà a sostituirmi la carta, ma che non può bloccare più i pagamenti.

Possibile che non ci sia alcun rimedio a situazioni simili?

Chi è responsabile di tali addebiti, se io non ho mai firmato nulla, né autorizzato la società che gestisce la mia Carta a pagare alcunché su ordini via Internet? È sufficiente oggi che chiunque, rubando un numero di carta di credito, possa ricevere delle somme

senza mia autorizzazione e poi sparire nel nulla senza che si possa fare nulla?
Chiedo a voi tutti più esperti lumi su questa situazione che penso possa riguardare tutti gli utenti di Internet

Ringrazio in anticipo chi darà aiuto (anche via *e-mail*)!

* Newsgroups: it.diritto

* From: studioxxxxx@writeime.com

* Subject: USO ABUSIVO DI CARTA DI CREDITO RIMEDI?

* Date: 20 Apr xxxx

Ciao a tutti. Leggendo l'ultimo estratto conto della mia Carta Si ho purtroppo constatato che alcune società o soggetti sconosciuti con strani nomi inglesi hanno ottenuto degli accrediti attraverso transazioni su Internet che ovviamente non ho mai fatto.

Ho appena scoperto che anche a me è successa la stessa cosa.

Darò battaglia fino in fondo ai Servizi Interbancari (società che gestisce la carta Si), finché non riotterrerò il riaccredito delle somme (fortunatamente basse) illegittimamente sottrattemi.

Non avendo dato alcun ordine di pagamento alla società, credo che le possibilità di successo siano notevoli.

Se sarà necessario coinvolgerò il Comitato difesa consumatori ed eventualmente le varie trasmissioni televisive (Mi manda Raitre o il programma di Lubrano).

Il problema è serio, in quanto le transazioni tramite Internet non hanno alcun tipo di controllo e chiunque può restare fregato, senza che usi la carta in Rete (è sufficiente che un cameriere poco corretto prenda nota del numero di carta e del nome di un qualsiasi cliente di un ristorante, e si diverta poi a fare acquisti in Rete).

Non me ne vogliano i camerieri, l'esempio poteva riferirsi a chiunque, senza voler criminalizzare nessuna categoria.

Comunque, se a qualcun altro è successo qualcosa di simile, propongo di coalizzarci facendo unico fronte contro le società che gestiscono le carte.

Inviatemi pure messaggi in *e-mail* e concorderemo cosa fare.

Non occorrono troppi commenti per capire l'utilità della diffusione delle notizie su canali aperti alle più diverse tipologie di utenti. Su Internet, in particolare attraverso questi gruppi di discussione, sono state smascherate organizzazioni e raggi che altri mezzi di comunicazione avrebbero fatto fatica a raggiungere.

6. I CANALI DI DISCUSSIONE IN TEMPO REALE (CHAT)

La Rete offre l'opportunità di chiacchierare in tempo reale su argomenti di proprio gradimento. Non esamineremo in questo caso i canali italiani di *chat-line* o meglio IRC - *Internet Relay Chat* -, conosciuti soprattutto dai giovani per particolari tipi di conversazione, ma mi limiterei ad indicare che, nonostante la difficoltà nel reperire una lista ufficiale e stabile di indirizzi, esistono alcuni canali preposti alla discussione di argomenti legati al commercio e alle nuove tecnologie. La ricerca, dunque, di questi canali può avvenire iscrivendosi ad una *mail-list* italiana dedicata a IRC e chiedere ai partecipanti notizie sullo specifico argomento. Un canale dove avvengono discussioni *on-line* delle problematiche con il pagamento su Internet attraverso le carte di credito, è denominato *#carding*.

Il vantaggio di poter chiedere e ricevere informazioni in tempo reale è innegabile. L'unico problema è che di queste conversazioni non rimane - almeno in apparenza ed alla portata di tutti - alcuna traccia scritta. Si è portati a pensare, - per episodi oggetto di indagine - che attraverso queste conversazioni si potrebbero diffondere i numeri di una carta di credito, in modo da utilizzarlo illecitamente nel più breve tempo possibile. Le conseguenze di un'ipotetica condotta sarebbero devastanti per colui che ha subito il furto in virtù delle considerazioni sulle problematiche contrattuali, già esposte, di un carta di credito. Non meno rilevante è la difficoltà tecnica di accertamento di tutte le violazioni, che avvengono attraverso l'uso di strumenti elettronici e soprattutto attraverso le reti telematiche.

7. LE DIFFICOLTÀ DI ACCERTAMENTO DELLE VIOLAZIONI

Il Consiglio dell'Unione Europea ha recentemente formulato una proposta che adotta un Piano pluriennale d'azione comunitaria per promuovere l'uso di Internet - pubblicato in gazzetta ufficiale delle Comunità europee, C 48/8 del 13/3/1998 - che evidenzia l'attuale difficoltà a "controllare" in qualche forma l'uso del nuovo strumento.

Nella premessa il Consiglio ritiene che Internet sta diventando un'industria che offre servizi al grande pubblico con conseguenze positive soprattutto per l'istruzione, le fonti di informazione e così via. Si aggiunge subito dopo la riflessione sulle conseguenze negative che tale fenomeno ha già evidenziato: ci si preoccupa dei contenuti nocivi e illegali

diffusi da Internet ritenendolo un ostacolo per lo sviluppo e l'instaurarsi di un ambiente propizio alle iniziative.

Soprattutto per l'industria si avverte l'esigenza di un controllo dei contenuti o di strumenti di filtraggio per promuovere un ambiente sicuro.

Ricordiamo che la discussione dei problemi posti dal rapido sviluppo di Internet è sorta in ambito europeo fin dai primi mesi del 1996. Il Parlamento europeo nella sua risoluzione del 24 aprile 1997 ha invitato gli Stati membri a definire nei rispettivi ordinamenti giuridici norme minime comuni e forme di cooperazione, per raggiungere l'obiettivo comune di rendere sicuro l'uso di Internet.

La Dichiarazione ministeriale adottata alla Conferenza internazionale sul tema "Realizzare le potenzialità delle reti globali di informazione", tenutasi a Bonn il 6-8 luglio 1997, ha sottolineato il ruolo che il settore privato può assumere nella tutela degli interessi dei consumatori ed incoraggia l'industria ad escogitare sistemi di valutazione del contenuto e proporre servizi di valutazione adeguati alle esigenze dei vari utenti con la salvaguardia degli interessi della società in generale, compresi quelli dei produttori e dei consumatori. Senza addentrarci nella valutazione di merito sui sistemi di filtraggio o di controllo che introducono la discussione su argomenti come la limitazione della libertà o della forma di espressione, la riflessione sulla discussione comunitaria evidenzia la preoccupazione di tutti di voler prevenire le violazioni, soprattutto se commesse attraverso strumenti sconosciuti agli organi di controllo.

Sono ormai note le diverse storie degli *hackers*, conosciuti come "pirati informatici", non solo perché riescono a dimostrare di essere più bravi degli amministratori dei sistemi, ma perché riescono a procurare danni nelle più svariate forme.

L'impresa che decide di utilizzare i nuovi strumenti tecnologici non può sottovalutare il rischio che da essi ne potrebbe derivare.

Prendiamo il caso della diffusione dei *virus* o di programmi atti a danneggiare altri sistemi informatici attraverso il collegamento in Rete. In merito, uno studente della Cornell University, Robert Tappan Morris, fu condannato nel 1991 in America per aver infettato 6.000 *computer* con un *virus*, al fine di dimostrare che i sistemi adottati per impedire l'accesso non autorizzato a Internet erano assolutamente inaffidabili.

L'osservatorio sulla criminalità informatica - FTI - fin dal Rapporto del 1997, ha distinto due filoni di violazioni informatiche: gli atti commessi per mezzo di tecnologie informatiche e gli atti a danno dei sistemi informatici e telematici.

In entrambi i casi le difficoltà dell'accertamento sono legate all'uso dei sistemi tradizionali d'investigazione. A parte qualche gruppo isolato, in generale non esiste a livello nazionale un nucleo di Polizia giudiziaria che si occupa di tutte le violazioni informatiche. E potrebbe non bastare il solo nucleo specializzato per ogni provincia senza la collaborazione di esperti che vivono - per lavoro - nei diversi settori delle nuove tecnologie. Il punto debole della materia è che non basta più studiare a scuola o all'università l'informatica. La velocità dell'evoluzione tecnologica, ad esempio nel settore dell'*internetworking*, richiede un lavoro di gruppo per fronteggiare il fenomeno della pirateria, cioè di coloro che per passione o interessi vivono *full-time* nel mondo digitale.

I termini, piazze telematiche, realtà virtuali, città invisibili non sono più racconti tratti dai libri di fantascienza.

Tornando al fenomeno delle violazioni, esaminiamo il caso di un furto del numero di una carta di credito e proviamo ad esaminare il suo sviluppo. Colui che ha subito il furto potrà denunciare l'accaduto presso l'autorità giudiziaria. La denuncia sarà contro gli ignoti. La polizia giudiziaria delegata dal magistrato comincerà a prendere contatti con l'istituto di credito presso cui era stata rilasciata la carta di credito. A questo punto la Banca offrirà la massima collaborazione, ma non potrà far altro che indicare la provenienza della richiesta di addebito delle somme prelevate. Si scopre così che magari la richiesta è pervenuta dall'estero e che si è costretti a chiedere una rogatoria internazionale per proseguire le ricerche. A questo punto le difficoltà non sono più solo operative, ma cominciano i problemi tecnici. Chi preleverà i *log*, cioè il tracciato delle operazioni registrate? Come controllare la differenza del fuso orario con le mille difficoltà dei differenti sistemi operativi in uso, con la precaria affidabilità dei supporti contenenti i dati o con quant'altro di imprevedibile possa accadere ad un sistema telematico che è pur sempre soggetto ad avarie? In molti casi, se il furto è opera di esperti la ricerca non si limiterà ad un solo sistema. Si innesca il cosiddetto fenomeno del ping-pong o rimbalzo, cioè collegandosi a più sistemi prima di compiere la violazione.

Ci sono stati diversi episodi, per quanto riguarda i messaggi di posta elettronica, in cui attraverso i *remailer* anonimi, cioè dei *computer* che consentono di cambiare il proprio nome e addirittura di rendersi anonimi cancellando ogni traccia o identità del mittente, sono state compiute violazioni e danneggiamenti vari.

La soluzione del problema è da ricercarsi nell'equilibrio tra maggiore sicurezza e migliori tecniche di accertamento delle violazioni. È vero che entrare in un'abitazione con la porta aperta o senza una parete è pur sempre violazione di domicilio e della proprietà privata, ma a quel punto bisogna punire anche la semplice curiosità.

Per finire, non sono le nuove norme che occorrono! Qualcuno già due secoli fa disse che le troppe leggi, che il cittadino non poteva conoscere a memoria, erano peggio delle poche leggi! Bisogna trovare il metodo per seguire, a vista d'occhio, l'evoluzione dell'informatica e della telematica, con gli strumenti a disposizione in quel momento.

8. NOTA BIBLIOGRAFICA

CILLI A., *Questioni di contratti* - Internet news, Tecniche nuove, aprile 1998.

FTI *Rapporto 1998*, Franco Angeli, 1998.

HANCE O., *Internet e la legge*, McGraw-Hill, 1997.

LARRY J., HUGES JR., *Tecniche di sicurezza Internet*, Jackson libri, 1996.

TORRENI O., PARIRE S., *Internet e diritto* - Il Sole 24 Ore, Norme e Tributi, 1997.

9. APPENDICE

Diapositiva 1

La sicurezza delle transazioni nel commercio elettronico

ALCUNE CIFRE



Transazioni on-line a livello mondiale:

- nel 1998 --> spese oltre 48 miliardi di dollari
- nel 2002 --> supereranno i 410 miliardi di dollari
- nel 2005 --> raggiungeranno i 3.000 miliardi

SITUAZIONE ITALIANA

- il 1998 è stato il primo anno significativo per il commercio elettronico
- per il 1999 è prevista la spesa di 800 miliardi
- per i primi anni del nuovo millennio la crescita è esponenziale

Copyright © 99 by Antonio Cilli

Diapositiva 2

La sicurezza delle transazioni nel commercio elettronico

DILEMMA: VANTAGGI/RISCHI



VANTAGGI:

- velocità
- attrattiva
- accessibilità 24 ore su 24
- apertura 7 giorni su 7

RISCHI:

- clienti e venditori non si possono guardare
- non è possibile controllare firme e carte d'identità
- è facile copiare la grafica del negozio virtuale

Copyright © 99 by Antonio Cilli

Diapositiva 3

La sicurezza delle transazioni nel commercio elettronico

DILEMMA: VANTAGGI/RISCHI



RISCHI:

- alcuni negozi hanno preso illegalmente i numeri di carta di credito
- numerose transazioni sono state intercettate
- sono stati sviluppati software in grado di generare numeri di carte di credito
- sono stati creati canali di chat per lo scambio di notizie sulle truffe con il pagamento on-line
- in molti casi non è stato implementato alcun sistema di sicurezza per il pagamento on-line

Copyright © 99 by Antonio Cilli

Diapositiva 4

La sicurezza delle transazioni nel commercio elettronico

TRANSAZIONI ON-LINE



COS'E' IL PAGAMENTO ON-LINE?

- il cliente acquista e paga con Carta di credito
- il negoziante chiede alla Banca del cliente la disponibilità e l'accredito
- la merce viene spedita

**I SISTEMI DI PAGAMENTO
GIOCANO IL RUOLO PIU' IMPORTANTE!**

E' frequente leggere la seguente avvertenza:
**"SI SCONSIGLIA L'USO DELLA CARTA DI
CREDITO IN CHIARO"**

Copyright © 99 by Antonio Cilli

Diapositiva 5

La sicurezza delle transazioni nel commercio elettronico

I SISTEMI DI PAGAMENTO

- * La prima forma fu il BARATTO
- * Nel 15° secolo nacquero le BANCHE
- * Nella 2° metà del '900 è avvenuta la rivoluzione:
attraverso l'informatica e la telematica



DISTINZIONE DEI SISTEMI DI PAGAMENTO:

- **SISTEMI BASATI SU SOLUZIONI HARDWARE**
- **SISTEMI BASATI SU SOLUZIONI SOFTWARE**

Copyright © 99 by Antonio Cilli

Diapositiva 6

La sicurezza delle transazioni nel commercio elettronico

SISTEMI BASATI SU SOLUZIONI HARDWARE
(Pagamento attraverso carte prepagate)



VANTAGGI:

- facilità di diffusione delle carte attraverso:
 - biglietterie
 - distributori automatici
 - giornali

SVANTAGGI:

- creazione di uno standard di carte
- implementazioni di lettori sui PC
- livelli di sicurezza accettabili

Copyright © 99 by Antonio Cilli

Diapositiva 7

La sicurezza delle transazioni nel commercio elettronico

SISTEMI BASATI SU SOLUZIONI SOFTWARE
(numerosa proposte)



DISTINZIONE IN 3 CLASSI:

1. Utilizzo di carte di credito
2. Impiego di assegni digitali
3. Utilizzo della moneta elettronica

PAGAMENTO CON CARTA DI CREDITO

- ordine del prodotto e comunicazione del numero di carta per fax o per telefono
- acquisto ed invio in CHIARO dei dati della carta di credito (**RISCHIO DI INTERCETTAZIONE**)

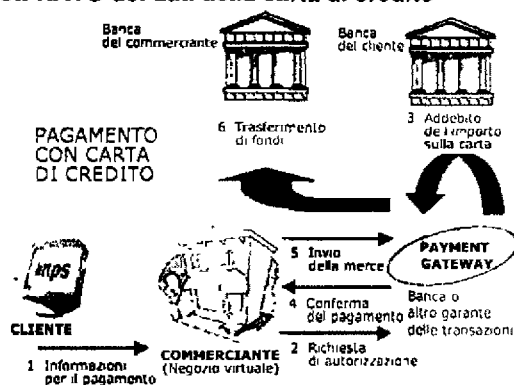
Copyright © 99 by Antonio Cilli

Diapositiva 8

La sicurezza delle transazioni nel commercio elettronico

PAGAMENTO CON CARTA DI CREDITO

- invio **CIFRATO** dei dati della carta di credito



Diapositiva 9

La sicurezza delle transazioni nel commercio elettronico

ASSEGNI DIGITALI

Presupposto:

Attivazione di un conto presso una BANCA ON-LINE



Utilizzo/Vantaggi:

- Compilazione di un assegno digitale
- Utilizzo di protocolli come SSL o SET per la codifica dei dati
- Richiesta di pagamento attraverso la propria banca di fiducia
- Rapidità del pagamento

Informazioni su alcuni sistemi sperimentati:

<http://gost.isi.edu/info/netcheque/distribution.htm>

Copyright © 99 by Antonio Cilli

Diapositiva 10

La sicurezza delle transazioni nel commercio elettronico

MONETA ELETTRONICA

COM'E' IL DENARO O UNA BANCONOTA VIRTUALE

E' costituita da una lunga serie di bit generata da un software



COME FUNZIONA

- L'acquirente fabbrica la banconota e la manda alla propria banca
- La banca verifica la disponibilità e rispedisce la banconota apponendovi un numero di serie

ASPETTO SICUREZZA?

NECESSARI ALGORITMI DI CRITTOGRAFIA

Copyright © 99 by Antonio Cilli

Diapositiva 11

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA

Protocollo SSL (Secure Socket Layer) come funziona

- **CRIPTA** le informazioni dal browser al sito Web
- **Rende illegibili le informazioni** intercettate



Come si riconosce chi lo usa?

Il protocollo S-Http (Secure Hypertext Transfer Protocol) instaura il collegamento sicuro:

- appare un lucchetto o una chiave
- il protocollo cambia da HTTP a HTTPS



COSA MANCA?

La certezza sull'identità di chi effettua la transazione!

Copyright © 99 by Antonio Cilli

Diapositiva 12

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA

NELL'USO DEL PROTOCOLLO DI SICUREZZA:

- **Manca la firma**, l'identità di chi effettua l'operazione
- **E' ripudiabile** dal legittimo titolare



VANTAGGI

- **E' un sistema semplice e veloce**
- **Ha avuto molto successo:**
es. amazon.com ---> oltre 9 milioni di clienti

NUOVI PROTOCOLLI: SET (Secure Electronic Transfer)

Copyright © 99 by Antonio Cilli

Diapositiva 13

La sicurezza delle transazioni nel commercio elettronico

ASPETTO SICUREZZA**IL PROTOCOLLO SET (Secure Electronic Transfer)**

Non è integrato in tutti i browser

E' necessario l'installazione di un software

Il titolare deve chiedere il rilascio di un codice personale (PIN)

Le transazioni non sono ripudiabili da parte del titolare

L'onere della prova è a carico del titolare

CERTIFICATI DIGITALI:

E' un documento elettronico reso valido da una

CERTIFICATION AUTHORITY

es. VERISIGN ---> (www.verisign.com)

Copyright © 99 by Antonio Cilli

**Diapositiva 14**

La sicurezza delle transazioni nel commercio elettronico

SITUAZIONE ITALIANA

• SONO STATI SPERIMENTATI E RESI DISPONIBILI MOLTI SISTEMI

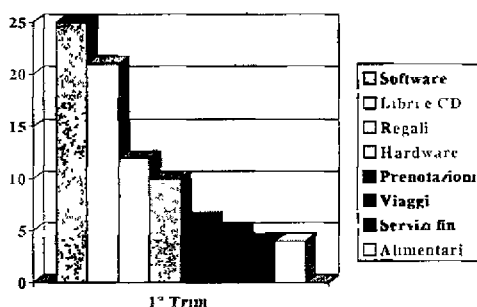
• ESISTE LA POSSIBILITA' DI FORMARE ED INVIARE UN DOCUMENTO INFORMATICO ASSICURANDO LA SUA INTEGRITA'

• ESISTONO SOFTWARE DI CRITTOGRAFIA A CHIAVE PUBBLICA

es. PGP (Pretty Good Privacy) di Zimmerman utilizza 2 algoritmi di crittografia: a chiavi pubbliche RSA e a chiavi private IDEA

Copyright © 99 by Antonio Cilli



*Diapositiva 15**La sicurezza delle transazioni nel commercio elettronico***ACQUISTI IN RETE IN ITALIA NEL 1998***Copyright © 99 by Antonio Cilli**Diapositiva 16**La sicurezza delle transazioni nel commercio elettronico***PRECAUZIONI PER L'USO****"SCONSIGLIAMO L'UTILIZZO IN CHIARO DEL VOSTRO****NUMERO DI CARTA SU INTERNET"**
oppure**"I SISTEMI DI SICUREZZA ATTUALMENTE IN USO NON
SONO PIENAMENTE RICONOSCIUTI DAI CIRCUITI
INTERNAZIONALI VISA E MASTERCARD/EUOCARD"****Consultabile al seguente indirizzo Internet:
<http://www.cartasi.it/java/istruzioni.html>***Copyright © 99 by Antonio Cilli*

Diapositiva 17

La sicurezza delle transazioni nel commercio elettronico

Siti di riferimento:



<http://www.netgallery.net/ecommerce>

<http://www.cybercash.com>

<http://www.digicash.com>

<http://www.netmarket.com>

<http://www.visa.com>

<http://www.cert.org>

<http://web.mit.edu>

<http://www.aipa.it>

<http://www.rsa.com>

<http://www.pgpi.com>

Copyright © 99 by Antonio Cilli

III SESSIONE

Presiede: Pietro Perlingieri

La tutela dei dati personali: la *privacy* e l'*e-commerce*

RICCARDO ACCIAI

SOMMARIO: 1. Trattamenti "visibili" ed "invisibili" - 2. La protezione dei dati personali in Italia - I flussi di dati "transfrontalieri" - 4. I negoziati bilaterali - 5. Il ruolo delle organizzazioni internazionali - 6. Le prospettive di soluzione.

1. TRATTAMENTI "VISIBILI" ED "INVISIBILI"

È ormai pacifico che fra i problemi che ostacolano il completo sviluppo del commercio elettronico, quello della protezione dei dati personali va assumendo un ruolo sempre più di primo piano.

Mentre, infatti, sino a poco tempo fa, in questo settore si era generalmente inclini a ritenere le questioni relative alla tutela della *privacy* come secondarie, rispetto ai più avvertiti temi della sicurezza della transazione, del regime fiscale applicabile, o del foro competente in caso di controversie, recentemente, i sondaggi effettuati da diverse organizzazioni¹ e le frequenti dichiarazioni di molte associazioni di consumatori dimostrano la rilevanza che la protezione della riservatezza ha ormai acquisito nella coscienza collettiva, soprattutto, per il modo assai poco trasparente con cui i dati vengono acquisiti e trattati.

Ogni transazione effettuata sul Web comporta, com'è noto, la propagazione di un certo numero di informazioni personali, le quali, talvolta, sono chieste espressamente all'interessato, tal'altra, vengono acquisite a sua totale insaputa.

La prima ipotesi si realizza generalmente quando i dati sono conferiti direttamente dalla persona che intende avvalersi di determinati servizi o che decide volontariamente di rispondere alle domande che, a vario titolo, gli vengono poste.

¹ Cfr., fra i molti, quello condotto da *Privacy & American Business* da cui risulta che l'82% del campione intervistato ritiene importante sapere che il sito che tratta i suoi dati adotta una corretta politica della *privacy* (i risultati del sondaggio sono pubblicati a margine dell'articolo citato).
PIRIATI - RO. IMPERIALI, *Internet e privacy: Usa e Italia a confronto*, in *Il Sole-24 Ore - Diritto e Pratica delle Società*, 10.5.1999, n. 8, pp. 36-42, spec. p. 37).

Al di là di questa consapevolezza iniziale, però, molto spesso alla stessa persona non viene detto nulla (o assai poco) circa le modalità con le quali tali informazioni sono gestite e, soprattutto, se ed a chi esse saranno ulteriormente comunicate; inoltre, molti dei dati richiesti risultano frequentemente del tutto eccedenti rispetto alle necessità proprie della specifica prestazione² e, in un numero considerevole di casi, acquisiti al solo scopo di inviare successivamente informazioni commerciali da parte dell'originario titolare o di altri ai quali essi vengono successivamente ceduti.

Un altro degli aspetti "dolenti" nella comune gestione dei dati è rappresentato dalla carenza di adeguate misure di sicurezza.

È fin troppo scontato, a questo riguardo, il riferimento al recente episodio di cronaca che ha visto la violazione dell'elenco degli abbonati di una rivista di informatica, attraverso una semplice operazione di accesso a quella banca dati; violazione che, com'è noto, ha portato alla conoscenza non autorizzata sia dei nominativi di tali abbonati, sia dei numeri delle loro carte di credito³.

Se è vero che la conoscenza di tali informazioni dà luogo, in prima battuta, ad un problema di tipo sostanzialmente "economico" per i malcapitati e per chi poi è chiamato (anche in termini di immagine) a riparare al danno, la relazione fra i nominativi degli abbonati ed il tipo di rivista di cui questi sono presumibilmente lettori costituisce un chiaro esempio del genere di violazioni della riservatezza che tali azioni possono comportare.

² Si pensi, ad esempio, alla richiesta dell'indirizzo di una persona nel caso di acquisto di un software tramite "scansione" diretto e con pagamento effettuato a mezzo di carta di credito. Un recente studio, effettuato su base comparativa internazionale, ha mostrato che fra i dati che più frequentemente sono richiesti al cliente, il nome e il cognome figurano nel 97% dei casi, l'indirizzo nel 90%, l'indirizzo di posta elettronica nell'89%, il numero di telefono nel 72%, il numero di carta di credito nel 69%, l'indirizzo al quale inviare la fattura (se diverso da quello di consegna) nel 63% dei casi (cfr. CONSUMER INTERNATIONAL, *Consumers shopping*, London, 1999, p. 30).

³ Il fatto è stato dettagliatamente narrato sulle pagine de *il Giornale*, al quale era giunta la segnalazione da parte della persona penetrata nell'archivio in questione. V., in particolare, M. Camera, *Carte di credito in balia di tutti. Il Garante aprirà un'inchiesta*, in *il Giornale*, 16.10.1999, p. 1 e P. Angelini, *Non sarebbe dovuto accadere. Il commercio on-line non è Far West ma fermare i pirati è impossibile*, in *il*, p. 3, v. anche A. Cherchi, *Un'indagine del Garante sulla privacy in Internet*, in *Il Sole-24 Ore*, 26.10.1999, p. 22.

Nel caso ricordato, sicuramente, gli effetti per la *privacy* degli interessati sono stati del tutto relativi, dato il tipo di rivista in questione, ma quali ripercussioni si sarebbero potute avere se l'accesso non autorizzato fosse avvenuto (tanto per rimanere nel campo editoriale) nei confronti di pubblicazioni di tipo diverso, tali da consentire, ad esempio, di risalire alle convinzioni religiose o politiche di una persona, ovvero alle sue condizioni di salute o alle sue preferenze sessuali?

Generalmente si è soliti sottovalutare questi aspetti, nella falsa convinzione che se non si è conosciuti da chi ha avuto accesso a determinati dati che ci riguardano, il danno che ne può derivare è sicuramente relativo; in effetti, la facilità con la quale determinate informazioni possono oggi essere elaborate, conservate, incrociate con altre ed ottenute "al momento opportuno" non sembrerebbe poter consentire tale condizione di tranquillità.

Oltre ai dati conferiti consapevolmente, poi, come si è accennato, un discorso del tutto peculiare è quello relativo alle "tracce" che inconsapevolmente si "lasciano" navigando su Internet ed ai dati che vengono intenzionalmente acquisiti senza che al soggetto interessato sia data alcuna informazione⁴.

In tale caso non si è tanto di fronte ad un rischio di violazione della riservatezza, quanto piuttosto ad un modo di trattare informazioni personali non compatibile con il quadro di garanzie che il legislatore comunitario e quello nazionale hanno voluto attribuire anche all'utente della Rete.

Il problema fondamentale, come si avrà modo di vedere, consiste proprio nella difficoltà di far rispettare un insieme di norme e di valori altamente condiviso nei Paesi occidentali che, troppo spesso, nel difficile temperamento con altri importanti principi (quali ad es. quello di libertà economica), vengono sacrificati oltre misura.

Generalmente, nell'affrontare i temi relativi alla protezione dei dati personali, prima di esaminare la situazione italiana, si è soliti ricordare i

⁴ Esempi tipici di questi trattamenti "invisibili", pur senza entrare nel dettaglio, sono il "chattering" a livello http, "hyperlink" automatici a terzi, il contenuto attivo (come Java, ActiveX o altre tecniche di scrittura basate sull'utente e il meccanismo dei "cookies", così come applicato nei comuni browser. Un'interessante panoramica in tal senso è offerta da V. Grippo, *Internet e dati personali*, in A. Clemente (a cura di), *Privacy*, Padova, Cedam, 1999, pp. 285-317, v. anche, G. Ciacci, *Internet e il diritto alla riservatezza*, in *Riv. trim. dir. proc. civ.*, 1999, pp. 233-252, spec. pp. 244-246.

riferimenti internazionali e comunitari da cui la legislazione nazionale prende le mosse; nel caso del commercio elettronico e, più in generale, della tutela della riservatezza su Internet è d'obbligo effettuare un percorso inverso, poiché le norme interne hanno scarso o nessun valore se non si inseriscono in un quadro internazionale soddisfacente.

2. LA PROTEZIONE DEI DATI PERSONALI IN ITALIA

Il nostro Paese, com'è noto, nel timore di rimanere escluso dal cosiddetto "spazio Schengen", che richiedeva fra l'altro l'esistenza di una normativa nazionale in materia di protezione dei dati personali, con un'accelerazione del tutto sorprendente, è riuscito a dotarsi entro la fine del 1996 di una legge che ha recepito in gran parte la più recente direttiva comunitaria in materia, la n. 95/46/CE⁵.

La "fretta" di adottare quella che sarebbe divenuta la legge 31 dicembre 1996, n. 675, nonché le indubbie difficoltà applicative di alcune norme comunitarie (sono ancora molti gli Stati membri che, a distanza di diverso tempo dall'entrata in vigore della direttiva, non hanno ancora avviato alcun passo ufficiale per il suo recepimento), hanno indotto il Parlamento a licenziare contestualmente una legge delega, la n. 676, che attribuiva al Governo il compito di integrare e modificare la legge principale.

Fra gli aspetti che avrebbero dovuto trovare completamente tramite la delega, l'art.1, comma 1, lettera n), della legge n. 676 faceva riferimento al settore che, pur con qualche esemplificazione, potremmo indicare come quello delle reti aperte.

Purtroppo la delega, dopo un primo rinnovo, è scaduta, così come è spirato il termine residuale previsto dalla legge comunitaria per il 1998, che dava la possibilità al Governo, fino al febbraio dell'anno successivo, di portare a completamento la trasposizione della direttiva del 1995. Al momento è fermo in Parlamento un ulteriore disegno di legge che potrebbe, da un momento all'altro, conferire una nuova delega all'esecutivo.

⁵ Direttiva 24 ottobre 1995, n. 95/46/CE del Parlamento europeo e del Consiglio relativa alla "Tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", in G.U.C.E. 23 11 1995, n. L 281/31

In attesa di conoscere se vi sarà la possibilità di arrivare ad un atto normativo specifico che regoli, per quanto possibile, i problemi che l'uso di Internet crea da un punto di vista della tutela della riservatezza, va precisato, tuttavia, chiaramente che le norme già dettate dalla legge n. 675 per la generalità dei trattamenti sono applicabili anche al particolare mondo della Rete.

Come autorevolmente precisato, infatti, i trattamenti che vengono effettuati tramite Internet non si svolgono "nel vuoto", ma, pur utilizzando uno strumento particolare, sono da considerarsi a tutti gli effetti soggetti al sistema di regole creato dalla legislazione (comunitaria e) nazionale⁶.

I dati personali utilizzati ai fini di transazioni commerciali *on-line*, pertanto, devono essere trattati in modo lecito e secondo correttezza, raccolti e registrati per scopi espliciti e legittimi, esatti e, se necessario, aggiornati, pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono stati raccolti; infine, essi devono essere conservati solo per periodi di tempo accuratamente valutati (art. 9, l. n. 675/1996).

Allo stesso modo, gli *internauti* o i potenziali clienti devono essere resi edotti del fatto che si stanno raccogliendo dati nei loro confronti, nonché per quali finalità e con quali modalità avviene tale raccolta; deve essere precisata inoltre la natura obbligatoria o facoltativa del conferimento di quei dati, oltre, ovviamente, alle categorie ed ai soggetti ai quali gli stessi possono essere comunicati (art. 10, l. n. 675/1996).

Ancora, l'interessato deve prestare il proprio consenso al trattamento dei dati che lo riguardano e tale consenso non può essere dato, per esplicita scelta del nostro legislatore, attraverso una semplice acquiescenza, ma deve essere liberamente manifestato, in forma orale se i dati sono di carattere "comune" (art. 11), in forma scritta se invece si riferiscono a dati "sensibili" (art. 22) o ad alcuni provvedimenti giudiziari (art. 24).

L'interessato deve poi essere messo in condizione di esercitare i penetranti diritti previsti dall'art. 13 della legge che gli consentono di accedere ai suoi dati personali, di ottenerne l'aggiornamento, la rettificazione o l'integrazione, nonché, se sono trattati in violazione di legge, anche la cancellazione o il blocco (cioè l'interruzione di ogni trattamento, ecce-

⁶ Tale considerazione è stata svolta, dapprima, dal Gruppo di lavoro istituito dall'art. 29 della citata direttiva (v. *infra*, nota n. 14) nella Raccomandazione n. 3/97 relativa all'"Anonimato su Internet", adottata il 3 dicembre 1997 e successivamente ribadita da alcune pronunce del Garante.

zion fatta per la mera conservazione). Inoltre, l'utente di Internet o il potenziale cliente può opporsi, senza dover avanzare alcuna particolare motivazione, all'uso dei suoi dati ai fini di prospezione commerciale.

Infine, secondo l'art. 15 della legge, ai dati personali detenuti dal "titolare", devono essere applicate idonee misure di sicurezza, con la possibilità di chiedere il ristoro di ogni danno subito qualora si dimostri che quelle adottate non si sono rivelate sufficienti ad evitare l'uso non autorizzato o la perdita anche accidentale degli stessi.

A breve distanza dall'entrata in vigore della legge n. 675, è stata poi trasposta in diritto interno un'ulteriore direttiva, la n. 97/66/CE⁷ (anche in questo caso l'Italia è risultato il primo Paese ad adeguarsi), che affronta i problemi della protezione dei dati con specifico riferimento al settore delle telecomunicazioni.

Il decreto legislativo 13 maggio 1998, n. 171⁸, estende (o, meglio sarebbe dire, dettaglia) alcune norme sulla protezione dei dati personali ai fornitori di un servizio di telecomunicazioni⁹, prevedendo, ad esempio, l'obbligo di informare gli abbonati e, ove possibile, gli utenti circa la sussistenza di situazioni che permettono di apprendere in modo non intenzionale il contenuto di comunicazioni o conversazioni da parte di soggetti ad esse estranei (art. 3).

Lo stesso decreto precisa poi che il fornitore di un servizio di telecomunicazioni è tenuto ad adottare le misure tecniche ed organizzative, previste in materia di sicurezza dall'art. 15 della legge del 1996, con l'obbligo di informare gli abbonati quando sussiste un particolare rischio di violazione della sicurezza della Rete indicando i possibili rimedi ed i relativi costi (art. 2)¹⁰.

⁷ Direttiva 15 dicembre 1997, n. 97/66/CE del Parlamento europeo e del Consiglio relativa al "Trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni", in *G.U.C.E.* 30 I 1998, n. 1, 24.

⁸ "Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica", in *G.U.* 3 giugno 1998, n. 127.

⁹ Per "servizio di telecomunicazioni", il decreto intende un servizio "la cui fornitura consiste, in tutto o in parte, nella trasmissione e nell'instradamento di segnali su reti di telecomunicazioni, ivi compreso qualunque servizio interattivo anche se relativi a prodotti audiovisivi, esclusa la diffusione circolare dei programmi radiofonici e televisivi" (art. 1, comma 1, lett. d).

¹⁰ È sulla base di quest'obbligo - tanto per fare un esempio concreto - che l'editrice della rivista che ha visto violato il proprio archivio abbonati ha dovuto provvedere ad una capillare informazione (ovviamente gratuita) degli interessati.

L'insieme di questi diritti ed obblighi introdotti dai due citati atti normativi, se rispettato, com'è agevole intuire, risolverebbe già una serie di importanti problemi in materia di reti aperte e di commercio elettronico.

Tuttavia, a parte un generalizzato scarso rispetto delle norme della legge n. 675¹¹, e la difficoltà applicativa di alcune norme, evidentemente scritte non avendo a mente il particolare mondo di Internet (si pensi ad esempio al problema del consenso scritto per i dati sensibili che, fino a quando non sarà a tutti gli effetti operativa la firma elettronica, avrà scarse possibilità di essere applicata¹²), la questione di maggior problematicità, al pari di molte altre che riguardano il commercio elettronico, è legata al principio di territorialità¹³ e, di conseguenza, a quello dei mezzi attraverso i quali tutelare efficacemente i diritti che si ritengono violati in un settore che ha nella "globalizzazione" il suo elemento identificativo.

Proprio per tale ragione, indipendentemente da quanto riuscirà a farsi sul piano nazionale per risolvere le pur non secondarie difficoltà di applicazione della normativa, la vera "sfida" per l'aumento della fiducia del consumatore e, quindi, per lo sviluppo del commercio elettronico, si gioca sul piano internazionale.

3. I FLUSSI DI DATI "TRANSFRONTALIERI"

Il grado di tutela assicurato ai dati che travalicano i confini nazionali è sicuramente soddisfacente se questi rimangono all'interno dell'Unione

¹¹ Il Garante, per fronteggiare tale stato di cose, dopo un approccio di carattere "persuasivo" avviato nei primi tre anni di applicazione della nuova normativa, ha annunciato l'avvio delle ispezioni presso i titolari e i responsabili dei trattamenti, ispezioni che possono culminare con semplici sanzioni amministrative (v. art. 39, l. n. 675), ma anche con la segnalazione di possibili reati, per i quali sono previste sanzioni di carattere penale (v. artt. 34-37, l. n. 675).

¹² Non pare, infatti, potersi condividere l'opinione di chi (P. TOSI, *Prime osservazioni sull'applicabilità della disciplina generale della tutela dei dati personali a internet e al commercio elettronico*, in *Dir. inf.*, 1999, pp. 591-607, spec. pp. 602-603) riterrrebbe valido un consenso manifestato senza l'utilizzo della forma telematica tipica introdotta dalla firma digitale di cui al d.P.R. n. 513/1997, sulla base dell'assunto che, in via generale, la legge n. 675 richiedendo —per i dati "comuni"— anche solo un consenso espresso oralmente, sarebbe più permissiva della normativa di diritto comune. Sul tema del consenso nel particolare ambiente on-line, v. anche R.G. Rodio, *Interconnessioni tra banche dati e disciplina del consenso nel trattamento dei dati personali*, in R. ZACCARIA (a cura di), *Informazione e telecomunicazione*, Trattato di diritto amministrativo diretto dal prof. G. Santaniello, XXVIII, Padova, Cedam, 1999, pp. 367-387.

¹³ L'art. 2 della legge n. 675, stabilisce infatti che la stessa si applica al trattamento di dati personali "da chiunque effettuato nel territorio dello Stato".

Europea, la quale, come si è accennato, si è dotata da tempo di rigide regole per la tutela della riservatezza, **tant'è che la direttiva sul commercio elettronico fa diretto riferimento alle le due già citate direttive specifiche del 1995 e del 1997.**

Tale elevato livello di garanzie si **realizza anche grazie alla collaborazione fra le autorità nazionali di controllo**, espressamente richiesta dalla direttiva n. 95/46/CE (art. 28, par. 6), le quali possono dar seguito alle segnalazioni effettuate dai cittadini dei diversi Paesi europei, indipendentemente dal loro luogo di residenza o da quello in cui si è verificato l'illecito trattamento dei loro dati.

Il discorso cambia sensibilmente quando le medesime informazioni personali superano l'ambito comunitario, il che, per quanto riguarda il commercio elettronico, accade sicuramente nella maggioranza dei casi.

Il legislatore europeo del 1995 era consapevole del problema, tant'è che l'intero Capo IV di quella direttiva è dedicato al tema dei flussi transfrontalieri di dati. In particolare, l'art. 25 prevede che gli Stati membri autorizzino la trasmissione verso Paesi terzi solo se questi garantiscono un livello di protezione "adeguato", precisando che la valutazione di tale adeguatezza deve tener conto di tutte le circostanze che assumono significato nel trasferimento (natura dei dati, finalità del trattamento, norme generali o settoriali vigenti nel Paese di destinazione, misure di sicurezza adottate, ecc.).

Gli Stati membri e la Commissione europea sono tenuti a comunicarsi a vicenda i casi in cui, a loro parere, un Paese terzo non garantisce un livello di protezione adeguato e, se tale situazione viene accertata dalla Commissione, gli Stati membri devono adottare le misure necessarie per impedire ogni successivo trasferimento di dati della stessa natura verso quel Paese.

La concreta individuazione dell'*adeguato* livello di protezione, com'è agevole comprendere, è cosa tutt'altro che semplice e, per via delle rilevanti ripercussioni di carattere economico, in grado di esplicare effetti negativi sulle relazioni fra i Paesi dell'Unione Europea e quelli eventualmente ritenuti non "affidabili", da un punto di vista di tutela della *privacy*. Per tali delicati risvolti, il tema è stato più volte oggetto di attenzione da parte del Gruppo di lavoro che l'art. 29 della direttiva del 1995 ha speci-

ficamente istituito per svolgere una funzione consultiva nei confronti della Commissione sui temi della protezione dei dati¹⁴.

Il primo e più generale parere su tale tematica si è soffermato sull'individuazione del significato di "tutela adeguata", concludendo che la valutazione da effettuarsi volta per volta deve tener conto, da un lato, dei principi fondamentali proclamati dall'ordinamento in esame e, dall'altro, degli strumenti che lo stesso ordinamento ha approntato per assicurarne un'efficace applicazione.

Per quanto riguarda i principi, sono da ritenersi essenziali, secondo tale Gruppo di lavoro, quelli che affermano la necessità di raccogliere dati aggiornati e precisi per finalità specifiche e quelli che garantiscono la sicurezza e la trasparenza dei trattamenti attraverso l'esercizio dei diritti di accesso, rettifica e opposizione, nonché quelli che tendono a tutelare in maniera specifica i dati più delicati ed a fornire precise garanzie nei casi di decisioni completamente automatizzate sulle persone.

Inoltre, se il trasferimento dei dati avviene per finalità di commercializzazione diretta, la persona interessata dovrebbe essere in grado di decidere in qualsiasi momento l'esclusione dei dati che la riguardano da un simile impiego.

Dal punto di vista dei meccanismi volti a garantire il rispetto di tali principi, questi dovrebbero tentare di:

- a) assicurare un buon livello di osservanza delle norme (anche attraverso l'approntamento di sanzioni efficaci e dissuasive);
- b) fornire aiuto e sostegno alla persona interessata nell'esercizio dei propri diritti;
- c) garantire un risarcimento adeguato alla parte lesa in caso di violazione delle norme.

Così fissati, in linea generale, i requisiti per individuare il livello di tutela adeguata, il Gruppo in questione, ha ritenuto (fermo restando il rispetto di determinate condizioni specifiche) rispondenti a tale livello tutti

¹⁴ Il Gruppo in questione, che ha carattere indipendente, è composto da un rappresentante delle autorità di controllo designate da ciascuno Stato membro e da un rappresentante della Commissione. Il Gruppo ha fra i suoi compiti quelli di: a) esaminare le questioni attinenti all'applicazione delle norme nazionali di attuazione della direttiva per contribuire alla loro applicazione omogenea, b) formulare ad uso della Commissione un parere sul livello di tutela nella Comunità e nei Paesi terzi, c) consigliare la Commissione in merito ad ogni progetto di modifica della direttiva stessa, d) formulare un parere sui codici di condotta elaborati a livello comunitario.

gli Stati che hanno ratificato la Convenzione n. 108/1981 del Consiglio d'Europa.

Relativamente agli altri Paesi invece, l'esame dovrà essere di volta in volta effettuato tenendo conto anche dei due principali strumenti utilizzati da alcuni ordinamenti in via concorrente o alternativa alle garanzie di tipo normativo, e cioè i sistemi di autoregolamentazione e le clausole contrattuali.

Per quanto riguarda i primi, questi possono essere ritenuti efficaci solo se sono realmente vincolanti per tutti coloro che vi si sono assoggettati e se esistono quindi dispositivi che assicurano effettivamente un buon livello di osservanza generale.

Le disposizioni contrattuali, dal canto loro, possono essere considerate particolarmente adatte in determinate condizioni, ma, ancora una volta, la loro possibilità di rappresentare un grado di tutela adeguata dipende dal tipo di garanzie che ad esse sono attribuite nel Paese in cui devono trovare applicazione.

Non è difficile, sulla base dei pochi elementi qui riassunti, individuare l'obiettivo difficile di accordare il grado di "tutela adeguata" ad alcuni dei paesi che pure gestiscono ampi settori del commercio elettronico, primi fra tutti gli Stati Uniti.

Il problema fondamentale, pur con i rischi che ogni semplificazione comporta, risiede nel fatto che in tale Paese la protezione della *privacy* è rinvenibile in un complesso intreccio di regolamentazione settoriale, a livello sia federale sia statale, unita all'autodisciplina che, dettata direttamente dalle imprese per regolare aspetti assai rilevanti, non è assistita da un adeguato sistema di controllo e di sanzione.

La differenza fra questa impostazione e quella europea, fortemente ancorata ad architetture di rango legislativo, rappresenta il punto nevralgico di un diverso modo di perseguire obiettivi che, per cultura e tradizioni, non possono non essere comuni.

In effetti, le posizioni sono tutt'altro che nettamente distinte. Per quanto riguarda l'Europa, ad esempio, la stessa Direttiva del 1995, affida ai codici di autodisciplina aspetti assai importanti del completamento della normativa primaria e secondaria¹⁵.

¹⁵ Tali disposizioni sono state recepite anche in Italia, ad esempio con il codice per la professione giornalistica (provvedimento 29 luglio 1998, in *GU* 3 8 1998, n. 179) che, concordato fra

Sull'altra sponda dell'Atlantico, poi, nonostante la ferrea difesa del principio di *self-regulation* da parte dell'amministrazione statunitense, recentemente si stanno valutando un numero senza precedenti di provvedimenti legislativi per tutelare la *privacy on-line*¹⁶ e diverse istanze politiche e giudiziarie, sollecitano l'introduzione di provvedimenti che consentano di arrestare la diffusione di informazioni di fonte governativa¹⁷.

Un sempre maggior numero di organizzazioni di tutela dei consumatori (il cui peso nelle decisioni politiche di quel Paese è sicuramente molto rilevante), poi, invoca a gran voce il superamento del sistema di autodisciplina a favore di regole generali garantite da un adeguato apparato sanzionatorio.

4. I NEGOZIATI BILATERALI

Nonostante questi "riavvicinamenti" sostanziali il divario fra le due posizioni è tuttavia ancora molto forte ed è per questo che gli Stati Uniti hanno sollevato energiche opposizioni al momento dell'entrata in vigore

L'Ordine nazionale dei giornalisti ed il Garante costituisce una seppure atipica fonte secondaria del diritto (cfr. U. De Siervo, *Dignità delle persone e diritto di informazione nel codice previsto dall'art. 25 della legge 675 del 1996*, in AA.VV., *Studi in onore di Leopoldo Elia*, Milano, Giuffrè, 1999, pp. 445-462, spec. p. 454), o in quella che dovranno essere adottati per la ricerca storica o scientifica la cui accettazione costituirà requisito fondamentale per poter accedere a determinati archivi o effettuare certe ricerche.

¹⁶ Tali progetti ed iniziative vengono sostituiti o superati con una certa rapidità, rendendo assai complesso un loro costante monitoraggio, tuttavia, secondo un recente articolo di stampa (cfr. *USA Today* del 20.1.2000, la cui traduzione compare all'interno della Newsletter n. 26 del Garante per la protezione dei dati personali), almeno una dozzina di Stati starebbero tentando di impedire alle banche di condividere le informazioni con soggetti affiliati, quali compagnie di assicurazione e di intermediazione immobiliare, imponendo l'obbligo di ottenere il consenso dei loro clienti prima di cedere ad altri informazioni che li concernono. Più di venti Stati dell'Unione, poi, intenderebbero affrontare il tema assai delicato della tutela delle informazioni mediche contenute in basi di dati (dodici Stati disporrebbero già di norme che prevedono la riservatezza delle cartelle cliniche), inoltre, diversi Stati vogliono impedire alle società operanti in Internet di vendere i dati personali ottenuti seguendo le tracce elettroniche lasciate dalla clientela, se non previa dichiarazione delle vendite effettuate.

¹⁷ Recentemente, la Corte Suprema degli Stati Uniti, con sentenza del 12 gennaio 2000 ha dichiarato all'unanimità l'illegittimità della diffusione, da parte delle amministrazioni statali, dei dati personali forniti dai cittadini per ottenere la patente di guida, confermando la validità di una legge federale del 1994 che invece la Carolina del Sud e numerosi altri Stati ritenevano incostituzionale perché invasiva della sfera di competenza statale (cfr., in attesa della pubblicazione di tale sentenza, l'articolo apparso sull'*International Herald Tribune* del 13.1.2000, la cui traduzione è in calce alla già citata Newsletter n. 26 del Garante per la protezione dei dati personali).

della direttiva n. 95/46, ritenendo che questa potesse costituire un grosso ostacolo allo sviluppo del commercio elettronico.

Tali timori hanno comunque impresso una forte accelerazione ai negoziati fra i due blocchi, che sono culminati nella predisposizione di un documento da parte del *Department of Commerce* statunitense nel quale si individuano alcune regole essenziali per fornire un "approdo sicuro" (*safe harbour* è il nome del documento) ai dati trasmessi verso quel Paese¹⁸.

Il Gruppo di lavoro di cui all'art. 29 della direttiva, si è occupato a più riprese dello stato di avanzamento dei negoziati e, in particolare, del documento da ultimo citato.

In una prima occasione¹⁹, l'avviso è stato sostanzialmente negativo, essendo stato ritenuto insufficiente il sistema di protezione delineato, soprattutto in relazione alla ridotta capacità di accesso ai dati personali da parte dell'interessato e all'inesistenza di meccanismi di controllo tali da rendere effettiva la tutela nei confronti di chi abbia avuto lesa un proprio diritto²⁰.

¹⁸ Il documento USA ruota intorno ad un sistema di autoregolamentazione basato su tre elementi fondamentali: a) un insieme di principi, l'adesione ai quali è lasciata alla scelta individuale delle imprese interessate e prende la forma di una "promessa al pubblico" accompagnata da una notifica al Dipartimento del Commercio USA, b) l'autocertificazione annuale di tali imprese circa l'esistenza di meccanismi di risoluzione extra-giudiziale delle controversie che dovessero sorgere ad oggetto il rispetto dei suddetti principi e all'esistenza di un organismo pubblico dotato dei necessari poteri di controllo ed ingiunzione rispetto all'eventuale violazione dei medesimi principi, c) la citazione a cura del Dipartimento del commercio (o di altro soggetto) di una lista delle imprese autocertificate, le quali beneficerebbero automaticamente di una presunzione di adeguatezza della protezione dei dati assicurata e potrebbero pertanto ricevere dati personali dai paesi UE senza vincoli o ulteriori limitazioni.

¹⁹ Cfr. il Parere n. 1/99 riguardante "Il livello di protezione dei dati negli Stati Uniti e le discussioni in corso tra la Commissione delle Comunità europee e il Governo degli Stati Uniti", adottato il 26.1.1999 e pubblicato in calce al comunicato stampa del Garante, n. 14 del 16.3.99 (in *Boll.* n. 8, pp. 70-72).

²⁰ Il parere in questione precisa chiaramente che le norme in materia di protezione dei dati non mirano esclusivamente a tutelare gli utilizzatori di nuove tecnologie (in particolare informatica e Internet), ma esprimono anche l'adesione ad una serie di principi e diritti fondamentali basati su una cultura comune di "rispetto per la privacy ed altri valori propri degli esseri umani, che è condivisa allo stesso modo dagli Stati membri dell'Unione Europea e dagli Stati Uniti". Il Gruppo, quindi, è rimasto del parere che al momento non si potesse fare affidamento "sull'attuale collage di legislazione settoriale ad alta specificità e autoregolamentazione su base volontaria quale garanzia di una protezione adeguata in tutti i casi di trasferimento di dati personali dall'Unione Europea". In tale ottica, sempre secondo il Gruppo, la definizione negli USA di uno standard concordato "di riferimento", il *safe harbour* appunto, costituisce un utile approccio che, in determinati casi, può però necessitare di integrazioni attraverso soluzioni contrattuali, in ogni caso, occorrono miglioramenti ulteriori, soprattutto per quanto riguarda l'osservanza di tali principi ai quali le impre-

In una successiva occasione²¹, su una versione rivista del progetto, il Gruppo, dopo aver ribadito il giudizio di generale insufficienza sul sistema statunitense di protezione dei dati, ha individuato nel dettaglio le carenze di tale sistema giudicandolo ancora non adeguato ad offrire la tutela necessaria ai dati trasmessi in quel Paese^{22 23}.

5. IL RUOLO DELLE ORGANIZZAZIONI INTERNAZIONALI

Quella dei negoziati bilaterali è sicuramente una strada molto importante che si sta percorrendo nell'ottica di portare a soluzione il problema, ma non è l'unica: in ambito internazionale, infatti, la tematica è all'esame di diversi consessi.

Fra questi, un ruolo preminente spetta all'OCSE, dove la presenza dei maggiori Paesi interessati alla questione e la particolare procedura di approvazione dei documenti, che si basa sul consenso generale dei rappresentanti, costituisce un punto di naturale composizione delle diverse posizioni²⁴.

se sono libere di aderire, ma una volta che tale adesione vi sia stata e che si sia usufruito dei relativi vantaggi, il loro rispetto deve essere obbligatorio e sottoposto ad un controllo indipendente, che assicuri anche l'effettivo esame dei reclami presentati da soggetti i cui dati sono stati trasferiti dall'Unione l'Europa.

²¹ Cfr. il parere n. 2/99 riguardante "L'adeguatezza dei 'principi internazionali per un approdo sicuro' stabiliti dal Ministero del commercio USA il 19 aprile 1999", adottato il 3 5 1999.

²² Sulla questione è intervenuta anche la TACD (*Trans Atlantic Consumer Dialogue*), una coalizione che riunisce sessanta fra le principali associazioni di consumatori degli USA e dei Paesi europei, la quale ha adottato il 23 aprile 1999 una risoluzione in cui si respinge l'adozione della proposta del "safe harbour", sulla base dell'assunto che essa non fornisce ai consumatori una tutela adeguata della privacy, e si raccomanda invece la definizione di una Convenzione internazionale in materia. Secondo tale organizzazione, l'accoglimento della proposta americana vanificherebbe le finalità della direttiva comunitaria. Le considerazioni della TACD sono state riprese dal prestigioso *Electronic Privacy Information Center* (EPIC) di Washington, che ha rilevato l'esigenza di un maggiore coinvolgimento dell'opinione pubblica nell'elaborazione della politica internazionale in materia di tutela della riservatezza. Il testo della risoluzione della TACD è pubblicata in calce al comunicato stampa del Garante n. 47 del 10 5 1999, in *Boll.* n. 8, pp. 91-92.

²³ Il Gruppo di lavoro, il 3 febbraio 2000, ha anche adottato il parere n. 1/2000, che ha esaminato "Alcuni aspetti del commercio elettronico", con particolare riferimento al problema del "marketing" elettronico, dimostrando come i principi delle due direttive possano fornire soluzione anche agli specifici problemi derivanti dall'uso di Internet.

²⁴ Recentemente, l'esame delle ripercussioni della tutela della privacy sullo sviluppo del commercio elettronico è stato inserito anche nell'agenda dell'Organizzazione mondiale per il commercio (WTO) e del Gruppo degli otto paesi più industrializzati (G8).

Dalle linee guida del 1980, che hanno individuato una serie di principi, ancora oggi rappresentanti il nucleo essenziale della tutela della *privacy*²⁵, si è passati ad una dichiarazione sui flussi transfrontalieri del 1985 ed alle linee guida sulla crittografia del marzo del 1997. Poco più di un anno fa, esattamente nell'ottobre del '98, la Conferenza ministeriale di Ottawa sul commercio elettronico ha dato nuovo vigore a queste linee guida, tant'è che si è deciso di incentivare le iniziative di avvicinamento fra le differenti impostazioni, anche attraverso incontri periodici fra le diverse componenti governative, produttive e dei consumatori, al fine di contribuire a ridurre progressivamente le divergenze esistenti²⁶.

Uno di questi incontri si è svolto, nell'ottobre del 1999, a Parigi²⁷ con l'obiettivo di esaminare i progressi compiuti ad un anno di distanza dalla citata Conferenza.

Fra le non molte novità emerse, merita menzione il nuovo approccio che si sta, pur con fatica, delineando nella contrapposizione fra i sistemi di regolamentazione pubblica e quelli di autodisciplina.

In tale occasione, infatti, è stato più volte evocato il principio della cosiddetta "co-regolamentazione", anche se, ancora una volta, le opinioni circa il significato da dare a tale concetto non sono del tutto univoche. da parte comunitaria s'intende con esso far riferimento ad una regolamentazione statale (o comunque pubblica) completata da una regolamentazione di dettaglio fissata nei codici deontologici; mentre, da parte statunitense, l'interpretazione più frequente sottintende una regolamentazione congiunta da parte degli organi centrali (statali e federali) e del mondo dell'impresa.

Ma il vero elemento di novità, emerso con rinnovato vigore durante il *Forum*, è stato rappresentato dalla forte richiesta delle organizzazioni di

²⁵ Nel citato parere n. 1/1999, il Gruppo istituito dall'art. 28 della direttiva, esaminando il progetto di "safe harbour", ha confermato, tra l'altro, che "qualsiasi insieme accettabile di principi costituenti un porto sicuro deve comprendere, quale requisito minimo, tutti i principi fissati nelle linee-guida in materia di *privacy* elaborate dall'POCSI nel 1980, adottate, fra gli altri, dagli USA"

²⁶ Il 9 dicembre 1999, poi, l'POCSI ha approvato le *Linee guida per la protezione del consumatore nel contesto del commercio elettronico* (in <http://www.oecd.org/dsti/sti/it/consumer/prod/guidelines>) che però, in materia di tutela della riservatezza, si limita a inviare alle citate Linee guida del 1980, così come integrate dalla dichiarazione ministeriale di Ottawa, "al fine di provvedere ad un'appropriata ed effettiva protezione per il consumatore"

²⁷ Si tratta del *Forum sul Commercio elettronico*, tenutosi il 12 e 13 ottobre 1999, il cui resoconto è rinvenibile all'indirizzo http://www.oecd.org/dsti/sti/it/cc/act/Paris_cc/pdf/forum_report/pdf

consumatori statunitensi di giungere a più elevati *standards* di sicurezza per le informazioni personali, anche attraverso un maggior ricorso alla regolamentazione ed al controllo pubblici.

Purtroppo, questi nuovi sentimenti non hanno finora trovato un'adeguata risposta in quegli organismi pubblici americani, come la *Federal Trade Commission*, che pure, per i rilevanti connotati di indipendenza e di tutela delle posizioni "più deboli", si sono nel passato caratterizzati per aver assunto decisioni di rottura rispetto a quelle governative²⁸.

Tale Commissione, in particolare, in un recente studio sulla *privacy* nel commercio elettronico²⁹, pur con qualche opinione dissenziente, ha sostanzialmente bocciato il ricorso ad una regolamentazione pubblica del problema, ritenendo senz'altro sufficiente l'attuale approccio basato sull'autodisciplina del mondo imprenditoriale.

6. LE PROSPETTIVE DI SOLUZIONE

Recentissimamente si è avuta notizia che è stato raggiunto un accordo di massima fra UE e USA sul "*safe harbour*"; questo accordo tuttavia richiede ancora diversi aggiustamenti e la ratifica ufficiale.

Sembra comunque che un ponte sia stato gettato e, anche se non mancheranno resistenze da parte dei sostenitori dell'una o dell'altra posizione, è certo che questo punto di incontro possa costituire almeno la base di partenza per sviluppare un successivo, più proficuo dialogo.

Questo riavvicinamento non può infatti essere considerato il passo finale, perché obiettivamente insufficiente e perché la posta in gioco è senza dubbio molto alta.

Giova forse precisare a tale proposito che il problema non si può (come pure purtroppo qualcuno tende a fare) limitare all'idea di una "difesa dalla pubblicità" o dallo "*spamming*": il rischio è molto maggiore e riguarda la possibile "fuga" o sottrazione di dati sensibilissimi, come quelli sulla salute, il cui grado di "appetibilità", in una società sempre più

²⁸ Tale commissione, la prima sorta negli Stati Uniti nel secolo scorso, nata con intenti di regolazione delle tariffe in campo ferroviario, si caratterizzò negli anni successivi per l'azione a tutela degli interessi più deboli tanto da meritare l'appellativo di *Poor men's Court* (cfr., sul punto, M. D'Alberti, voce "Autorità indipendente", in *Enc. giur. Treccani*, 1995, pp. 1-8, spec. p. 2).

²⁹ Cfr. *Federal Trade Commission, Self-regulation and Privacy on-line: a Report to Congress*, luglio 1999, reperibile al sito Internet www.ftc.gov

“globalizzata”, è elevatissimo (si pensi, ad esempio, al valore economico che la conoscenza delle condizioni di salute di una persona può avere al momento della stipula di un contratto assicurativo o della concessione di un finanziamento per la conseguente valutazione del rischio).

Si tratta di dati che, una volta sfuggiti al controllo dell'interessato, se vengono utilizzati fuori dal quadro di garanzie con tanta fatica conquistate dall'odierna civiltà, possono dar vita a nuove forme di emarginazione basate forse non più (o non solo) sulle differenze religiose, politiche o razziali, ma anche sulla “salute” e sulle aspettative di vita riferibili ad una determinata persona.

Non si tratta quindi di una battaglia soltanto commerciale rivolta verso l'affermazione di uno o di un altro *standard* economico, ma di una difesa, in primo luogo, di valori, valori che certo non sono estranei alla cultura di altri paesi come gli Stati Uniti, ma che, qualche volta, rischiano di essere messi a repentaglio dalla ricerca del profitto a tutti i costi e da un'eccessiva fiducia negli effetti equilibratori del mercato.

Commercio elettronico e tutela del consumatore

ALBERTO MARIA GAMBINO

1. Iniziamo con il definire le espressioni con cui è titolata questa relazione.

Commercio elettronico. Come è noto, Internet non nasce come mezzo per attuare rapporti economici, ma come strumento di comunicazione. È un dato che occorre tenere presente per lo studio del sistema normativo, che mira alla tutela, o, vorrei dire, “alle tutele” del consumatore.

Nel corso degli anni, accanto all'utilizzo del sistema della rete, quale *medium communicandi*, si affaccia però un utilizzo economico. A dire: cominciano ad essere offerti servizi, beni; vi è circolazione di ricchezza anche attraverso la Rete.

Il primo problema per il giurista è quello di identificare quali relazioni siano da annoverare tra i rapporti “di cortesia”; quali, invece, tra quelli “a titolo gratuito”, là dove assumano profili di giuridicità; infine, quali siano rapporti “a titolo oneroso”.

In chiave pragmatica, si è detto: i rapporti a titolo gratuito in Internet non esistono; esistono rapporti di mera cortesia e rapporti a titolo oneroso.

Questa prima osservazione deriva dalla difficoltà oggettiva di identificare la giuridicità di un'offerta telematica, là dove non vi sia un esborso da parte dell'utente, del fruitore del servizio.

Immaginiamoci, prima di partire per un viaggio, di chiedere ad un corrispondente via Internet informazioni sul tempo in Australia. L'erroneità della sua risposta, che implica dei costi, magari semplicemente il riacquisto del vestiario, purtroppo non ci porterebbe a citare in giudizio il nostro maldestro informatore. Ma se queste informazioni le avessimo chieste a un istituto di meteorologia, operante su un sito Internet, là dove le informazioni fossero state errate avremmo potuto legittimamente chiedere il risarcimento dei danni?

Sì, se ci fosse stato un pagamento; no, se questo pagamento non fosse avvenuto: quale giudice avrebbe infatti accolto la nostra istanza?

La metamorfosi della Rete da un iniziale parallelismo tra le due situazioni di comunicazione di informazioni e di scambio economico ha

comportato oggi la necessità di creare una rete soltanto per rapporti economici.

Tutela del consumatore. Dunque, direi "tutele" del consumatore. Il consumatore, infatti, si pone, dinanzi alla Rete, in vesti differenti.

Risparmiatore: artt. 30 e 32 d. lgs. 24 febbraio 1998, n. 58, c.d. Testo Unico della finanza, ove ci si riferisce ad un soggetto sì "cliente", ma che investe il denaro attraverso la Rete. **Rispetto alle tecniche comunicative**, indicate dal regolamento di attuazione n. 11522 del 1998 emanato dalla Consob, vi sono dei criteri che possono estendersi ad ampio raggio a tutto lo scenario del commercio elettronico.

Cittadino. Nei rapporti con la Pubblica Amministrazione il fatto che, oggi, nonostante sia stato attuato il sistema della firma digitale, venga valorizzata l'archiviazione in chiave ottica sul supporto fisico, significa che ancora c'è necessità di un originale e di una copia. La prassi chiede certezza, che si consegue con la **conservazione del dato informatico** in un supporto tangibile. Ciò dà fiducia al consumatore, che in questo caso è il cittadino, è l'utente del servizio che viene offerto dalla Pubblica Amministrazione. La tecnologia della firma digitale non offre all'evidenza garanzie maggiori.

Quindi, "consumatore come acquirente", "contraente debole". Su questo scenario considererei, con i limiti delle semplificazioni, tre filoni normativi.

Il primo riguarda la tutela della riservatezza: ci si riferisce alla tutela dei dati personali, alla *privacy* nelle telecomunicazioni.

Un secondo filone riguarda la tutela della cosiddetta "presa di coscienza". Il fenomeno si muove dalla contrattazione a sorpresa a quella che potremmo definire della contrattazione "con mezzi tecnologici non consueti all'utente", dei quali, dunque, non si ha quella dimestichezza abituale propria dell'utilizzo di un mezzo tradizionale.

Nell'ambito di questo filone s'inseriscono: la normativa - ormai risalente - delle vendite fuori dei locali commerciali (d. lgs. n. 50 del 1992) - sebbene tale legge già aveva considerato all'art. 9 l'ipotesi dei contratti a distanza; la proposta di direttiva comunitaria sul commercio elettronico; la direttiva n. 97/7, adesso attuata dal decreto legislativo n. 185 del 1999, sui contratti a distanza. Si aggiunga anche la normativa civilistica dei contratti su moduli e formulari, il D.P.R. n. 513 del 1997 sulla firma di-

gitale e il regolamento Consob già richiamato di attuazione del Testo unico sulla finanza, relativamente alla parte della contrattazione a distanza, che viene in questo caso individuata nell'ambito dell'unico *genus* dell'offerta fuori sede.

Poi, ci sono altre normative di settore, si pensi alla subfornitura e alla multiproprietà, che hanno norme di protezione della presa di coscienza.

Un terzo filone racchiude l'aspetto dell'equità negoziale: le clausole vessatorie di tradizione codicistica, le clausole vessatorie introdotte con la novella degli artt. 1469^{bis} ss. c.c. e, ancora, le leggi speciali sulla subfornitura e sulla multiproprietà, nell'ambito delle quali si propone appunto anche un problema di equità negoziale.

2. I provvedimenti normativi che più interessano questa relazione, sono quelli relativi all'attuazione della direttiva sulle vendite a distanza, cioè il d. lgs. 22 maggio 1999, n. 185, e la proposta di direttiva comunitaria sul commercio elettronico, come da ultimo emendata.

Nell'ambito del primo provvedimento, segnalo due aspetti. Il primo riguarda il momento antecedente alla contrattazione - art. 3 relativo all'informazione per il consumatore, che in tempo utile prima della conclusione del contratto, deve ricevere tutta una serie di informazioni a iniziare dall'identità del fornitore, il prezzo del bene ecc., insomma tutti quegli elementi che gli permettono di manifestare un consenso il più libero possibile e, in qualche maniera, il più informato possibile.

"In tempo utile prima della conclusione". Questa è già una definizione che stona nell'ambito della varietà dei sistemi a distanza: il tempo utile si diversifica a seconda dello strumento utilizzato; è chiaro che nel rapporto epistolare il tempo utile sarà più esteso che in un rapporto telematico. In questo senso lo stesso d. lgs. considera che l'utilizzo dello strumento possa valere come criterio interpretativo per la chiarezza delle informazioni da fornire (art. 3, comma 2).

In questa prima fase dello scambio, prima di acconsentire all'operazione economica, c'è un richiamo normativo da valorizzare, che tutte le informazioni circa l'identità, il prezzo, le spese di consegna e così via, "devono essere fornite in modo chiaro e comprensibile con ogni mezzo adeguato alla tecnica di comunicazione a distanza impiegata, osservando in particolare i principi di buona fede e di lealtà in materia di

transazioni commerciali, valutati alla **stregua delle esigenze di protezione delle categorie di consumatori particolarmente vulnerabili**". Tale è il tenore del comma 2 dell'art. 3 del decreto legislativo.

Si ripropone quello che, per chi ha studiato il fenomeno pubblicitario, è il noto dibattito se il consumatore **da tutelare** sia "il più sprovveduto" oppure il cosiddetto "consumatore medio".

Nel d. lgs. n. 185 del 1999 il richiamo a "categorie di consumatori particolarmente vulnerabili" implica che ci sia già nell'ambito della definizione, pur collettiva, della figura di **consumatore**, l'elemento della debolezza cognitiva rispetto al bene che si va ad offrire.

L'altro profilo interessante di questo secondo comma è il richiamo alla lealtà e alla buona fede; lealtà e buona fede che rendono l'offerta - offerta a distanza - dotata di un requisito in più rispetto a quelli tradizionali: la correttezza. A dire: il modulo comunicativo utilizzato per far conoscere all'utente, al consumatore, al risparmiatore - ove vi sia la possibilità di estensione (il d. lgs. non si applica al risparmiatore, ma i principi, come detto, si rinvengono nel T.U. fin.) - deve corrispondere a canoni di lealtà.

Lealtà che deve sussistere tra l'operatore commerciale, che utilizza la tecnica di comunicazione a distanza, e l'utente consumatore.

Proprio perché ci s'imbatte in tecnologie non conosciute, l'operatore deve illustrare all'utente quali sono i passi da compiere, quali sono i passaggi tecnologici incidenti sul profilo negoziale, che il potenziale acquirente deve porre in essere affinché abbia buon esito l'operazione, si arrivi alla conclusione "voluta" del contratto.

Questo è un aspetto che viene valorizzato anche nelle modifiche apportate alla proposta di direttiva comunitaria sul commercio elettronico.

Il secondo aspetto della normativa sulle vendite a distanza è legato all'art. 4, e riguarda, in particolare, gli elementi informativi che devono essere resi noti al contraente nel momento stesso in cui ha già deciso, attuando il rapporto, di effettuare l'ordine d'acquisto. In questo caso devono essere fornite alcune informazioni, *in primis* la conoscenza dello *ius poenitendi*, cioè della possibilità di recedere dal contratto posto in essere.

In questo caso ci si domanda: gioca ancora il richiamo alla buona fede, alla lealtà, richiamato dall'art. 3?

Un esempio varrà a chiarire la rilevanza del quesito.

Se io stipulo un contratto a distanza con un editore che ben conosco, con cui normalmente ho dei rapporti commerciali, anzi magari lo conosco in carne ed ossa, è necessario che nella fase dell'informazione preventiva di cui all'art. 3 si segua tutto l'*iter* informativo, che volenti o nolenti, rallenta il momento perfezionativo del consenso? Direi di no, perché, come si è visto proprio nella fase informativa dell'art. 3 gioca il richiamo alla lealtà e alla buona fede. Qui c'è un rapporto pregresso, una familiarità che dà per acquisita una certa conoscenza di tutta una serie di requisiti, appunto l'identità del fornitore, le spese di consegna, che evidentemente sono dati già condivisi in passato. Direi che proprio la clausola generale richiamata, della buona fede e della lealtà, ci permette di valutare il caso singolo con una certa elasticità circa le informazioni da fornire: ciò sta nella *ratio* della legge, proprio rispetto alla parte dell'informazione preventiva dell'art. 3. Che succede con riferimento all'art. 4, e alle altre informazioni che devono essere date nel momento dell'esecuzione del contratto?

Da un punto di vista testuale non vi è più il richiamo alla lealtà, alla buona fede, alla correttezza: dunque già da un'interpretazione letterale andrebbe esclusa la possibilità di considerare il grado dell'effettività dell'informazione fornita.

Torniamo all'esempio dell'editore e del rapporto commerciale, già attivato nel tempo. Ci troviamo dinanzi ad una nuova tecnica dello stipulare, proprio con riferimento alla predisposizione della tutela normativa. La tecnica a distanza, infatti, pur già conosciuta dal consumatore, nel momento in cui viene normativizzata, implica una serie di dati giuridici innovativi. Evidentemente le vendite a distanza sono assai risalenti, ma non esisteva *ab origine* lo *ius poenitendi*. Da oggi è obbligatorio offrire al momento della conclusione alcune informazioni, in particolare quella sullo *ius poenitendi*, che è vincolo giuridico assegnato all'operatore per la protezione della scelta dell'acquirente. Non sussiste deroga: l'informazione è imposta dalla legge e non è derogabile in quanto non riguarda un dato di fatto la cui conoscenza può essere evinta dalla prassi stipulatoria. C'è, del resto, una norma specifica dello stesso decreto che sanziona l'inderogabilità delle norme di protezione (art. 11, comma 1).

3. L'altro provvedimento regolatorio è la proposta di direttiva sul commercio elettronico. Gli aspetti che più interessano da vicino la tutela

del consumatore sono: la trasparenza delle comunicazioni; la responsabilità dell'operatore della Rete; in particolare, la validità e la conclusione dei contratti in Rete.

Rispetto alla trasparenza, sebbene ci troviamo in un'ottica liberalizzatrice, la scelta è quella di informare al massimo l'utente, il consumatore, sulle caratteristiche, le idoneità anche professionali dei soggetti che offrono beni o servizi in Rete.

La proposta di direttiva enuncia che l'indirizzo del sito di posta elettronica non ha valore di comunicazione commerciale. Su questo non si può non essere d'accordo proprio ove si tenti di ricostruire la natura dei *domain names*, natura non solo distintiva, con richiamo al marchio, ma determinata dalla funzione primaria informativa, richiamata all'inizio, conseguente al fatto che la Rete nasce come strumento comunicativo. Il *domain name*, pur possedendo una funzione identificativa dei soggetti che agiscono nella Rete, può richiamare anche il nome di un'azienda e, evidentemente, consistere anche in una frase pubblicitaria, in questi casi rimane comunque prevalente il tratto identificativo.

L'art. 7 consente di rendere più comprensibile la differenza che esiste tra sollecitazione e pubblicità.

Su questo punto la direttiva n. 97/7, poi attuata con il d. lgs. n. 185 del 1999 di cui si è detto, riguardante la protezione dei consumatori in materia di contratti a distanza, offre, alla luce dell'*iter* preparatorio, spunti significativi.

Con riguardo al messaggio commerciale telematico ed alla sua peculiare forma comunicativa, infatti, nella prima redazione della direttiva del 7 ottobre 1993, si assumeva all'ex 6° Considerando, dopo aver premesso che "la costante evoluzione di queste tecniche (*le tecniche di comunicazione a distanza*) non consente di redigerne un elenco esaustivo ma richiede che vengano definiti principi validi anche per quelle tecniche che sono ancora poco impiegate" (parte ancora vigente nell'attuale 9° Considerando), che "occorre fissare chiaramente la differenza tra pubblicità e sollecitazione". Il legislatore comunitario assimilava, poi, la sollecitazione alla mera proposta contrattuale, in cui il consumatore, pur senza essere stato "sollecitato", dispone "degli elementi necessari per negoziare".

Al successivo ex 9° Considerando, pur constatandosi che "il consumatore riceve sollecitazioni tramite molteplici tecniche di comunicazione", si riteneva opportuno specificare che le "sollecitazioni vengano

chiaramente identificate come proposte commerciali". Tuttavia il dato empirico che nelle comunicazioni telematiche non possa parlarsi di sollecitazioni telematiche in senso tecnico, di fatto inattuabili *a parte venditoris*, ha stimolato il legislatore comunitario ad eliminare la distinzione tra pubblicità e sollecitazione e a rilevare che nel telematico il parallelismo corre, piuttosto, sul filo offerta *ad personam*-pubblicità.

Ora, l'art. 7 della direttiva sul commercio elettronico distingue tra pubblicità commerciale sollecitata per posta elettronica e pubblicità non sollecitata. L'unica sollecitazione ipotizzabile in Rete è, dunque, quella dell'utente che chiede maggiori informazioni e che nulla ha a che vedere con la sollecitazione *ad personam* operata tradizionalmente "porta a porta".

4. Con riferimento alla responsabilità dei dati immessi nella Rete, esemplificherei le ipotesi previste dalla proposta di direttiva.

La prima è quella del *provider* che si limita a trasmettere in Rete le informazioni su richiesta dell'utente, ovvero si limita ad offrire all'utente la connessione (attività di *mere conduit*): qui viene in mente la connessione per il *browsing* (la navigazione) ma anche il profilo della trasmissione della posta elettronica. Siamo davanti alla funzione del *provider* di mero strumento che permette il passaggio di una comunicazione da una parte a un'altra.

Non ci sono responsabilità sui contenuti, a meno che non vi siano modifiche degli stessi ad opera del *provider*.

La seconda ipotesi è quando vi è un'operazione di memorizzazione automatica delle informazioni provenienti dall'utente (cosiddetta attività di *caching*). Sono le operazioni di stoccaggio temporaneo denominate *system caching*: si pensi ai profili della temporanea conservazione della posta elettronica nella memoria del *provider* prima di essere appresa dall'utente. Sono comunicazioni preconfezionate dal soggetto utente che sta in dialogo con un corrispondente: lo strumento, il *server provider*, offre una modalità tecnica per operare la circolazione del messaggio, memorizzandolo fino a che non viene "scaricato" dal destinatario. Vi saranno oneri di aggiornamento dell'informazione, ove sia richiesta.

L'ipotesi più delicata è invece quella in cui il *provider* fornisca il servizio di memorizzazione di informazioni fornite da un utente (*hosting*). In que-

sto caso pensiamo alla fornitura di pagine *Web*, ad uno spazio per un gruppo di discussione: entriamo nello scenario di tutto ciò che è direttamente diffuso al pubblico tramite Internet. Emergono profili di eventuale illecito civile anche del *provider*.

Un esempio. Il signor Rossi di Livorno vuole registrare un nome a dominio con la dizione *assitalia.it*; lo chiede al *provider*: il *provider* non può far finta di nulla e registrarglielo, mandare in Rete la pagina *Web* con il richiamo ad *assitalia.it*. Una giurisprudenza del Tribunale di Roma ritiene che in questo caso vi sarebbe complicità all'atto illecito, consistente nella contraffazione di marchio.

Ci sono delle responsabilità ove si fornisca il servizio di memorizzazione, là dove l'attività del *provider* permetta la connessione col richiamo a dati che, pur forniti dall'utente, implicino situazioni di illegalità, perfezionatesi con la messa in connessione da parte del *provider*.

Ciò nella proposta della direttiva è previsto: il *provider* sarà ritenuto responsabile a ritirare immediatamente tutte le informazioni ove venga a conoscenza successiva della loro illegalità, ma anche prima per fatti o circostanze per i quali l'illegalità sia apparente (art. 14, comma 1, lett. a e b) (non è stato accolto l'emendamento del Parlamento che faceva riferimento all'essere "in grado di sapere" dell'illegalità dell'attività). In questo caso il *provider* deve evitare di permettere il compimento dell'illecito civile.

5. All'art. 11 si stabilisce il momento della conclusione del contratto con riferimento al consenso espresso tramite l'utilizzo di mezzi informatici, come il fatto di cliccare su un'icona.

Nel caso, il contratto si ritiene concluso quando l'utente ha ricevuto per via elettronica da parte dell'offerente la conferma del ricevimento della manifestazione del consenso dell'utente-accettante.

In particolare si specifica che il ricevimento della ricevuta di ritorno si considera avvenuto quando la parte cui è destinata (l'utente-accettante) può accedervi.

Il che significa - come avviene per il sistema delineato nella posta elettronica - che la conclusione coincide con il momento in cui il messaggio sia accessibile alla memoria della macchina del destinatario senza

che sia rilevante l'effettiva presa di visione e conoscenza del messaggio da parte del destinatario.

In particolare si specifica che l'offerente-prestatore è obbligato ad inviare immediatamente l'avviso di ricevimento.

Occorre, dunque, domandarsi se la procedura descritta sia applicabile effettivamente anche alla posta elettronica.

In linea teorica il richiamo al mero utilizzo di mezzi informatici e, solo in via esemplificativa, il richiamo al cliccaggio sull'icona sembrerebbero contemplare anche la procedura per posta elettronica. Anzi quest'ultima situazione, come si è anticipato, appare la più congrua proprio con riferimento al meccanismo di ricezione che considera la conferma di ricevimento come effettivamente ricevuta allorché l'utente abbia la possibilità di accedervi. Nella posta elettronica, infatti, come si è detto, l'utente deve collegarsi al sito del *provider* per "scaricare" la posta.

Il procedimento delineato dalla direttiva, tuttavia, è differente da quanto previsto dall'art. 1335 c.c., ove non è certo necessario l'ulteriore passaggio dell'invio della ricevuta di ritorno all'accettante. Né del resto potrebbe ipotizzarsi che l'utente, nel caso, rivesta il ruolo di offerente, in quanto la direttiva stessa parla di offerta del prestatore ed accettazione del destinatario della prestazione.

Non si giustificerebbe, poi, neanche l'obbligo dell'immediato invio della ricevuta di ritorno da parte del prestatore, che ove fosse accettante sarebbe invece libero di non dar séguito all'offerta.

Ove dunque l'art. 11 della direttiva sul commercio elettronico si applicasse anche alla posta elettronica si modificherebbe il meccanismo previsto dall'art. 1335 c.c.

In questo senso, peraltro, occorre chiedersi che cosa accade se l'offerente, innanzi al ricevimento dell'accettazione dell'oblato, poi non invii la ricevuta di ritorno.

Secondo la direttiva il contratto non si sarebbe certo concluso, perfezionandosi questo soltanto con il ricevimento della ricevuta di ritorno in capo all'utente.

All'utente allora non rimarrebbe che agire per il risarcimento del danno oppure ipotizzare la possibilità di dare esecuzione all'obbligo di invio della ricevuta di ritorno, così imponendo la conclusione del contratto.

Il meccanismo ipotizzato dal legislatore comunitario sembra essere congeniale al caso in cui l'avviso di ricevimento avvenga automaticamente, un attimo dopo l'accettazione dell'utente operata con una cliccata (su un'icona o anche nell'invio della posta elettronica).

In questo caso, anzi, il mancato immediato arrivo (anche dunque per posta elettronica da scaricare subito dopo) dell'avviso di ricevimento permetterà di constatare che l'ordine in realtà non è giunto a destinazione o, comunque, non ha trovato l'offerente idoneo a concludere l'accordo.

Ma allora, accanto a quest'ipotesi, potrà sopravvivere il meccanismo tradizionale dell'art. 1335, così lasciando nel dubbio l'utente circa il buon esito dell'accordo?

Devono qui individuarsi due fattispecie: le operazioni ove il consenso sia espresso con una cliccata e le operazioni in cui il consenso si esprime attraverso una dichiarazione di senso compiuto poi inviata con una cliccata.

Per la prima vale la regola del commercio elettronico della necessità di un avviso di ricezione in capo all'utente. Ove ciò non si verifichi vorrà dire che non vi è alcun accordo, perché il meccanismo non ha consentito la stipula di un contratto per via elettronica ai sensi della direttiva sul commercio elettronico.

Nei casi in cui invece l'accordo si perfezioni attraverso un dialogo effettivo e dunque vi sia necessità di reciproche comunicazioni intelligibili allora si seguirà, ove la legge italiana dia applicabile, l'iter previsto dall'art. 1335 c.c.

6. Lo scenario telematico rimane, comunque, uno scenario improntato per le relazioni umane, che appartengono a quella sfera di socialità primaria consueta a tutti i soggetti dell'ordinamento, a tutte le persone fisiche che fanno parte di una comunità.

Questo a dire, che sì, possono esserci dei rischi nell'utilizzo del sistema con possibili distorsioni della volontà rispetto all'operazione economica che si vuole porre in essere: ma tutto questo va soppesato, prendendo come riferimento un utente, che non è detto che conosca il sistema, che non è detto che sia informato tecnicamente. Se il paradigma di riferimento è quello della socialità primaria, cosicché tutti i soggetti possano un giorno entrare nella Rete, bisogna permettergli di comprendere,

rendendoli più familiari, i modi d'utilizzo della Rete. Bisogna permettergli di commettere degli errori, degli errori che non portano a delle conseguenze, a dei vincoli eccessivi.

Allora se questa sfera di socialità primaria esiste anche all'interno della rete telematica (e questo è richiamato dalla proposta di direttiva, ove c'è un espresso richiamo in capo agli operatori della Rete di rendere il più possibile familiare l'utilizzo di questi strumenti) va valorizzato il momento preliminare della formazione del consenso: ciò deve essere posto come criterio di valutazione della legittimità delle comunicazioni commerciali telematiche nell'ambito di un dibattito che coinvolga le tutele da apprestare al consumatore.

Funzioni e poteri pubblicistici in materia di commercio elettronico

FRANCESCO CARDARELLI¹

Nel concordare questo intervento con il prof. Vito Rizzo, ci siamo posti due ordini di problemi: uno relativo all'ambito sostanziale ed uno relativo alla determinazione del titolo.

Riguardo a quest'ultimo aspetto si è optato per "Funzioni e poteri pubblicistici in materia di commercio elettronico", che costituisce in realtà il punto di mediazione rispetto ad una serie di problemi estremamente ampi, scaturiti dall'impatto della società dell'informazione con le attività di stampo pubblicistico, in particolare della P.A.

Riguardo all'aspetto sostanziale, tenuto conto anche della necessità contingente di diversificare i contenuti del presente intervento da quelli delle altre relazioni, si è presentata in concreto la questione della scelta dell'approccio alla tematica:

- di tipo formale, che tenesse conto della distinzione tradizionale tra i due profili *de iure condito* e *de iure condendo*;
- o di tipo funzionale, al fine di considerare profili di maggiore importanza; ad esempio come i principi regolatori, cui si deve ispirare lo svolgimento dell'attività amministrativa, sono condizionati da elementi di forte tecnicismo (e non mi riferisco qui soltanto all'informatica o alle telecomunicazioni); quali fossero sostanzialmente le funzioni e in generale i poteri collegati in qualche modo allo svolgimento delle attività informatiche all'interno dell'intera società e dunque anche del mercato; quali fossero, in base alla vigente disciplina, il rapporto e le configurazioni attribuibili alla funzione delle singole amministrazioni e, sotto questo profilo, verificare l'applicabilità delle nuove discipline anche nei confronti della P.A., in particolare con riferimento al commercio elettronico.

¹ cardarelli@pronet.it

Chiaramente si è optato per l'approccio funzionale, più complesso, ma sicuramente più stimolante. Si devono fare, però, alcune considerazioni preliminari.

Certamente la forte connotazione tecnologica di diversi settori merceologici (e di nuovo va precisato che non si fa riferimento soltanto all'informatica e alle telecomunicazioni) ha determinato alcune trasformazioni funzionali, organizzative e procedurali dell'attività dell'amministrazione.

Sul piano dogmatico questo si traduce presumibilmente in quattro fattori evidenti, pur senza pretese di esaustività.

1. Un'accentuazione da parte dell'Amministrazione di ruoli di controllo tecnico, ovvero in qualche misura la perdita della capacità d'indirizzo politico in determinate materie, che molti commentatori hanno accompagnato in sostanza ad una certa perdita di sovranità dello Stato, ad esempio rispetto allo sviluppo dell'ordinamento comunitario.
2. La necessità di partecipazione della P.A. in ruoli non più tipicamente autorizzativi, ma per la definizione di norme tecniche (cosa che rappresenta senz'altro una novità, almeno per la nostra Amministrazione)
3. Un'accentuata divaricazione del ruolo di garanzia di determinate strutture amministrative, del loro ruolo di regolazione, con la conseguenza abbastanza evidente che anche l'approssimazione di modelli strutturali amministrativi nuovi, quali le autorità amministrative indipendenti, in realtà non corrisponde ad un modello unitario, ma a modelli che di volta in volta sono mutuati rispetto alle funzioni (di garanzia o di regolazione del mercato) da espletare. Emblematico sotto questo punto di vista, ad esempio, il caso del commercio elettronico, in cui su una medesima fattispecie intervengono funzioni di garanzia, espletate dal Garante per la protezione dei dati personali, e funzioni di regolazione del settore, espletate dall'Autorità per l'Informatica nella Pubblica Amministrazione. Questa divaricazione di funzioni, dunque, si è addirittura tradotta in qualche modo in una divaricazione di Enti e di strutture organizzative.
4. Una sopravvivenza dell'uso di una discrezionalità tecnica come momento partecipativo della discrezionalità amministrativa. La tradizione giuspubblicistica utilizza il criterio della discrezionalità amministrativa come figura ellittica, nella quale, però, si traduce in concreto

l'esercizio di un potere pubblico. La discrezionalità tecnica sarebbe stata, invece, sottratta ad una connotazione di discrezionalità amministrativa con l'esercizio di un potere vero e proprio, in quanto connotata sotto profili di scienza e conoscenza che in certa misura sono stati imputati all'Amministrazione come punto di riferimento difficilmente smentibile.

Sul piano pratico chi si occupa di tutela giurisdizionale dei diritti sa perfettamente che, mentre un uso scorretto della discrezionalità amministrativa, in senso lato dell'amministrazione, è sindacabile sotto il profilo dell'eccesso di potere di fronte al giudice amministrativo, la discrezionalità tecnica è stata tradizionalmente sottratta ad un sindacato giurisdizionale ed è dunque rimasta una fattispecie intangibile.

In determinate materie abbiamo assistito ad una sostanziale sovrapposizione o coincidenza di questi fattori. Basti pensare (e faccio un esempio diverso dall'informatica, che tra l'altro essendo l'oggetto del Convegno e sicuramente più delle altre soggetta a questo tipo di riflessione) alla tutela in materia ambientale, settore connotato da un fortissimo tecnicismo, in cui fondamentalmente non esiste un problema di discrezionalità tecnica, ma di un controllo di parametri tecnici, quali i valori delle emissioni, i tassi di inquinamento, l'adeguatezza o meno da un punto di vista tecnico di determinate norme; anche sotto un profilo strettamente normativo assistiamo ad una produzione di direttive talmente dettagliate e specifiche, da non richiedere spesso forme di implementazione formali, ma addirittura da essere traducibili direttamente in singoli decreti ministeriali applicativi.

Questo meccanismo tuttavia è in qualche modo destinato a modificarsi e vado così a spiegare la premessa essenziale per affrontare il problema del commercio elettronico e delle funzioni e dei poteri pubblicistici in materia.

La discrezionalità tecnica è in realtà in qualche modo sindacabile sotto tre particolari profili, non propri o esclusivamente propri della nostra tradizione giurispubblicistica, ma evidenziati da parte del diritto comunitario come requisiti dell'attività dell'amministrazione.

Sono in particolare il principio di proporzionalità - che non è immanente nel nostro ordinamento, mentre è presente, per esempio, in quello tedesco - e i profili della ragionevolezza e della pertinenza e congruità,

introdotti in qualche misura all'interno del nostro ordinamento e di alcune sentenze di giudici più accorti.

Inoltre, in relazione a materie fortemente caratterizzate tecnicamente, in cui l'intervento di organismi amministrativi, o comunque di diritto pubblico, consiste nella definizione di norme tecniche, che in qualche misura condizionano lo svolgimento dell'agire dell'uomo, si pone evidentemente il problema della centralità del valore dell'uomo nel sistema.

Questo problema si presenta con evidenza in alcuni esempi pragmatici.

Certamente è nota a tutti la recentissima vicenda della prova di preselezione informatica del concorso in magistratura ed il fatto che il Consiglio di Stato, con ordinanza, ha ritenuto irrazionale il sistema di preselezione informatica e contrario alla *ratio legis* valutare anche un solo errore commesso nei quiz proposti come assolutamente discriminante. Non voglio enfatizzare più di tanto questo tipo di decisione; mi sembra evidente, però, che in qualche modo vi sia stata una presa di coscienza di profili di ragionevolezza sotto il profilo strettamente formale.

Inoltre profili di connotazione tecnica in diverse materie sono già oggetto di numerose critiche, anche in sede comunitaria. Si parla esplicitamente di un deficit di rappresentanza della democrazia, in un certo senso, nella produzione di norme tecniche. E sotto questo profilo pare che il modello stesso di creazione della norma tecnica, presente in gran parte delle norme imperative o autoritative dettate in materie simili, sia un modello in mano ad oligarchie connotate tecnicamente ed economicamente e che in realtà sconti un processo di scarsa rappresentazione delle categorie coinvolte, ad esempio i consumatori, ed in genere difetti di forme di democraticità.

Passiamo ora ad esaminare i reali condizionamenti sostanziali dell'attività amministrativa, in questo caso fortemente connessi al settore dell'informatica e delle telecomunicazioni.

Sul piano strettamente funzionale, il primo problema, di fronte al quale si sono trovati il legislatore nazionale e gli organismi, ancorché indipendenti della P.A., è il fenomeno della cosiddetta smaterializzazione documentale, che comporta diverse conseguenze. Una realizzabile a livello normativo, o più precisamente ermeneutico: si tratta di riadattare istituti risalenti a tecnologie fondamentalmente nuove.

Sul piano tipicamente strutturale e organizzativo, vi è il fenomeno dell'identificazione delle competenze, che segue in realtà un processo di individuazione della diversa rilevanza delle funzioni. Infatti cose diverse sono la garanzia, la regolazione, le norme tecniche ed infine la disciplina delle situazioni giuridiche soggettive qualificabili come diritti.

Sempre sul piano organizzativo, come palesemente espresso all'interno delle norme generali sul pubblico impiego, sono affermati principi di collegamento delle attività fra uffici, adeguandosi a doveri di comunicazioni interne ed esterne ed interconnessione mediante sistemi informatici e statistici pubblici; questa è una regola contenuta nell'art. 2 del decreto legislativo n. 29 del 1993 in materia di pubblico impiego.

Sul piano procedimentale, è evidente il fatto che le tecnologie dell'informazione si devono adeguare a quanto stabilito dalla legge generale sul procedimento amministrativo, la quale, contrariamente agli altri Paesi appartenenti alla Comunità, è entrata in vigore soltanto nel 1990, e l'azione amministrativa deve essere compatibile con i valori tutelati dall'ordinamento e le situazioni giuridiche soggettive qualificate come diritti.

Il limite della tutela della riservatezza è fortemente sentito rispetto all'utilizzazione di strumenti, sistemi o modalità informatiche dell'agire amministrativo, ed a condizionamenti informatici dell'attività amministrativa in senso lato. Tuttavia in questa materia rileva anche la circostanza per cui non sono più qualificabili situazioni giuridiche soggettive, quali gli interessi legittimi, per una resistenza formale, concettuale e dogmatica rispetto all'impatto del diritto comunitario, fenomeno visibile in particolare in alcuni settori specifici, come gli appalti pubblici, ed oggi enfatizzato dalla nota sentenza della Corte di Cassazione sez. un. n. 500 del 1999.

Fin qui si è parlato di condizionamenti rispetto all'azione amministrativa anche nella proposizione di nuove norme, laddove effettuabile con particolari garanzie dell'ordinamento.

Un ultimo ed ulteriore aspetto, *de iure condendo*, riguarda la possibilità che la stessa Pubblica Amministrazione possa essere considerata protagonista di attività di commercio elettronico, come rilevato anche nelle interpretazioni della prassi amministrativa.

La stessa Comunità, in un Libro Verde pubblicato in data 20 gennaio 1999 su "L'informazione del settore pubblico nella Società

dell'Informazione", affronta esplicitamente almeno tre ordini di problemi:

- un problema di democrazia elettronica e, dunque, di forme partecipative alla gestione della cosa pubblica attraverso il mezzo elettronico;
- un secondo problema, tradizionale, già ben esaminato dalla nostra dottrina di diritto del processo;
- un terzo, più complesso da comprendere, ma forse di maggior attualità pratica, relativo a elementi potenzialmente distorsivi della concorrenza.

Nello schema dell'approccio seguito meritano una collocazione particolare delle considerazioni effettuate in base alle disposizioni normative vigenti; d'altra parte non poteva essere diversamente, trattandosi di Pubblica Amministrazione costretta nel suo comportamento al rispetto del principio di legalità.

Un primo profilo, probabilmente già toccato in termini generali nei precedenti interventi, è quello della rilevanza dell'attuale disciplina in materia di commercio, cioè del decreto legislativo n. 114 del 1998. Tale decreto fa riferimento al commercio elettronico ed individua una mera funzione di promozione da parte dell'amministrazione, anzi individua nel Ministero dell'Industria, del Commercio e dell'Artigianato il soggetto deputato allo svolgimento di tale attività.

Questa promozione consiste nel sostenere una crescita equilibrata del fenomeno del commercio elettronico, la tutela dei consumatori, opportune campagne di apprendimento, il miglioramento della qualità globale di promozione delle attività delle piccole e medie imprese e garanzie di partecipazione e cooperazione europea ed internazionale ai processi di formazione delle norme tecniche.

Tutto ciò appartiene ad una funzione di promozione, in parte attuata.

Il Ministero dell'Industria, del Commercio e dell'Artigianato, infatti, ha già prodotto un documento, datato 30 luglio 1998 ed intitolato "Linee di politica per il commercio elettronico"; in verità è un documento povero (e non poteva essere diversamente) di connotazioni giuridiche particolari, trattandosi appunto di una funzione di promozione, e dunque più di politica industriale che di politica del diritto, e pertanto richiama temi

già abbondantemente noti al legislatore, come la firma digitale e la carenza di disposizioni particolari sul commercio elettronico.

Un'altra funzione in materia di commercio elettronico, desumibile dall'attuale vigente disciplina, si basa sull'art. 18 del decreto legislativo n. 114 del 1998, che in sostanza pone dei profili di liberalizzazione dell'attività; in pratica chi desidera svolgere un'attività di commercio, attraverso sistemi di comunicazione televisivi o di altri tipo, ha come unici obblighi quelli di darne comunicazione al Comune e di possedere determinati requisiti, stabiliti dall'art. 5 a seconda del settore merceologico (alimentare o non alimentare), che si vuole utilizzare.

È evidente che sotto questo profilo tutti i divieti propri del commercio attraverso il mezzo televisivo devono essere estesi anche ai casi di commercio elettronico tramite Internet o altre reti telematiche, cioè l'impossibilità della vendita all'asta e l'applicazione delle norme in materia di contratti negoziati fuori dei locali commerciali, oltre che della direttiva 97/7/CE, già ricordata dal relatore che mi ha preceduto.

Riguardo alla possibilità di far ricorso all'analogia in relazione a due fattispecie previste nell'ambito dell'art. 18, essendo in questo caso evidente un vuoto normativo, occorre risolvere preliminarmente la questione se il mezzo televisivo sia assimilabile a quello telematico, al fine dell'impedimento del vincolo della limitazione dello svolgimento di un'attività commerciale.

Fin qui le norme applicabili in materia di commercio elettronico, più complessa mi pare invece l'analisi della disciplina della firma digitale, a torto a volte confusa con le prime.

Uno dei problemi di questa materia magmatica, che vedremo poi sollevati anche in sede comunitaria, è rappresentato da una notevole fluidità, coincidenza potenziale e sovrapponibilità di definizione di ambiti di applicazione.

Certamente si può ritenere che la firma digitale sia una componente, importante ma non necessaria, del commercio elettronico. Tuttavia, ai fini dell'evidenziazione di funzioni e poteri pubblicistici, è su questa che personalmente appunterei le maggiori critiche, in attesa di analizzare eventuali norme specifiche per il commercio elettronico, fattispecie peraltro considerata molto al di là da venire come fenomeno di massa.

Il D.P.R. n. 513 del 1997 sulla firma digitale, infatti, evidenzia alcune funzioni pubbliche: ci sono, ad esempio, vari richiami a funzioni svolte dall'Autorità per l'Informatica nella Pubblica Amministrazione e a successivi decreti, poi emanati, quali il D.P.C.M. dell'8 febbraio 1999 sulle regole tecniche (torna qui la questione delle norme tecniche, ma la cosa che forse può ostacolare la realizzazione dell'intero sistema è quella relativa alle funzioni di certificazione).

Nel D.P.R. 513 suddetto il legislatore italiano, ancorché delegato (pur non dimenticando il valore fondamentale della norma di riferimento, ovvero l'art. 15 della prima legge Bassanini, cioè la n. 59 del 1997), ha utilizzato un meccanismo che in realtà mette fortemente in crisi il sistema della firma elettronica, poiché non compatibile né con norme nazionali, né con quelle comunitarie.

Anzitutto è prevista l'esistenza di un elenco, tenuto dall'AIPA, di soggetti certificatori, che, oltre a far domanda, devono possedere alcuni requisiti specifici (essere società per azioni, detenere un capitale sociale pari a quello necessario per lo svolgimento di un'attività bancaria - 12,5 miliardi - ed altri requisiti tecnici); si ricorda, inoltre, che al soggetto certificatore sono attribuiti, oltre alle normali funzioni di certificazione, poteri che vanno fino alla revoca e alla sospensione dei certificati relativi a chiavi di sottoscrizione.

Si può presumere che chi ha redatto la norme del D.P.R. e del D.P.C.M. attuativo ha pensato allo svolgimento di funzioni tipicamente amministrative, dal momento che la funzione di certificazione è tradizionalmente appartenuta allo Stato. Soltanto in ambito comunitario, e per fattispecie diverse, si assiste ad una forma di certificazione di qualità, basata su presupposti di carattere non autoritativo, ma mercatorio, richiedendosi che i soggetti certificatori possiedano solo un'astratta abilità e capacità tecnica a svolgere un determinato tipo di funzioni per lo svolgimento di attività di certificazione relative alla corrispondenza dei prodotti agli *standards* internazionali, orientati ed originati dal mercato.

Il meccanismo, invece, utilizzato dal legislatore italiano per i certificatori, sorge da un modello autoritativo; il certificatore è un soggetto che di fatto sembra partecipare almeno nelle locuzioni utilizzate - "potere di sospensione, potere di revoca, strutturazione, necessità di verifica di requisiti da parte dell'Autorità per l'Informatica nella Pubblica Amministrazione" - all'esercizio di un pubblico potere di certificazione, fidefa-

cente tra l'altro (per chi sa della giurisprudenza della Corte di Giustizia quel potere di certificazione fidefacente è una delle connotazioni ai sensi dell'art. 55 del Trattato, che determina la sottrazione di determinati soggetti a meccanismi di tipo concorrenziale in quanto viene considerato come un soggetto che partecipa, sia pure occasionalmente, all'esercizio di pubblici poteri).

La conseguenza è perfida, perché il meccanismo inventato dall'Autorità potrebbe far ritenere l'attività del certificatore come un *modus* della Pubblica Amministrazione, e questo stesso soggetto come una sorta di organo indiretto, incardinato attraverso un provvedimento falsamente discrezionale, ma sostanzialmente autorizzatorio; ciò con tutte le conseguenze relative alle responsabilità, anche sotto il profilo penale, dal momento che il certificatore sarebbe quanto meno considerabile come un incaricato di pubblico servizio, con tutto ciò che ne deriva rispetto allo svolgimento della sua attività; inoltre una serie di norme siffatte determina effetti distorsivi sul mercato, contrariamente alla proposta di direttiva comunitaria sul commercio elettronico, laddove questo profilo viene affrontato in modo diametralmente opposto.

Infatti, il certificatore si presenta in essa come un soggetto che non viene immesso nel sistema in base a requisiti strutturali particolari, ma solo per capacità e abilità tecnica; non esistono albi o elenchi, ma un'astratta abilità e idoneità tecnica; di fatto viene imposto a ciascuno Stato membro di riconoscere come valida l'attività di certificazione svolta senza limiti di barriere linguistiche o culturali, in omaggio al principio della libera prestazione di servizi e di libertà di stabilimento in ambito comunitario. Ulteriore effetto distorsivo sul mercato è rappresentato dal fatto che, adottando uno Stato membro misure particolarmente restrittive solo nei confronti dei suoi amministrati; società o soggetti di certificazione di tale Stato sarebbero discriminati per l'impossibilità di praticare prezzi competitivi rispetto a soggetti certificatori di altri Stati, a cui chiunque peraltro potrebbe tranquillamente rivolgersi in un mondo virtuale come quello attuale.

Si pone inoltre il problema della compatibilità dell'intero sistema, così delineato, all'interno del sistema comunitario, laddove, come è noto, la Comunità si è già orientata verso l'approvazione definitiva di una direttiva sulla firma digitale e di una seconda direttiva dedicata esclusivamente al commercio elettronico.

Non pretendo di analizzare le singole disposizioni, mi riferisco soltanto ad alcune connotazioni principali della disciplina comunitaria, che mi sembrano peraltro difficilmente compatibili col sistema autoritativo definito dalle norme nazionali.

Innanzitutto il commercio elettronico è collocato, in sede comunitaria, nell'ambito sistematico dei servizi della società dell'informazione; cioè ha una collocazione dogmatica non stravagante, come potrebbe sembrare quella del caso italiano, dove si introduce da parte di un'autorità amministrativa indipendente la regolamentazione della firma elettronica, del documento elettronico, dell'archiviazione ottica, ecc., sovrapponendo norme di diversa imputazione e forza formale, che troverebbero miglior collocazione in un D.P.R. o addirittura in leggi.

Inoltre coerentemente vi è un generale criterio di applicazione dei principi di libertà sostanziale, su cui si fonda il Trattato: libera prestazione di servizi, libera circolazione dei capitali e delle persone e libertà di stabilimento. Quanto a quest'ultimo principio la commissione asserisce testualmente che il fornitore è obbligato, se residente in uno Stato membro, a dare comunicazione della sua esistenza e dello svolgimento della sua attività ad un determinato soggetto o autorità dello Stato di appartenenza. E questo è probabilmente l'unico meccanismo di controllo.

Anche in questo caso il legislatore comunitario non ha scelto un sistema di abilitazione, di autorizzazione o di licenza, né presumibilmente poteva farlo, in quanto contrastante con i principi di libertà del Trattato, non trattandosi né di attività riservata, né di attività basate su scarse risorse, unici casi in cui il legislatore italiano assoggetta a forme di natura autorizzatoria lo svolgimento di attività rientranti in principi di sostanziale libertà economica.

Tutto ciò sembra coincidere con le prospettive costituzionali ribadite ieri nella relazione del prof. Costanzo.

Mi si consenta prima delle conclusioni un'ulteriore connotazione in relazione alle possibili applicazioni del commercio elettronico da parte di una Pubblica Amministrazione. Nel documento del Ministero del Commercio, dell'Industria e dell'Artigianato si legge esplicitamente che il commercio elettronico è improntato ai rapporti fra imprese e consumatori, Pubblica Amministrazione e imprese, e Pubblica Amministrazione e cittadino.

Sull'ultimo punto si potrebbe osservare che il rapporto fra Pubblica Amministrazione e cittadino è un rapporto che attiene a profili di democrazia e di partecipazione procedimentale, e non è semplicemente inquadrabile come commerciale; diverso, invece, è il caso del rapporto fra Pubblica Amministrazione e imprese, comprensivo di tutte le fattispecie di accordi in qualche modo realizzabili (sia frutto di un'attività contrattuale, procedimentalizzata, intermediata cioè da una procedura di selezione del contraente, sia frutto di un'attività, anche questa convenzionale, procedimentalizzata per la dazione di sovvenzioni, incentivi o altro).

È interessante notare che già il Libro Verde della Commissione del 1996 in materia di appalti pubblici aveva dedicato un capitolo alla possibilità di esperire forme non solo di pubblicità, ma anche di competizione, selezione e aggiudicazione di definitiva stipulazione contrattuale, tramite sistemi informatici da parte delle pubbliche amministrazioni comunitarie.

Questo concetto è stato ribadito in un secondo Libro Verde del 1998 ed è finalizzato all'accesso delle piccole e medie imprese al mercato degli appalti pubblici. Dunque una prima applicazione è certamente possibile; ovviamente, ed è qui che vengono in evidenza negativa i formalismi del modello autoritativo scelto dal legislatore italiano, i meccanismi da rispettare sono più semplici (se vogliamo, meno connotati formalmente, ma più pregnanti sotto il profilo sostanziale): il principio di proporzionalità (non si può evidentemente obbligare un'impresa a sottostare a meccanismi di aggravio del procedimento partecipativo); il principio di non discriminazione (palese o occulta in base alla razionalità); il principio dell'utilizzazione di specifiche tecniche ugualmente non discriminatorie; il principio della forma scritta, realizzabile anche attraverso meccanismi di chiavi asimmetriche o anche di altre forme, in quanto il legislatore comunitario riconosce che alcune decisioni o discipline in ambito nazionale rappresentano solo una delle possibili forme applicabili all'interno dei singoli Stati membri di meccanismi di certezza o comunque di riconoscibilità o di imputazione delle fattispecie convenzionali.

In conclusione mi pare che si possano tracciare queste quattro considerazioni.

1. Esiste sicuramente un profilo di definizione dell'ambito giuridico delle applicazioni di siffatte materie, che deve tener conto almeno di tre questioni:

- a) la collocazione dogmatica nell'ambito dei servizi della società dell'informazione, laddove la Commissione, prima ancora che gli Stati membri, si è già attivata da almeno tre anni per tracciare un solco delle possibili iniziative;
- b) la definizione dell'ambito di commercio elettronico, se cioè riguardi solo ed esclusivamente attività commerciali o se possa riguardare attività gratuite o necessariamente onerose;
- c) una corretta dinamica pubblico-privato nella disciplina della materia, che tenga conto del progressivo venir meno dell'autoritatività di modelli di questo genere.

2. C'è un'evidente mancanza nel disegno, sia pure abbozzato, del legislatore italiano (mi riferisco in modo particolare ai problemi della firma elettronica) di una considerazione che invece è immanente in tutto il sistema comunitario, cioè quella dei profili della tutela giurisdizionale. In altri termini, in base al rapporto, che possiamo addirittura ricostruire come autoritativo, fra autorità e certificazione è probabile che se il tizio certificato si sente in qualche modo violato per una revoca o per una sospensione, che ritiene illegittime, possa avere il dubbio se rivolgersi ad un giudice amministrativo o ordinario, in quanto in fondo il rapporto con il certificatore è un rapporto di tipo contrattuale, anche se questi utilizza strumenti parapubblicistici, se non addirittura veri e propri provvedimenti autoritativi.

3. Le autorità di regolazione (destinate poi sostanzialmente a dare norme non tecniche, dato che il meccanismo di formazione della norma tecnica anche in questo caso è regolato fortunatamente in sede comunitaria), e mi riferisco ovviamente all'Autorità per l'Informatica nella Pubblica Amministrazione, hanno due limiti strutturali: il primo, derivante direttamente dalla legge, ovvero il fatto che possano dispiegare concretamente i propri effetti solo nei confronti delle pubbliche amministrazioni centrali; il secondo, derivante dalla natura degli interessi protetti, in quanto l'autorità di regolazione è l'autorità per l'informatica nella Pubblica Amministrazione e non l'autorità per l'informatica *tout court*, la differenza non è semplicemente terminologica ma concettuale.

È evidente che l'attribuzione del potere di dettare norme tecniche, che condizionino non solo le amministrazioni, ma, come abbiamo visto, soprattutto i soggetti privati e addirittura il mondo delle imprese, costituisce un surrettizio ampliamento dei poteri originariamente affidati dal

legislatore a questa Autorità, nata per la protezione di interessi tipicamente amministrativi, ma che sta diventando implicitamente un'autorità di regolazione di un intero segmento di mercato; e di ciò si potrebbe anche prendere atto, operando le opportune modifiche normative.

4. In definitiva il vero conflitto, già più volte notato da chi si occupa in generale di tecnologie e di studi relativi alla Pubblica Amministrazione, sta nella differenza tra il modello normativo e quello di equilibrio tra l'esercizio di poteri condizionanti e il mercato, che nel nostro sistema è tradizionalmente un modello di carattere autoritativo (questo nasce dal contesto pre-repubblicano e in un certo qual modo si è trasferito nell'ambito del nostro dettato costituzionale, in particolare nell'art. 43 della Costituzione).

Concludendo il modello comunitario è un modello non autoritativo, ma tipicamente liberale, basato su principi di autoregolazione ed autocorrezione da parte del mercato e ha dunque una configurazione strutturale, organizzativa e dei poteri relativi sostanzialmente diversa dal modello imperativo seguito dal legislatore italiano.

Strumenti di pagamento *on-line* e *l'e-cash*

GIANLUIGI CIACCI¹

SOMMARIO: 1. *Il problema* - 2. *Il commercio elettronico* - 3. *Analisi dei sistemi di pagamento elettronici* - 4. *Le fonti* - 5. *Analisi dei principali problemi giuridici* - 6. *Conclusioni*.

1. IL PROBLEMA

È sempre più avvertita dagli operatori del settore l'importanza crescente del commercio elettronico, terreno privilegiato di circolazione della ricchezza, importanza testimoniata dalle altisonanti stime che ne individuano il valore: stime di solito riportate con variazioni notevoli tra le differenti cifre indicate nelle proiezioni degli esperti, e che si dimostrano poi tendenzialmente errate perché in genere non realizzate.

Il motivo della mancata realizzazione di tali previsioni può essere individuato attraverso la lettura di un documento ufficiale della Commissione europea (COM 97/157)², "Un'iniziativa europea in materia di commercio elettronico": *l'e-commerce* si sviluppa solo in presenza di sistemi di pagamento elettronici, validi, di agevole impiego per l'utilizzatore, efficaci e sicuri.

La problematica della moneta elettronica può quindi essere considerata il "punto focale" dello sviluppo del commercio svolto a distanza attraverso reti telematiche, insieme al collegato problema dell'identificabilità e non ripudiabilità dei messaggi inviati attraverso i nuovi *media*, e contenenti ad esempio proposte contrattuali, risolto dalla nuova disciplina della firma digitale: e questo sia dal punto di vista del cliente (il cui interesse in tale ambito è vedere protetto il suo acquisto), sia dal punto di vista del fornitore (ad ottenere l'adempimento della vendita attraverso il pagamento del prezzo).

L'approccio all'indicato problema deve iniziare da una descrizione del fenomeno del commercio elettronico e delle applicazioni concrete di pa-

¹ redazione@jer.it

² Pubblicata nel sito Web all'indirizzo <http://www.aspo.ccc.be/ecommerce/legal/legal.html> consultato il 10 dicembre 1999

gamenti attraverso sistemi informatici e telematici, per poi analizzarne gli aspetti giuridici.

2. IL COMMERCIO ELETTRONICO

Il commercio elettronico può essere definito come ogni forma di transazione commerciale nella quale le parti interagiscono per via elettronica, piuttosto che nei tradizionali scambi e contatti fisici³. Il relativo mercato promette per il nuovo millennio un giro di affari pari a 300 miliardi di dollari⁴, e ha visto nascere nell'ultimo anno nei soli U.S.A. più di 250.000 *cyberimprese* che utilizzano Internet in vario modo per scopi commerciali, e si pone quindi come un terreno privilegiato di circolazione della ricchezza. Una circolazione che, grazie proprio ai nuovi *media*, ed alla loro diffusione esponenziale e globale, ha raggiunto oggi velocità impressionanti, come risulta dalle cifre che stimano i risultati di tale mercato: ad esempio per il 1997 il giro di affari è stato tra gli 8 miliardi di dollari (secondo la Forrester Research e solo per gli U.S.A.) e i 2 miliardi e mezzo di dollari (secondo la *Active Media*), e le testimonianze dirette delle imprese che già operano nel nuovo mercato confermano le ricerche degli specialisti⁵. Infatti lo svolgimento di attività economica a fini di lucro per via telematica rappresenta uno dei rari casi dove la necessità di cambiamento e le nuove tecnologie si uniscono per rivoluzionare il modo in cui sono condotte le attività economiche. Così, si ha da una

³ La Commissione europea, nella comunicazione "Un'iniziativa europea in materia di commercio elettronico" [Com (97) 157] lo definisce come "lo svolgimento di attività commerciali e di transazioni per via elettronica che comprende attività diverse quali la commercializzazione di beni e servizi per via elettronica, la distribuzione *on-line* di contenuti digitali, l'effettuazione per via elettronica di operazioni finanziarie e di borsa, gli appalti pubblici per via elettronica ed altre procedure di tipo transattivo delle Pubbliche Amministrazioni". Per consultare la Comunicazione si veda al sito <http://www.cordis.lu/espri/stt/ecomcom.htm> visitato il 10 dicembre 1999.

⁴ Stime Forrester Research riferite solo agli U.S.A. (dati tratti, come gli altri di questo paragrafo da L. La Posta, *Nell'era dello shopping on-line*, in *Il Sole 24 Ore - Informatica*, 21 ottobre 1998, pag. 1).

⁵ La Dell Computer, società che vende *hardware*, nel 1995 dichiarava di guadagnare circa un milione di dollari al giorno dalle vendite su Internet, cifra oggi quasi triplicata, il *leader* del mercato del commercio elettronico di fiori che, insieme ai viaggi, rappresenta l'oggetto della metà delle transazioni sulla Rete, ha fatturato per il 1996 circa 30 milioni di dollari, una delle più grandi società europee di vendita per corrispondenza ha realizzato nello stesso anno 250 milioni di dollari dal settore della propria attività che si svolge *on-line*, Amazon, la più grande libreria del mondo (non solo virtuale), nel quarto trimestre 1998 ha venduto libri con ricavi per un valore di circa 250 milioni di dollari.

parte il commercio moderno, caratterizzato dal continuo sviluppo delle capacità di fornitura, della competizione a livello mondiale, delle attese dei consumatori; dall'altra il commercio elettronico, un mezzo per consentire e sostenere tali cambiamenti a livello globale⁶.

Basato, come si è detto, sull'elaborazione e trasmissione dei dati per via elettronica, comprende attività disparate⁷, che permettono comunque di distinguere due diverse modalità: da una parte un commercio elettronico "indiretto", nel caso di conclusione di contratti per via elettronica aventi ad oggetto beni materiali, la cui concreta prestazione può svolgersi attraverso modalità tradizionali; e, dall'altra, una sua forma "diretta", nel caso non solo di conclusione telematica, ma anche di distribuzione on-line di beni immateriali⁸.

Non è un fenomeno nuovo, ma fino a poco tempo fa era limitato ad attività di imprese su reti chiuse di tipo "proprietario" (conosciuto sotto il nome di E.D.I., cioè *Electronic Data Interchange*), mentre ora si sta espandendo in una complessa connessione di relazioni commerciali svolte su scala globale tra un crescente numero di partecipanti (anche privati) su reti aperte mondiali, come ad esempio Internet: raggiungendo la diffusione e l'importanza di cui si è detto. Ma le differenze tra le due realtà, quella "chiusa" dell'E.D.I. e quella "aperta" di Internet, non si li-

⁶ In particolare infatti esso consente, alle imprese, di essere più efficienti e flessibili nelle loro operazioni internazionali, di lavorare maggiormente in contatto con i propri fornitori (permettendo di selezionare il migliore a prescindere dalla sua dislocazione geografica), e di essere più pronte a rispondere ai bisogni ed alle attese dei propri clienti, operando comunque in un mercato senza confini, agli utenti, di ottenere prezzi più vantaggiosi, di riuscire a trovare prodotti rari, o ancora non distribuiti, instaurando un rapporto immediato con il produttore, mediante un *customer care on-line* (cioè un servizio clienti per via telematica) rapido e diretto.

⁷ Tra queste la commercializzazione di prodotti (ad esempio di consumo, come *hardware e software*, ma anche libri, dischi, fiori, gioielli e salami), servizi (di informazione, giuridici e finanziari), attività di tipo tradizionale (assistenza sanitaria e istruzione, previdenza), attività "nuove", che si svolgono nell'ambito della rete telematica (ne costituiscono esempio i centri commerciali virtuali).

⁸ Ipotesi particolari di commercio elettronico sono poi l'*electronic trading* (scambi elettronici) in cui il fornitore effettua una prestazione di beni o servizi ad un cliente in cambio del pagamento di un prezzo, e l'*electronic retailing* (vendita elettronica al minuto), nel caso il cliente sia un consumatore ordinario piuttosto che un'altra impresa.

⁹ Nel 1989 la Commissione delle Comunità Europee ha definito l'*Electronic Data Interchange* come "*l'échange de données structurées, sur base de messages normalisés après, d'ordinateurs à ordinateur, par voie électronique*" (definizione tratta dal rapporto *Situation juridique des Etats membres au regard du transfert électronique de données*, pubblicato nel settembre 1989 dalla Commissione nell'ambito del programma TEDIIS).

mitano ad aspetti "storici" o numerici, ma sono più profonde e concettuali: infatti, per il commercio elettronico di tipo convenzionale, la rete di telecomunicazione è un mezzo per convogliare dati; per il commercio elettronico su Internet, la Rete è il mercato. Tali differenze si estendono poi ai soggetti che vi partecipano, al numero ed alle peculiarità degli stessi, alle esigenze di sicurezza.

L'elemento fondamentale nel nuovo mercato è comunque rappresentato dal modo in cui avviene concretamente la circolazione della ricchezza attraverso i nuovi *media*, ed in particolare di quella dell'adempimento delle obbligazioni pecuniarie nei contratti relativi a beni e servizi offerti in Rete: circolazione automatica che deve essere attentamente analizzata se si vuole poi affrontare correttamente la problematica giuridica dei mezzi di pagamento su Internet.

3. ANALISI DEI SISTEMI DI PAGAMENTO ELETTRONICI

Un esame delle modalità pratiche relative ai sistemi di pagamento usati su Internet, correlati alla circolazione di beni e servizi, permette di individuarne tre diverse "generazioni": "generazioni" che si distinguono non tanto a livello di validità temporale degli stessi (ancora oggi infatti si utilizzano in maniera preponderante la modalità corrispondenti alla I generazione), quanto per il momento della loro introduzione e per alcune caratteristiche comuni dei singoli strumenti.

La I generazione riguarda in particolare il pagamento in forme ordinarie, cioè con modalità che potremo definire tradizionali: motivo per cui essa registra la massima fiducia e familiarità da parte dell'utente, ma che la fa restare comunque al di fuori della realtà di Internet. Gli strumenti sono quelli noti: bonifico bancario, conto corrente postale, pagamento con assegno, pagamento in contrassegno, pagamento tramite carta di credito. In quest'ultimo caso l'invio del numero della carta può avvenire con due diversi sistemi: il primo, che potremo definire *off-line*, implica la trasmissione dello stesso con metodologie tradizionali, ad esempio via posta, *fax*, oppure attraverso una comunicazione telefonica; il secondo avviene invece mediante sistemi *on-line*, cioè attraverso la stessa comunicazione via Internet, sia essa un messaggio di posta elettronica¹⁰, oppure

¹⁰ Grazie a specifici *software*, ed alle autorità che coordinano Internet nel mondo (assegnando gli indirizzi dei vari utenti senza possibilità di erronee duplicazioni), si è sviluppato un servizio di

l'invio di uno specifico modulo tramite il *Web*¹¹. La prima modalità, pur configurando alcuni aspetti positivi ai fini dell'attività contrattuale (l'invio del numero della carta con modalità tradizionali consente sempre, infatti, di acquisire elementi per individuare con maggiore sicurezza la controparte, e quindi permette di scegliere se procedere o meno nella conclusione del contratto), in realtà sono preponderanti gli aspetti negativi rispetto al mondo di Internet (nella specie i costi o la lentezza del mezzo, in contrasto con la velocità e in genere l'economicità delle comunicazioni nel nuovo mercato del commercio elettronico); nel caso invece di invio tramite sistemi *on-line*, si sfruttano al massimo le caratteristiche del *media*, ma aumentano i rischi per gli utenti: non solo per l'acquirente (si pensi alle possibilità di intercettazione dei numeri della carta, in realtà non così comuni come vengono riportati dagli organi di informazione¹², nonché

messaggistica elettronica (cioè di posta formata, recapitata e letta attraverso un *computer*) a diffusione globale: servizio che sempre più sta diventando uno *standard* di comunicazione che mina l'esistenza stessa della tradizionale *snail mail* (la lenta posta cartacea), e che ben si adatta alle modalità pratiche di commercio elettronico.

¹¹ Il *World Wide Web* (WWW, ovvero semplicemente *Web*), la cosiddetta "ragnatela ipermediale", nuovo rivoluzionario mezzo di informazione e di conoscenza, integra tecniche multimediali per consentire una comunicazione aperta su Internet. tra i servizi della Rete, insieme alla posta elettronica, è quello che maggiormente può essere considerato la causa della diffusione repentina ed esponenziale del fenomeno. Esso costituisce un vero e proprio organo di informazione, rappresenta infatti la sede in cui è possibile visionare, ascoltare, comunicare apertamente sulla Rete delle reti, attraverso pagine di testo, illustrazioni, clip sonori. Tali pagine, che costituiscono il cosiddetto "sito", possono essere pubblicate da chiunque abbia accesso ad uno spazio di memoria su un *computer* "ospite" collegato alla Rete (in genere quello dello stesso *provider*, cioè colui che fornisce a livello tecnico l'accesso al mondo di Internet e che allo stesso tempo concede l'uso, gratuitamente o a pagamento, di tale spazio di memoria), il cosiddetto *Web server*, che utilizza l'opportuno *software*. I contenuti dei siti possono essere i più diversi, ludici o professionali, informativi o di servizio, leciti o meno. Colui che gestisce il sito, graficamente e/o a livello contenutistico, è il cosiddetto *Webmaster*.

¹² Le ipotesi di intercettazione di numeri di carta di credito quando inviate su Internet raramente sono così rilevanti rispetto a quanto denunciato, in genere con toni eccessivamente allarmistici, dalla stampa: si tenga presente che le intercettazioni dei messaggi di posta su Internet non sono di fatto così facili (non solo perché protetti da sistemi tecnici, tipo il protocollo *SET* dei circuiti Visa o Mastercard, ma anche perché si calcola che circolino 4.000 *e-mail* al secondo, rendendo quindi praticamente di difficile o impossibile intercettazione proprio il messaggio contenente il numero di carta di credito), e comunque le eventuali truffe risultano essere non superiori a quelle che si verificano al di fuori del circuito telematico. A tale proposito Roberto Dadda, del Banco Ambrosiano Veneto, nel suo intervento all'*Alta Vista World Convention '98* nell'ambito del *Future show 1998* (riportato da M. Ferrari Rolli, *Sviluppo e futuro del commercio elettronico*, 3 aprile 1998, consultabile su *Repubblica.it* all'indirizzo <http://www.repubblica.it/online/speciale/futur4/futur4/futur4.html> consultato il 10 dicembre 1999) afferma che "la pericolosità di Internet è un luogo comune da smentire", e riporta una serie di statistiche che evidenziano come le "perdite" di denaro in Rete siano inferiori sia all'uso della carta di credito nelle modalità tradizionali, sia all'uso del cellulare (1

alla più frequente possibilità dell'uso indebito della stessa carta da parte del destinatario del messaggio), ma anche per il venditore (si immagina la perdita economica che questo sarà chiamato ad affrontare ad esempio nel caso di uso da parte di un suo cliente di una carta falsa o rubata, oppure di una carta con disponibilità finanziarie non coperte).

Per i motivi di non totale sicurezza, o comunque di limitata efficienza dei mezzi di I generazione, si è sviluppata una II generazione di sistemi di adempimento dell'obbligazione pecuniaria attraverso la telematica: tale generazione riguarda il pagamento attraverso un "intermediario elettronico", che permette di garantire sicurezza ed identità di chi acquista o vende in Rete¹³. Ne costituiscono esempi i sistemi della *First Virtual Holding Bank* e quello recentissimo della *Global Trust Authority* (G.T.A.).

Nel primo caso sia il fornitore che l'utente sottoscrivono con *First Virtual* uno specifico contratto, in cui autorizzano la società bancaria a svolgere la funzione di "garante" dell'esatto adempimento dei successivi accordi negoziali tra i vari soggetti suoi clienti. Per rendere effettivo tale sistema, l'utente invia gli estremi della propria carta di credito con le già ricordate modalità *off-line* all'intermediario, che procede negli opportuni controlli per "validare" sia la stessa carta, sia la capacità solutoria del soggetto. In caso non vengano riscontrati problemi, l'intermediario invia la conferma dell'attivazione del sistema al proprio utente, insieme ad uno specifico *personal identification number*, chiamato *Virtual PIN*; da questo momento, il cliente che vuole acquistare un bene su Internet manda il proprio codice al venditore, che lo gira alla *First Virtual Holding Bank*; questa chiede quindi conferma dell'ordine all'utente, ulteriore garanzia al fine di evitare l'inoltro di ordini non autorizzati; in caso di risposta affermativa, l'intermediario comunicherà al fornitore la conferma dell'operazione, il quale fornitore procederà quindi all'adempimento della propria obbligazione, spedendo la merce. In seguito la *First Virtual* accredita la somma pagata dall'utente al fornitore, trattenendo una commissione sull'operazione. Fin dalla sua descrizione il sistema appare però estremamente macchinoso, tanto da farlo considerare di non facile o immediata realizzazione e gestione: si è così pensato ad un intermediario maggiormente efficiente.

dollaro ogni mille di media contro 2 ogni mille per le carte di credito e addirittura 46 per i telefoni cellulari)

¹³ Così, G. Hancu, *Internet e la legge*, Mc Graw Hill, 1997, p. 136

A tale fine si è creato, sulla base di un recentissimo accordo tra 11 Paesi e circa 800 banche, un istituto senza fini di lucro per verificare le chiavi di crittografia che verranno fornite dalle banche ai propri correntisti, e per garantire l'identità di chi effettua transazioni: tale istituto prende il nome di *Global Trust Authority* (G.T.A.), e per l'Italia ha visto l'adesione dell'A.B.I. e della S.I.A..

Anche le modalità di seconda generazione, nonostante si svolgano prevalentemente attraverso la telematica, risultano però essere ancora troppo complicate, tanto da portare alla creazione di una III generazione: è quella che consente il pagamento delle transazioni sostituendo al denaro un importo, una somma "virtuale": ipotesi in cui è possibile parlare effettivamente di "moneta elettronica". Ne costituiscono esempi, sulla base delle sperimentazioni fino ad oggi svolte:

- *gli assegni elettronici*, certificati digitali (sono documenti elettronici) sottoscritti con firma digitale, che vengono inviati da utente a fornitore, e da questo (dopo a sua volta essere stati firmati) alla banca per l'incasso. Il sistema è attuato ad esempio dalla società *NetCheque*;
- *il cosiddetto borsellino elettronico*, carta prepagata e ricaricabile, tecnicamente è una *smart card*, cioè una tessera che contiene un *chip* che permette di memorizzare informazioni; vi si registra una stringa di *bit* alla quale è attribuito un certo valore in denaro, che potrà essere prelevato al momento dell'acquisto digitando uno specifico codice; ogni volta che si usa viene scalata la somma in concreto spesa; la *smart card* può essere poi ricaricata a seconda delle esigenze dell'utente; esempi di tale sistema sono quelli attuati dai circuiti *Mimpay* e *Mondex*¹⁴;
- *Digicash* (moneta elettronica in senso stretto¹⁵: la stringa di *bit* corrispondente alla somma di denaro viene questa volta memorizzata direttamente sul *computer*; in pratica l'utente paga il fornitore con *cyberdollar*; questo esegue con la banca un controllo sul numero di serie delle banconote digitali, con apposito *software*, per verificare che non si tratti di denaro contraffatto, o già speso in precedenza;

¹⁴ Per quanto riguarda il circuito Mondex è possibile visitare il sito Web all'indirizzo <http://www.mondex.com/>, consultato il 10 dicembre 1999.

¹⁵ Su *Digicash* è possibile consultare il sito Web all'indirizzo <http://www.ecashtechologies.com/> visitato il 10 dicembre 1999.

la gestione del sistema avviene attraverso la crittografia asimmetrica¹⁶.

4. LE FONTI

In molti Paesi sono state dettate discipline specifiche che regolano la materia dei pagamenti attraverso sistemi automatizzati. Ai fini dell'analisi condotta nel presente lavoro verranno tenuti in considerazione le esperienze più significative di U.S.A., dell'Unione Europea e dell'Italia.

Negli Stati Uniti la prima normativa che sembrerebbe doversi applicare alla materia esaminata nel presente scritto è quella generale dei trasferimenti elettronici di fondi¹⁷, ed in particolare quindi l'*Electronic Funds Transfer Act* (E.F.T.A.)¹⁸ che, seppur emanato nel 1978 ed in tema di rapporti tra banche e clienti¹⁹, riporta principi ancora validi anche nella diffe-

¹⁶ La crittografia è la tecnica che permette, con l'aiuto di un algoritmo matematico, di trasformare un messaggio leggibile da tutti in una forma illeggibile per quegli utenti che non possiedono una chiave segreta di decifrazione. La funzione è reversibile, per cui l'applicazione dello stesso algoritmo e della chiave segreta al testo cifrato restituisce il testo originale. È possibile distinguere due diversi tipi di tecniche crittografiche: quelle che richiedono l'uso di una sola chiave segreta, la stessa per criptare e decrittare il testo, e perciò dette "simmetriche", e quelle che utilizzano una coppia di chiavi, diverse per "chiudere" ed "aprire" il documento (utilizzate insieme per diverse finalità, come si vedrà oltre), di cui una viene resa pubblica, e dette "asimmetriche". Sul punto si vedano le numerose pubblicazioni in materia di firma digitale, ed in particolare il mio scritto *Firma Digitale*, in *Sole 24 Ore* Ltd., 1999, capitolo 2, p. 49.

¹⁷ Gli *Electronic Funds Transfer* (E.F.T.) possono essere definiti, in senso stretto, come tutte le operazioni il cui scopo diretto è quello di spostare fondi o ricchezza da un patrimonio all'altro senza movimenti attuali di denaro, ma soltanto attraverso istruzioni impartite ed adempiute elettronicamente, in senso ampio, come gli ordini di trasferire fondi da una persona all'altra eseguiti mediante sistemi elettronici. La differenza tra le due definizioni è netta, in quanto nella prima accezione (E.F.T. in senso "stretto"), lo spostamento di ricchezza o di fondi da un patrimonio all'altro avviene soltanto attraverso istruzioni comunicate ed eseguite elettronicamente, e quindi senza alcun movimento materiale di denaro o di titoli. L'ordine elettronico di trasferimento di fondi, diventa così un effettivo trasferimento elettronico di fondi che avviene *on-line*, cioè senza alcun apprezzabile intervallo di tempo tra ordine di addebito o di accredito ed esecuzione dell'ordine (così, E. Giannantonio, *Manuale di diritto dell'informatica*, Padova, 1997, p. 269 ss.). Sul trasferimento elettronico di fondi v., in dottrina, R. Boruso, *Computer e diritto*, II, Milano, 1988, p. 274 ss., E. Giannantonio, *Trasferimenti elettronici di fondi e autonomia privata*, Milano, 1986, pp. 3-187, F. Trojani, *Trasferimenti elettronici di fondi e moneta elettronica*, in *Informatica ed enti locali*, Rimini, 1995, 4, p. 54 ss., L. Devescovi, *Titoli di credito e informatica*, Padova, 1991, pp. 1-375, P. NUVOLONI, *La trasmissione elettronica di fondi e la tutela dell'utente*, in *Dir. inf. e inform.*, 2, 1988, p. 593 ss.

¹⁸ Per un commento sull'E.F.T.A. e per poterne leggere il testo, v. E. Giannantonio, *Trasferimenti elettronici di fondi e autonomia privata*, cit. p. 95 ss.

¹⁹ Aspetto che in realtà non rende sempre così pacifica la sua applicazione alla materia considerata nel presente scritto.

rente realtà dei pagamenti che avvengono attraverso la rete Internet. Si veda poi l'art. 4a dell'*Uniform Commercial Code*, che disciplina gli E.F.T. di notevole ammontare effettuati dalle imprese, e il *Truth in Lending Act* (T.I.L.A.) che regola le operazioni economiche effettuate mediante carte di credito²⁰. Oltre a tali fonti "pubbliche", debbono poi essere presi in considerazione i vari accordi e contratti stipulati con i differenti gestori dei sistemi di pagamento che vengono effettuati su Internet.

Per quanto riguarda l'Unione Europea, vanno segnalate la Raccomandazione 97/489/CE del 30 luglio 1997²¹ e la Direttiva 97/7/CE del 20 maggio 1997 riguardante la protezione dei consumatori in materia di contratti a distanza: la prima relativa proprio alle operazioni mediante strumenti di pagamento elettronico, con particolare riferimento alle relazioni tra gli emittenti ed i titolari di tali strumenti; mentre la seconda, recepita nel nostro ordinamento con la l. 22 maggio 1999, n.185, prevede solo alcuni riferimenti sull'argomento²².

Rispetto infine alla situazione italiana, devono essere riportate diverse disposizioni che in qualche modo prendono in considerazione la possibilità di effettuare pagamenti attraverso sistemi automatizzati, anche se nessuna particolarmente significativa.

Così, il primo riferimento esplicito in una legge nel nostro Paese a sistemi di pagamento elettronici si può trovare nell'art. 14 D.P.R. 10 novembre 1997, n. 513²³, la disciplina in materia di firma digitale: anche se la norma risulta essere di scarsa redazione, e contiene tra l'altro un rinvio alle regole tecniche (previste dallo stesso D.P.R. n. 513 nel suo art. 3 per la concreta realizzazione del sistema italiano di firma digitale, e pubblicate con D.P.C.M. 8 febbraio 1999), poi non recepito dalle stesse²⁴. Van-

²⁰ Così, G. Binocchiaro, *Il problema dei mezzi di pagamento*, in AA.VV., *I problemi giuridici di Internet*, Milano, 1999, p. 123.

²¹ In G.U.C.E., L. 208, 2 agosto 1997, p. 52.

²² Sulla Direttiva 97/7/CE v., su tutti, G. Alpa, *La nuova Direttiva 97/7/CE del 20 maggio 1997, riguardante la protezione dei consumatori in materia di contratti a distanza*, Atti del convegno *I contratti elettronici negoziati a distanza*, Milano, 5 novembre 1997.

²³ Art. 14: "Il trasferimento elettronico dei pagamenti tra privati, pubbliche amministrazioni e tra queste e soggetti privati è effettuato secondo le regole tecniche definite col decreto di cui all'articolo 3". Per un commento al d.P.R. n. 513 del 1997, v. M. Niccoli, *Documento e commento telematico*, Milano, 1998, e G. Ciacci, *La firma digitale*, in *Il Sole 24 Ore Ed.*, Milano, 1999.

²⁴ Infatti il D.P.C.M. 8 febbraio 1999, "Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici ai sensi dell'articolo 3, comma 1, del Decreto del Presidente della Repubblica, 10 novembre 1997, n. 513", non presenta disposizioni specifiche attinenti al tema indicato nell'art. 14,

no quindi segnalati gli artt. 3, comma 1, lett. e, 4, comma 1 (in materia di obbligo di informazione al consumatore sulle modalità di pagamento della prestazione oggetto del contratto, da adempiere in tempo utile prima della conclusione dell'accordo), e l'art. 8 (sul pagamento mediante carta) del già ricordato d. lgs. n. 185 del 1999, che ha recepito la Direttiva 97/7/CE sui contratti a distanza. Altre discipline applicabili alla materia sono quelle in genere della normativa relativa alle carte di credito, come ad es. l'art. 12 l. 5 luglio 1991, n. 127 (disciplina emanata al fine di prevenire l'utilizzo del sistema finanziario a scopo di riciclaggio), l'art. 17, comma 87, l. 15 maggio 1997, n. 127 (in materia di uso di strumenti elettronici o informatici per riscuotere tributi, sanzioni o prestazioni di natura pecuniaria in forma diretta da parte delle Regioni), ed il recentissimo art. 7 D.P.R. 22 ottobre 1999, n. 437²⁵, che introduce nel nostro Paese la carta di identità elettronica, articolo che prevede espressamente i pagamenti informatici²⁶, ulteriore possibile utilizzo di tale carta.

5. ANALISI DEI PRINCIPALI PROBLEMI GIURIDICI

L'efficacia del sistema di pagamento adottato nelle transazioni economiche su Internet al fine di "accrescere la fiducia dei consumatori negli strumenti di pagamento elettronico nel mercato unico" (Commissione Europea, COM 97/353), può essere verificata da due differenti prospettive: dal punto di vista dell'affidabilità del sistema di pagamento e da quello della sua validità giuridica.

ed anzi, nonostante il diretto richiamo al Regolamento contenuto nel suo testo, non si occupa affatto del tema dei pagamenti informatici, se non a livello di sistema generale di firma digitale (gli standard tecnici, e le modalità d'uso relative alla sottoscrizione elettronica di documenti informatici valgono cioè anche se tale documento consiste in un ordine di pagamento). Considerando l'importanza della prestazione del pagamento del bene e/o servizio, in prospettiva del definitivo avvio del nuovo mercato del commercio elettronico l'argomento avrebbe sicuramente meritato un maggior approfondimento.

²⁵ Il "Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico, a norma dell'articolo 2, comma 10, della legge 15 maggio 1997, n. 127 come modificato dall'articolo 2, comma 4, della legge 16 giugno 1998, n. 191", pubblicato in *GU*, 22 novembre 1999, n. 277, il cui testo è leggibile nella rubrica "*Cittadino Lex*" del sito "Repubblica.it", all'indirizzo Internet http://www.repubblica.it/cittadino.lex/societa/societa991126_1_carta/societa991126_1_carta.html, consultato il 10 dicembre 1999.

²⁶ Art. 7 "La carta d'identità elettronica può essere utilizzata anche per il trasferimento elettronico dei pagamenti tra soggetti privati e pubbliche amministrazioni, previa definizione, d'intesa tra il comune interessato e l'intermediario incaricato di effettuare il pagamento, delle modalità di inserimento e validazione dei dati necessari".

Secondo la prima prospettiva, per raggiungere l'indicato fine il sistema deve essere chiaramente affidabile, e quindi solo le "istituzioni del credito" (quelle cioè controllate da una banca centrale o da altra autorità) devono essere autorizzate a rilasciare denaro elettronico, e deve inoltre essere garantita tecnicamente l'integrità del metodo di pagamento in sé stesso: questo sia nei confronti di possibili interventi delle parti che concretamente lo utilizzano, sia di terzi estranei.

Dal punto di vista della sua validità giuridica, invece, il sistema di pagamento deve essere idoneo in concreto ad estinguere l'obbligazione, cioè a liberare chi ha effettuato il pagamento della prestazione con i nuovi strumenti.

Per stabilire se la moneta elettronica soddisfi tale requisito, occorre quindi ora accertare se è accertabile il pagamento elettronico quale modo di estinzione dell'obbligazione pecuniaria nell'ambito dell'ordinamento giuridico italiano. Le norme di riferimento sono in questo caso l'art. 1277 c.c., per il quale i debiti pecuniari si estinguono con moneta avente corso legale nello Stato al tempo del pagamento, mitigato dall'art. 1197 c.c., il quale infatti prevede che con il consenso del creditore il debitore possa liberarsi eseguendo una prestazione diversa da quella dovuta, e che l'obbligazione si estingua con l'esecuzione della diversa prestazione.

Sulla base di tali norme la giurisprudenza ha inoltre affermato che qualora la pratica costante e preesistente tra le parti, o la pratica costante per il tipo di affari cui il contratto appartiene, sia quella di un pagamento diverso, il creditore non può rifiutare il pagamento se non adducendo specifici motivi²⁷.

I pagamenti elettronici possono quindi essere ammessi quale sistema valido di estinzione dell'obbligazione pecuniaria con il consenso del creditore, dunque con riferimento all'art. 1197 c.c., oppure nelle fattispecie ricordate dalla giurisprudenza. Ma nello specifico caso del commercio su Internet, il pagamento elettronico può essere addirittura considerato "la"

²⁷ Sul punto, v. Cass., 19 luglio 1993, n. 8013, in *Rassegna delle locazioni e del condominio*, 1994, p. 57 ss.; Cass., 24 giugno 1997, n. 5638; Cass., 10 febbraio 1998, n. 1351, in *Foro it.*, 1998, c. 1914; Cass., 3 aprile 1998, n. 3427.

prestazione, e non già la sostituzione di questa²⁸, per la cui validità non sarebbero quindi più necessari gli indicati requisiti.

Accertata quindi la capacità solutoria dei nuovi strumenti, occorre ora affrontare il diverso problema dell'accertamento del momento in cui avviene l'estinzione dell'obbligazione, rispetto al quale vengono in genere richiamate le norme in materia di trasferimenti elettronici di fondi: così, portando come esempio quello del pagamento mediante carta di credito, può essere stabilito il momento dell'addebito nel conto del mandante, quello dell'accredito sul conto del beneficiario, oppure quello dell'invio dell'estratto conto al beneficiario²⁹.

Di fondamentale importanza, a fronte dell'immediatezza con cui vengono instaurati i rapporti giuridici nel nuovo mercato del commercio elettronico, sono poi i precisi obblighi di informazione dell'utente che gravano in capo a chi offre i servizi in Rete, previsti esplicitamente dalle recenti produzioni normative emanate a disciplinare il settore. Ad essi è infatti dedicata l'intera sezione II della già ricordata Raccomandazione 97/489/CE, relativo alle operazioni mediante strumenti di pagamento elettronici, e gli artt. 3 e 8 d. lgs. n. 185 del 1999, che recepisce la direttiva 97/7/CE in tema di tutela del consumatore in materia di contratti a distanza³⁰.

Per quanto riguarda invece la responsabilità per inesecuzione, inesatta esecuzione o per operazioni non autorizzate nei pagamenti elettronici, anche in questo caso soccorrono diverse norme, pur se non dettate specificamente per i sistemi di pagamento su Internet, ma a questi certamente adattabili. Si vedano in particolare la sezione III della Raccomandazione 97/489/CE e l'art. 8 d. lgs. n. 185 del 1999.

Con riferimento proprio a questi due ultimi argomenti, l'obbligo di informazione dell'utente, e le responsabilità in caso di non adeguato funzionamento del sistema, rimangono aperti i problemi relativi al coordinamento, non limitato al tema trattato nel presente scritto, tra le esigenze di identificazione dei soggetti che utilizzano tali strumenti per attività

²⁸ Quindi il debitore pagando con mezzi telematici eseguirebbe esattamente la prestazione dovuta, e non una sua sostituzione (così, G. Ilnocchiaro, *Il problema dei mezzi di pagamento*, cit., p. 121).

²⁹ A tale proposito, v. F. De Vescovi, *Titoli di credito e informatica*, Padova, 1991.

³⁰ Sul punto, v. A. Stracuzzi, *Il commercio elettronico e l'impresa*, in *Il Sole 24 Ore* Ed., 1999, p. 92, e G. Ilnocchiaro, *op. cit.*, p. 126.

commerciali, con le speculari esigenze di riservatezza degli stessi: problemi che si sono visti anche con riferimento alla stessa ammissibilità di sistemi forti di crittografia asimmetrica e di firma digitale, e che risultano ancora oggetto delle riflessioni degli studiosi della materia, in attesa di una loro soluzione.

Da non trascurare, infine, i profili penalistici legati all'uso dei nuovi strumenti, in genere riconducibili alle problematiche del riciclaggio del denaro, all'evasione fiscale, al gioco di azzardo, ed alla possibilità di costituire a loro volta oggetto di frodi. Problemi che comunque un attento studio delle fattispecie indicate può benissimo portare a superare: ad esempio, per il riciclaggio del denaro proveniente da reati, attività che potrebbe avvenire attraverso i sistemi di pagamento automatizzati, in ogni caso si riuscirebbe a controllarne l'utilizzo e ad impedirne lo sfruttamento a tali fini nel momento della conversione dalla moneta elettronica dallo stato virtuale di *cyberdollar* in moneta reale.

6. CONCLUSIONI

Come si è visto, i pur rilevanti problemi giuridici del pagamento attraverso strumenti elettronici non sembrano costituire un serio ostacolo allo sviluppo di tali mezzi di adempimento delle obbligazioni pecuniarie sulla rete Internet: una seria analisi del fenomeno, soprattutto dal punto di vista delle applicazioni concrete, permette infatti di ricondurre le nuove modalità nell'alveo della disciplina giuridica tradizionale.

Neanche dal punto di vista della tecnologia, che deve svolgere l'importante compito di assicurare la fiducia degli utenti del commercio elettronico, sembrano sorgere seri impedimenti a tale sviluppo: i nuovi sistemi infatti, anche se continuamente messi alla prova dai soggetti che per lavoro o per divertimento tentano di violarli, grazie in particolare alle tecniche di crittografia ed alla facile reattività delle stesse allo svilupparsi della conoscenza nel settore, permettono di garantire la sicurezza delle transazioni on-line.

Resta allora solo la convinzione degli utenti (intesi in senso ampio, quindi non solo gli acquirenti di beni o servizi, ma anche i venditori degli stessi) ad iniziare effettivamente ad usare tali nuove modalità di commercio: sia dei fornitori, che devono cominciare ad investire nell'e-commerce, proponendo offerte di prodotti e servizi in linea con le peculiarità del

nuovo *media*, sia dagli utenti/clienti (quindi utenti in senso stretto), che devono innanzitutto utilizzare le nuove tecnologie, e poi utilizzarle in maniera consapevole sulla base di un'acquisita cultura delle stesse. Aspetti che permettono comunque un certo ottimismo, a fronte del sempre crescente interesse per Internet e per il fenomeno del commercio elettronico, oggi sostenuto da più o meno adeguati interventi a livello economico e normativo.

Profilo tributario delle vendite *on-line* di beni e di servizi

UMBERTO RAPETTO¹, UGO POGGI

SOMMARIO: 1. *Fisco e Web. Premessa. La neutralità fiscale del Web. La bit-tax* - 2. (continua) *Il commercio elettronico diretto ed indiretto* - 3. (continua) *Il tempo ed il luogo della conclusione del contratto* - 4. *Principi generali. Cyberspazio: quale sovranità fiscale* - 5. (continua) *La stabile organizzazione* - 6. (continua) *Il concetto di residenza* - 7. (continua) *L'imposizione diretta ed indiretta* - 8. (continua) *Il controllo sugli adempimenti fiscali* - 9. (continua) *I diritti di confine.*

1. FISCO E WEB. PREMESSA. LA NEUTRALITÀ FISCALE DEL WEB. LA BIT-TAX

La diffusione ma, soprattutto, la sempre maggior quota di mercato che il commercio elettronico sta occupando hanno evidenziato Internet come una rete flessibile, capace di adattarsi sia alle esigenze di intercomunicabilità aziendale, sia alle necessità ed alle opportunità di diffusione del prodotto nei confronti del mercato.

Con la rapidità che connota la costante crescita dell'informatica, Internet ha consentito un costante sviluppo dell'*e-business*, degli affari in tempo reale (si pensi che in base ad una recente ricerca, su 1.5 milioni di italiani che navigano sulla Rete la percentuale di chi acquista *on-line* è di circa il 25%).

Ciò che più rileva però è il fatto che ha consentito altresì la nascita di un commercio "anonimo" dal punto di vista fiscale ingenerando un forte pericolo di evasione, anche tenuto conto del fatto che al giorno d'oggi pochi sono stati gli sforzi per una specifica regolamentazione, sia per il mantenimento dell'imposizione diretta ed indiretta, sia per l'acquisizione di possibilità di controllo da parte degli Organi della polizia tributaria.

A fronte di un utilizzo sempre più diffuso della Rete, pur evitando di comprimere quelli che ormai sono indiscussi diritti, rimane pertanto fuori di ogni dubbio la necessità a breve del fatto che vengano imposte re-

¹ rapetto@aipa.it

gole le quali disciplinino i comportamenti degli utenti dovendosi dare riscontro, indirizzo e contezza a questi anche dal punto fiscale.

Linee guida per lo sviluppo di una politica fiscale sull'*e-business* sono tutt'oggi in fase di evoluzione, spaziandosi da posizioni liberali a posizioni restrittive. Tra queste ne emergono due: 1) la neutralità fiscale del *Web*; 2) la *bit-tax*.

La prima delle due è richiamata in un documento del Tesoro statunitense (consultabile nel sito www.finanze.it) e riporta una tesi tipica di quel sistema liberale. Secondo quest'ultimo nell'imposizione delle transazioni ci si dovrebbe comportare in maniera tale da non considerare il mezzo attraverso il quale le stesse avvengono, ovvero *sia tamquam non esset*. Avverrebbe in tale ipotesi una parificazione tra l'uso della Rete e di qualsiasi altro mezzo di comunicazione.

La tesi che sembrerebbe di facile applicazione (e d'altronde chi potrebbe negare che sembra cosa abbastanza simile un contratto concluso via *fax* ed il contratto sottoscritto tramite *Web*), si potrebbe prestare ad una facile diffusione, ma, tuttavia, non coglie a pieno alcuni presupposti e soprattutto la necessità di dare una "fisicità" o meglio una soggettività al proprio interlocutore ai fini dell'imposizione.

Se dei concetti di residenza e di stabile organizzazione si tratterà più avanti, viene spontanea comunque fin d'ora la considerazione dell'individuazione di obblighi fiscali e comunque di certezza del diritto applicabile in capo ai soggetti terzi con i quali si opera.

In tale maniera, senza con ciò voler decretare inapplicabile la tesi sulla neutralità del *Web*, che, peraltro, come detto, promana da un'autorevole fonte, si ritiene che la tesi potrebbe avere un ambito territoriale di applicazione diverso da quello italiano.

Con uno spirito più europeo, nata forse dal desiderio di definire un sistema di regole certo e vincolante per tutti gli utilizzatori della Rete, si presenta la seconda tesi, quella della cosiddetta "*bit-tax*", proposta da un gruppo di esperti indipendenti istituito dalla Commissione Europea. La stessa, indubbiamente, come riportato nel testo della sua diffusione, ha ingenerato incredulità e sostanzialmente rifiuto.

Il novello "mostro fiscale di Loch Ness" (come i suoi contestatori la hanno definita) ha la sua principale argomentazione nella previsione dello spostamento dei consumi dai beni tangibili ai beni intangibili e

quindi del criterio di tassazione sui *bit* ricevuti (unità di misura degli stessi). Tale postulato, che comporta secondo il gruppo di studio un **cambiamento della base impositiva**, argomenta l'aspetto della non neutralità dei differenti sistemi di distribuzione e comunicazione. Il Professor Soete, responsabile del gruppo di studio, **approfondendo a tal proposito specificatamente la parte riguardante il valore aggiunto (VAT od IVA) conclude affermando come "in generale si possa dire che per come sono attualmente configurati i metodi di prelievo fiscale sulla distribuzione di beni e servizi dei governi è probabile che le reti elettroniche porteranno sistematicamente ad un calo del livello di imposizione e di riscossione delle tasse"**.

Ma, se pur è vero che la principale imposta applicata su produzione e consumi, nei Paesi dell'Unione Europea, è l'imposta sul **valore aggiunto** (di facile **applicazione e calcolo nelle intermediazioni di beni materiali**), e se pure **corrisponde al vero che si ha un diverso valore aggiunto nella produzione se ad esempio si utilizzano i canali normali di comunicazione od i canali informatici** (si pensi alla **richiamata spedizione affrancata di una fattura con francobollo od alla spedizione della stessa via posta elettronica**), di **dubbia applicazione, se non interpretazione**, rimane la proposta di tassazione dell'informazione ricevuta **tramite la Rete**.

La tassazione dell'informazione ricevuta **elettronicamente** (misurabile come detto attraverso il numero dei *bit*, da cui la "*bit-tax*" prende il nome) presenta infatti alcune gravi lacune nel suo impianto.

Lo stesso professor Mario Monti, della **Direzione della fiscalità della CEE**, se ne dissocia, sottolineando come la stessa si distacchi dai principi elementari della fiscalità. Questi ultimi infatti pretenderebbero che "oggetto dei tributi sia sempre e soltanto una **manifestazione di ricchezza** o comunque di **capacità contributiva** (acquisti, vendite, possesso di un reddito o di un patrimonio ecc.)". Considerando dunque come non ogni utilizzo della Rete sia effettuato per i fini su richiamati avendo solo alcuni tipi d'informazione un effettivo **valore economico**, ulteriori perplessità sorgono sull'opportunità di una tassazione che **diverrebbe effettivamente priva di capacità discriminante** con riferimento a quale flusso di dati debba essere oggetto di tassazione e quale no.

Paese a tal proposito la possibilità di tassare **flussi d'informazioni privi di valore e che non producono reddito** (ad esempio le *e-mail*), come l'incapacità di distinguere sul **valore economico dei beni scambiati**.

Si tralasciano, a fronte delle precedenti considerazioni, le valutazioni sugli effetti "ecologici" secondari che il professor Soete effettua sulla *bit-tax*, significando come una tassazione del *bit* possa ridurre la congestione informatica e la quantità di "spazzatura" e di informazioni irrilevanti trasmesse. La stessa, che limiterebbe la diffusione dell'informazione, sarebbe di per sé stessa anche contraria allo spirito che ha animato la nascita della Rete quale autostrada informatica vettore di notizie (non necessariamente utili dal punto di vista economico), potenzialmente capaci di raggiungere ogni utente.

In conclusione, se si può affermare che l'individuazione di un quadro fiscale per il commercio elettronico è tuttora in corso, si segnala come l'unica presa di posizione sull'argomento in via ufficiale da parte di uno Stato sia quella degli Stati Uniti che il 21 ottobre 1998 hanno fatto entrare in vigore l'*Internet tax freedom act*, con il quale s'impone una moratoria che blocca ogni pretesa impositiva per tre anni.

Ma di fatto si tratta di una non-posizione.

2. (CONTINUA) IL COMMERCIO ELETTRONICO DIRETTO ED INDIRETTO

Iniziando ora ad approfondire quelli che sono i presupposti di fatto per poter parlare di tassazione dell'*e-business*, si rende necessario effettuare una distinzione tra il commercio elettronico diretto e quello indiretto.

È opportuno a tal fine, precisare ciò che è il fulcro del commercio elettronico e cioè la possibilità di effettuare transazioni via elettronica.

Le transazioni attraverso il *Web* possono riguardare acquisti di beni materiali o beni immateriali, così come beni che possono essere fruiti o ceduti direttamente *on-line* (caso paradigmatico è a tal proposito quello dell'ascolto di riproduzioni musicali o della visione di fotografie) oppure beni la cui consegna non può essere perfezionata via telematica, ma necessitano di una successiva consegna fisica attraverso i canali tradizionali (è questo il caso dell'acquisto di un libro da libreria virtuale). E così in seguito ad un ordine effettuato via *Web*, cui seguirà una "consegna" telematica parleremo di commercio elettronico indiretto (*off-line*), mentre allorquando la consegna seguirà i richiamati canali tradizionali saremo di fronte ad un esempio di commercio elettronico diretto (*on-line*).

Però, se pur è vero che il commercio elettronico, elidendo distanze tra produttori e consumatori, consente **transazioni commerciali** senza soluzione di continuità prescindendo dai confini geografici e sfruttando al meglio tutte le potenzialità del mercato globale, è anche tuttavia vero che analizzando le fattispecie dal punto di vista tributario risulta evidente come soprattutto il commercio elettronico indiretto possa essere considerato "invisibile" al Fisco i cui principi non possono trovare facile applicazione nel cyberspazio.

Ovvio d'altronde che la già difficile identificazione degli operatori economici che operano nell'*e-busines* comporta consequenzialmente una difficoltà oggettiva nell'applicazione dei metodi di prelievo sulla distribuzione di beni e servizi. Il calo della **tassazione locale**, già verificatosi oltremare, sarà connesso pertanto sia con la difficoltà dell'applicazione di concetti alla nuova realtà, sia con la conseguente difficoltà nel controllo.

3. (CONTINUA) IL TEMPO ED IL LUOGO DELLA CONCLUSIONE DEL CONTRATTO

E se una società francese acquistasse un pezzo di ricambio, tramite un *server* canadese, da un cantiere navale che negli Stati Uniti si occupasse di **aggiustare una barca** della società francese all'ancora nei pressi del canale di Panama?

La definizione del tempo e del luogo della conclusione del contratto pur avendo senza dubbio una maggiore importanza per un'analisi di tipo civilistico, che consenta l'approfondimento di punti rilevanti ai fini del dispiegamento delle conseguenze dell'atto stipulato, ha tuttavia una sua valenza anche sotto il profilo tributario. Si pensi ad esempio alla **cessione di software** direttamente dalla Rete. A seconda di quando si considera avvenuto il passaggio della proprietà (cioè se al momento della spedizione, al momento della consegna o al momento della soddisfazione di un'eventuale clausola di gradimento), saranno conseguenti momenti diversi per l'obbligo di fatturazione. Alle nozioni richiamate, infatti, le singole normative riguardanti i diversi settori impositivi ricollegano il momento dell'effettuazione di determinati obblighi fiscali quali l'obbligo di fatturazione, l'obbligo della tenuta e conservazione della contabilità, la registrazione delle operazioni ecc. Si ritiene pertanto proficuo un richiamo seppur schematico e riepilogativo agli stessi.

Con riferimento al tempo della conclusione delle transazioni commerciali via Internet si deve premettere che anche in questo caso non si deve fare riferimento alla normativa speciale, ma si possono applicare le norme del codice civile.

Pertanto il contratto stipulato si potrà ritenere concluso allorquando, ex art. 1326 c.c., "chi ha fatto la proposta ha conoscenza dell'accettazione dell'altra parte" ed inizierà a dispiegare i suoi effetti, ex art. 1334, "dal momento in cui pervengono a conoscenza della persona cui sono destinati".

Per quanto concerne la presunzione di conoscenza si applicherà il successivo art. 1335 c.c., che prevede una presunzione semplice per cui "la proposta ... ed ogni altra dichiarazione diretta ad una determinata persona si reputano conosciute al momento in cui giungono all'indirizzo del destinatario, se questi non prova di essere stato, senza sua colpa, nell'impossibilità di averne notizia".

Si tralasciano al momento le considerazioni (che comporterebbero i richiamati approfondimenti di diritto civile) sul concetto di indirizzo del ricevente o sui contratti stipulati *on-line* direttamente a mezzo *computer* con la compilazione dei moduli inseriti nel sito d'interesse.

La definizione del luogo di conclusione del contratto si presta ad altre considerazioni importanti dal punto di vista tributario in quanto hanno estrema importanza al fine della determinazione della legge da applicare al rapporto soprattutto in considerazione di eventuali rapporti internazionali. Se d'altronde, sempre in considerazione della particolarità della nuova materia e dell'effettiva difficoltà di conciliare il nuovo istituto con le tecnologie ad esso correlate, non esiste tuttora una capacità sicura di stabilire un luogo di conclusione del contratto (si pensi a chi attraversando il confine in treno si collega con il *provider*), si può ciò nondimeno tentare di stabilire una regola di massima.

Ancora una volta è d'aiuto il mutuare della disciplina dal campo civilistico, dove si ritiene che il contratto sia concluso nel luogo ove il proponente ha notizia dell'accettazione. Ma se, come visto, tale luogo non è sempre identificato né identificabile, si può ritenere che solo in tale occasione possa sopperire nei casi dubbi il luogo dal quale il soggetto "scarica" l'informazione e cioè il *provider*. Sarà dunque in base alla determinazione della località ove tale *provider* ha sede che si riterrà come luogo

ove il contratto è stato concluso dovendosi considerare in tale occasione quest'ultimo come domicilio del contraente.

Sempre con riferimento al necessario adattamento che il commercio elettronico ha comportato nel settore tributario, si ritiene utile in conclusione fare anche un richiamo a quella che è la conseguenza normale della stipula di tali contratti e cioè alla conservazione delle risultanze contabili.

Si fa nello specifico riferimento alla modifica apportata all'art. 2220 c.c. dalla legge n. 489 del 1994 dettata in tema di conservazione su supporti di immagini delle scritture e dei documenti contabili.

La nuova novella dell'articolo, come noto, ha imposto l'obbligo di conservare "le fatture, le lettere e i telegrammi ricevuti e le copie delle fatture, delle lettere e dei telegrammi spediti" per un periodo di dieci anni dalla data dell'ultima registrazione. Sulla base di tale disposizione il comma 3 prevede che le scritture ed i documenti rilevanti ai fini delle disposizioni tributarie possano essere conservati sotto forma di registrazioni su supporti di immagini.

Orbene alla luce del fatto che l'apposito decreto ministeriale disciplinante la materia *de qua* non risulta al momento ancora emanato, è opportuno sottolineare il fatto che le transazioni avvenute necessitano al momento (seppur siano già "informatizzate" come nel caso del commercio *on-line*) un riscontro fisico sull'originale.

Possibilità di microfilmatura esistono al momento per le sole fatture e le bollette doganali ricevute, le fatture emesse nonché per le note di credito o di debito.

4. PRINCIPI GENERALI. CYBERSPAZIO: QUALE SOVRANITÀ FISCALE

Come noto Internet nacque quale sviluppo di una Rete militare (ARPANET) collegante elaboratori della Difesa, imprese operanti nel medesimo settore ed Istituti universitari deputati alla ricerca. Una delle caratteristiche fondamentali della stessa era l'essere priva di un nodo principale, in maniera tale che in caso di attacco non potesse essere paralizzata a séguito di distruzione fisica. In caso di distruzione di una linea di connessione, non essendovi necessità per i messaggi scambiati di viaggiare lungo una strada predefinita, non si sarebbe pertanto interrotta la possibilità di comunicazione.

Il successivo sviluppo civile della Rete, seguito secondo il medesimo schema, ha fatto sì che mancasse un soggetto di diritti esclusivi od un accordo tra Stati valido e recepito che consentisse di configurare una sfera giuridica per Internet. Ma se i moderni ordinamenti devono esplicitare una sovranità affinché un controllo su persone e cose sia effettivo e non sfuggente, come sarà possibile applicare un limite a ciò che è stato costruito per esserne privo?

Infatti i dati, come detto, non hanno un tracciato definito e possono trovare una via di comunicazione a mezzo di milioni di diverse interconnessioni e dunque di strade. Non esiste pertanto un soggetto che sia portatore di diritti esclusivi in base a legge statale o meglio ancora ad accordo internazionalmente valido e recepito nella legislazione interna.

Il cyberspazio, così come lo intendiamo, è dunque privo della dimensione autoritaria che è propria di un ordinamento e quindi è da considerarsi uno spazio senza sovranità.

Se dunque la sovranità è escludibile non potendovi essere un controllo che sia di competenza di un Ente sovrano, effettuando una similitudine, si potrebbe cercare di ricondurre il fenomeno Internet alla disciplina delle telecomunicazioni. In tale disciplina non potendosi controllare le trasmissioni mentre viaggiano nell'etere, attraversando i confini e gli spazi sottoposti a sovranità, si è provveduto a controllare le stazioni di partenza o di arrivo.

Se anche le informazioni, le volontà ed i dati viaggiano liberi attraversando spazi sovrani e confini, le stesse (puri fenomeni fisici, *bit*, all'atto del trasferimento) devono al termine del loro percorso riacquistare consistenza e manifestarsi. Sarà pertanto quello il momento in cui assumeranno un valore dal punto di vista giuridico iniziando a produrre effetti.

Riferendosi alla situazione specifica si dovrebbe pertanto effettuare un controllo su quelli che sono i punti in cui le richiamate informazioni-volontà hanno il loro punto di partenza e di arrivo e cioè dove hanno la loro valenza legale: i cosiddetti *servers*.

Questi ultimi sono elaboratori elettronici capaci di immagazzinare e scambiare informazioni attraverso la mediazione di una rete telefonica e di un *modem* consentendo all'utente di accedere alle informazioni ed ai servizi della Rete.

Si giunge dunque così alla sovranità fiscale, che di fatto è quella che rileva ai fini dell'imposizione. Ma proprio a tal proposito bisogna precisare in via preliminare che ciò che rileva per l'esercizio del potere impositivo non è esclusivamente il limite geografico dato dal territorio, che pure di per se stesso sarebbe definito con l'individuazione della collocazione geografica del *server*. Seguendo tale criterio (che si rammenta poter essere un solo indice e non un elemento essenziale) si faciliterebbe la possibilità di evadere le imposte unicamente collocando quest'ultimo nei cosiddetti paradisi fiscali.

Il carattere "ultraterritoriale" delle norme tributarie e cioè la possibilità di disciplinare fatti avvenuti in territorio estero ma che manifestano comunque un determinato collegamento con lo Stato, consente *de relato* l'applicazione delle stesse anche a fatti avvenuti al di fuori del territorio nazionale. Nel caso specifico la determinazione dei criteri di collegamento (siano essi di natura reale o personale) consente una vera e propria estensione della legge nello spazio e, per tale ragione, potranno essere riferiti anche a determinati soggetti passivi sedenti all'estero la conclusione di atti rilevanti ai fini dell'imposizione.

In conclusione sarà possibile affermare che se anche non è dato conoscere la sovranità di ciò che è comunemente chiamato cyberspazio, ai fini della determinazione della sovranità fiscale incombente sugli atti compiuti da un soggetto che opera nello stesso è possibile determinare criteri che consentano di collegare ad obblighi impositivi.

In considerazione delle premesse sopra effettuate, ciò che comporterà criterio di collegamento reale di un soggetto con il territorio sarà l'esistenza di una stabile organizzazione nello stesso (cfr. art. 20 Tuir, lett. e - v. *infra* -) mentre il criterio di collegamento personale ai fini della determinazione dell'appartenenza di un contribuente ad un determinato sistema impositivo sarà dato dalla residenza fiscale.

APPARTENENZA DI UN CONTRIBUENTE A UN SISTEMA IMPOSITIVO

● CRITERIO DI COLLEGAMENTO REALE

—————> Stabile organizzazione nel territorio

● CRITERIO DI COLLEGAMENTO PERSONALE

—————> Residenza fiscale

5. (CONTINUA) LA STABILE ORGANIZZAZIONE

Strettamente connesso con il concetto di residenza, e tra i tanti interrogativi che le transazioni commerciali nella Rete pongono con riferimento al cosiddetto reddito *internet-based* ed alla determinazione del regime fiscale da applicare al reddito d'impresa scaturente, è senza dubbio quello sulla stabile organizzazione.

Come noto molti dei siti presenti in Rete offrono la possibilità di effettuare transazioni commerciali che si possono concretizzare indifferentemente in cessioni di beni o prestazioni di servizi. Tali transazioni avvengono tramite i cosiddetti *server*, localizzabili ovunque. Orbene come bisogna valutare le funzioni che il soggetto economico deve esercitare a mezzo del *server* o meglio del sito ivi presente?

Ordini, pagamenti di commesse, diffusione della pubblicità non sono altro che funzioni svolte a mezzo dello stesso e che servono ad inquadrarne la centralità.

Se, come detto nel nostro ordinamento, un soggetto non residente che trasferisce nel territorio nazionale la sua sede legale acquista una delle caratteristiche che lo rendono soggetto passivo d'imposta essendo "fiscamente residente", è altrettanto vero che affinché questi abbia anche una stabile organizzazione occorre sicuramente un *quid pluris*.

Sulle modalità per definire la stabile organizzazione nell'*e-commerce*, dalla dottrina sono state identificate alcune casistiche. Le stesse che al momento non hanno avuto riscontro legislativo, né tantomeno giurisprudenziale, risultano nella loro formazione (si veda l'allegato riquadro) tuttavia lacunose e spesso non prontamente applicabili.

La stabile organizzazione

- **"fixed place of management"**. È forse il caso più semplice, scolastico. In base allo stesso si ha stabile organizzazione laddove vi sia sede fissa d'affari nel Paese estero. Rapportando ciò alla presenza dei *server*, attraverso cui avvengano tutte quelle funzioni sopra richiamate, in un Paese straniero si potrebbe riuscire ad affermare che si ha stabile organizzazione di un soggetto economico laddove lo stesso abbia il luogo dove di fatto avvengono le transazioni. Ne deriverebbe una soggettività fiscale del soggetto economico. L'OCSE per il verificarsi di questa circostanza fissa tre parametri: 1) l'esistenza di un luogo fisico adibito a sede di affari; 2) la condizione di una durata nella permanenza dello stesso; 3) lo svolgimento dell'attività a mezzo della sede.

- **“agency clause”**. È il caso dell'agente commerciale. Il fattore decisivo per determinare nello specifico l'esistenza di una **stabile organizzazione sul territorio** ove opera l'agente risiederebbe nella dipendenza o, viceversa, indipendenza, dello stesso rispetto al Paese ove ha sede la società mandante. Qualora infatti l'agente abbia indipendenza dalla società mandante pur avendo il potere d'impegnarla, non si avrà **stabile organizzazione** mancando il vincolo determinante della subiezione e quindi si tratterebbe di una stabile organizzazione a carattere personale.
- **“construction clause”**. È questo in verità un criterio mutuato principalmente dall'edilizia e si basa sul periodo di tempo di sedenza dell'attività dell'azienda sul territorio.

Al di là delle considerazioni dottrinali effettuate, si sottolinea ancora una volta come di fatto manchi una definizione normativa. Rifacendosi alla definizione maggiormente accreditata (a quella promanante dal Comitato degli affari fiscali dell'OCSE, cui si rifanno le convenzioni stipulate tra Italia e Stati stranieri) si può affermare che per stabile organizzazione debba intendersi quantomeno “un centro di attività che abbia consistenza minima, data dalla presenza permanente dei mezzi umani e tecnici necessari”.

Anche in tale ipotesi si osserva come appaia un'interpretazione eccessivamente estensiva quella che considera un sito od il *server* utilizzato quali stabili organizzazioni. Sarebbe forse più opportuno confessare che al momento il concetto di stabile organizzazione nell'ambito dell'e-business sia pressoché inapplicabile, avendosi con ciò riflessi sulle norme del sistema fiscale italiano che la prevedono (cfr. art.113, comma 1, e art. 118, comma 1, lett. c, del Tuir che estendono le norme di determinazione del reddito d'impresa ai soggetti non residenti con stabile organizzazione).

ELEMENTI NECESSARI AI FINI DELLA STABILE ORGANIZZAZIONE

- SEDE FISSA

AMBITO TEMPORALE

- ◇ permanenza per periodo determinato

AMBITO TERRITORIALE

- ◇ elemento soggettivo volitivo
- ◇ elemento oggettivo di localizzazione

- NECESSITÀ CHE L'ATTIVITÀ SIA SVOLTA TRAMITE INTERNET

6. (CONTINUA) IL CONCETTO DI RESIDENZA

Altro fattore importante da stabilire per definire la tassazione del commercio elettronico è quello consequenziale inerente alla residenza fiscale. Il nuovo tipo di commercio porta infatti con sé la tendenza di un concetto di tassazione ancorato, piuttosto che sulla fonte di reddito, sulla residenza; e se tale spinta verrà confermata a livello legislativo, sarà opportuno modificare le attuali definizioni delle norme fiscali.

In alcune delle transazioni virtualmente "anonime", come quelle che avvengono nella Rete, sicuramente difficoltoso è l'accertamento della sede dell'amministrazione ai fini dell'individuazione della residenza fiscale della società operante. Come stabilire, infatti, tra siti virtuali e server posizionati indifferentemente in varie nazioni, quale sia il luogo ove "l'attività di gestione si svolge e nel quale vengono a convergere le volontà delle persone che formano la società?"

Soccorre in ciò il già richiamato Comitato degli affari fiscali dell'OCSE, divenuto punto di riferimento nella materia *de qua*, che definisce residente in uno Stato membro colui che in forza del suo domicilio, della sua residenza, della sede della sua direzione o in base ad altri criteri, è soggetto d'imposta di detto Stato.

Tralasciando quelli che sono i criteri che non possono prestarsi a dubbie interpretazioni, poiché formati in base a dati di fatto, rimane da analizzare il criterio che si basa sull'individuazione della "sede della direzione".

Quest'ultima, che consiste nel luogo ove effettivamente viene svolta l'attività, e pertanto serve già di per sé a definire i casi di doppia residenza, può essere mutuata dal diritto civile. Gli articoli 46 c.c. (sedi delle persone giuridiche), 2197 c.c. ("sedi secondarie"), 2505 c.c. ("società costituite all'estero con sede nel territorio dello Stato"), e 2506 c.c. ("Società estere con sede secondaria nel territorio dello Stato"), che completano il quadro legislativo richiamato, presuppongono infatti l'effettuazione di particolari attività, quali ad esempio la convocazione di assemblee o l'iscrizione all'Ufficio delle imprese. Ma, ancora una volta, il presupposto per una identificazione materiale, non basata cioè su dati formali, è dato dal nodo della stabile organizzazione. È proprio su ciò che la dottrina più accreditata fa convergere la discriminante *de qua*, ponendo l'accento cioè su considerazioni materiali.

7. (CONTINUA) L'IMPOSIZIONE DIRETTA E INDIRETTA

Venendo ora al vero *core-business* (dal punto di vista fiscale) dell'*e-commerce*, occorre analizzare l'applicazione delle più importanti imposte allo stesso. È da premettere però a tale trattazione che poco o nulla è stato disposto dal legislatore per regolamentare lo specifico settore. Un tentativo, peraltro ancora in fase di gestazione, è contenuto nel disegno di legge (atto Senato n. 3264) presentato e giacente in Parlamento che prevede un regime fiscale preferenziale per le transazioni telematiche sviluppatesi via Internet, oltre che agevolazioni per gli investimenti in *hardware* e *software*.

Imposte sui redditi

Con riferimento alle II.DD. è necessario innanzi tutto porre l'attenzione sulla tassazione in Italia del reddito d'impresa prodotto *off-line* da operatore commerciale straniero.

Il commercio elettronico indiretto, che ne deriverà, "non sarà sottoposto a tassazione".

Infatti alla luce dell'art. 20, comma 1, lett. e, D.P.R. 22 dicembre 1986, n. 917, se è vero che "ai fini dell'applicazione dell'imposta nei confronti dei non residenti si considerano prodotti nel territorio dello Stato ... i redditi di impresa derivanti da attività esercitate nel territorio dello stato mediante stabili organizzazioni", argomentando *a contrario* ne deriva che la società straniera, che non abbia stabile organizzazione nel nostro territorio, ma effettui le proprie transazioni virtuali direttamente dall'estero, non sia soggetta d'imposta.

Spontanea e segnalata da tutta la dottrina, la possibilità di residenze di comodo per gli operatori dello specifico commercio, i quali, disponendo di un solo punto d'appoggio per il recapito della corrispondenza telematica e documentale, possano sottrarsi alle leggi d'imposta semplicemente indicando sul proprio sito un recapito estero.

Per il discorso contrario (cioè quello di un soggetto residente con stabile organizzazione che commerci via Internet dall'Italia verso l'estero) varrà la tassazione dei redditi prodotti ed a tal proposito dovrà essere posta attenzione alle norme convenzionali che regolano il fenomeno delle doppie imposizioni, al fine di evitare che lo stesso reddito venga assoggettato a tassazione anche laddove il bene virtuale viene fornito.

Imposta sul valore aggiunto

Se è vero che a livello comunitario l'IVA è l'imposta che maggiormente è stata armonizzata bisogna comunque ammettere che tuttora esistono aliquote diverse nei Paesi UE.

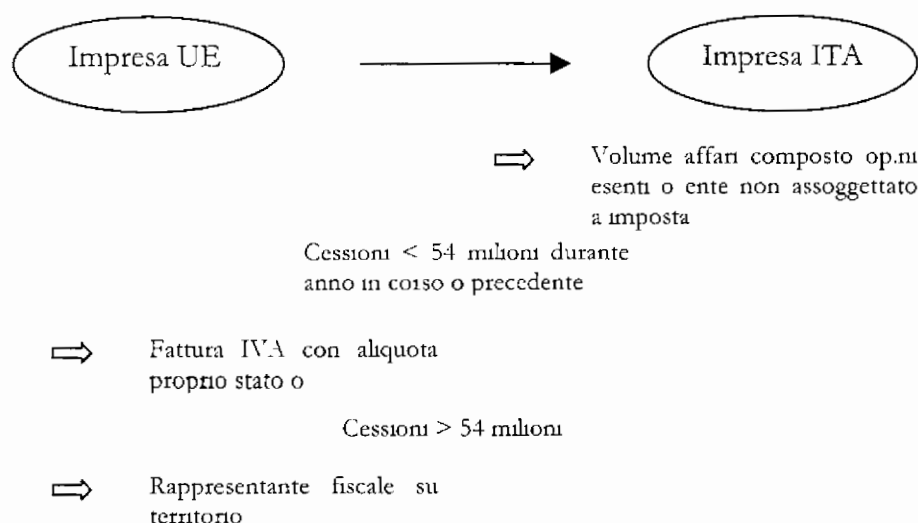
Il pericolo che un commercio che non conosce confini porti a creare danni ingiusti alle imprese operanti negli Stati con aliquota maggiore, ha condotto ad accettare normativamente o convenzionalmente che il luogo di tassazione sia nel Paese ove avviene il consumo finale del bene.

Definiamo ora l'applicazione dell'imposta nei casi di commercio elettronico indiretto e commercio elettronico diretto:

a) Commercio elettronico diretto

Come già ricordato (v. § 1) è il caso in cui la Rete non serve per la consegna del bene, ma la stessa deve essere perfezionata separatamente seguendo i canali tradizionali; in questo caso, se la transazione avviene tra soggetti residenti in Stati appartenenti all'Unione Europea si rende applicabile la normativa in materia di IVA intracomunitaria e, in particolare, quella relativa all'acquisto di beni a distanza, in base a cataloghi, per corrispondenza o simili. La tassazione del bene oggetto dello scambio avverrà nel Paese di origine o in quello di destinazione a seconda dei casi.

Si richiamano nello specifico le disposizioni di cui all'art. 40, commi 3 e 4, lett. b, e dell'art. 44, comma 4, d. lgs. 30 agosto 1993.



b) commercio elettronico indiretto

Il questo caso il perfezionamento della transazione economica avverrà via telematica con la consegna del bene virtuale via elettronica.

Seguendo ancora una volta l'orientamento del Comitato per gli affari fiscali dell'OCSE dovremo nel caso inquadrare la fattispecie come un caso di prestazione di servizio.

Si ricadrebbe nella fattispecie prevista dall'art. 7 D.P.R. n. 633 del 1972, per cui "le prestazioni di servizi si considerano effettuate nel territorio dello Stato quando sono rese da soggetti che hanno il domicilio nel territorio stesso o da soggetti ivi residenti che non abbiano stabilito il domicilio all'estero, nonché quando sono rese da stabili organizzazioni in Italia di soggetti domiciliati e residenti all'estero".

SOFTWARE STANDARD E SOFTWARE PERSONALIZZATO

È opportuno effettuare una differenziazione, ai fini fiscali, tra il *software standard* e quello personalizzato. Mentre il primo viene considerato un bene materiale, il secondo - in base ad un precedente dato dall'autorità doganale britannica - è stato considerato una prestazione di servizio.

In considerazione di quanto esposto.

- ai fini dell'IVA intracomunitaria in caso di cessione di *software standard* ci si troverà innanzi ad una comune cessione di bene da registrarsi sul registro delle vendite o degli acquisti, mentre in caso di *software personalizzato* si farà riferimento all'art. 4, lett. d, D.P.R. n. 633 del 1972. Grazie a quest'ultimo infatti il *software personalizzato* è equiparabile alla materia protetta dalla legge sul diritto d'autore, per cui se il cessionario non avrà un rappresentante fiscale sul territorio nazionale che adempia gli obblighi imposti dalla legge, l'acquirente dovrà emettere auto-fattura.
- di fronte ad un importazione effettuata da cedente extracomunitario, concordemente a quanto affermato dalla circolare ministeriale 142/D, "per i supporti informatici contenenti programmi per elaboratore prodotti in serie - *software standard* - concorre a formare il valore imponibile anche quello dei dati e delle istruzioni in esso contenuti" oltre che "il valore dei beni importati determinato ai sensi delle disposizioni doganali" (art. 69, comma 1, D.P.R. n. 633 del 1972 così modificato dall'art. 1, comma 1, l. 18 febbraio 1997, n. 28). Per l'importazione di *software personalizzato* si procederà ancora una volta all'auto-fatturazione commisurata al prezzo del solo supporto.

8. (CONTINUA) IL CONTROLLO SUGLI ADEMPIMENTI FISCALI

Internet, consentendo come più volte ricordato la possibilità di operare transazioni economiche nel più completo anonimato dal punto di vista materiale e dunque fiscale, si manifesta come potenzialmente pericolosa dal punto di vista contributivo. E, se tale anonimato è senza dubbio favorito dalla totale assenza di norme e di regolamentazione, il controllo necessario di tale fenomeno esplosivo e globalizzante - doveroso e necessario - risulta ancor più limitato da effettive carenze di tipo tecnico da parte degli Organismi a ciò deputati che di fatto non possiedono ancora strumentazioni capaci di un potere invasivo sufficiente.

Il problema, ovviamente, è già stato avvertito da tutte le pubbliche amministrazioni che stanno già predisponendo le opportune difese innanzi alla nuova sfida.

Ad esempio i 33 Paesi aderenti al CIAT (*Interamerican Center of Tax Administration*) hanno già previsto un sistema di scambio d'informazioni tra le amministrazioni tributarie internazionali, mentre anche il nostro Ministero delle Finanze sta predisponendo un progetto di rete Intranet che miri a neutralizzare i cyberevasori. E se l'allarme si estende sull'effettivo mantenimento della sovranità da parte degli Stati innanzi a fenomeni quali i nuovi *cyber paradisi fiscali* o le triangolazioni telematiche, viene spontaneo il chiedersi se la risposta al fenomeno debba essere di tipo tecnico (potenziamento dei sistemi tecnici di controllo) o nell'approccio diverso al problema.

Il superamento dei potenziali conflitti non potrebbe anche avvenire mediante un bilanciamento degli interessi, ossia scoraggiando l'evasione? Non si fa ovviamente riferimento ad una politica fiscale repressiva che richiederebbe nello specifico una capacità di effettuare controlli 24 ore su 24, quanto ad esempio (mutuando dalla situazione statunitense) dalla possibilità di ingenerare nell'acquirente l'interesse alla certificazione della transazione a séguito d'incentivi di carattere fiscale.

È però importante sottolineare, come giustamente ha già fatto accreditata dottrina, che nello specifico i mezzi d'indagine tecnica o le metodologie di controllo delle pubbliche amministrazioni, nella "ricerca dell'evasione virtuale", non potrebbero imporre obblighi a carico delle società *Internet provider* - di fatto meri contenitori e strumenti tecnici della trasmissione delle informazioni necessarie per l'e-commerce - o alle agenzie di certificazione. L'identificazione del sito e della successiva soggettività

tributaria sottesa dallo stesso rimarrebbero dunque ricerca dell'Organismo deputato al controllo.

9. (CONTINI A) IL CONCETTO DI RESIDENZA

Ultimo aspetto da analizzare è quello inerente ai diritti di confine; infatti in presenza di un operatore commerciale straniero, indipendentemente dal fatto che si sia in presenza di transazione classificabile come commercio elettronico diretto o commercio elettronico indiretto, il bene per giungere a destinazione deve attraversare una frontiera. Poiché le spedizioni che transitano attraverso la linea di frontiera devono assolvere i diritti doganali prima di essere consegnate, viene spontaneo domandarsi come la nuova realtà possa adeguarsi a ciò.

Per il commercio elettronico diretto, ove il bene passa la frontiera in maniera telematica giungendo dall'operatore mittente direttamente nelle mani dell'acquirente, la soluzione risiederebbe nella "buona volontà" di quest'ultimo, che per regolarizzare l'operazione, *a posteriori*, dovrebbe recarsi in dogana provvedendo a versare i diritti dovuti.

Solo a séguito di questa "spontanea presentazione" in dogana, infatti, dopo il pagamento dei diritti e dei dazi, l'operazione di acquisto si potrebbe definire perfezionata.

Nel caso del commercio elettronico indiretto (a tutt'oggi il caso più frequente) gli operatori economici a séguito di un ordine telematico spediscono, di norma a mezzo di corrieri internazionali, ai clienti la merce. Tali *partners* dei fornitori on-line curano il transito attraverso la dogana, e dunque provvedono al necessario sdoganamento. L'IIVA all'importazione e gli eventuali dazi rimangono in questo caso a carico del destinatario (che se li vedrà addebitati come costo di consegna) oppure a carico del mittente a séguito di sua espressa richiesta.

Permangono, e sono comunque preoccupanti in una visione d'insieme del problema, i problemi per il mancato gettito per le casse dell'Eranio a séguito della spedizione della merce ordinata attraverso i canali ordinari postali.

Il problema prima che essere di carattere operativo (sulle modalità con cui effettuare tali controlli) è di tipo normativo e nasce dalla lettura degli artt. 1 e 70 D.P.R. n. 633 del 1972. Il combinato disposto di tali articoli permetterebbe infatti di poter procedere alla tassazione delle im-

portazioni di tali pacchi viaggianti via posta ordinaria, se non fosse che il regolamento cui è stata delegata la funzione di disciplinare in concreto tale esercizio ad oggi non è stato emanato. A tale lacuna ha sopperito il Dipartimento delle Dogane con risoluzioni di tipo pratico che non trovano però al momento sistematicità e regolarità nell'applicazione.

DOGANA /1

Nell'ipotesi di un soggetto comunitario che acquisti un bene offerto da soggetto residente in un Paese *extra* UE, dovranno evidentemente essere osservate le procedure e le formalità previste dalla normativa doganale. Da quest'ultimo punto di vista, lo sviluppo della Rete potrebbe comportare un'ulteriore intensificazione delle vendite a distanza e del fenomeno del frazionamento delle spedizioni e dei trasporti, per i quali esistono procedure di carattere semplificato rispetto a quelle ordinarie.

L'interesse ad incentivare il commercio informatico potrebbe determinare le competenti autorità comunitarie ad elevare le soglie di esenzione per le imposte e per i dazi, attualmente previste per la spedizione di plichi postali di dimensioni, in linea peraltro con il processo di contenimento delle restrizioni doganali ormai pienamente avviato a séguito degli accordi dell'Uruguay Round.

Tabella / 11 dd

Particolarmente importante ai sensi delle convenzioni fiscali è il fine della qualificazione del reddito: mentre infatti il reddito d'impresa in assenza di una stabile organizzazione all'estero è tassato esclusivamente nel Paese di residenza, sui redditi di capitali (dividendi interessi e *royalties*) lo Stato in cui il reddito si è generato può legittimamente operare una ritenuta alla fonte.

Al settore in esame appartiene poi l'ulteriore problema degli adempimenti di carattere strumentale che devono essere osservati da parte dei soggetti residenti in Italia che, a seguito della negoziazione conclusa tramite Internet, effettuano trasferimenti da o verso l'estero di denaro, qualora l'ammontare complessivo dei movimenti effettuati nel corso dell'anno, ovvero quello degli investimenti e delle attività finanziarie detenute all'estero alla fine del periodo d'imposta, sia superiore ai 20 milioni di lire. Al riguardo occorre ricordare che, a norma degli artt. 2 e 4 d. lgs. 28 giugno 1990, n. 167, convertito in l. 4 agosto 1990, n. 227, come modificato tra l'altro dal d. lgs. 30 aprile 1997, n. 125 (c.d. monitoraggio fiscale):

- le persone fisiche, gli enti non commerciali e le società semplici ed equiparate ex art. 5 Tuir, residenti in Italia, devono indicare i trasferimenti di cui sopra - qualora effettuati senza il tramite di banche, società d'intermediazione mobiliare, ovvero dell'Ente Poste ovvero di altri intermediari - nella dichiarazione annuale dei redditi,
- gli stessi soggetti sopra menzionati devono indicare nella dichiarazione dei redditi gli investimenti all'estero ovvero le attività estere di natura finanziaria detenute al termine del periodo d'imposta, qualora d'importo superiore a 20 milioni, nella dichiarazione dei redditi deve altresì essere indicato l'ammontare dei trasferimenti da, verso e sull'estero che nel corso dell'anno hanno interessato i predetti investimenti ed attività, anche se al termine del periodo d'imposta non siano detenuti investimenti ed attività della specie.

Detti obblighi di indicazione non ricorrono, tra l'altro per i titoli affidati in gestione agli intermediari residenti, nonché per i contratti conclusi con il loro interessamento, a condizione che i redditi derivanti dalle attività estere di natura finanziaria siano riscossi mediante l'intervento degli intermediari stessi.

L'osservanza di questi adempimenti non è necessaria, ovviamente, né per gli acquisti di beni di modesto importo che al termine dell'anno non superino i 20 milioni di lire, né per quelli pari a quest'ultima somma regolarizzati a mezzo d'intermediari finanziari; di contro i suddetti adempimenti devono essere regolarizzati qualora il predetto importo riguardi pagamenti regolarizzati attraverso canali diversi da quelli messi a disposizione dal sistema finanziario nazionale ovvero per investimenti od acquisizione di attività finanziarie operative direttamente all'estero. Se la normativa ricordata sembra destinata ad influire modestamente sulle decisioni di acquisto dei beni offerti via Rete da parte delle imprese e dei consumatori nazionali, maggiore attenzione dovrà essere posta da questi soggetti per quanto riguarda l'acquisto all'estero di titoli offerti da intermediari esteri tramite Internet.

Commercio elettronico: una breve guida alle risorse in Rete

MARIA CONCETTA DE VIVO¹

SOMMARIO: 1. Premessa - 2. Siti che fanno transazioni on-line: Libri e dischi on-line - 3. (continua) I supermercati in Rete - 4. (continua) Il decollo dell'e-commerce - 5. (continua) Le aste on-line - 6. (continua) Il turismo on-line - 7. (continua) La moneta elettronica - 8. (continua) Le Banche in Internet - 9. (continua) Finanza in Rete - 10. Siti informativi sull'e-commerce - 11. Appendice: 24 diapositive.

1. PREMESSA

La mia relazione è il risultato di una navigazione mirata fra le risorse presenti in Rete che trattano del commercio elettronico. L'esposizione non ha alcuna pretesa d'essere completa o esaustiva, innanzitutto per la continua dinamicità dell'ambiente Internet e poi perché, per motivi di "spazio" espositivo e di tempo, ho dovuto effettuare delle scelte e dei tagli necessari.

I siti visitati durante la navigazione in Rete sono di due tipi: siti che fanno commercio elettronico e siti che danno informazioni sul commercio elettronico.

2. SITI CHE FANNO TRANSAZIONI ON-LINE: LIBRI E DISCHI ON-LINE

Fino a poco tempo fa, gli imprenditori pensavano (a torto) che la Rete "non servisse a fare una lira", poi la tendenza è improvvisamente cambiata e non poteva essere altrimenti visto che una realtà come la Rete, frequentata da milioni di utenti, non può non far gola a chi cerca nuove vie per il commercio, sfruttandole per un nuovo tipo di comunicazione: quella commerciale. Molti imprenditori proiettati in Rete sono andati "oltre" questa presa di coscienza ed hanno colto l'innovazione che l'utilizzo di Internet può portare nell'attività commerciale non limitando il ruolo del *Web* a quello di semplice vetrina virtuale, dove esporre la propria merce. Occorre, infatti, precisare che Internet non è un canale

¹ devivo@camsserv.unicam.it

distributivo bensì un "facilitatore" di accessi, e, nel caso di commercio *on-line*, un accesso privilegiato ai prodotti disponibili in Rete.

Una recente statistica, letta sul Resto del Carlino dell'8 ottobre, ha evidenziato alcune cifre: 700.000 circa sono gli italiani che acquistano *on-line*; 500 miliardi è il giro d'affari che gravita in Rete; 10.000 sono le aziende italiane che hanno un sito su Internet; 900 soltanto sono quelle che fanno commercio *on-line*. Nel 2003 si prevede che i siti attivi arriveranno a 5.000.

Per quanto riguarda i settori trainanti, il più attivo è quello della vendita di libri e dischi.

Internet, solo limitatamente a questo settore, offre più di 5000 siti, la maggior parte dei quali attua una vendita *on-line*. Ciò significa che attraverso Internet si possono avere a disposizione, da casa propria e senza alcuna fatica, centinaia di "negozi" alternativi specializzati nella vendita di libri. Molti di questi "negozi" hanno una scelta più vasta di qualunque negozio "fisico": spesso si tratta di cataloghi gestiti elettronicamente, e solo al momento dell'ordine viene individuata la libreria o il distributore che possiede una copia "fisica" del libro richiesto, in modo da poterlo spedire al cliente. Questa procedura riesce ad abbassare drasticamente i costi con la conseguenza che le librerie *on-line* possono offrire forti sconti rispetto alle librerie "fisiche".

La navigazione inizia dalla mitica Amazon book (<http://www.amazon.com>) con oltre due milioni di titoli in vendita. Nata nel '95 ha avuto sin dall'inizio la geniale idea di presentarsi all'utente non come un semplice catalogo di prodotti bensì come un *database* che offre la possibilità di utilizzare gli strumenti di comunicazione "anche" per svolgere una vera e propria attività di *marketing*. E quell'"anche" è stata la sua carta vincente.

In Italia altri siti interessanti sono: Rinascita (<http://www.rinascita.it/>), che permette di consultare i cataloghi dei libri disponibili ed effettuare direttamente gli ordini; Alice.it, il sito "ufficiale" del libro italiano (<http://www.internetbookshop.it/>); Laterza (<http://www.laterza.it/laterza/libri/libri.asp>) sito che ha attuato, oltre alla vendita, anche la politica della distribuzione gratuita *on-line* di alcuni volumi, fra i quali un manuale Internet.

3. (CONTINUA) I SUPERMERCATI IN RETE

Ovviamente libri e dischi sono solo una parte dei beni e dei servizi reperibili in Rete. Con la stessa facilità si possono acquistare biglietti d'aereo e macchine usate, *computer* e vini, case e monete antiche, cosmetici e piante ornamentali e quant'altro si vuole. Fra questi supermercati, sorta di centri commerciali virtuali, aperti 24 ore su 24, si segnalano: in Italia i siti di Cybermercato (<http://www.cybermercato.it/>); Casarossi (<http://www.casarossi.it/>); per quanto riguarda il resto del mondo: Internet shopping network (<http://www.isn.com>), con più di 1000 fornitori e un movimento di 35.000 prodotti.

4. (CONTINUA) IL DECOLLO DELL'E-COMMERCE

Attraverso una statistica inglese di alcuni anni fa, quando c'era ancora molta diffidenza sul commercio elettronico e questo veniva praticato solo da pochi pionieri (prevalentemente piccoli artigiani), si cercò di individuare le cause che impedivano all'e-commerce di decollare. Fra queste, due fattori risultarono rilevanti: la carenza dell'elemento "fiducia" fra contraenti, cioè fra negoziante e consumatore, dovuto alla mancanza del rapporto fisico, ossia alla "virtualità" ed all'anonimato dello strumento utilizzato; la "asetticità" dell'ambiente che veniva ricreato in Internet.

In effetto, le numerose forme ed i diversi gradi di anonimato che la Rete in pratica permette, finiscono col creare un pericoloso elemento di disturbo nel delicato rapporto fra venditore e consumatore, così come l'invio di formulari invadenti la *privacy* dell'utente. In questo ultimo periodo si è assistito, quindi, ad un'inversione di tendenza, dovuta alla consapevolezza che certe richieste eccessivamente particolareggiate (del tipo: età, sesso, razza, titolo di studio, *hobby* ecc.) sono controproducenti e finiscono con l'irritare il potenziale acquirente. Così si è assistito, da una parte, ad una forte limitazione del fenomeno chiamato *spamming* e, dall'altra, alla creazione di "spazi" in grado di personalizzare e rendere più accogliente il negozio virtuale ricreato in ambiente Internet. Sono stati introdotti, così, *forum* di discussione o *community* con funzioni di salotti virtuali dove i consumatori, volendo, possono incontrarsi e scambiare opinioni sui prodotti acquistati o da acquistare e non solo su questi.

Esiste, inoltre, un progetto finanziato dalla Commissione europea con la partecipazione di Università, Enti di ricerca e Banche, che sta studian-

do lo sviluppo di un *help desk* umano chiamato Avatar, sorta di "commesso digitale", ossia di figura umana tridimensionale in grado di riconoscere ed interagire con i potenziali clienti ed "aiutarli" nelle operazioni di acquisto attraverso sofisticati sistemi di riconoscimento vocale.

Il progetto, che sembra collegato più al mondo della fantascienza che a quello del commercio elettronico, si inserisce in un più ampio ed articolato studio sullo sviluppo dell'*e-commerce* chiamato Trade e consultabile all'indirizzo: <http://trade.cosi.it>

L'umanizzazione della Rete ha ovviamente intenti affatto missionari, al punto da far pensare che queste "innovazioni" rappresentano, in realtà, una forma alternativa di raccolta di dati per fini statistici sugli utenti frequentatori di determinati siti. In proposito in Rete sta affermandosi una nuova strategia cosiddetta di "marketing negativo", per cui il prodotto viene inviato automaticamente all'utente che è già cliente del sito, a meno che questi non manifesti la volontà di non riceverlo. Questa forma di vendita *on-line* se da una parte risulta particolarmente vantaggiosa per l'azienda, dall'altra è pericolosa per l'utente in quanto rappresenta una raccolta di interessanti informazioni per creare profili personali sui frequentatori di determinati siti. La BMG (<http://www.Bmgmusicservice.com/>) è un sito specializzato in prodotti musicali ed ha reso attivo questo tipo di servizio. Un altro caso simile è quello della Sony station (<http://www.station.sony.com>), un *Web* con un movimento di 100 mila utenti in contemporanea, con oltre 1 milione di utenti registrati ed oltre 10 milioni di messaggi pubblicitari mirati inviati ogni settimana. Fra le tante opportunità offerte ai propri utenti c'è quella di prelevare un SonyPass che li informa, tra le altre cose, dei movimenti degli altri utenti che sono presenti in Rete, lo stesso programmino, tuttavia, permette all'azienda di elaborare i dati così raccolti ed utilizzarli per creare annunci pubblicitari mirati da spedire successivamente attraverso la Rete.

In questo contesto appare evidente, quindi, come sia superata, nell'odierno mercato virtuale, la "strategia" iniziale del "guarda-scegli e compra", sostituendola con sofisticati meccanismi che rielaborano, personalizzandola, la realtà dei "mercatini" popolati da bancarelle o dei mercati di aste, in cui vige il principio del "chi offre di più" e del "chi vende a meno".

5. LE ASTE ON-LINE

In materia di aste in Rete ci sono vari siti interessanti. Per districarsi fra questi si possono utilizzare dei motori di ricerca *ad hoc* quali ad esempio: *Auction watchers* (<http://www.auctionwatchers.com>) in cui si può selezionare la categoria della merce che interessa. Attraverso la ricerca si estrapola, così, una vasta panoramica dei siti d'asta che trattano il materiale richiesto. A questo punto ci si iscrive al sito scelto, si ottiene una *Userid* ed una *password* (in cambio di dati personali necessari per l'eventuale acquisto) e con queste si partecipa attivamente all'asta *on-line*. L'acquirente viene messo al corrente via *e-mail* delle offerte superiori alla propria, così che possa gareggiare sino a quando lo riterrà opportuno. Leggermente diversa è la posizione del venditore del prodotto, il quale deve registrarsi presso il sito fornendo, oltre ai propri dati personali, anche i numeri delle carte di credito necessari per garantire il pagamento delle percentuali spettanti alla cassa. Inoltre, per mettere in vendita l'oggetto, deve fornire una descrizione dettagliata su modulo, insieme al prezzo base, alle modalità di pagamento scelte ed alla durata dell'asta. Si attende, quindi, l'apertura della vendita e si ricevono via *e-mail* dal sito, che cura l'asta, le proposte fatte dai vari compratori.

L'espansione del commercio elettronico soprattutto in questo campo può sollevare questioni di ordine legale non solo per quanto riguarda la sicurezza della trasmissione dei dati o la tutela della *privacy*, bensì anche in merito a controlli e restrizioni su determinate categorie di beni oggetto di commercio elettronico, quali ad esempio farmaci o armi. Molti sono, infatti, i prodotti trattati nelle aste, alcuni sorprendenti (anche isole ed isolotti a modiche cifre), altri insoliti (aerei), altri ancora preoccupanti (come ad esempio armi da guerra, pistole e mitragliatrici).

Tra i vari siti di aste pubbliche *on-line* si citano: il Qxl (<http://italia.qxl.com/cgi-bin/qxl.storefront/it>), che è italiano e dove è possibile seguire in tempo reale le puntate in corso e ribattere con una propria offerta. Il suo equivalente statunitense EBAY (<http://www.ebay.com>), il primo e più grande sito di aste in Rete.

Nell'interessante panoramica, che il mercato in Internet offre, appare indubbio che chiunque abbia interesse ed un pizzico di inventiva può entrare in Rete e fare *business*. Da non perdere, quindi, il sito: Shopsummit (<http://www.shopsummit.com>), la cui caratteristica è che il suo ideatore, nonché gestore e novello imprenditore del futuro, è un tredi-

cenne con uno *sponsor* d'eccezione, un premio Nobel (Penzias - guru delle nuove tecnologie) ed un giro d'affari che coinvolge una ventina d'aziende americane che vendono i loro prodotti attraverso il sito.

• 6. (CONTINUA) IL TURISMO ON-LINE

Altro prodotto presente in Rete è il turismo *on-line*. Molti sono i siti di veri e propri "agenti di viaggio" virtuali. Tra di loro: Expedia (<http://www.expedia.com>), attivo negli Stati Uniti; fra i tanti siti italiani si citano i primi che compaiono catalogati fra le Agenzie di viaggio APT e *tour operator* nell'elenco dei due motori di ricerca GoItaly e Virgilio: Clupviaggi (<http://www.clupviaggi.it>), che prevede prenotazioni *on-line* ed un programma chiamato *e-club* in grado di effettuare la conferma ed i pagamenti a mezzo carta di credito, in modalità sicura; 123... e via (<http://www.123.it>), dove si prenota unicamente con le carte di credito, il sito ha una convenzione con la Banca Sella e offre la possibilità di scegliere i viaggi, la loro prenotazione *on-line*, mette a disposizione un *memorandum* dei documenti di viaggio e del controllo degli orari delle partenze, oltre ad una gamma di offerte vantaggiose.

7. (CONTINUA) LA MONETA ELETTRONICA

Nel commercio elettronico continua a sussistere il grosso problema delle modalità dei pagamenti in Rete, e così è stata fatta una navigazione mirata verso siti che trattano della cosiddetta moneta elettronica.

Quale può essere la moneta di scambio valida in questo mondo virtuale? Per quanto riguarda le carte di credito ed il loro utilizzo pare che il problema sia tecnicamente risolto in maniera abbastanza soddisfacente, attraverso l'adozione di protocolli di comunicazione sicuri e di *server* capaci di garantire, nei casi necessari, l'adozione di questi protocolli.

Si presenta, allora, un problema pratico: se, cioè, la carta di credito sia utile in quei casi di cosiddetti micro-acquisti, dove risulta eccessivo e controproducente il suo utilizzo. A questo punto si inserisce il discorso della moneta elettronica. Inventata da un olandese, David Chaum, e gestita all'inizio da un consorzio denominato *digicash*, è stata adottata da vari siti commerciali.

Per un percorso storico si rinvia al sito *History of money* (<http://www.ex.ac.uk>). Invece nel sito di *Omega generation* (<http://www.omega.it/digicash/ecash.html>) viene presentata la moneta elettronica e viene spiegato, per i non addetti ai lavori, il suo funzionamento. Poiché è necessario, per il suo concreto utilizzo, che vi sia un preventivo deposito tramite conto corrente in una *virtual bank*, nel sito della Mercantil bank è possibile effettuare un servizio di conversione di valuta reale in elettronica.

A livello europeo è interessante il sito della Banca virtuale europea (<http://www.bve.com>), che tra le altre cose contiene un elenco della banche italiane in Internet e numerose altre informazioni ed indirizzi per muoversi nel mondo dell'e-commerce.

In Italia un corrispondente della Mercantil Bank è il sito Cilme, acronimo del Consorzio Interbancario Lombardo per la Moneta Elettronica (http://www.cilme.it/minipay/ind_pay.htm), che prevede una sezione speciale denominata Minipay - sorta di borsellino elettronico - pensato per la sostituzione del contante nelle spese di piccolo importo.

Un sito italiano molto documentato sulla banca virtuale è quello della Tsi (<http://www.tsi.it/>). Fra gli altri siti che permettono di "scaricare" direttamente dalla Rete questo borsellino elettronico, ovvero un programma capace di gestire le proprie cybermonete, c'è E-cash technologies Inc. (<http://www.ecashtecnologies.com>). Inoltre, in Italia, il sito di Telepay (<http://telepay.ssb.net>) curato da una società per servizi bancari fa sì che l'utente possa prelevare dal sito un programma che permette di criptare i dati durante la transazione e rendere così il pagamento sicuro al massimo.

8. (CONTINUA) LE BANCHE IN INTERNET

Altro aspetto strettamente collegato al mercato globale in Rete è quello del legame fra merce, denaro, banche e finanza.

Le banche in Rete trovano la loro giustificazione naturale nella gestione e nel traffico di valuta e nella possibilità di utilizzare via Internet alcuni servizi bancari, come l'"Internet banking" che fa uso della Rete per lo svolgimento di vere e proprie transazioni bancarie.

Per avere un'idea del tipo di servizi offerti in Internet ci si può collegare con i siti di alcune delle banche italiane che sono *on-line*. Un elenco delle Banche italiane in Rete è fornito da Topnet (<http://www.topnet.it/>)

banche.htm) e da Voyager (<http://www.voyager.it/sitivari.htm#banche>). Per ovvi motivi di spazio e di tempo si segnalano solo alcune delle banche *on-line*: la Banca delle Marche (http://www.bancamarche.it/ita/dx_home.htm); la Cariplo (<http://www.cariplo.it>), che con la sua QuiCariplo Home Banking offre l'acquisto e la vendita di azioni a condizioni

Particolari; il Banco Ambrosiano Veneto (<http://www.ambro.it>); la Banca Popolare di Milano (<http://www.bpm.it/prodotti/aziende.html>); il Banco di Sicilia (<http://www.bancodisicilia.it/hmbk/welcom.htm>) con una *demo on-line* del servizio di *home banking*; la Banca Sella (<http://www.sella.it>), sito storico in quanto è stato tra i primi a lanciare i servizi di *e-commerce*. Comprende anch'esso una *demo* sull'Internet Banking; Banca Popolare di Novara (<http://www.bpn.it>), considerato, dagli esperti, uno fra i migliori *Web* presenti in Rete. Permette di fare acquisti *on-line* attraverso un proprio negozio virtuale <http://www.bpn.it/vetrina/acquisti/acquisti.htm>, e di chiedere mutui *on-line*. Contiene, inoltre, una sezione in cui vengono proposti numerosi *links* ed altri negozi virtuali tra cui il già citato cybemercato, i Grandi Magazzini, Italstore, De Agostini, Compuline, Italiashopping, Venicemall.com.

9. (CONTINUA) FINANZA IN RETE

In campo finanziario si citano due siti per tutti: Charlesschawb (<http://www.schawb.com>), sito di una società di investimenti. Contiene dimostrazioni pratiche di come funziona una transazione in Rete attraverso una chiara, semplice ed efficace *demo*; Fineco (<http://online.fineco.it>), sito italiano di negoziazione telematica dei titoli, adatto anche ai neofiti della Rete.

10. SITI INFORMATIVI SULL'E-COMMERCE

I siti che danno informazioni sul commercio elettronico si dividono a loro volta in siti che contengono materiale informativo generico, prevalentemente di tipo giornalistico anche se di alto livello specialistico, e siti a contenuto giuridico. Nella prima "categoria" si elencano come esempi: Il sole 24 ore (<http://www.sole24ore.it/24oreinformatica/>), sito rilevante per la mole di informazioni contenute anche se è prevalentemente rivolto alle aziende; Enterprise (<http://enterprise.tn.it/bu>

siness/ebusiness/pagina_1.html), un vero e proprio portale predisposto, anch'esso, prevalentemente per aziende e professionisti, realizzato con l'intento mirato di fornire le strategie per una presenza vincente in Rete: contiene sondaggi, *forum* ed ogni altra attività collegata all'ottimizzazione del *business* in Rete. Interessante è la sezione denominata "Contenuti" che offre informazioni ed analizza i tipi di clientela da contattare. Ed il *forum* sul mondo del diritto <http://forum.tin.it/cgi-bin/WNthread?tin.it.diritto>. Soldion-line (<http://www.soldionline.it>), è un sito per la Finanza, accessibile anche agli investitori internetiani alle prime armi, ideato come supporto per il piccolo imprenditore. Interessante la *newsletter*. Village commerce (<http://www.village-commerce.com>) della Telecom Italia per chi vuole aprire il proprio negozio *on-line*. Contiene una serie di informazioni sui servizi e una guida al commercio elettronico.

Fanno parte della seconda categoria i siti: Commercio elettronico ed Unione Europea (<http://www.ispo.cec.be/ecommerce/Welcome.html>); Osservatorio del commercio elettronico (<http://www.minindustria.it/Osservatorio/index.html>) che presenta i propri obiettivi, le linee strategiche del Governo e la politica industriale attuata per il commercio elettronico. Il ricco sito del Ministero delle finanze (<http://www.finanze.it>) che tra le varie sezioni ne contiene una che riguarda le problematiche di una regolamentazione del *Web* (<http://www.finanze.it/regolweb.htm>) ed un'interessante parte sulle "tesi *on-line*", con l'elenco delle tesi disponibili sul commercio elettronico. Lex mercatoria (<http://lexmercatoria.net/>) con informazioni e *links* riguardo alla legislazione che regola il commercio internazionale ed una sezione *ad hoc* sull'*e-commerce*. Ipno (<http://www.netword.com/ipno/>), nasce come un *repository* di informazioni organizzate in ipertesto. Tra gli argomenti trattati: Documento informatico, firma digitale e commercio elettronico. Il sito è ricco di informazioni ha un'impostazione tecnico-specialistica e dedica particolare attenzione alle normative ed alle regole sull'*e-commerce*. Per una più corretta presentazione del sito si rinvia alla lettura di quella che è la sua storia cliccando sull'omonimo *link* presente in *home page*. Sempre in ambito giuridico: Jure page (<http://www.geocities.com/Athens/Crete/2958/>) l'ideatrice del sito ha sviluppato la sua passione per l'argomento (nel sito pubblica stralci della propria tesi di laurea sul trasferimento elettronico dei fondi) ideando una pagina *Web ad hoc* comprensiva di rassegna stampa, dottrina e normativa sull'argomento. Commercenet Italy, (<http://www.commercenet.it/normativa.html>) il sito tratta gli aspetti

normativi del fenomeno dell'*e-commerce* e ne fornisce un'aggiornata panoramica. Dal *Web* si può scaricare direttamente un *Memorandum* sul commercio elettronico. Il sito sulla *Privacy* (<http://www.privacy.it/>) non ha bisogno di presentazioni e prevede nella sezione dei *links* la voce "il mondo e il commercio elettronico" (<http://www.privacy.it/linkcomm.html>) ricca di indirizzi verso siti specializzati nell'argomento e la voce "il mondo e la sicurezza elettronica" (<http://www.privacy.it/linksic.html>).

Una categoria a sé è rappresentata dai Motori di ricerca che, a mio avviso, stanno subendo delle preoccupanti trasformazioni, perché da strumenti di ricerca di informazioni stanno diventando vere e proprie guide mirate per l'acquisto in Rete e vere e proprie vetrine virtuali. Si segnalano il recente Katalogo.it (<http://www.katalogo.it>), che nella voce Shopping riserva una propria sezione alla Guida agli acquisti in linea; l'inossidabile Yahoo http://it.dir.yahoo.com/Affari_e_economia/Commercio_elettronico/ che propone Yahoo *Shopping* una guida dei servizi in linea e che ha attivato un canale diretto a siti che fanno commercio elettronico; Goitaly (<http://www.goitaly.it/testo.htm>), che si autodefinisce un portale italiano di *e-commerce*. In questo ambito non è da sottovalutare il fatto che i Motori di Ricerca sono degli strategici strumenti di raccolta di informazioni sugli utenti e permettono, quindi, di ottenere dei veri e propri profili *demografici* della clientela presente in Rete, profili che sono molto ricercati da chi fa *marketing*.

Dai Motori di Ricerca, che diventano Guide sul Commercio Elettronico si passa a vere e proprie Guide sull'*e-commerce*, ideate e costruite esclusivamente per questo. Ne sono esempi i siti di: Zivago (<http://www.zivago.it>); Indis (<http://www.indis.unioncamere.it/>), costruito in collaborazione con Mondimpresa e Commercenet, che si presenta come una guida per le Piccole e Medie Imprese Italiane. Internet Business Guide (<http://www.ibguide.com/>).

Navigando in Rete ci si è accorti di come molte aziende fanno *business* su "come" fare del commercio elettronico, danno, cioè, indicazioni, suggerimenti, lezioni, offrono *stage*, reperiscono dati, e propongono strategie per costruire negozi virtuali, studiano le tattiche migliori per "catturare" clientela, si offrono di cercare fornitori, gestendo ordini ed offrendo sistemi di sicurezza per le transazioni *on-line*. Fra questi: il sito di Bella Italia

(<http://www.bella-italia.com/ita/negozio.shtml>), con i suoi servizi per le aziende italiane

La carrellata termina con la visita a *Web* che svolgono attività di ricerca sul Commercio elettronico, cioè che pubblicano in Rete i risultati dei loro studi sulla materia. Questo viene fatto sia da siti universitari, prevalentemente americani, tra i quali il più volte citato: *Center for research in electronic commerce* (<http://cism.bus.utexas.edu/>), sia da siti governativi, quali gli statunitensi www.ecommerce.gov e www.digitaleconomy.gov, che sono in grado di offrire *on-line* un'eccezionale mole di documentazione sull'economia digitale.

Anche in Italia molti sono i siti universitari che si stanno facendo carico di questa impresa, o che sono sensibili alle varie applicazioni che il commercio elettronico può offrire anche in ambiente universitario. Tra i tanti Atenei se ne citano solo alcuni come esempio anche per tutti gli altri: Università di Pisa (<http://www.di.unipi.it/%7eattardi/Talk/SicurezzaReti/tsld002.htm>); Osservatorio internet dell'Università Bicconi di Milano (<http://www.uni-bocconi.it>); Università degli studi G. D'Annunzio (<http://giuriweb.unich.it/>); il Politecnico di Milano (<http://www.polimi.it/>); Cratos - Centro di Ricerca Applicazioni della Telematica (<http://cratos.pc.unicatt.it/didattica/corsi/>); il Cineca; L'Università di Pavia che ha al suo attivo la promozione di vari Master sulla tecnologia e i media reperibili all'indirizzo (<http://media.iuss.unipv.it/>) e si è fatta promotrice di un interessante esperimento che riguarda gli studenti universitari: una carta di servizi dotata di *microchips* che offre agli universitari che ne sono in possesso la possibilità di usufruire di un Borsellino elettronico ricaricabile Minipay, attraverso il quale è possibile effettuare piccoli pagamenti presso mense universitarie o esercizi convenzionati (http://www.tsp.it/notizie_com20luglio99.htm).

Per tutti gli altri, innumerevoli, siti visitati e non menzionati in questa breve esposizione, si rinvia alla consultazione della voce "Commercio elettronico" ne "La Rubricetta", sezione del sito *Web* della Scuola di specializzazione in diritto civile dell'Università degli Studi di Camerino (<http://www.unicam.it/ssdici/agenda.html>).

11. APPENDICE

*Diapositiva 1***BREVE GUIDA ALLE RISORSE
IN RETE***Diapositiva 2*

- **SITI CHE FANNO** commercio elettronico
- **SITI CHE DANNO INFORMAZIONI** sul commercio **elettronico**

Diapositiva 3

700.000 gli italiani che acquistano on line
2.500 miliardi il giro d'affari della Rete
800 in Italia
10.000 le imprese italiane che sono in Rete
900 soltanto quelle che fanno commercio on line

Diapositiva 4

SITI CHE FANNO TRANSAZIONE ON LINE

SETTORE VENDITA LIBRI E DISCHI

AMAZON - <http://www.amazon.com>

RINASCITA - <http://www.rinascita.it>

ALICE.IT - <http://www.internetbookshop.it>

LATERZA - <http://www.laterza.it>

Diapositiva 5

... I SUPERMERCATI DEI PRODOTTI

CYBERMERCATO

- <http://www.cybermercato.it>

CASAROSSO

- <http://www.casarossi.it>

INTERNET SHOPPING NETWORK

- <http://www.isn.com>

Diapositiva 6

AVATAR: IL COMMESSE DIGITALE

TRADE

- <http://trade.cosi.it>



Diapositiva 7

4 IL MARKETING NEGATIVO

BMG

- <http://www.bmgmusicservice.com>

SONY STATION

- <http://www.station.sony.com>



Diapositiva 8

↘ ASTE E MOTORI DI RICERCA

[Http://www.auctionwatchers.com](http://www.auctionwatchers.com)

Diapositiva 9

LE ASTE IN RETE

QXL

- <http://italia.qxl.com>

EBAY

- <http://www.ebay.com>*Diapositiva 10*IL COMMERCIO ELETTRONICO
NON HA ETA'

SHOPSUMMIT

<http://www.shopsupmit.com>

Diapositiva 11

: IL TURISMO ON LINE

EXPEDIA

- <http://www.expedia.com>

CLUPVIAGGI

- <http://www.clupviaggi.it>

123 ... e via

- <http://www.123.it>

Diapositiva 12

: LA MONETA ELETTRONICA

HISTORY OF MONEY - <http://www.ex.ac.uk/~Rdavies/arian/11yfr.html>

OMEGA GENERATION - <http://www.omega.it/digicash/ecash.html>

MERCANTIL BANK - <http://www.marktwain.com>

BANCA VIRTUALE EUROPEA - <http://www.bvc.com>

CILME - <http://www.cilme.it>

TSI - <http://www.tsi.it>

E-CASH TECHNOLOGY - <http://www.ecashtecnologies.com>

TELEPAY - <http://telepay.ssb.net>

Diapositiva 13**LE BANCHE IN RETE**

Un elenco è presente in

TONET - <http://www.topnet.it/banche.htm>

ed in

VOYAGER - <http://www.voyager.it/situvari.htm#banche>

Diapositiva 14**LE BANCHE IN RETE**

BANCA DELLE MARCHE - <http://www.bancamarche.it>

CARIPLO - <http://www.cariplo.it>

BANCO AMBROSIANO VENETO - <http://www.ambro.it>

BANCA POPOLARE DI MILANO -
<http://www.bpm.it/prodotti/aziende.html>

BANCO DI SICILIA <http://www.bancodisicilia.it/lmbk/welcome.htm>

BANCA SELLA - <http://www.sella.it>

BANCA POPOLARE DI NOVARA -
<http://www.bpn.it/acquisti/acquisti.htm>

Diapositiva 15

✦ IN CAMPO FINANZIARIO

CHARLESSCHAWB - <http://www.schawb.com>

FINECO - <http://online.fineco.it>

Diapositiva 16

✦ SITI INFORMATIVI

1) tipo giornalistico ed altamente specializzati

2) di tipo tecnico-giuridico

Diapositiva 17

DEL I TIPO

IL SOLE 24 ORE

- <http://www.sole24ore.it/24oreinformtica/>

ENTERPRISE

- http://enterprise.tin.it/business/ebusiness/pagina_1.html

SOLDIONLINE

- <http://www.soldionline.it>

VILLAGE COMMERCE

- <http://www.villagecommerce.com>

Diapositiva 18

DEL II TIPO

COMMERCIO ELETTRONICO ED UNIONE EUROPEA

- <http://www.ispo.cec.be/ecommerce/Welcome.html>

OSSERVATORIO DEL COMMERCIO ELETTRONICO

- <http://www.minindustria.it/Osservatorio/index.htm>

MINISTERO DELLE FINANZE - - <http://www.finanze.it>

LEX MERCATORIA - <http://lexmercatoria.net>

IPNO - <http://www.netword.com/ipno/>

JURE PAGE

- <http://www.geocities/Athens/C1etc/2958>

Diapositiva 19

◆ DEL II TIPO

COMMERCE.NET ITALY

- <http://www.commercenet.it/normativa.html>

WWW.PRIVACY.IT - <http://www.privacy.it/>

• sezione Link "Mondo e commercio elettronico"
... / linkcomm.html

• sezione "Mondo e sicurezza elettronica"
... / linksic.html

Diapositiva 20

◆ MOTORI DI RICERCA

KATALOGO.IT - <http://www.katalogo.it>

YAHOO - it.dir.yahoo.com/Affari_e_economia/Commercio_elettronico/

GOITALY - <http://www.goitaly.it>

Diapositiva 21**\ SITI-GUIDE**

INDIS - <http://www.indis.unioncamere.it/>

ZIVAGO - <http://www.zivago.it>

INTERNET BUSINESS GUIDE - <http://www.ibguide.com>

❖ SITI DI SERVIZI

BELLA ITALIA - <http://www.bellaitalia.com/ita/negozio.shtml>

Diapositiva 22**❖ SITI UNIVERSITARI E DI ENTI DI RICERCA**

CENTER OF RESEARCH IN ELECTRONIC COMMERCE
- <http://cism.bus.utexas.edu>

WWW.ECOMMERCE.GOV

e

WWW.DIGITALECONOMY.COM

Diapositiva 23

☛ SITI UNIVERSITARI E DI ENTI DI RICERCA

UNIVERSITA' DI PISA - <http://www.di.unipi.it>

OSSERVATORIO INTERNET BOCCONI MI
- <http://www.uni-bocconi.it>

UNIVERSITA' DEGLI STUDI D'ANNUNZIO
- <http://giunweb.unich.it>

POLITECNICO DI MILANO - <http://www.polimi.it>

CRATOS - <http://cratos.pe.unicatt.it/didattica/corsi/>

UNIVERSITA' DI PAVIA - <http://media.russ.unipv.it>

Diapositiva 24

☛ SEGNALAZIONE ALTRI SITI

UNIVERSITA' DEGLI STUDI
DI CAMERINO

SCUOLA DI SPECIALIZZAZIONE
IN DIRITTO CIVILE

LA RUBRICETTA
<http://www.unicam.it/ssdici/agenda.html>

Intervento conclusivo

Documento informatico, firma digitale e commercio elettronico

PIETRO PERLINGIERI

Ringrazio il Direttore della Scuola, Prof. Vito Rizzo, che ha voluto attribuirmi l'onore e l'onere di concludere questo Convegno da lui organizzato.

Evito di soffermarmi su questioni ampiamente illustrate e ripetute ed ormai abbastanza acquisite per porre in rilievo alcuni punti che, a mio avviso, sono di più pregnante interesse.

Innanzitutto mi pare opportuno affrontare secondo un approccio più corretto la triade "informatica, informazione e formazione". In tal senso inizierei proprio dalla "formazione" volta a favorire l'acquisizione di una cultura idonea a garantire lo sviluppo della capacità critica dei singoli soggetti; successivamente il discorso deve necessariamente soffermarsi sulla "informazione", la quale consente di verificare e controllare l'informazione stessa e senza la quale l'informazione critica acquisita risulterebbe priva di supporto; infine, "l'informatica" (e la telematica) ovvero la trasmissione dell'informazione e la sua idoneità ad essere veicolo per la formazione culturale, che resta situata al vertice della scala dei valori.

L'informatica e la telematica fondano una nuova era storica, esse costituiscono lo strumento tecnologico innovativo di trasmissione dei contenuti. Malgrado ciò, la società tecnologica è pur sempre una società e l'aggettivo "tecnologica" è semplicemente idoneo a qualificarla tanto che il primato rimane senz'altro all'uomo, senza possibilità di critiche o revisioni.

Le problematiche affrontate in questo Convegno sono per definizione pluridisciplinari, non tanto sotto il profilo strettamente giuridico - data l'unitarietà del diritto - ma in una prospettiva sociologica, tecnologica, culturale, etica. Sì che il rapporto etica-diritto, mercato-Stato, etica-tecnologia costituisce uno dei punti essenziali da porre in rilievo, nonostante l'attuale momento storico segnato dalla crisi dello Stato a causa della globalizzazione dell'economia e della conseguente globalizzazione

della sovranità. La sovranità è ormai diffusa non soltanto entro i confini del singolo Stato, ove si sostanzia nell'attribuzione di poteri autonomi alle regioni, alle provincie, agli enti locali, al Parlamento nazionale ed infine alla Comunità Europea, ma è tale soprattutto a livello mondiale. Ciò induce a tentare di individuare, come è stato fatto egregiamente in questa sede, le istituzioni internazionali alle quali dovrebbe competere la risoluzione dei problemi posti dai nuovi strumenti informatici, dalla telematica ed ancor di più dal Governo del mondo. Appare pertanto necessario mutare l'approccio al problema che stiamo trattando.

In particolare con riferimento al mercato è palese l'attuale superamento della territorialità, come dimostrato da tutti gli interventi in materia di commercio elettronico ascoltati in questi giorni. E' altresì evidente la non attualità della distinzione mercato interno e mercato estero, nonostante siano ancora attivati diplomi per il "commercio estero". Di conseguenza le nozioni di distribuzione commerciale e di organizzazione dell'attività di distribuzione sono completamente mutate a favore della creazione di nuove forme di distribuzione commerciale e di nuove attività commerciali.

A tal proposito è lecito aggiungere che ormai appare insufficiente una regolamentazione nazionale del mercato, poiché nonostante l'acquisita consapevolezza dell'importanza dei principi fondamentali del nostro ordinamento essi hanno pur sempre una vigenza territorialmente definita e soprattutto subiscono la concorrenza dei principi comunitari ed internazionali. Si rende, allora, palese il mutamento che non soltanto coinvolge la nozione di mercato, ma persino il medesimo concetto di economia. A quest'ultimo non pare più ascrivibile un significato di tipo classico e tradizionale, bensì acquista una natura digitale alla quale deve seguire un mutamento sia nell'organizzazione di poteri sia nella sovranità.

Oggi si intravede una nuova democrazia, quella digitale.

Tutta la nostra ingegneria costituzionale è organizzata sulla partecipazione, espressa attraverso il voto, mediante il quale sono eletti i nostri rappresentanti. Tuttavia ora la rappresentanza diretta, che caratterizzava la *polis* greca, può forse diventare possibile attraverso la telematica e la partecipazione di una società tecnologica computerizzata. Per quanto questa prospettiva lasci attoniti, non è da escludere che il governo mondiale possa rinvenire proprio in questa partecipazione diretta del cittadino nuove forme di collaborazione e decisione.

È, dunque evidente che la transnazionalità non è soltanto una caratteristica del mercato, ma lo è inevitabilmente anche della sovranità.

Molti tentano di rinvenire alla base del mercato europeo una forte spinta liberista e dunque scorgere nella sua struttura il riconoscimento della totale libertà di mercato, ma ciò rispecchia soprattutto un'ottica anglosassone o comunque riconducibile all'Europa centrale più che a quella mediterranea. Tuttavia tale impostazione non appare corretta data la incessante produzione normativa comunitaria spiccatamente economica. Una regolamentazione che si auspica corretta, ovvero rispondente non soltanto ai valori della libera concorrenza a tutela del produttore e del consumatore, ma anche a valori forti quali la tutela della persona e dei suoi diritti fondamentali. Valori questi ultimi ai quali è certamente più vicina la nostra tradizione di quanto non possa esserlo quella americana o anglo-americana, più legata al profitto, al mercato e alla società materiale. Tra l'altro queste propensioni sono il risultato del nostro percorso storico, delle nostre filosofie, della nostra preparazione culturale e della nostra educazione. Sembrano chiare, a tal punto, le mie riserve a riconoscere alla base del mercato europeo la presenza di una concezione liberale, in particolar modo quando è palese l'esistenza di un controllo e di una programmazione. Non è certo una concezione dirigistica, ma probabilmente essa non è tale neppure nell'apparato costituzionale interno, anche se qualcuno negli ultimi tempi ha esasperato questo aspetto con riferimento all'art. 41 Cost.

Tuttavia la nostra Costituzione è fondata su uno stato sociale di diritto, quindi non tesa esclusivamente a garantire "il fate come vi pare" e "il più forte vinca", ma a garantire costantemente *standards* minimi come la qualità, ma soprattutto valori imprescindibili quali la tutela della persona. Alla luce di ciò non pare possibile guardare alla Comunità europea come disegnata dal trattato di Roma. Ciò è, altresì dimostrato dal passaggio dal mercato comune all'Unione Europea che si richiama, nel Trattato di Maastricht, ma più ancora in quello di Amsterdam, ai diritti fondamentali dell'uomo, alla tradizione e al costituzionalismo europeo.

Non è corretto, dunque, affermare che il vento proveniente dall'Europa è un vento liberista, se per liberismo si intende quanto sopra abbiamo cercato di smentire.

È indubbio che l'iniziativa economica privata non è e non può rientrare tra le concessioni statali, ma per quanto il suo esercizio non sia

condizionato da forme autorizzative, essa comunque deve svolgersi in un mercato regolamentato. Peraltro, la stessa regolamentazione della quale si discorre non è altro che uno statuto normativo, nel quale rientrano regole che, per quanto di carattere economico, restano pur sempre giuridiche. In particolare esse si rivelano necessarie al fine di stabilire controlli che garantiscano l'assenza di eccessi, di abusi di posizioni dominanti ovvero non permettano il sorgere di meccanismi anticoncorrenziali, che seppur tollerati dalla cultura nordamericana non possono essere condivisi.

In sintesi tra le due posizioni, anche in questa sede emerge, liberalizzazione e nuove regole, non c'è contraddizione. In verità si riscontra un'inadeguatezza degli strumenti e ancor di più delle professionalità necessarie per gestire il mutamento in atto. Di qui l'esigenza della certezza delle transazioni, una esigenza da sempre avvertita da tutti i mercanti e in tutti i mercati. Una certezza che con l'avvento dell'era tecnologica assume connotati diversi e pertanto diversi appaiono gli strumenti per la sua realizzazione.

Altresì con riferimento alla tutela della *privacy* e in particolare all'utilizzo non corretto dei dati personali non pare opportuno esasperare il problema. Facilmente si passa da una condizione dove tutto appare lecito ad una forma di limitazione del diritto di manifestare liberamente il proprio pensiero come massima espressione della personalità. Anche con riferimento ad *Internet* e all'utilizzo delle reti telematiche è opportuno tenere distinti i due aspetti ovvero differenziare il commercio elettronico dalle attività meramente comunicative.

Il surrettizio utilizzo dei dati personali nel commercio elettronico, ove sia stato preventivamente manifestato il consenso, introduce un problema di portata più ampia, quello culturale. Sì che appare superfluo istituire nuove *Authorities* per tutelare il consumatore o l'utente inconsapevole quando tale tutela potrebbe essere rafforzata con una migliore formazione culturale del soggetto. Investimento certamente più proficuo si presenta quello rivolto a curare maggiormente la formazione culturale. E' pur vero che il diffondersi di notizie inerenti le abitudini personali dei soggetti all'interno di *Internet* per favorire il commercio elettronico potrebbe apparire pericoloso, d'altro canto la loro diffusione apporta vantaggi in sede di politica commerciale e di distribuzione mirata di beni e

prodotti. In tale contesto non appare opportuna la creazione di un tutore del tutore.

Tutt'altro discorso merita, invece, il processo comunicativo, che deve essere fortemente incentivato e garantito quale forma di espressione del pensiero, e che si distacca fortemente dal settore commerciale.

Un profilo di particolare rilevanza è certamente quello inerente la tutela delle invenzioni e delle opere dell'ingegno, dati i grandi risultati ottenuti proprio da chi ha scelto di investire nella ricerca ed ha lavorato per produrre nuovi sistemi.

Appare, dunque, necessario tutelare sia le opere dell'ingegno sia le opere artistiche al fine di incentivare l'investimento di nuove energie in tal senso. D'altronde va combattuto la omogeneizzazione e l'uniformazione della cultura. La telematica e l'organizzazione informatica oltre che nell'ambito commerciale devono trovare applicazione anche nell'organizzazione strutturale dell'impresa nonché della Pubblica Amministrazione. La stessa Autorità per l'Informatica nella Pubblica Amministrazione si sta sviluppando in forma surrettizia, svolgendo un'attività che va oltre le sue competenze. Appare opportuno, dunque, non lasciare alle leggi-delega la disciplina di settori di tale rilievo; il problema deve essere ricondotto al sistema educativo.

È necessario distinguere il diritto dell'informatica dall'informatica giuridica e senza considerare quest'ultima soltanto come un'informatica applicata. Pur riconoscendo un incredibile impegno culturale degli amici, primo fra tutti Vittorio Frosini, che hanno sviluppato in questi anni il problema dell'informatica giuridica da filosofi, ritengo che un siffatto sistema universitario non sia più adeguato. L'informatica giuridica non può essere limitata all'area disciplinare relativa alla filosofia del diritto; è necessario un raggruppamento disciplinare autonomo al fine di aprirle nuovi spazi nella didattica. D'altra parte è difficile che presenze, pur culturalmente validissime, ma non esclusivamente dedicate allo studio dell'informatica giuridica, possano garantirle un futuro. A tal proposito può essere utile l'esempio fornito dall'Università del Sannio, dove sono state rese obbligatorie per gli studenti appartenenti a tutte le facoltà, le conoscenze della lingua, dell'informatica, dei diritti e dei doveri dei cittadini e del diritto ambientale.

In un periodo storico caratterizzato dalla comunicazione appare inopportuno escludere l'insegnamento dell'informatica giuridica. Sareb-

be, dunque auspicabile, redigere un documento contenente una forte presa di posizione sull'argomento.

Avrei molte altre considerazioni da aggiungere, ma mi sono imposto di dare un termine preciso a queste mie conclusioni.

Gli interventi che mi hanno suscitato maggiore interesse sono quelli dei pubblicisti poiché è utile, soprattutto in questa materia, ragionare utilizzando i principi comunitari. Principi che animano non soltanto il legislatore, ma anche l'interprete.

A tal proposito ho apprezzato il tentativo di rileggere la Costituzione, non soltanto per la sua parte economica, alla luce dei principi comunitari. Particolare interesse destano le problematiche inerenti il diritto di accesso alla rete comunicativa, l'obbligo della neutralità dei fornitori del servizio, la stessa sicurezza dei dati personali. Tuttavia non va tralasciata una questione di fondo, ovvero il riconoscimento che il sistema comunicativo, l'atto di comunicazione, l'atto di informazione assumono una valenza diversa se inseriti in un'attività di impresa. Dunque, la medesima attività di comunicazione immessa nel contesto commerciale appare estranea all'art. 21 Cost. e quindi tutelabile non quale manifestazione della libertà di pensiero, come vorrebbe la Corte Europea, bensì quale attività rientrante nella previsione dell'art. 41 Cost.

Vorrei ancora aggiungere qualcosa con riferimento alla concorrenza.

La nostra Costituzione non sembra molto sensibile a questa tematica, eppure un riconoscimento della tutela del mercato concorrenziale si rinviene indirettamente nella libertà di iniziativa economica privata come sancita dall'art. 41 Cost. In tal senso appaiono lesivi del principio di uguaglianza e della libera concorrenza tutti quei meccanismi volti ad incentivare e sostenere l'impresa. L'impresa è rischio, dunque va liberalizzata e non assistita se inidonea a permanere sul mercato.

Occorre, dunque chiarire i principi da rispettare.

Riguardo a quanto affermato dal relatore notaio Zagami con riferimento all'autenticazione della firma e all'identificazione, vorrei porre in rilievo l'importanza del controllo di legalità del contenuto per gli atti non pubblici. Questo altro non è che il riconoscimento di quanto da tempo sosteniamo circa l'importanza del controllo di merito degli atti *ex art. 28* della legge notarile vigente. Si che il documento sottoscritto non deve essere in contrasto con l'ordinamento giuridico. Si riconosce, quindi, al

notariato latino una funzione che già venticinque anni fa era emersa, proprio qui a Camerino, ed oggi viene riscoperta attraverso l'aspetto telematico.

Osservazioni molto interessanti sono state esposte anche dall'amministrativista Cardarelli che con un intervento mirato anche nella scelta del titolo, "Funzioni e poteri pubblicistici in materia di commercio elettronico" ha fatto emergere un'altra diffusione del potere.

Abbiamo accennato prima alla sovranità diffusa a livello statale nonché internazionale e abbiamo già posto in rilievo come nuove autorità cosiddetti indipendenti non siano facilmente collocabili in alcun settore dello Stato. A ciò consegue l'impossibilità di definire se i loro atti abbiano natura amministrativa, giurisdizionale o ancora regolamentare. In tal senso un esempio è fornito dalla Banca d'Italia, la quale è uno dei primi organismi cosiddetti indipendenti. Tale organismo regola e controlla allo stesso tempo il mercato creditizio, da un lato opera per stabilizzare il sistema bancario, ovvero creare un monopolio, dall'altro è chiamata a controllare il rispetto delle regole sulla concorrenza delle stesse imprese.

Risulta, allora, veramente importante affermare che anche la discrezionalità tecnica deve essere sindacabile, ma sindacabile sulla base di principi e valori quali la proporzionalità, la ragionevolezza e la congruità.

Nella teoria dell'interpretazione alcuni erroneamente affermano la non incidenza dei summenzionati principi e valori nella fase interpretativa; per contro secondo un'altra impostazione che fa capo ad Emilio Betti, ben nota qui a Camerino, riveste una importanza fondamentale il costante riferimento ai principi. Questa non è altro che la consapevolezza dello strumento che il giurista deve necessariamente avere per essere tale ed è ciò che consente di sostenere che la discrezionalità tecnica, oggi più importante di quella amministrativa, deve avere una sua sindacabilità proprio mediante un'interpretazione basata costantemente sui valori.

Un altro contributo importante, relativo ad una delle pagine più nere della nostra Carta Costituzionale, è stato quello relativo alla distinzione tra diritto soggettivo e interesse legittimo. Tutto il sistema della giustizia poggia sulla distinzione tra diritti soggettivi e interessi legittimi, due concetti dogmatici difficilmente definibili. Distinzione attualmente non utile dato il ritorno alla unità della giurisdizione. Peraltro lo stesso Costituente nel garantire autonomia e indipendenza alla magistratura ordinaria non menziona affatto quella amministrativa.

A questo punto perde attualità la problematica inerente l'interesse legittimo atteso che essa rappresenta **un inutile fardello soprattutto alla luce del diritto comunitario**. L'unità della giurisdizione appare come uno dei punti cruciali per rendere più efficiente il meccanismo giudiziario nel nostro Paese, in particolare quando la giustizia di tipo amministrativo si palesa come una giustizia soltanto apparente.

A questo proposito sono state formulate utili considerazioni con riferimento al buon funzionamento e all'imparzialità della Pubblica Amministrazione, che non sono altro che applicazioni dell'art. 97 Cost.

Vi sono, dunque, molti elementi potenzialmente distorsivi della concorrenza; spesso è la stessa Pubblica Amministrazione che, attraverso una cattiva utilizzazione della sua discrezionalità tecnica, favorisce la creazione di elementi distorsivi.

Al fine di entrare in Europa è necessario meglio ripartire le competenze attualmente attribuite alla sola Pubblica Amministrazione.

Alla nostra attenzione restano dei modelli da studiare, riflessioni sul tipo di mercato da realizzare e sul tipo di organizzazione dello Stato. Sono questi i problemi ai quali i giuristi devono dare risposta, non soltanto in chiave *de iure condito*, ma anche *de iure condendo*. Da più parti è emersa la mancanza di una cultura appropriata del legislatore per regolare queste materie. Se la comunità scientifica non riesce a proporre un adeguato articolato legislativo sul commercio elettronico si assume una notevole responsabilità e dimostra di non avere consapevolezza del ruolo che può svolgere in un Paese civile come l'Italia. Piacevole è notare la presenza di molti giovani, che probabilmente hanno una maggiore sensibilità verso queste tematiche rispetto alla mia generazione.

Ringrazio i relatori, tutti coloro che hanno ascoltato questo mio intervento conclusivo, nonché coloro che ci hanno ospitato.

INTERVENTI SELEZIONATI

Intervento su:

L'arbitrato nelle reti telematiche e il commercio elettronico: un rapido strumento di risoluzione delle controversie sorte nella "Rete delle reti"

FULVIO SARZANA DI S. IPPOLITO

SOMMARIO: 1. L'arbitrato e le reti telematiche - 2. La validità delle decisioni arbitrali effettuate tramite la rete telematica - 3. La sede dell'arbitrato telematico - 4. La sottoscrizione digitale e l'arbitrato - 5. L'arbitrato telematico: il progetto "the virtual magistrate" - 6. Il requisito dell'obbligatorietà del lodo arbitrale telematico - 7. Sistemi di risoluzione delle controversie telematiche a carattere conciliativo e procedimenti arbitrali on-line.

1. L'ARBITRATO E LE RETI TELEMATICHE

Nel campo della giurisdizione, così come in quello della risoluzione alternativa delle controversie nel campo telematico possono essere seguite due metodologie: La prima considera direttamente applicabile il diritto, sia esso statale o sovranazionale alle controversie nascenti dagli scambi telematici. Gli adattamenti, necessari al mutato contesto in cui opera la rete telematica, vengono creati per evitare un'insanabile frattura nel sistema. Il secondo approccio considera il *medium* telematico come un diverso modo di intendere le relazioni tra soggetti con caratteristiche proprie. La considerazione è importante per capire se gli strumenti di trasmissione della volontà adoperati nella rete telematica possano considerarsi equiparabili a quelli già conosciuti o se la comunicazione via Internet costituisca un substrato fisico a sé stante. Nel campo dei metodi di risoluzione delle controversie diversi dal procedimento cognitivo ordinario questo significa equiparare le modalità di trasmissione a quelle conosciute ed applicare dunque la disciplina, nazionale ed internazionale, esistente, o ipotizzare la nascita di un arbitrato telematico con modalità procedurali adeguate alle caratteristiche della rete telematica. Quale che sia la soluzione prescelta un dato è certo: i metodi di risoluzione delle controversie, che potranno affermarsi nella rete telematica, contribuiranno, come sembra aver preso coscienza anche il legislatore comunitario, a deflazionare gli organi di giustizia e a rendere più effettiva la tutela del singolo consumatore telematico. Le procedure arbitrali, affiancate da uf-

fici di mediazioni e *ombudsman* telematici, contribuiranno a rendere più effettiva la tutela giurisdizionale o giustiziale rendendo di attualità l'adagio volteriano secondo cui "mix vaut un mauvais accord qu'un bon proces" e costringendo i legislatori nazionali ad abbandonare, per particolari tipi di controversie, l'esclusivo approccio giuridico-centrico sin qui seguito.

La definizione di procedure arbitrali telematiche ha riguardato in primo luogo le organizzazioni internazionali interessate alla diffusione di metodi di risoluzione delle controversie fra imprese commerciali. Nonostante i procedimenti arbitrali commerciali e le regole esistenti dovessero essere considerate probabilmente applicabili agli arbitrati telematici, le organizzazioni internazionali hanno ipotizzato una serie di regole *standard* adottabili nel contesto del commercio elettronico.

Fra le prime *rules* in materia di arbitrati commerciali si segnalano quelle predisposte da organizzazioni quali l'*American Arbitration Association* (con il progetto *the virtual magistrate* di cui si dirà in seguito) e quello predisposto dalla *International Chamber of Commerce*.

In che rapporto queste forme di arbitrati o meglio queste *rules* siano con le fonti del diritto arbitrale internazionale, quali la Convenzione di Ginevra del 21 aprile 1961 che disciplina l'arbitrato commerciale, e la *Uncitral Model Law on International Commercial Arbitration*, non è dato allo stato attuale comprendere, in considerazione del fatto che le regole approntate per l'arbitrato commerciale telematico generalmente non affrontano esplicitamente il rapporto tra le Convenzioni esistenti e le nuove regole dettando semplicemente una serie di regole procedurali specifiche della rete telematica.

L'approccio metodologico innovativo, sperimentato dalle organizzazioni internazionali, presuppone già risolto il problema della definizione dei procedimenti arbitrali telematici senza ipotizzare una adattabilità delle fonti regolamentari esistenti alla realtà telematica.

Il sistema delineato dal codice di procedura civile italiano, che è stato più volte modificato nel corso degli anni, deve invece presumibilmente essere adattato alla realtà telematica in quanto contiene alcune definizioni che mal si adattano al mutato contesto sociale della realtà dei traffici. La differenziazione fra arbitrato interno, arbitrato internazionale ed arbitrato estero con regole a volte differenti e discrasie normative evidenti è un esempio di tecnica legislativa ridondante, che può nuocere allo sviluppo

di queste forme di risoluzione delle controversie alternative alla giurisdizione ordinaria.

Si pensi, come si dirà in seguito, che il codice di procedura civile considera valida la videoconferenza a fini deliberativi solo per l'arbitrato internazionale, escludendo di fatto il ricorso a tale modalità comunicativa per l'arbitrato domestico.

Ciò significa che non sarà possibile validamente deliberare un arbitrato fra arbitri che risiedono sul territorio nazionale e sarà invece ipotizzabile un arbitrato "videotelefonico" tra un arbitro italiano ed uno residente all'estero.

2. LA VALIDITÀ DELLE DECISIONI ARBITRALI EFFETTUATE TRAMITE LA RETE TELEMATICA

Passando ad analizzare più dettagliatamente la disciplina italiana in materia di arbitrato e la compatibilità di quest'ultima con la rete telematica è possibile evidenziare alcuni spunti di riflessione.

Le problematiche da risolvere relative all'arbitrato nell'ambito delle reti telematiche sono essenzialmente di tre tipi.

In primo luogo occorre stabilire se il mezzo telematico sia valido a tutti gli effetti di legge come mezzo trasmissivo della volontà e se la deliberazione del lodo arbitrale effettuata secondo le modalità proprie della rete Internet, quale la "videoconferenza", e cioè tramite programmi appositi in grado di collegare più soggetti contemporaneamente, abbia valore legale a tutti gli effetti. Il valore giuridico della videoconferenza è stato riconosciuto di recente dal legislatore italiano. La legge n. 25 del 1994 prevede infatti la validità della deliberazione del lodo effettuato in videoconferenza, ma solo relativamente all'arbitrato internazionale. Poiché la norma in materia di videoconferenza (l'art. 837 c.p.c.) si riferisce espressamente solo a quella "telefonica", sorge il problema se le modalità comunicative sopra descritte possano essere equiparate a quelle prese in considerazione dal legislatore, ovvero occorra una definizione normativa della "videoconferenza telematica". Per stabilire se la videoconferenza telefonica sia analoga alla videoconferenza via Internet, occorre evidenziarne le similitudini e le differenze: la videoconferenza telefonica permette infatti di considerare validamente effettuata una deliberazione *inter absentes* sul presupposto che gli arbitri, decidendo la controversia, in una

camera di consiglio ideale possano rendere equivalente la loro presenza fisica ad un *medium* virtuale che protegga in primo luogo le modalità di deliberazione. Nel sistema ideato dall'associazione arbitrale statunitense, di cui si dirà in séguito, le procedure arbitrali avvengono tramite scambio di memorie per posta elettronica, ovvero tramite discussione su *newsgroup*, ovvero ancora tramite programmi denominati di *chat*, che consentono di discutere la controversia in tempo reale, in modalità che comunque non sembrano garantire lo stesso livello di sicurezza e di riservatezza garantito dalla videoconferenza telefonica.

Va osservato al riguardo che già in fase strutturale la rete telematica presenta caratteristiche fisiche e di sicurezza profondamente differenti dalle comunicazioni telefoniche. Il collegamento con la rete Internet può infatti avvenire tramite la normale linea telefonica, ovvero tramite la connessione di una sottorete proprietaria al nodo di rete più vicino, utilizzando modalità di comunicazione non perfettamente assimilabili a quelle telefoniche. Visto che la connessione può anche non avvenire tramite telefono, è già revocabile in dubbio che la definizione adottata dal legislatore in tema di arbitrato internazionale si possa applicare *sic et simpliciter* alla conferenza telematica.

Un ulteriore dubbio sorge analizzando le modalità pratiche di redazione del lodo.

In materia di deliberazione del lodo, infatti, l'ultimo periodo dell'art. 837 c.p.c. prevede la successiva redazione per iscritto del lodo, principio che induce a ritenere che ai fini della validità della "videodeliberazione" vi debba essere la redazione di un documento cartaceo o ad esso equiparato. Se si dovesse intendere la norma in senso letterale, si dovrebbe escludere la redazione del lodo con un documento informatico, tuttavia la piena equiparazione fra documento cartaceo e documento informatico effettuata dal D.P.R. n. 513 del 1997 induce a ritenere che non vi siano ostacoli alla redazione di un lodo in forma elettronica, né alla sottoscrizione dello stesso lodo mediante firma digitale, secondo le modalità prescritte dall'art. 10 D.P.R. citato.

3. LA SEDE DELL'ARBITRATO TELEMATICO

Un ulteriore problema connesso all'ipotizzata praticabilità della via telematica all'arbitrato è rappresentato dalla necessaria indicazione della

sede dell'arbitrato. Non vi è dubbio che la legge 5 gennaio 1994, n. 25, disponendo la necessaria indicazione della sede dell'arbitrato e disponendo che la medesima possa non coincidere con il luogo di deliberazione dell'arbitrato stesso, intendeva riferirsi ad un luogo fisico. La sede dell'arbitrato è rilevante a diversi fini, tra i quali l'assoggettabilità del lodo alla disciplina prevista dall'art. 807 ss, in quanto lodo nazionale, ovvero alla diversa disciplina prevista dagli artt. 839-840 c.p.c. Il criterio per stabilire la sede, e quindi la nazionalità, dell'arbitrato può essere un criterio geografico ovvero un criterio procedurale. Il criterio fisico ha ad oggetto il luogo in cui materialmente è stata stabilita la sede dell'arbitrato: tuttavia il criterio geografico non permette di stabilire con esattezza ove la sede dell'arbitrato sia effettivamente. In un "ipotetico" arbitrato telematico, infatti lo svolgimento delle udienze tramite videoconferenza, ovvero lo scambio di documenti digitalmente firmati, può avvenire tra luoghi fisicamente molto diversi, a seconda del luogo in cui è situato il computer che materialmente utilizza il programma in grado di supportare la videoconferenza, ovvero si incarica di smistare la posta elettronica degli arbitri. Un ulteriore criterio in grado di orientare l'interprete può essere rappresentato dal criterio della legge procedurale applicabile. In considerazione di quest'ultimo, anche se le parti decidessero di effettuare le udienze tramite videoconferenza, ovvero anche se gli arbitri dotati di *personal computers* portatili si scambiassero gli atti in luoghi fisici destinati a mutare nel corso della procedura, la legge applicabile permanerebbe quella scelta dagli arbitri o dalle parti con l'indicazione della normativa applicabile: tale criterio sembra compatibile con il sistema processuale italiano. Nel prevedere la determinazione della sede dell'arbitrato in Italia, il legislatore italiano non vincola le parti allo svolgimento di particolari attività materiali, né ad un collegamento di carattere materiale. È dunque ipotizzabile l'ipotesi di un arbitrato sottoposto al diritto italiano con svolgimento dell'attività deliberativa ed istruttoria completamente all'estero. Tuttavia il criterio fisico non può essere del tutto abbandonato e quindi il *locus* virtuale costituito da un flusso di *bit* in movimento, se non vi è uno specifico luogo come sede dell'arbitrato o non viene enunciata la norma applicabile, non può probabilmente essere considerato come un luogo dove stabilire la sede dell'arbitrato. Il procedimento arbitrale che si svolge all'interno della rete telematica, in quanto sfornito di un aggancio reale, resterebbe quindi al di fuori della disciplina prevista dal codice di procedura civile potendo al più, ove le modalità di formazione possano soddi-

sfare i requisiti di forma e di sostanza previsti dal codice civile, valere come accordo contrattuale di composizione della controversia.

Anche in questo caso, tuttavia, dovranno intendersi rispettati alcuni requisiti minimi, quali la necessaria ascrivibilità dei provvedimenti arbitrali agli arbitri stessi e alle stesse parti e la non ripudiabilità dei documenti così trasmessi tra le parti e gli arbitri. Si dovrebbe quindi escludere *a priori* la possibilità di considerare validamente costituito un collegio arbitrale che, operando tramite la rete telematica, non consenta di identificare con certezza l'identità delle parti e degli arbitri, così come invece avviene quando il lodo è deliberato mediante "videoconferenza telefonica".

4. LA SOTTOSCRIZIONE DIGITALE E L'ARBITRATO

L'equiparazione fra documento cartaceo e documento informatico può avere dei riflessi anche nella disciplina dell'arbitrato. Per quel che riguarda il requisito della sottoscrizione, ci si deve chiedere se sia possibile sottoscrivere digitalmente tutti gli atti della procedura arbitrale ed in particolare lo stesso lodo. L'art 823 c.p.c., che stabilisce i requisiti della deliberazione e del lodo, non sembra porre ostacoli alla sottoscrizione digitale, contenendo inoltre una disposizione che sotto il profilo effettuale sembra pienamente applicabile alla rete telematica: il punto 6 dell'art. 823, infatti, stabilisce che "... se gli arbitri sono più di uno, le varie sottoscrizioni, senza necessità di ulteriore conferenza personale, possono avvenire in luoghi diversi", senza specificare le modalità di sottoscrizione del lodo. Il requisito dello scritto può essere dunque pienamente soddisfatto dal documento digitalmente firmato. In considerazione di questo richiamo normativo si deve ritenere che ogniquale volta le parti decidano di compromettere in arbitri una controversia ed intendano inserire la clausola compromissoria, pur essendo per ipotesi il contratto a cui accede la clausola formato secondo requisiti difformi da quelli previsti dal D.P.R. n. 513 (ad esempio contratto di licenza di *software* ad esecuzione istantanea), la relativa clausola debba comunque essere approvata per iscritto secondo le tradizionali forme cartacee, ovvero secondo il procedimento previsto dalla normativa sulla firma digitale.

5. L'ARBITRATO TELEMATICO: IL PROGETTO "THE VIRTUAL MAGISTRATE"

Nel maggio del 1996, a séguito di un convegno organizzato dall'*American Arbitration Association*, cinquanta esperti, provenienti da diversi settori, dettero vita ad un progetto di risoluzione delle controversie sorte sulla rete telematica. L'iniziativa denominata *virtual magistrate* ha portato alla creazione di una camera arbitrale "virtuale", il cui maggior pregio è rappresentato dalla possibilità di risolvere la controversia nel giro delle 72 ore. L'arbitrato "virtuale" ha visto decidere diverse controversie nell'anno 1998, con una crescita esponenziale pari allo sviluppo del commercio elettronico sulle reti telematiche.

Quanto il progetto potrà dirsi effettivo è presto per dirlo. Il documento tuttavia non considera, a parere di chi scrive, uno dei fattori di successo dell'arbitrato commerciale internazionale: la riservatezza. Esistono infatti seri dubbi sulla reale funzionalità della risoluzione alternativa delle controversie in un contesto "aperto" come quello della rete telematica.

Ed infatti, analizzando la procedura utilizzata dal "magistrato virtuale", è riscontrabile che le informazioni che vengono scambiate tra le parti e gli arbitri, non sono coperte da segreto: le comunicazioni, ivi compresa la notificazione della decisione, sono scambiate con il sistema del *listserve*, cioè del gruppo di discussione chiuso a cui accedono gli interessati alla procedura e a cui l'ufficio del *virtual magistrate* concede il diritto di ottenere una *password* di accesso. Coloro che sono in possesso della *password* sono in grado di leggere immediatamente le comunicazioni depositate in questa "bacheca elettronica". La bacheca contiene: la descrizione del fatto come indicata dalle parti, le ragioni di diritto indicate dalle parti alla trattazione dell'arbitro, il nome, l'indirizzo reale ed informatico dell'istante, il nome l'indirizzo reale ed il domicilio informatico delle altre parti del procedimento e gli eventuali commenti, che possono essere formulati in qualsiasi momento dalle parti coinvolte nella procedura. La concessione della *password* consente a tutti gli interessati di prendere visione degli atti relativi ad altri procedimenti e quindi tale sistema esclude la presenza di due requisiti fondamentali ai fini dell'ammissibilità di un arbitrato telematico: la *privacy*, come diritto a non veder divulgate le informazioni relative al proprio status, e la "privacy giudiziaria", così apprez-

zata dagli operatori commerciali internazionali, desiderosi di mantenere la riservatezza sull'andamento delle proprie controversie.

La pubblicità telematica comporta per le aziende il rischio di divulgazione di dati che per motivi fiscali e di reputazione commerciale dovevano rimanere segreti. Non è un mistero che gli arbitrati sinora decisi dal *virtual magistrate*, riguardando principalmente grandi società di servizi telematici danneggiate dal comportamento dei singoli utenti, siano stati accettati per motivi di immagine, quando la questione era divenuta oramai di dominio pubblico, più che per reali esigenze di celerità o di "giustizia" del caso concreto.

6. IL REQUISITO DELL'OBLIGATORietà DEL LODO ARBITRALE TELEMATICO

Il maggior problema che la dottrina d'oltreoceano ha dovuto affrontare in tema di risoluzione giustiziale delle controversie nelle reti telematiche è stato quello di dotare il lodo pronunciato dall'arbitro virtuale del requisito dell'*Enforceability*, dell'espreso potere, cioè, di imporre la realtà alle parti del lodo. Se il progetto *the virtual magistrate* fosse stato inteso dai suoi estensori come un progetto diretto a rendere il responso dell'arbitro virtuale equiparabile in tutto e per tutto a quello reso a séguito di un normale procedimento arbitrale, il problema della obligatorietà non si sarebbe posto. In base, infatti, all'*United States Arbitration Act*, conosciuto più semplicemente come *Federal Arbitration Act*, le Corti Federali sono obbligate a riconoscere efficacia ai lodi arbitrali *affecting interstate commerce*. La stessa cosa avviene in campo Statale ove l'*Uniform Arbitration Act* impone alle Corti Statali di effettuare il medesimo riconoscimento. Lo stesso principio dell'*United States Arbitration Act* si rinviene nella disciplina convenzionale sull'arbitrato, in quanto la decisione dell'arbitro telematico, per avere valore di arbitrato recepibile dall'ordinamento, deve, ai sensi dell'art. V, n. 1, lett. e, della Convenzione di New York, essere obbligatorio, in quanto riconoscibile dall'ordinamento in cui è stato emesso. Viceversa, se il lodo arbitrale viene considerato alla stregua di un accordo negoziale non eseguibile sul territorio dello Stato, la disciplina applicabile sarà quella del tipo di contratto e del conseguente *breach of contract* ove l'accordo non venga rispettato. La preoccupazione di dotare il lodo di questo requisito dimostra il dubbio della dottrina statunitense a considerare l'arbitrato telematico come una reale istituzione in grado di conside-

rarsi alternativa alla giurisdizione ordinaria. Più che di un vero e proprio arbitrato telematico, è possibile parlare di un arbitraggio ed il ruolo del *virtual magistrate* sarebbe riconducibile a quello di un "privato arbitratore". Secondo parte della dottrina il progetto di arbitrato virtuale realizzerebbe uno strumento del tutto consensuale e negoziale, una forma di arbitrato irrituale, con decisione di equità. Un problema di difficile soluzione è rappresentato dal fatto che difficilmente si potrà imporre l'affermazione di un arbitro operante sulla rete telematica senza il consenso delle parti interessate. La sottoscrizione del contratto di accesso alla rete Internet, comprensivo della clausola compromissoria, avverrebbe fra soggetti diversi quelli che poi effettivamente potranno adire l'arbitro telematico: ogni *provider* potrebbe infatti indicare un collegio arbitrale differente con il risultato che le controversie sorte fra un utente di un *provider* ed il cliente di un altro dovrebbero essere decise da collegi arbitrali differenti. La soluzione potrebbe essere la sottoscrizione di un contratto che indica il magistrato virtuale come "unico soggetto in grado di dirimere le controversie sorte tra utenti della rete Internet", ipotizzando la nascita di un arbitrato obbligatorio per le controversie telematiche.

7. SISTEMI DI RISOLUZIONE DELLE CONTROVERSIE TELEMATICHE A CARATTERE CONCILIATIVO E PROCEDIMENTI ARBITRALI ON-LINE.

Un'altra procedura arbitrale attinente alle reti telematiche gestita da organismi internazionali è quella predisposta dalla WIPO (*World Intellectual Property Organization*). Essa tende a dirimere le controversie nascenti dall'assegnazione dei «nomi di dominio». Non è questa la sede per approfondire le tematiche attinenti alla tutela dei «nomi di dominio» su Internet, pur se una breve trattazione preliminare appare necessaria.

L'assegnazione dei «nomi di dominio», cioè dei nomi che nella rete Internet identificano con precisione il tipo di elaboratore (cioè il suo numero identificativo I.P.) viene assegnata da un organismo privato denominato *Internet Network Information Center* (InterNIC), che sta però passando le consegne ad un organismo denominato *Internet Corporation for Assigned Names and Numbers* (ICANN) e che applica il criterio della priorità della richiesta. In sostanza, e senza particolari riguardi per il marchio distintivo di un'azienda, l'InterNIC fornisce al richiedente l'identità virtuale necessaria per essere conosciuti nel mondo telematico. In tal modo può accadere che una grande azienda, contraddistinta da un marchio fa-

moso, non possa utilizzare il proprio marchio su Internet perché è stata da altri preceduta nella registrazione del nome di dominio.

La soluzione è stata individuata nell'equiparazione, ad opera della giurisprudenza statunitense ed italiana, fra marchio e nome di dominio. Ma non vi è dubbio che occorra una risposta da parte degli organismi internazionali.

Tra questi si segnala il Wipo (*World Intellectual Property Organization*), che ha ideato l'istituzione di un organismo arbitrale in grado di decidere con efficacia obbligatoria sulle controversie relative ai «nomi di dominio».

La proposta, denominata *Expedited arbitration*, prevede la presenza di un solo arbitro, il termine di tre giorni per le audizioni delle parti e di tre mesi per la conclusione della procedura.

La novità della proposta è che per la prima volta l'intera procedura può svolgersi direttamente nella rete telematica: è infatti possibile compilare la richiesta di arbitrato direttamente dal sito della organizzazione, effettuare notifiche automatiche (ma con quale valore giuridico, almeno ai sensi della legge italiana?), effettuare il pagamento elettronico degli onorari, utilizzare strumenti messi a disposizione dall'organizzazione per effettuare la videoconferenza.

Esistono anche procedimenti arbitrali per le controversie sui «nomi di dominio» nazionali, che però di "virtuale" hanno ben poco. In Italia la *Naming Authority* italiana (l'Istituto CNUCE del CNR), all'atto dell'assegnazione del nome di dominio, impone al richiedente la sottoscrizione di una clausola di accettazione della procedura arbitrale in caso di controversia. La prassi di impedire all'istante il controllo sul nome dell'arbitro che deciderà la controversia, e la configurazione di un "procedimento arbitrale obbligatorio", richiamano alla mente quelle fallimentari esperienze di arbitrati obbligatori che la legislazione italiana ha conosciuto in questi anni, soprattutto in materia di accordi collettivi di lavoro, e che hanno fatto dubitare della reale differenza tra giurisdizione ordinaria e procedure alternative di risoluzione delle controversie.

Intervento su:

La cifratura e il sistema digitale del notariato

MANLIO CAMMARATA

Nella relazione del notaio Zagami quando si parla di "cifratura del documento" si intende dire "cifratura dell'impronta del documento", inserita con la firma digitale. Infatti il documento informatico non è cifrato, è in chiaro e può essere eventualmente cifrato per renderlo segreto, ma a questo punto viene cifrato con la chiave pubblica del destinatario, che lo apre con la sua chiave privata.

Con la chiave privata di colui che forma il documento viene cifrato un brevissimo riassunto del documento stesso, che si chiama impronta di Hash, proprio perché viene ottenuto con la cosiddetta funzione di Hash, cioè l'ombra del documento.

Il documento in sé dunque è immediatamente leggibile e non da decifrare, anche perché se fosse cifrato con la chiave privata del mittente, chiunque lo decifrebbbe con la chiave pubblica: è inutile cifrare un documento che chiunque può aprire.

Un'altra osservazione, che volevo aggiungere, si riferisce all'ultima parte dell'intervento di Zagami, dove si parlava di atto pubblico, della non possibilità dell'atto pubblico e della sua non previsione nel D.P.R. n. 513.

Anzitutto va detto che non era compito di questo D.P.R. occuparsi dell'atto pubblico, inoltre, cosa di cui ancora solo poche persone sono a conoscenza, i notai hanno già una Intranet perfettamente funzionante, in grado di comunicare, per ora solo con alcuni, ma presto con tutti, gli Uffici del Registro, con cui scambiare atti telematici, iscrizioni telematiche, visure telematiche, autenticate con un sistema di firma digitale, che possiamo definire proprietario, ma che appena possibile sarà la firma digitale ex D.P.R. 513.

Dunque il notariato è già pronto e si guarda bene dal far introdurre altre norme in materia di firma digitale sul documento notarile.

Intervento su:

L'atto pubblico notarile e il servizio digitale dei notai

RAIMONDO ZAGAMI

Ringrazio Cammarata per la precisazione sul concetto di cifratura del documento, che d'altra parte io avevo trascurato di fare per non appesantire la relazione con concetti troppo tecnici e non rilevanti ai nostri fini.

Per quanto riguarda l'atto pubblico notarile, invece, è vero che esiste una Intranet notarile, che io stesso utilizzo, ma non è corretto affermare che oggi si fanno atti pubblici notarili.

Attualmente su questa Intranet viaggiano semplicemente dati senza valore giuridico, che si limitano all'invio di posta elettronica e alla consultazione di banche dati, quali il Catasto, il Registro delle imprese e, tra poco, le Conservatorie.

Riguardo poi alla possibilità di effettuare la registrazione degli atti a distanza, la trascrizione a distanza, questo è già consentito dal D.P.R. n. 513, che non prevede la redazione di un atto pubblico notarile originale su carta, ma la possibilità di farne copie informatiche.

Quindi, dal punto di vista pratico, il notaio redige come sempre l'atto pubblico su carta ed effettua poi una copia informatica accompagnata da un'attestazione di conformità, con cui egli stesso dichiara che si tratta di copia conforme all'originale cartaceo.

Quest'ultimo può, dunque, essere inserito nei volumi del notaio e dimenticato, mentre la copia informatica circolerà ex D.P.R. suddetto "con la stessa efficacia giuridica dell'originale cartaceo" e con essa si potranno effettuare registrazioni degli atti, trascrizioni e tutti gli adempimenti connessi ad una stipula notarile.

In alcun modo, però, si può affermare che oggi sia possibile redigere atti pubblici originali.

Intervento su:
**Alcuni concetti relativi ai sistemi
di firma digitale**

MASSIMILIANO MINERVA

I sistemi di firma elettronica sono destinati **gradatamente**, ma **inesorabilmente**, a **sostituirsi** alle **tecniche** di firma tradizionali; non si tratta di una **mia affermazione personale**, ma lo dicono il mercato, l'evoluzione **tecnologica** e tanti atti **normativi** internazionali, comunitari e ora anche nazionali.

Sgombrato il campo da questa **premessa generale**, occorre fare una premessa di tipo terminologico: purtroppo molti dei **termini** utilizzati dal nostro legislatore, sia nel D.P.R. 513, che nel D.P.C.M., sono il frutto di una **traduzione** di termini anglosassoni.

Passiamo ora alla parte **sostanziale** del mio intervento.

La **certificazione** non è una **certificazione** amministrativa, ma **tecnica**, quindi la **soluzione** per il **problema** della **certificazione** sta proprio nel **ritenerla** appunto non un fenomeno **amministrativo**, bensì **tecnico**, cioè l'accertamento tecnologico della **corrispondenza fra la chiave pubblica** e il **soggetto**, per cui si tratta di un fenomeno di **titolarità**, consistente nell'**attribuzione tecnologica** di una **sequenza di elementi** informatici ad una **chiave pubblica**.

Non c'è, quindi, una **certificazione dell'identità personale** e questo potrebbe essere un **problema** e lo è senz'altro sotto il profilo della **manca**za di un'**identità personale** certa dal **punto di vista fisico**.

La **certificazione** ci interessa, dunque, in quanto **elemento tecnico**, il **certificato** appunto, che si allega alla **firma**, **elemento tecnico di una fattispecie tecnologica complessa**, la **firma digitale**.

Questo **significa** che l'autorizzazione non è un'autorizzazione ad un'**attività di tipo pubblicistico** e, quindi, il sistema previsto dal nostro legislatore non andrebbe ricondotto ad un sistema di **autorizzazione preventiva**, come è stato fatto prima della direttiva, che ora impone di **considerarla facoltativa**.

Ha ragione Cardarelli quando sostiene che vi è una disarmonia da correggere, ma il sistema delle fonti è stato pensato quando ovviamente non esisteva quest'opzione in sede comunitaria.

Secondo problema, che desidero far notare, è quello della certificazione incrociata (*cross certification*) ed intendo sempre la certificazione della chiave pubblica.

A differenza ad esempio degli Stati Uniti, noi abbiamo disegnato un sistema di certificazione orizzontale, lasciando liberi i certificatori di scegliere tra due o più *standards* di fatto, identificati nel D.P.C.M. Ciò significa che ogni certificatore possiede la facoltà di scelta dell'algoritmo di decifratura tra i due indicati (RSA e DSA) e può scegliere il formato del certificato; conseguenza inevitabile è che se i certificatori, che sono soggetti privati, scelgono formati e criteri diversi tra loro, i sistemi non si parlano in assenza di accordi di certificazione.

Quindi il vero problema sarà far sì che i certificatori utilizzino gli stessi sistemi o stipolino accordi di certificazione incrociata, in modo che, come oggi si teme, la firma elettronica non finisca per valere in ambiti settoriali distinti: un certificatore, un ambito settoriale, una firma elettronica. A questo fine sarà opportuno studiare delle soluzioni in proposito.

Concludo, infine, con una considerazione di gerarchia delle fonti, facendo notare che sicuramente esiste un problema a monte.

Nell'articolo 15 della legge n. 59 non abbiamo potuto decidere di utilizzare il sistema Legge di delega - decreto legislativo - regole tecniche, ma il sistema è diverso: Legge n. 59 del 1997 - D.P.R. ai sensi del comma 2 dell'art. 17 della legge 400-Regolamento, con tutte le relative conseguenze in termini di disapplicabilità e di impugnabilità, che sappiamo.

Il sistema è dunque strutturalmente debole e ciò va tenuto sempre presente, sforzandoci, a mio parere, per individuare le situazioni giuridiche e tecnologiche in grado di far sì che questo sistema, destinato a sostituire le tecniche di firma elettronica tradizionali, si realizzi compiutamente.