V. Rizzo (a cura di), "Documento informatico, firma digitale e commercio elettronico"
Collana ITTIG-CNR, Serie "Studi e documenti", n. 2, Napoli, ESI, 2000, pp. 161-176

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 organizzazioni[1] 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 propalazione di un certo numero di informazioni personali, le quali, talvolta, sono chieste espressamente all'interessato, talaltra, 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 di PALAZZI – 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 prestazione[2] 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 credito[3].

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 "scaricamento" 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 F. Angeli, *"Non sarebbe dovuto accadere. Il commercio on-line non è Far West ma fermare i pirati è impossibile"*, *ivi*, 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 informazione[4].

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 contemperamento con altri importanti principî (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, "*hiperlink*" 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/CE[5].

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 completamento 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) nazionale[6].

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/CE[7] (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. 171[8], estende (o, meglio sarebbe dire, dettaglia) alcune norme sulla protezione dei dati personali ai fornitori di un servizio di telecomunicazioni[9], 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.* 30.1.1998, n. L. 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] E' 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. 675[11], 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 applicata[12]), la questione di maggior problematicità, al pari di molte altre che riguardano il commercio elettronico, è legata al principio di territorialità[13] 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 (E. 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) riterrebbe 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 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'àmbito 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 dati[14].

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 principî 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 principî, 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 principî, 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'obiettiva difficoltà 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 secondaria[15].

[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 governativa[17].

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 quelli 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 Paese[18].

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 occasione[19], 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 leso un proprio diritto[20].

---

[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 creazione 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 occasione[21], 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 àmbito 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 posizioni[24].

---

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 Europea.

[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 "*mailing*" elettronico, dimostrando come i principî 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 principî, 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 esistenti[26].

Uno di questi incontri si è svolto, nell'ottobre del 1999, a Parigi[27] 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 principî costituenti un *porto sicuro* deve comprendere, quale requisito minimo, tutti i principî fissati nelle linee-guida in materia di *privacy* elaborate dall'OCSE nel 1980, adottate, fra gli altri, dagli USA"

[26] Il 9 dicembre 1999, poi, l'OCSE ha approvato le *Linee guida per la protezione del consumatore nel contesto del commercio elettronico* (in http //www oced org//dsti/sti/it/consumer/prod/guidelines) che però, in materia di tutela della riservatezza, si limita a rinviare 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 oced org//dsti/sti/it/ec/act/Paris_ec/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 una 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 governative[28].

Tale Commissione, in particolare, in un recente studio sulla *privacy* nel commercio elettronico[29], 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 indipendenti"*, 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.