5.7.2 Utilizzazione di disposizioni contrattuali nel trasferimento di dati personali verso Paesi terzi

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV
Mercato interno e servizi finanziari
Libera circolazione delle informazioni - Diritto delle società e informazioni finanziarie
Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

DG XV D/5005/98 def.
WP 9

Gruppo di lavoro per la tutela delle persone fisiche
con riguardo al trattamento dei dati personali

Documento di lavoro: Pareri preliminari circa l'utilizzazione di disposizioni contrattuali nel contesto del trasferimento di dati personali verso paesi terzi

approvato dal gruppo di lavoro il 22 aprile 1998

1. Introduzione

Nel documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997 e intitolato «Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza», il gruppo di lavoro ha promesso di esaminare nei suoi lavori futuri le circostanze nelle quali soluzioni contrattuali *ad hoc* possano costituire mezzi idonei per garantire la tutela delle persone fisiche ove dati personali vengano trasferiti verso un paese terzo in cui il livello di protezione non sia in genere adeguato. Il presente documento mira a fornire una base per tale esame.

In base al principio di cui all'articolo 25, paragrafo 1 della direttiva relativa alla protezione dei dati (95/46/CE), il trasferimento di dati personali verso paesi terzi può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato. All'articolo 26, paragrafo 1, figurano alcune deroghe a tale norma, che non vengono però esaminate nel presente documento. Obiettivo di quest'ultimo è quello di esaminare l'eventuale ulteriore possibilità di deroga al principio della «protezione adeguata» dell'articolo 25 come stabilito all'articolo 26, paragrafo 2. Tale disposizione permette a uno Stato membro di autorizzare un trasferimento o una categoria di trasferimenti verso un paese terzo «non adeguato» «qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi». La disposizione in seguito specifica che «tali garanzie possono segnatamente risultare da clausole contrattuali». Ai sensi dell'articolo 26, paragrafo 4, inoltre la Commissione può, secondo la procedura di cui all'articolo 31, decidere che alcune clausole contrattuali tipo offrono le garanzie sufficienti di cui all'articolo 26, paragrafo 2.

L'idea di avvalersi di contratti come mezzo per regolamentare i trasferimenti internazionali di dati personali non è stata ovviamente inventata dalla direttiva. Già nel 1992 il Consiglio d'Europa, la Camera di commercio internazionale e la Commissione europea avevano svolto insieme uno studio in merito [39]. In tempi più recenti un numero sempre crescente di esperti e di commentatori, forse notando l'esplicito riferimento nella direttiva, hanno formulato in studi e articoli osservazioni circa l'utilizzazione di contratti. Questi ultimi hanno continuato ad essere utilizzati nel «mondo reale» come mezzo per ovviare ai problemi inerenti alla protezione dei dati derivanti dal trasferimento di dati personali da alcuni Stati membri Ue. I contratti sono stati largamente utilizzati in Francia a partire dalla fine degli anni '80, mentre in Germania il recente caso della «Bahncard» che ha coinvolto la Citibank è stato oggetto di notevole pubblicità [40].

2. Utilizzazione di contratti come base per flussi intracomunitari di dati

Prima di esaminare i requisiti delle disposizioni contrattuali nel contesto dei flussi di dati verso paesi terzi, occorre chiarire la differenza tra la situazione in un paese terzo e quella esistente all'interno della Comunità. In quest'ultimo caso, il contratto rappresenta il meccanismo utilizzato per definire e regolamentare la ripartizione delle responsabilità in materia di protezione dei dati ove più di un ente sia interessato al trattamento dei dati in questione. Ai sensi della direttiva un ente, il «responsabile del trattamento», deve assumersi la responsabilità principale per conformarsi ai principi essenziali di protezione dei dati. Il secondo ente, l'»incaricato del trattamento», è responsabile unicamente della sicurezza dei dati. Per responsabile del trattamento si intende un ente che abbia poteri decisionali circa le finalità e le modalità di trattamento dei dati, mentre l'incaricato del trattamento è unicamente l'ente che fornisce fisicamente il servizio di trattamento dei dati. La relazione tra i due enti è definita nell'articolo 17, paragrafo 3, della direttiva:

– *l'esecuzione dei trattamenti su commissione deve essere disciplinata da un contratto o da un atto giuridico che vincoli l'incaricato del trattamento al responsabile del trattamento e che preveda segnatamente: - che l'incaricato del trattamento operi soltanto su istruzioni del responsabile del trattamento; - che gli obblighi di cui al paragrafo 1 (disposizioni essenziali riguardo alla sicurezza dei dati), quali sono definiti dalla legislazione dello Stato membro nel quale è stabilito l'incaricato del trattamento, vincolino anche quest'ultimo.*

Ciò deriva dal principio generale di cui all'articolo 16 in base al quale l'incaricato del trattamento o chiunque agisca sotto l'autorità del responsabile del trattamento non deve elaborare i dati personali, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi legali.

---

[39] «Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows, with Explanatory Memorandum», studio effettuato congiuntamente dal Consiglio d'Europa, dalla Commissione delle Comunità europee e dalla Camera di commercio internazionale, Strasburgo, 2 novembre 1992.

[40] Cfr. la presentazione di Alexander Dix del caso in questione in occasione dell'«International Data Protection and Privacy Commissioners' Conference», settembre 1996, Ottawa.

Anche nel caso di trasferimento di dati personali verso paesi terzi, in genere sarà coinvolta più di una parte. In questo caso la relazione è tra l'ente che trasferisce i dati (il «cedente») e l'ente che riceve i dati nel paese terzo (il «destinatario»). In questo contesto uno degli obiettivi del contratto dovrebbe essere quello di determinare le modalità di ripartizione della responsabilità in materia di protezione dei dati tra le due parti. Peraltro il contratto deve mirare anche ad altro, cioè a fornire garanzie supplementari alla persona interessata dal trattamento dei dati, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto a un complesso di norme vincolanti in materia di protezione dei dati, atte a garantire un livello adeguato di tutela.

3. Obiettivo di una soluzione contrattuale

Nell'ambito del trasferimento verso paesi terzi, quindi, il contratto costituisce un mezzo per il responsabile del trattamento di fornire garanzie adeguate al momento di trasferire i dati al di fuori della Comunità (e quindi al di fuori della tutela prevista dalla direttiva, nonché dal contesto generale della legislazione comunitaria [41]) verso un paese terzo in cui il livello generale di protezione non sia adeguato. Per soddisfare tale funzione, una disposizione contrattuale deve compensare in modo soddisfacente la mancanza di un livello generale di protezione adeguata e comportare gli elementi essenziali di tutela che possono mancare in una qualsiasi situazione particolare.

4. Requisiti specifici di una soluzione contrattuale

Il punto di partenza per valutare il significato di «garanzie sufficienti» quali utilizzate all'articolo 26, paragrafo 2, è la nozione di «tutela adeguata» già elaborata in parte nel documento di discussione «Primi orientamenti ...» [42]. Tale documento illustra una strategia consistente in una serie di principi fondamentali in materia di protezione dei dati nonché in tre ulteriori requisiti: che nella pratica sussista un buon livello di osservanza di tali principi, che siano forniti sostegno e assistenza alle persone interessate dal trattamento dei dati per l'esercizio dei propri diritti e che vi sia una riparazione adeguata alla parte lesa ove tali principi non vengano osservati.

(i) Norme essenziali in materia di protezione dei dati

Il primo requisito della soluzione contrattuale è, quindi, che le parti interessate al trasferimento dei dati siano obbligate a garantire l'applicazione del complesso di principi fondamentali in materia di protezione dei dati figuranti nel documento «Primi orientamenti» all'atto del trattamento dei dati trasferiti verso il paese terzo. Tali principi fondamentali sono:

---

[41] L'esercizio dei diritti in materia di tutela dei dati da parte di una persona fisica è facilitato nell'ambito del contesto giuridico generale della Comunità, come ad esempio dall'Accordo di Strasburgo (1977) circa la trasmissione di richieste di assistenza giuridica.

[42] «Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza», documento di discussione approvato dal gruppo di lavoro il 26 giugno 1997.

1) **il principio della finalità limitata:** i dati dovrebbero essere trattati per una finalità specifica e successivamente utilizzati o ulteriormente comunicati soltanto nella misura in cui non vi sia incompatibilità con la finalità del trasferimento. Le uniche deroghe a tale norma sarebbero quelle necessarie in ogni società democratica per una delle ragioni elencate nell'articolo 13 della direttiva (ad esempio, sicurezza dello Stato, accertamento di infrazioni penali) [43];

2) **il principio della qualità e della proporzionalità:** i dati dovrebbero essere precisi e, se del caso, aggiornati. Essi dovrebbero essere adeguati, pertinenti e non andare al di là delle finalità per cui sono oggetto di trasferimento o di ulteriore trattamento;

3) **il principio della trasparenza:** la persona dovrebbe ricevere informazioni riguardanti la finalità del trattamento dei dati e l'identità del responsabile del trattamento nel paese terzo, nonché qualunque altra informazione necessaria ad assicurare una procedura equa. Le uniche deroghe consentite dovrebbero essere conformi all'articolo 13 della direttiva, o all'articolo 11, paragrafo 2, che consente alle organizzazioni che non hanno raccolto i dati direttamente dalla persona interessata di essere dispensate da tale disposizione se l'informazione della persona interessata si rivela impossibile o richiede sforzi sproporzionati;

4) **il principio della sicurezza:** il responsabile del trattamento dei dati dovrebbe adottare misure di sicurezza tecnica e organizzativa commisurate ai rischi che il trattamento presenta. Chiunque operi sotto l'autorità del responsabile del trattamento, compreso un incaricato del trattamento, si occupa del trattamento dei dati solo su istruzione del responsabile medesimo;

5) **i diritti di accesso, rettifica e opposizione:** la persona interessata dovrebbe avere il diritto di ottenere una copia di tutti i dati trattati che la riguardano, nonché il diritto di far rettificare i dati di comprovata inesattezza. In determinate situazioni, la persona interessata dovrebbe inoltre potersi opporre al trattamento dei dati che la riguardano. Le uniche deroghe a tali diritti dovrebbero essere conformi all'articolo 13 della direttiva;

6) **restrizioni ai successivi trasferimenti verso parti non firmatarie del contratto**: ulteriori trasferimenti dei dati personali dal destinatario verso terzi non dovrebbero essere consentiti, a meno di trovare un metodo contrattuale che vincoli i terzi in questione a fornire alle persone interessate le stesse garanzie di protezione dei dati.

Inoltre, in alcune situazioni, vanno applicati principi supplementari:

1) **dati sensibili**: se il trattamento riguarda categorie «sensibili» di dati (quelle elencate all'articolo 8), si dovrebbero porre in essere misure di salvaguardia supplementari, come ad esempio l'obbligo del consenso esplicito al trattamento da parte della persona interessata;

2) **commercializzazione diretta**: 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;

---

[43] Occorre rilevare che le finalità statistiche e di ricerca scientifica sono in genere considerate compatibili, a condizione che siano offerte garanzie adeguate.

3) **decisioni individuali automatizzate**: se la finalità del trasferimento consiste nell'adozione di una decisione automatizzata ai sensi dell'articolo 15 della direttiva, l'individuo dovrebbe avere il diritto di conoscere la logica che muove tale decisione e si dovrebbero prendere altri provvedimenti per garantire la salvaguardia del suo interesse legittimo.

Nel contratto andrebbe specificato in modo dettagliato il metodo in base al quale il destinatario del trasferimento dei dati dovrebbe applicare tali principi (ad esempio, andrebbero specificate le finalità, le categorie di dati, i termini di conservazione, le misure di sicurezza, ecc.). In altre situazioni, ad esempio quando in un paese terzo la protezione dei dati è fornita nell'ambito di una legislazione generale di protezione dei dati simile a quella specificata nella direttiva, potrebbero essere presenti altri meccanismi atti a chiarire il modo in cui le norme di protezione dei dati si applicano nella pratica (codici di comportamento, notifica, funzione di consulenza dell'autorità di controllo). In una situazione contrattuale ciò non avviene, ed è quindi indispensabile, quando il trasferimento avviene in base a un contratto, specificare i dettagli.

(ii) Rendere efficaci le norme essenziali

Nel documento «Primi orientamenti ...» figurano tre criteri in base ai quali andrebbe valutata l'efficacia del sistema di protezione dei dati. In base a tali criteri, il sistema dovrebbe:

1) fornire un **buon livello di osservanza** delle norme (non esiste alcun sistema che possa garantire un'osservanza del 100%, anche se alcuni sistemi sono migliori di altri). Un buon sistema è in genere caratterizzato da un elevato grado di consapevolezza dei propri obblighi da parte dei responsabili del trattamento e dei propri diritti e mezzi per esercitarli da parte delle persone interessate. L'esistenza di sanzioni efficaci e deterrenti è importante per garantire il rispetto delle norme, come lo sono pure sistemi di verifica diretta da parte di autorità, revisori o funzionari indipendenti addetti alla protezione dei dati;

2) fornire **sostegno e assistenza alle persone interessate dal trattamento dei dati** nell'esercizio dei propri diritti. La persona dev'essere in grado di far valere i propri diritti tempestivamente e in modo efficace, senza costi proibitivi. A tal fine, occorre la presenza di un tipo di struttura o meccanismo che consenta un controllo indipendente dei reclami;

3) fornire una **riparazione adeguata** alla parte lesa, quando le norme non vengono osservate. Si tratta di un elemento chiave, che deve comportare un sistema che fornisca giudizi imparziali e che consenta il risarcimento dei danni e l'imposizione di sanzioni a seconda dei casi.

Nel valutare l'efficacia di una soluzione contrattuale vanno applicati gli stessi criteri. Si tratta chiaramente di una sfida difficile ma non impossibile. Occorre trovare un mezzo che possa compensare l'assenza di meccanismi di controllo e di imposizione e fornire sostegno, assistenza e, in ultima analisi, una riparazione adeguata alla persona interessata, anche se non firmataria del contratto.

Ognuno di questi aspetti va esaminato nei dettagli. Per facilitare l'analisi, essi vengono esaminati in ordine inverso.

Fornire una riparazione alla persona interessata

Fornire un ricorso legale alla persona interessata (ad esempio, il diritto di presentare un reclamo ad un arbitro indipendente che possa giudicare in merito e il diritto di ricevere se del caso una riparazione) tramite un contratto tra il «ce-

dente» e il «destinatario» dei dati non è una questione semplice. Molto dipenderà dalla natura della legislazione in materia di contratti prescelta come legge nazionale applicabile al contratto. Prevedibilmente la legge applicabile sarà in genere quella dello Stato membro in cui la parte cedente è insediata. In alcuni Stati membri la legislazione in materia di contratti consente l'istituzione di diritti di terzi, che invece non è possibile in altri Stati membri.

In genere, comunque, quanto più il destinatario è limitato per quanto riguarda la possibilità di scegliere le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, tanto maggiore è la sicurezza giuridica per la persona interessata. Tenendo presente che si sta trattando di casi di protezione generale inadeguata, la soluzione migliore sarebbe quella di specificare nel contratto le modalità secondo le quali il destinatario deve applicare i principi fondamentali in materia di protezione dei dati in modo così dettagliato che, in pratica, il destinatario del trasferimento in questione non ha alcun potere autonomo di decisione per quanto riguarda i dati trasferiti o il modo in cui essi vengono trattati successivamente. Il destinatario è tenuto ad agire soltanto dietro istruzioni del cedente e, anche se i dati potrebbero essere stati fisicamente trasferiti al di fuori dell'Ue, il controllo decisionale sui dati spetta sempre all'ente, insediato nella Comunità, che ha effettuato il trasferimento. In tal modo il cedente resta il responsabile del trattamento, mentre il destinatario è semplicemente un subappaltatore incaricato del trattamento. In questo caso, dato che il controllo dei dati è esercitato da un ente che risiede in uno Stato membro dell'Ue, la legislazione dello Stato membro in questione continuerà ad essere applicabile al trattamento effettuato nel paese terzo [44], e inoltre il responsabile del trattamento continuerà, ai sensi della legislazione di tale Stato membro, ad essere responsabile di eventuali danni cagionati da un trattamento illecito [45].

Questo tipo di accordo non è molto dissimile da quello stabilito dall'»Accordo inter-territoriale» che ha risolto il caso Citibank «Bahncard» menzionato in precedenza. In questo caso, l'accordo contrattuale fissava nei dettagli le disposizioni riguardanti il trattamento dei dati, in particolare quelle relative alla sicurezza dei dati, e ne vietava qualsiasi altra utilizzazione da parte del destinatario del trasferimento. Nell'accordo la legislazione tedesca veniva applicata al trattamento dei dati effettuato nel paese terzo, garantendo in tal modo un ricorso legale alle persone interessate [46].

Naturalmente si verificheranno casi in cui sarà impossibile avvalersi di tale soluzione. Potrebbe darsi che il destinatario del trasferimento non debba semplicemente fornire un servizio di trattamento dei dati al responsabile del trattamento insediato nell'Ue, ma abbia, ad esempio, noleggiato o acquistato i dati per utilizzarli per i propri interessi o i propri scopi. In tali circostanze il destinatario dovrà disporre di una certa libertà nel trattamento dei dati, diventando in pratica a tutti gli effetti un «responsabile del trattamento» dei dati.

---

[44] Ai sensi dell'art. 4, paragrafo 1, lettera a), della direttiva 95/46/CE.

[45] Cfr. art. 23 della direttiva 95/46/CE.

[46] Peraltro, dato che il caso è sopravvenuto nell'ambito di una legislazione precedente alla direttiva, la legislazione stessa non è stata applicata automaticamente a tutti i trattamenti controllati da un responsabile del trattamento insediato in Germania. Il ricorso legale per le persone interessate è stato invece possibile grazie alla legislazione contrattuale tedesca che consente di istituire diritti di terzi.

In casi del genere non è possibile fare affidamento sull'applicabilità automatica permanente della legislazione di uno Stato membro e sulla responsabilità permanente del cedente per eventuali danni causati. Per fornire alle persone interessate un adeguato ricorso legale vanno concepiti altri meccanismi più complessi. Come detto in precedenza, alcuni sistemi giuridici consentono a terzi la rivendicazione di diritti nell'ambito di un contratto, e questa possibilità potrebbe essere utilizzata per istituire i diritti delle persone interessate grazie ad un contratto pubblico e pubblicato tra il cedente e il destinatario. La posizione delle persone interessate verrebbe ulteriormente rafforzata ove, come parte del contratto, le parti si impegnassero a sottoporsi ad una specie di arbitrato vincolante qualora una persona interessata dal trattamento dei dati contestasse la loro osservanza. Alcuni codici di autodisciplina settoriale includono tali meccanismi di arbitrato, e potrebbe essere utile prevedere l'utilizzazione di contratti abbinata a tali codici.

Un'altra possibilità consiste nello stipulare, eventualmente al momento dell'ottenimento iniziale dei dati, un accordo contrattuale a parte tra il cedente e la persona interessata dal trattamento dei dati, in base al quale il cedente rimarrebbe responsabile di eventuali danni o difficoltà causate dall'inosservanza, da parte del destinatario del trasferimento dei dati, dell'insieme convenuto di principi fondamentali in materia di protezione dei dati. In questo modo la persona interessata ha la garanzia di un ricorso contro il cedente per le infrazioni del destinatario. Spetterebbe allora al cedente ottenere il risarcimento dei danni pagati alla persona interessata, intentando causa al destinatario per inadempienza contrattuale.

Una soluzione a tre così complessa è forse più attuabile di quanto possa sembrare a prima vista. Il contratto con la persona interessata potrebbe diventare parte integrante delle condizioni generali tipo in base alle quali una banca o un'agenzia di viaggi, ad esempio, fornisce servizi ai clienti, presentando inoltre il vantaggio della trasparenza: la persona interessata è pienamente cosciente dei suoi diritti.

Infine, come alternativa a un contratto con la persona interessata, si potrebbe prospettare la possibilità, per uno Stato membro, di disporre per legge una responsabilità permanente dei responsabili del trattamento che trasferiscono dati al di fuori della Comunità per quanto riguarda eventuali danni causati dalle azioni del destinatario del trasferimento.

Fornire sostegno e assistenza alle persone interessate dal trattamento dei dati

Una delle principali difficoltà cui devono far fronte le persone i cui dati vengono trasferiti verso una giurisdizione straniera è quello di essere incapaci di scoprire la causa originaria del problema particolare che le affligge e di trovarsi quindi nell'incapacità di giudicare se le norme di protezione dei dati siano state correttamente osservate oppure se sussistano motivi di ricorso legale [47]. Per un livello di tutela adeguato è quindi necessario un certo tipo di meccanismo istituzionale che possa indagare sui reclami.

---

[47] Anche se i diritti delle persone interessate sono stati garantiti nell'ambito di un contratto, tali persone spesso non saranno in grado di giudicare se si sia verificata un'inadempienza contrattuale e da parte di chi. È quindi necessaria una procedura investigativa al di fuori delle procedure legali del diritto civile ufficiale.

Il controllo e la funzione investigativa dell'autorità di controllo di uno Stato membro si limitano al trattamento dei dati effettuato nel territorio dello Stato membro in questione [48]. Quando i dati vengono trasferiti verso un altro Stato membro, un sistema di assistenza reciproca tra le autorità di controllo garantisce che un eventuale reclamo di una persona interessata nel primo Stato membro venga sottoposto ad un'indagine adeguata. Quando invece il trasferimento è effettuato verso un paese terzo, nella maggior parte dei casi tale garanzia non esiste. Si tratta quindi di esaminare che tipo di meccanismo di compensazione possa essere adottato nel contesto di un trasferimento di dati sulla base di un contratto.

Una possibilità potrebbe essere quella di esigere semplicemente una clausola contrattuale che garantisca all'autorità di controllo dello Stato membro in cui è insediato il cedente il diritto di controllare il trattamento effettuato dall'incaricato del trattamento nel paese terzo. Nella pratica, tale controllo potrebbe essere effettuato da un agente (ad esempio, una società di certificazione specializzata) designato dall'autorità di controllo, ove necessario. Una difficoltà inerente a un metodo del genere, tuttavia, consiste nel fatto che l'autorità di controllo in genere [49] non è parte firmataria del contratto e, di conseguenza, in alcune giurisdizioni potrebbe non avere i mezzi di appellarsi ad esso per avere accesso. Un'altra possibilità potrebbe essere un obbligo legale fornito dal destinatario nel paese terzo direttamente all'autorità di controllo dello Stato membro dell'Ue interessato, in base al quale il destinatario dei dati autorizza l'accesso all'autorità di controllo o a un agente designato qualora sorgessero sospetti di inadempienza dei principi in materia di protezione dei dati. Tale obbligo potrebbe anche richiedere alle parti interessate dal trasferimento dei dati di informare l'autorità di controllo circa qualsiasi reclamo ricevuto dalle persone interessate dal trattamento dei dati. Ai sensi di tale accordo tale obbligo sarebbe una condizione da soddisfare prima dell'autorizzazione al trasferimento dei dati.

Indipendentemente dalla soluzione prescelta, permangono tuttavia seri dubbi quanto all'opportunità, praticità o invero fattibilità, da un punto di vista delle risorse, di assumersi - da parte di un'autorità di controllo di uno Stato membro dell'Ue - la responsabilità di esaminare e controllare il trattamento di dati effettuato in un paese terzo.

Fornire un buon livello di osservanza

Anche in mancanza di un particolare reclamo o difficoltà riscontrata da una persona interessata dal trattamento dei dati, è indispensabile un elevato grado di fiducia nell'osservanza delle condizioni contrattuali da parte dei firmatari. Il problema con la soluzione contrattuale consiste nella difficoltà di fissare sanzioni per inosservanza del contratto che siano sufficientemente significative e ottenere l'effetto deterrente necessario per garantire tale fiducia. Anche qualora un controllo efficace dei dati continuasse ad essere esercitato dall'interno della Comunità, il destinatario del trasferimento potrebbe non incorrere in alcuna sanzione penale diretta, anche se il trattamento dei dati avvenisse in violazione del contratto. La responsabilità incomberebbe invece al cedente insediato nella

---

[48] Cfr. art. 28, paragrafo 1, della direttiva 95/46/CE.

[49] Secondo la delegazione francese potrebbero verificarsi situazioni in cui l'autorità di controllo è parte firmataria del contratto.

Comunità, che dovrebbe poi ottenere il risarcimento di eventuali danni intentando una causa a parte contro il destinatario. Una responsabilità indiretta del genere potrebbe non essere sufficiente a indurre il destinatario all'osservanza di tutti i dettagli del contratto.

Stando così le cose, è probabile che nella maggior parte dei casi una soluzione contrattuale dovrà essere integrata da quanto meno la possibilità di una qualche forma di controllo esterno delle attività di trattamento del destinatario, ad esempio una verifica effettuata da un ente di normalizzazione o da una società di certificazione specializzata.

5. Il problema della legge dirimente

Una difficoltà particolare insita nel metodo contrattuale è la possibilità che la legislazione generale del paese terzo contempli l'obbligo, per il destinatario del trasferimento dei dati, di rivelare - in determinati casi - dati personali alle autorità pubbliche (polizia, tribunali o fisco, ad esempio) e che tali obblighi legali abbiano la precedenza su qualsiasi contratto che l'incaricato del trattamento abbia sottoscritto [50]. Per gli incaricati del trattamento all'interno della Comunità questa possibilità figura all'articolo 16 della direttiva, secondo cui l'incaricato del trattamento può elaborare i dati solo dietro istruzione del responsabile del trattamento oppure *in virtù di obblighi legali.* Ai sensi della direttiva, peraltro, la rivelazione di informazioni (che sia per sua stessa natura per finalità incompatibili con quelle per le quali i dati sono stati raccolti) va limitata al minimo necessario in società democratiche e per uno dei motivi di «ordine pubblico» di cui all'articolo 13, paragrafo 1, della direttiva. Anche l'articolo 6 del trattato di Amsterdam garantisce il rispetto dei diritti fondamentali stabiliti nella Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. In paesi terzi non sempre potrebbero esistere analoghe limitazioni per i poteri pubblici di ottenere dati personali da società e da altre organizzazioni operanti sul loro territorio.

Non esiste un metodo facile per superare tale difficoltà, da cui si evincono chiaramente le limitazioni del metodo contrattuale. In alcuni casi il contratto è uno strumento troppo fragile per offrire garanzie adeguate di protezione dei dati, e non andrebbero autorizzati trasferimenti verso certi paesi.

6. Considerazioni pratiche in merito all'utilizzazione di contratti

Dall'analisi precedente si è visto che qualsiasi soluzione contrattuale deve essere particolareggiata e opportunamente adeguata al trasferimento di dati in questione. Questo bisogno di dettaglio, per quanto riguarda le finalità e le condizioni precise di trattamento dei dati trasferiti, non esclude la possibilità di elaborare un modello di contratto tipo che però, per ogni contratto, andrà completato in modo da adeguarlo alle circostanze particolari del caso.

---

[50] La portata dei poteri pubblici per quanto concerne l'obbligo di rivelare informazioni è un aspetto di cui tener conto anche al momento di una valutazione più generale dell'adeguatezza della tutela in un paese terzo.

L'analisi ha inoltre dimostrato che esistono difficoltà pratiche particolari nell'indagine dell'inosservanza di un contratto quando il trattamento avviene al di fuori dell'Ue e ove il paese terzo in questione non fornisca alcuna forma di autorità di controllo. Insieme, queste due considerazioni significano che si verificheranno alcune situazioni in cui la soluzione contrattuale potrebbe essere la soluzione adeguata, mentre in altre situazioni potrebbe essere impossibile fornire per contratto le necessarie «garanzie sufficienti».

Vista l'esigenza di un adeguamento particolareggiato di un contratto alle peculiarità del trasferimento in questione, un contratto è particolarmente adatto in situazioni in cui i trasferimenti di dati sono simili e di natura ripetitiva. Date le difficoltà inerenti al controllo, una soluzione contrattuale potrebbe essere maggiormente efficace quando le parti firmatarie del contratto sono rappresentate da operatori importanti già sottoposti a sorveglianza e regolamentazione pubblica [51]. Le grandi reti internazionali, ad esempio quelle utilizzate per le transazioni nel campo delle carte di credito e per le prenotazioni aeree, presentano entrambe queste caratteristiche e fanno riscontrare situazioni in cui i contratti si potrebbero rivelare estremamente utili. In queste circostanze, essi potrebbero addirittura essere integrati da convenzioni multilaterali intese a fornire una migliore sicurezza giuridica. Allo stesso modo, quando le parti interessate dal trasferimento sono affiliate o formano parte dello stesso gruppo di imprese, la capacità di indagare in merito all'inosservanza di un contratto è presumibilmente molto rafforzata, dati gli stretti legami tra il destinatario nel paese terzo e l'ente insediato nella Comunità. I trasferimenti intra-aziendali costituiscono pertanto un altro settore che presenta un chiaro potenziale per lo sviluppo di soluzioni contrattuali efficaci.

Conclusioni e raccomandazioni principali

– Nell'ambito della Comunità i contratti vengono utilizzati come mezzo per stabilire la ripartizione delle responsabilità in materia di osservanza della protezione dei dati tra il responsabile del trattamento e il subappaltatore incaricato del trattamento. Un contratto utilizzato per flussi di dati verso paesi terzi deve fare molto di più: fornire garanzie supplementari alle persone interessate dal trattamento dei dati, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto a un complesso di norme vincolanti in materia di protezione dei dati atte a fornire un livello di tutela adeguato.

– La base per la valutazione dell'adeguatezza delle garanzie fornite da una soluzione contrattuale è la stessa che per la valutazione del livello generale di adeguatezza in un paese terzo. Una soluzione contrattuale deve comprendere tutti i principi fondamentali in materia di protezione dei dati e fornire mezzi con cui rendere applicabili tali principi.

– Nel contratto andrebbero specificati in dettaglio le finalità, i mezzi e le condizioni di trattamento dei dati trasferiti, nonché le modalità di applicazione dei principi fondamentali in materia di protezione dei dati. Una maggiore sicurezza giuridica è fornita da contratti in cui viene limitata la libertà del destinatario dei dati di trattare questi ultimi in modo autonomo per proprio conto. Il con-

[51] Nel caso Citibank «Bahncard» il sovrintendente alla tutela dei dati di Berlino ha cooperato con le autorità di controllo bancario americane.

tratto andrebbe quindi utilizzato, nei limiti del possibile, come mezzo con cui l'ente che trasferisce i dati mantiene il controllo decisionale sul trattamento effettuato nel paese terzo.

– Ove il destinatario abbia un certo grado di autonomia quanto al trattamento dei dati trasferiti, la situazione non è chiara, e un solo contratto tra le parti interessate al trasferimento può non sempre costituire una base sufficiente per l'esercizio dei diritti da parte delle persone interessate dal trattamento dei dati. Potrebbe essere necessario un meccanismo in base al quale la parte insediata nella Comunità che provvede al trasferimento resta responsabile di eventuali danni causati dal trattamento effettuato nel paese terzo.

– I trasferimenti successivi verso enti o organizzazioni non legate dal contratto andrebbero specificatamente esclusi dal contratto in questione, a meno che non sia possibile vincolare per contratto tali terzi a rispettare gli stessi principi in materia di protezione dei dati.

– Il grado di fiducia nel rispetto dei principi in materia di protezione dei dati dopo il trasferimento dei dati stessi verrebbe rafforzato se l'osservanza dei principi di protezione dei dati da parte del destinatario del trasferimento fosse sottoposta ad una verifica esterna da parte, ad esempio, di una società di certificazione specializzata o di un istituto di normalizzazione.

– Qualora una persona interessata dal trattamento dei dati incontrasse un problema derivante eventualmente da una violazione delle disposizioni in materia di protezione dei dati garantite nel contratto, il problema generale è quello di garantire che il reclamo della persona interessata venga adeguatamente esaminato. Le autorità di controllo degli Stati membri dell'Ue riscontreranno difficoltà pratiche nell'effettuare tale controllo.

– Le soluzioni contrattuali sono probabilmente più adatte a grandi reti internazionali (carte di credito, prenotazioni aeree) caratterizzate da notevoli quantità di trasferimenti di dati ripetitivi di natura simile e da un numero relativamente esiguo di importanti operatori in settori industriali già sottoposti ad un elevato grado di controllo e di regolamentazione pubblica. I trasferimenti intra-aziendali di dati tra varie branche dello stesso gruppo di imprese è un altro settore in cui esiste un notevole potenziale per l'utilizzazione dei contratti.

– I paesi in cui i poteri delle autorità pubbliche in materia di accesso alle informazioni superano quelli consentiti dalle norme internazionalmente accettate in materia di tutela dei diritti dell'uomo non rappresentano destinazioni sicure per i trasferimenti basati su clausole contrattuali.

Fatto a Bruxelles, il 22 aprile 1998

Per il gruppo di lavoro
Il presidente P.J. Hustinx

5.7.3 Raccomandazione 1/98 in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV
Mercato interno e servizi finanziari
Libera circolazione delle informazioni, diritto delle società ed informazione finanziaria
Libera circolazione delle informazioni e protezione dei dati, compresi gli aspetti internazionali

XV/ D/5009/98 def.
WP 10

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Raccomandazione 1/98 in materia di sistemi telematici di prenotazione (CRS) nel trasporto aereo

adottata dal Gruppo il 28 aprile 1998

IL GRUPPO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [52)],

Visto l'articolo 29 e l'articolo 30, paragrafo 3 della menzionata direttiva,

Visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO LA PRESENTE RACCOMANDAZIONE:

1. INTRODUZIONE

L'articolo 6, paragrafo 1, lettera *b)* della direttiva 95/46 impone agli Stati membri di disporre che i dati personali siano «rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità»; a norma del § 1, lettera *e)* del medesimo articolo, i dati devono essere «conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati».

[52)] GU L 281 del 23.11.1995, pag. 31.

L'art. 8 della direttiva impone agli Stati membri di vietare il trattamento di dati personali che rivelino, tra l'altro, l'origine razziale o etnica, le convinzioni religiose e le condizioni di salute. Sono ammesse deroghe a questo principio per i motivi specificati nell'art. 8, paragrafi 2 e 3, ed uno di tali motivi è costituito dal consenso esplicito della persona interessata.

Ai sensi della direttiva la persona interessata gode di specifici diritti, compreso il diritto di essere informato circa il trattamento dei suoi dati personali (articoli 10 e 11), nonché i diritti di accesso, di rettifica e di cancellazione (art. 12).

In considerazione degli aspetti peculiari alle prenotazioni nel trasporto aereo e delle recenti iniziative della Commissione in tale settore [53)], il Gruppo ha deciso di creare un sottogruppo in materia di sistemi telematici di prenotazione (CRS). Esso si è riunito due volte ed ha stabilito di presentare al Gruppo gli esiti dei suoi lavori in vista dell'adozione della presente raccomandazione.

2. Relazione

Il settore del trasporto aereo è caratterizzato da un uso estremamente avanzato di sistemi informatici. Esistono banche dati contenenti dati personali in molti ambiti: in particolare presso le compagnie aeree, gli agenti di viaggio ed i sistemi telematici di prenotazione (CRS). Diverse banche dati (in particolare, ma non esclusivamente, i CRS) sono ubicate al di fuori del territorio della Comunità.

In considerazione della natura internazionale del trasporto aereo, le soluzioni di carattere generale sono, in linea di principio, le più appropriate.

Il Gruppo ritiene che i seguenti aspetti meritino di essere considerati in via prioritaria:

1. Informazione e diritto di accesso:

– La grande maggioranza dei dati personali viene raccolta dagli agenti di viaggio e dai vettori aerei. Per motivi pratici, e senza pregiudizio della definizione di «responsabile del trattamento» ai sensi della direttiva 95/46/CE, la questione del diritto di accesso della persona interessata dovrebbe pertanto investire in primis tali operatori.

– Tuttavia, taluni aspetti relativi all'accesso possono anche essere regolamentati direttamente assieme ai CRS, e ciò potrebbe avvenire nel progetto di regolamento relativo al codice di comportamento per i CRS proposto dalla Commissione.

– Il codice di comportamento in materia di sistemi telematici di prenotazione ribadisce il diritto dei passeggeri di essere informati in modo dettagliato circa il trattamento dei dati. Tale diritto potrebbe essere rafforzato attraverso il coinvolgimento degli abbonati (ad esempio gli agenti di viaggio) e dei vettori aerei.

2. Cancellazione di dati:

– È auspicabile assicurare che i dati personali siano cancellati dai sistemi computerizzati di prenotazione non appena cessino di essere utilizzati ai fini del viaggio.

[53)] Proposta di regolamento (CE) del Consiglio che modifica il regolamento (CEE) n. 2299/89 del Consiglio relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione (CRS); COM (97) 246 def. del 9 luglio 1997.

– Mentre tali dati possono servire nel caso di contenzioso e pertanto potrebbe risultare necessario conservarli per un certo periodo di tempo, essi dovrebbero essere utilizzati soltanto a tale fine specifico ed essere successivamente distrutti.

– Ciò non pregiudica la possibilità che gli abbonati ed i vettori aerei ottengano il consenso da parte di viaggiatori abituali al fine del trattamento dei loro dati personali in conformità della direttiva 95/46/CE.

3. Conclusioni

In considerazione di quanto precede, il Gruppo raccomanda che:

– La proposta di regolamento che modifica il regolamento (CEE) n. 2299/89 del Consiglio relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione (CRS) sia integrata prevedendo:

– Il preciso obbligo di fornire **informazioni** al cliente circa il trattamento dei dati personali nel sistema telematico. Tali informazioni, che possono essere diffuse ad esempio con opuscoli illustrativi, dovrebbero includere il nome e l'indirizzo del venditore del sistema, gli scopi del trattamento dei dati, il periodo di conservazione degli stessi, nonché le modalità e gli strumenti necessari per l'esercizio del diritto di accesso da parte della persona interessata.

– L'obbligo per gli abbonati (ad esempio, agenti di viaggio) ed i vettori aerei di ottenere dalle persone interessate l'esplicito consenso alla raccolta di dati di natura delicata (condizione di disabile, pasti conformi ai precetti islamici, ecc.). Qualora il CRS includa la possibilità di emissione diretta di biglietti, tale obbligo deve essere applicato al venditore del sistema [54].

– L'obbligo delle parti citate di rispondere immediatamente ad una richiesta di **accesso** da parte di un passeggero che desideri prendere visione dei propri dati.

– L'obbligo per il CRS di assicurare che tutti i dati personali identificati siano archiviati fuori linea entro le 72 ore successive al termine del viaggio in questione [55] e distrutti entro un periodo non superiore ai tre anni. L'accesso a tali dati dovrà essere consentito soltanto ai fini della composizione di controversie relative alla fatturazione. Nonostante l'obbligo di distruggere i dati entro tre anni, i dati personali possono essere conservati per un periodo più lungo e per tutto il tempo necessario nel caso specifico al fine di espletare una richiesta di indennizzo per danni ovvero per il periodo stabilito da disposizioni di legge (ad esempio, le disposizioni in materia contabile e fiscale).

– L'obbligo di effettuare le necessarie modifiche al fine di estendere l'ambito di applicazione del controllo previsto dall'art. 21 bis.

– Inoltre, il Gruppo raccomanda che vengano presi in esame in via prioritaria gli specifici problemi sollevati dalle prenotazioni in linea che non rientrano nell'ambito di applicazione del CRS (ad esempio, agenti di viaggio o vettori aerei che propongono l'acquisto diretto di biglietti via Internet) e che la Commis-

---

[54] Secondo la definizione contenuta nel citato codice di comportamento, si intende per «venditore del sistema» «qualsiasi impresa e le sue affiliate che provveda alla gestione o commercializzazione di un CRS».

[55] Come indicato nella relazione, rimane impregiudicato il diritto degli abbonati e dei vettori aerei di trattare i dati di natura delicata relativi ai viaggiatori abituali nei propri sistemi informatici, dietro consenso esplicito della persona interessata.

sione proponga con urgenza delle soluzioni appropriate. A tale proposito, invita la Commissione a precisare se tale aspetto è disciplinato dalla direttiva 97/66/CE [56] ed in che misura.

La presente raccomandazione, adottata dal Gruppo in data 28 aprile 1998, è rivolta alla Commissione europea, al Parlamento europeo, al Consiglio dell'Unione europea ed al Comitato economico e sociale.

Fatto a Bruxelles, addì 28 aprile 1998

Per il Gruppo
Il Presidente P.J. HUSTINX

[56] Direttiva 97/66/CE del Parlamento Europeo e del Consiglio del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni (GU L 24 del 30.1.1998, pag. 1).

5.7.4 Parere n. 1/98: preferenze in materia di protezione della vita privata e la «norma aperta per i profili»

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV
Mercato interno e servizi finanziari
Libera circolazione delle informazioni - Diritto delle società e informazione finanziaria
Libera circolazione delle informazioni, tutela dei dati e relativi aspetti internazionali

XV D/5032/98
WP 11

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

Parere n. 1/98: Piattaforma per le preferenze in materia di protezione della vita privata (P3P - *Platform for Privacy Preferences*) e la «norma aperta per i profili» (OPS - *Open Profiling Standard*)

Adottato dal gruppo il 16 giugno 1998

PARERE DEL GRUPPO

Il progetto della piattaforma per le preferenze in materia di protezione della vita privata (P3P - *Platform for Privacy Preferences*) considera la tutela della vita privata e dei dati personali come un elemento che deve essere stabilito di comune accordo fra l'utente Internet di cui si raccolgono i dati ed il sito Web che li registra. Il principio di base prevede che l'utente acconsenta alla raccolta dei suoi dati personali da parte di un sito (l'*Open Profiling Standard* è volto a fornire la trasmissione sicura di un profilo standard di dati personali), solo se le pratiche dichiarate del sito in termini di protezione della vita privata (per esempio le finalità della raccolta dei dati, l'eventuale uso a fini secondari o la cessione a terzi) soddisfano le esigenze dell'utente. Il World Wide Web Consortium ha cercato di elaborare un unico vocabolario che permettesse di esprimere le preferenze dell'utente e le pratiche del sito. Non è prevista la possibilità di adattare questo vocabolario alle esigenze e al quadro normativo di regioni geografiche specifiche. Sorprende il fatto che, malgrado la prevista applicabilità universale della P3P, il suddetto vocabolario non sia stato messo a punto facendo riferimento alle norme conosciute di livello più elevato nella protezione dei dati personali e della vita privata, ma si limiti a formalizzare norme comuni di livello inferiore. Queste decisioni di strategia fanno sì che l'applicazione della P3P e dell'OPS in seno all'Unione europea abbia buone probabilità di sollevare una serie di problemi specifici, discussi più avanti. Affinché la P3P e l'OPS abbiano ricadute positive sulla protezione della vita privata «in linea», è di fondamentale importanza che siano affrontati questi argomenti.

– Una piattaforma tecnica per la protezione della vita privata non sarà di per sé sufficiente a garantire tale protezione sul Web. Occorre che una piattaforma del genere sia applicata in un quadro di regole esecutive sulla tutela dei dati, in