tario 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 [70].

Naturalmente in certi casi sarà impossibile ricorrere a questa soluzione. Potrebbe darsi che il destinatario del trasferimento non debba semplicemente fornire un servizio di trattamento dei dati al responsabile del trattamento stabilito 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.

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 si è detto in precedenza, alcuni ordinamenti giuridici consentono a terzi la rivendicazione di diritti in forza 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 qualora, nell'ambito del contratto, le parti si impegnassero a sottoporsi ad una specie di arbitrato vincolante nel caso in cui una persona interessata dal trattamento dei dati contestasse un'inadempienza. 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 separato tra il cedente e la persona interessata dal trattamento dei dati, in base al quale il cedente mantiene la responsabilità di eventuali danni o difficoltà causate dall'inosservanza, da parte del destinatario del trasferimento dei dati, dei principi fondamentali concordati 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 sembri 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 perfettamente a conoscenza dei suoi diritti.

---

[70] 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.

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 l'incapacità di scoprire la causa originaria del problema particolare che le affligge, da cui consegue l'impossibilità di giudicare se le norme di protezione dei dati siano state correttamente osservate oppure se sussistano motivi di ricorso legale [71]. Per un livello di tutela adeguato è quindi necessario un qualche meccanismo istituzionale che permetta indagini indipendenti in caso di reclamo.

Le funzioni di vigilanza e di investigazione esercitate dall'autorità di controllo di uno Stato membro si limitano al trattamento dei dati effettuato nel territorio dello Stato membro in questione [72]. 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 sarebbe quella di esigere semplicemente una clausola contrattuale che garantisca all'autorità di controllo dello Stato membro in cui è stabilito 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 [73] non è parte del contratto e, di conseguenza, in alcune giurisdizioni potrebbe non avere i mezzi di appellarsi ad esso per avere accesso. Un'altra possibilità sarebbe un impegno legale assunto dal destinatario nel paese terzo direttamente nei confronti dell'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 insorgano sospetti di inosservanza dei principi in materia di protezione dei dati. In virtù di tale impegno, le parti interessate dal trasferimento dei dati potrebbero anche informare l'autorità di controllo circa qualsiasi reclamo ricevuto dalle persone interessate dal trattamento dei dati. In questo caso tale impegno sarebbe una condizione preliminare per l'autorizzazione al trasferimento dei dati.

---

[71] 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.

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

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

Indipendentemente dalla soluzione prescelta, resta assai dubbio se sia opportuno, pratico o semplicemente fattibile, dal punto di vista delle risorse, che un'autorità di controllo di uno Stato membro dell'Ue assuma la responsabilità di esaminare e controllare il trattamento di dati effettuato in un paese terzo.

Garantire un buon livello di osservanza

Anche in mancanza di un particolare reclamo o di difficoltà riscontrate 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 della soluzione contrattuale consiste nella difficoltà di stabilire, in caso di inadempienza del contratto, sanzioni che siano sufficientemente significative per ottenere l'effetto dissuasivo 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 stabilito nella 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 quanto meno dalla 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 prevalente

Una difficoltà propria del 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 prevalgano su qualsiasi contratto che l'incaricato del trattamento abbia sottoscritto [74]. Per gli incaricati del trattamento all'interno della Comunità questa possibilità è prevista dall'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 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. Nei paesi terzi non sempre esistono per i poteri pubblici analoghe limitazioni all'ottenimento di dati personali da società e da altre organizzazioni operanti sul loro territorio.

---

[74] 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.

Non è facile venire a capo di questa difficoltà, che dimostra chiaramente i limiti 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 sull'uso dei contratti

Dall'analisi precedente si è visto che qualsiasi soluzione contrattuale deve essere definita in modo dettagliato e opportunamente adatta al trasferimento di dati in questione. Questa necessità di precisare le finalità e le condizioni 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 adattarlo alle circostanze particolari del caso.

L'analisi ha inoltre dimostrato che esistono difficoltà pratiche particolari nell'esame dei casi di inadempienza di un contratto quando il trattamento avviene al di fuori dell'Ue e quando nel paese terzo in questione non esiste alcuna forma di autorità di controllo. Questo significa che in alcune situazioni la soluzione contrattuale potrà essere quella appropriata, mentre in altre il contratto non potrà garantire la necessaria tutela adeguata.

La necessità di adattare in modo particolareggiato il contratto alle peculiarità del trasferimento in questione implica che un contratto è particolarmente adatto a situazioni in cui i trasferimenti di dati sono simili e di natura ripetitiva. Date le difficoltà inerenti al controllo, una soluzione contrattuale può essere maggiormente efficace quando le parti del contratto sono operatori importanti già sottoposti a controllo e regolamentazione pubblica [75]. 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; sono queste le situazioni in cui i contratti possono rivelarsi più utili. In queste circostanze possono anche essere integrati da convenzioni multilaterali intese a fornire una migliore sicurezza giuridica. Allo stesso modo, quando le parti interessate dal trasferimento sono affiliate o fanno parte dello stesso gruppo di imprese, la capacità di indagare in merito sull'inadempienza di un contratto è presumibilmente molto rafforzata, dati gli stretti legami tra il destinatario nel paese terzo e il soggetto stabilito nella Comunità. I trasferimenti all'interno di una stessa impresa sono quindi un altro settore in cui il ricorso a soluzioni contrattuali può rivelarsi particolarmente efficace.

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 subcontraente incaricato del trattamento. Quando ha luogo un trasferimento di dati verso paesi, il contratto deve fornire alle persone interessate dal trattamento dei dati garanzie supplementari, rese necessarie dal fatto che il destinatario nel paese terzo non è soggetto in materia di protezione dei dati a norme vincolanti atte a fornire un livello di tutela adeguato.

---

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

– 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 offerta da contratti in cui viene limitata la libertà del destinatario dei dati di trattare questi ultimi in modo autonomo per proprio conto. Il contratto andrebbe quindi utilizzato, nei limiti del possibile, come mezzo con cui il soggetto che trasferisce i dati mantiene il controllo decisionale sul trattamento effettuato nel paese terzo.

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

– I trasferimenti successivi verso enti od organizzazioni non vincolate dal contratto andrebbero esplicitamente 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.

– Nel caso in cui una persona interessata dal trattamento dei dati subisca le conseguenze di una violazione delle disposizioni in materia di protezione dei dati previste dal 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 incontreranno difficoltà pratiche nel procedere a tale esame.

– Le soluzioni contrattuali sono probabilmente più adatte alle grandi reti internazionali (carte di credito, prenotazioni aeree) caratterizzate da grandi quantità di trasferimenti di dati ripetitivi di natura simile e da un numero relativamente esiguo di importanti operatori in settori già sottoposti ad un elevato grado di controllo e di regolamentazione pubblica. I trasferimenti tra le filiali di uno stesso gruppo costituiscono un altro campo che si presta in modo particolare all'utilizzazione dei contratti.

– I paesi in cui le autorità pubbliche dispongono in materia di accesso alle informazioni di poteri più estesi di quelli ammessi dalle norme internazionalmente riconosciute in materia di tutela dei diritti dell'uomo non sono da considerarsi destinazioni sicure per i trasferimenti basati su clausole contrattuali.

5. Deroghe al principio dell'adeguatezza

L'articolo 26, paragrafo 1 della direttiva prevede, per un numero limitato di situazioni, la possibilità di derogare al principio della «adeguatezza» per i trasferimenti in paesi terzi. Queste deroghe, che sono descritte dettagliatamente, riguardano soprattutto casi in cui i rischi per l'interessato sono ridotti o in cui altri interessi (interessi pubblici o quelli della persona stessa cui i dati si riferiscono) prevalgono sul diritto dell'interessato alla riservatezza. In quanto deroghe a un principio generale, devono essere interpretate in modo restrittivo. Inoltre, nella legislazione nazionale gli Stati membri possono stabilire che le deroghe non si applicano in determinati casi. Ciò può succedere, ad esempio, quando è necessario tutelare gruppi di individui particolarmente vulnerabili, come i lavoratori o i pazienti.

La prima di queste deroghe comprende i casi in cui l'interessato dà in modo *inequivocabile* il proprio consenso al trasferimento proposto. Un punto importante da tenere presente è che il consenso, secondo la definizione dell'articolo 2, lettera *h)* della direttiva, va dato liberamente, in maniera specifica e informata. L'obbligo d'informazione è particolarmente importante dato che prescrive che l'interessato sia informato adeguatamente sul rischio specifico che i suoi dati vengano trasferiti in un paese che non garantisce una tutela adeguata. Se non viene data quest'informazione, la deroga non si applica. Poiché il consenso dev'essere inequivocabile, anche il dubbio sul fatto che esso sia stato dato rende la deroga inapplicabile. Ciò potrebbe significare che molte situazioni in cui il consenso è implicito (ad esempio perché un individuo è stato informato su un trasferimento e non si è opposto) non giustificano questa deroga. Tuttavia, la deroga potrebbe essere utile nei casi in cui chi effettua il trasferimento ha un contatto diretto con la persona interessata e in cui le informazioni necessarie possono essere fornite facilmente e il consenso ottenuto in modo inequivocabile. Questo avviene spesso nel caso di trasferimenti effettuati quando, ad esempio, si stipula un'assicurazione.

La seconda e la terza deroga riguardano i trasferimenti *necessari* per l'esecuzione di un contratto fra l'interessato e il responsabile del trattamento (o l'applicazione delle misure precontrattuali prese su richiesta dell'interessato) oppure per la conclusione o l'esecuzione di un contratto concluso *nell'interesse della persona interessata* tra il responsabile del trattamento e un terzo. Potenzialmente, queste deroghe appaiono abbastanza ampie, ma in pratica, come per la quarta e quinta deroga esaminate più avanti, la loro applicazione può essere limitata dalla «test di necessità»: tutti i dati trasferiti devono essere necessari per l'esecuzione del contratto. Quindi, se vengono trasferiti dati supplementari non essenziali o se il trasferimento non è finalizzato all'esecuzione del contratto, bensì ad altri obiettivi (ad esempio la successiva commercializzazione) la deroga non si applica. Per quanto riguarda le situazioni precontrattuali, queste comprenderebbero soltanto situazioni poste in essere per iniziativa dell'interessato (come la richiesta di informazioni su un determinato servizio) e non quelle risultanti da approcci di commercializzazione effettuati dal responsabile del trattamento.

Nonostante queste restrizioni, la seconda e terza deroga non rimarranno senza conseguenze. È probabile che saranno applicate frequentemente, ad esempio, ai trasferimenti necessari per prenotare un biglietto aereo per un passeggero, per le operazioni di una banca internazionale o per i pagamento mediante carta di credito. La deroga per i contratti «nell'interesse della persona

interessata» (articolo 26, paragrafo 1, lettera *c)* comprende infatti in particolare il trasferimento di dati sui beneficiari di pagamenti bancari, che, sebbene interessati, spesso non sono parte di un contratto con il responsabile del trattamento che effettua il trasferimento.

La quarta deroga ha due elementi costitutivi. Il primo comprende i trasferimenti necessari o prescritti dalla legge per la salvaguardia di un interesse pubblico rilevante in base a importanti motivi di interesse pubblico. Si può trattare di trasferimenti limitati fra le amministrazioni pubbliche, ma occorre fare attenzione a non interpretare questa disposizione in modo troppo ampio. Il semplice interesse pubblico non basta a giustificare un trasferimento, è necessario che sia una questione di interesse pubblico *rilevante*. Il considerando 58 indica che saranno compresi in generale i trasferimenti di dati fra le amministrazioni fiscali o doganali o fra i servizi responsabili della sicurezza sociale. Anche i trasferimenti fra gli organi di controllo nel settore dei servizi finanziari possono beneficiare della deroga. Il secondo elemento costitutivo riguarda i trasferimenti che avvengono nell'ambito di controversie internazionali o di procedimenti giudiziari, in particolare i trasferimenti necessari per costatare, esercitare o difendere un diritto per via giudiziaria.

La quinta deroga riguarda i trasferimenti necessari per la salvaguardia degli interessi vitali della persona interessata. Ad esempio, potrebbe trattarsi del trasferimento urgente di documenti medici a un paese terzo, dove un turista che ha usufruito precedentemente di cure mediche nell'Ue, ha subito un incidente o si è ammalato gravemente. Occorre tenere presente, tuttavia, che il considerando 31 della direttiva dà una definizione di «interesse vitale» abbastanza limitata, nel senso che dev'essere un interesse «essenziale alla vita della persona interessata». Questo escluderebbe normalmente, per esempio, gli interessi finanziari, patrimoniali o familiari.

La sesta ed ultima deroga riguarda i trasferimenti effettuati a partire da registri destinati per legge alla consultazione da parte del pubblico, purché siano rispettate nel caso specifico le condizioni previste per la consultazione. La ragione di questa deroga è che se in uno Stato membro un registro può essere consultato pubblicamente o dalle persone che dimostrano un interesse legittimo, il fatto che la persona autorizzata a consultare il registro si trovi in un paese terzo e che la consultazione richieda di fatto un trasferimento di dati non deve impedire che l'informazione gli sia trasmessa. Il considerando 58 precisa che questa deroga non permette il trasferimento della totalità dei dati o delle categorie di dati contenuti nel registro. In ragione di tali restrizioni, questa deroga non dev'essere considerata una deroga generale per il trasferimento di dati dei registri pubblici. Chiaramente, essa non intende permettere il trasferimento massiccio di dati dei registri pubblici per scopi commerciali o l'utilizzo di dati disponibili pubblicamente per individuare persone con un profilo specifico.

6. Questioni procedurali

L'articolo 25 dispone che la valutazione dell'adeguatezza avvenga caso per caso, in relazione ai singoli trasferimenti o alle singole categorie di trasferimenti. Tuttavia, considerati l'elevato numero di trasferimenti di dati personali in uscita dalla Comunità ogni giorno e la molteplicità delle parti interessate da tali trasferimenti, è evidente che nessuno Stato membro, qualunque sia il sistema

adottato per l'applicazione dell'articolo 25 [76], sarà in grado di garantire che ogni singolo caso sia esaminato in dettaglio. Ovviamente ciò non significa che nessun caso sarà esaminato in dettaglio, ma indica piuttosto la necessità di elaborare meccanismi volti a razionalizzare il processo decisionale per un gran numero di casi e a consentire l'adozione di decisioni, almeno a carattere provvisorio, senza ritardi inutili e senza dispendio eccessivo di risorse.

Tale razionalizzazione si impone a prescindere da chi decide, che si tratti di un responsabile del trattamento dei dati, dell'autorità di controllo o di un altro organismo istituito secondo le procedure vigenti nello Stato membro.

(i) Ricorso all'articolo 25, paragrafo 6 della direttiva

Un modo ovvio di contribuire a questa razionalizzazione, previsto nella direttiva stessa, consisterebbe nel determinare che certi paesi terzi assicurano un adeguato livello di tutela. Tali constatazioni avrebbero un valore «puramente indicativo» e quindi non si applicherebbero a casi presentanti difficoltà particolari. Tuttavia, questa sarebbe una soluzione pratica del problema. Queste indicazioni permetterebbero in particolare agli operatori economici di sapere quali paesi assicurano in generale un livello «adeguato» di tutela e costituirebbero un incentivo chiaro e pubblico per i paesi terzi che stanno sviluppando o migliorando i loro sistemi di tutela. Una serie di indicazioni a livello comunitario contribuirebbe inoltre ad affrontare in modo coerente questa questione ed eviterebbe il proliferare di «liste bianche» diverse ed eventualmente in conflitto fra loro, stabilite dai governi degli Stati membri o dalle autorità di tutela dei dati.

Comunque, questo approccio non è privo di difficoltà, la principale delle quali è che molti paesi terzi non garantiscono una tutela uniforme in tutti i settori economici. Molti paesi sono dotati ad esempio di una normativa sulla tutela dei dati nel settore pubblico ma non in quello privato. In alcuni paesi, per esempio negli Stati Uniti, esistono norme specifiche solo per particolari settori (per es. le informazioni sulla solvibilità e gli archivi per il noleggio video nel caso degli USA). Un'ulteriore difficoltà deriva dallo statuto federale di alcuni paesi come gli USA, il Canada e l'Australia, dove le norme sono spesso diverse da uno Stato all'altro della federazione. Ne risulta che attualmente molti paesi terzi non possono essere considerati in grado di offrire una tutela globale adeguata. Se il numero di paesi per i quali possono essere date indicazioni positive è esiguo, diminuisce naturalmente anche l'utilità dell'esercizio, nel senso che dà minore certezza ai responsabili del trattamento. Un altro rischio è che alcuni paesi terzi possano interpretare la mancanza di una constatazione come una provocazione politica o una discriminazione, poiché tale mancanza potrebbe essere una conseguenza sia del fatto che il loro caso non è stato esaminato sia di un giudizio sul loro sistema di tutela dei dati.

Dopo aver considerato attentamente questi diversi argomenti, il gruppo di lavoro è tuttavia dell'opinione che sarebbe utile avviare i lavori necessari per procedere alle constatazioni previste dall'articolo 25, paragrafo 6. Dovrebbe trattarsi di un processo permanente, che darebbe modo di stabilire un elenco di paesi non definitivo, ma costantemente aggiornato e riveduto alla luce dei

[76] Gli Stati membri possono istituire procedure amministrative diverse per l'adempimento degli obblighi previsti dall'articolo 25: per esempio, possono imporre un obbligo diretto al responsabile del trattamento dei dati e/o mettere a punto un sistema di autorizzazione preventiva o di verifica retroattiva del parte dell'autorità di controllo.

nuovi sviluppi. Una constatazione positiva non dovrebbe, in linea di principio, limitarsi ai paesi in cui esistono leggi orizzontali sulla tutela dei dati, ma dovrebbe riguardare anche specifici settori di un paese per i quali la tutela dei dati è adeguata, anche se in altri settori dello stesso paese la tutela dovesse risultare inadeguata.

Occorre osservare che il gruppo istituito dall'articolo 29 non ha funzioni decisionali esplicite in merito a particolari trasferimenti di dati o alla determinazione dell'«adeguatezza» ai sensi all'articolo 25, paragrafo 6. In entrambi i casi si applica la procedura del comitato di cui all'articolo 31. Va comunque notato che uno dei compiti specifici del gruppo consiste nel fornire alla Commissione un parere sul livello di tutela nei paesi terzi (vedi articolo 30, paragrafo 1, lettera *b)*. Rientra quindi tra i compiti del gruppo esaminare la situazione in determinati paesi terzi e formulare un parere provvisorio sull'adeguatezza della tutela. Le constatazioni positive, una volta confermate a norma dell'articolo 25, paragrafo 6, per essere utili dovrebbero essere ampiamente diffuse. Nel caso in cui si sia constatato che un paese non assicura una tutela adeguata, ciò non dovrà significare l'iscrizione di tale paese, implicita o esplicita, in una «lista nera». Il messaggio pubblico sarà piuttosto l'impossibilità di fornire per il momento un'indicazione generale riguardo a quel particolare paese.

(ii) Analisi dei rischi relativi a trasferimenti specifici

Sebbene il ricorso all'articolo 25, paragrafo 6 analizzato sopra possa facilitare notevolmente le decisioni relative a molti casi di trasferimento di dati, resteranno comunque numerosi i casi in cui il paese terzo in questione non è oggetto (globalmente o parzialmente) di un parere favorevole. Il trattamento che gli Stati membri riservano a casi del genere può variare a seconda delle modalità di recepimento dell'articolo 25 nella normativa nazionale (cfr. la precedente nota a piè di pagina). Se all'autorità di controllo è attribuita una competenza specifica per l'autorizzazione preventiva dei trasferimenti dei dati ovvero per l'esecuzione di una verifica retroattiva, l'elevato volume di trasferimenti in gioco renderà necessario un sistema che consenta di stabilire un calendario di priorità per le attività di detto organismo. Tale sistema potrebbe consistere in una serie concordata di criteri che permettano di determinare se un trasferimento o una categoria di trasferimenti siano da considerarsi prioritari in quanto rappresentano una particolare minaccia per la vita privata delle persone interessate.

Un sistema del genere non comporterebbe alcuna modifica dell'obbligo per ciascuno Stato membro di autorizzare soltanto i trasferimenti verso paesi terzi con un adeguato grado di protezione. Esso sarebbe d'aiuto per stabilire quali casi di trasferimenti di dati debbano essere esaminati o anche investigati in via «prioritaria» e permetterebbe di dirigere le risorse disponibili verso quei trasferimenti che sollevano le maggiori preoccupazioni in materia di protezione della persona interessata.

Il gruppo ritiene che fra le categorie di trasferimenti che rappresentano una minaccia particolare per la vita privata e meritano quindi particolare attenzione siano comprese le seguenti:

– trasferimenti riguardanti le categorie particolari di dati di cui all'articolo 8 della direttiva;

– trasferimenti che comportano rischi di perdite finanziarie (ad esempio pagamenti con carta di credito attraverso Internet);

– trasferimenti che comportano rischi per la sicurezza personale;

– trasferimenti finalizzati all'adozione di una decisione particolarmente importante per la persona interessata (assunzioni, promozioni, concessione di un credito, ecc.);

– trasferimenti che rischiano di causare un grave imbarazzo a una persona o di lederne la reputazione;

– trasferimenti che possono condurre ad azioni specifiche che costituiscono un'ingerenza grave nella vita privata della persona (per esempio, telefonate indesiderate);

– trasferimenti ripetuti che riguardano grandi volumi di dati (per es. dati su transazioni elaborati su reti di telecomunicazioni, Internet, ecc.);

– trasferimenti che comportano la raccolta di dati per mezzo di nuove tecnologie secondo modalità particolarmente occulte o clandestine (per es. i cosiddetti «cookies» di Internet).

(i) Clausole contrattuali tipo

Come è stato discusso ampiamente nel capitolo 4, la direttiva prevede la possibilità che anche nel caso in cui il livello di tutela non sia adeguato, il responsabile del trattamento possa ottenere una protezione adeguata del trasferimento dei dati mediante un contratto. L'articolo 26, paragrafo 2 della direttiva permette agli Stati membri di autorizzare trasferimenti in base a disposizioni contrattuali, una decisione che deve essere notificata in seguito alla Commissione. Se esistono opposizioni all'autorizzazione, la decisione può essere respinta o confermata dalla Commissione conformemente alla procedura del comitato di cui all'articolo 31. Oltre alle autorizzazioni concesse dagli Stati membri, l'articolo 26, paragrafo 4 della direttiva permette anche alla Commissione, sempre in conformità alla procedura del comitato di cui all'articolo 31, di decidere se certe clausole contrattuali tipo offrono garanzie sufficienti. Tali decisioni sono vincolanti per gli Stati membri.

Data l'evidente complessità e difficoltà di queste soluzioni contrattuali, è necessario che i responsabili del trattamento che intendono utilizzare i contratti in questo modo possano avvalersi di un orientamento. A livello degli Stati membri, spetterà alle autorità nazionali competenti la responsabilità principale di questo orientamento, particolarmente per quanto riguarda la preparazione delle autorizzazioni nell'ambito dell'articolo 26, paragrafo 2. Le autorità degli Stati membri e la Commissione dovrebbero cooperare e scambiare opinioni sulle clausole contrattuali loro presentate.

Quando le clausole tipo proposte vengono presentate alle autorità degli Stati membri o direttamente alla Commissione, dovrebbe essere adottata una procedura che consenta l'esame delle clausole anche da parte del gruppo, per evitare differenze nello sviluppo delle pratiche nazionali e per far sì che la Commissione possa usufruire della consulenza specialistica appropriata prima di prendere qualsiasi decisione ai sensi dell'articolo 26, paragrafo (4).

ALLEGATO 1

CONSEGUENZE PRATICHE DEGLI ARTICOLI 25 E 26 DELLA DIRETTIVA SUL TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

INTRODUZIONE

La questione del trasferimento verso paesi terzi è affrontata in questo documento secondo un approccio globale comprendente:

– una valutazione della tutela adeguata ai sensi dell'articolo 25 della direttiva sulla tutela dei dati;

– una valutazione dei mezzi alternativi per garantire una protezione adeguata tramite soluzioni contrattuali, come previsto dall'articolo 26, paragrafo 2;

– una valutazione delle deroghe al principio della tutela adeguata previste dall'articolo 26, paragrafo 1.

La problematica non sarebbe trattata in modo esauriente se non si esaminassero le conseguenze pratiche di questo approccio globale per i trasferimenti di dati personali. Nel presente allegato, perciò, alcuni casi realistici, ma fittizi, di trasferimenti di dati sono esaminati secondo il metodo che dovrebbe essere adottato quando saranno entrate in vigore le leggi nazionali d'attuazione della direttiva.

Vengono presentati tre casi diversi, per ognuno dei quali si valuta dapprima se la tutela nel paese destinatario è adeguatamente assicurata da leggi pertinenti o da un'efficace autodisciplina del settore privato. In caso negativo, si procede alla ricerca di una soluzione del problema nell'ambito delle possibilità previste dall'articolo 26, paragrafi 1 (deroghe) e 2 (soluzioni contrattuali). Soltanto in mancanza di una soluzione appropriata si passerà al blocco del trasferimento.

CASO (1): UN TRASFERIMENTO DI DATI RIGUARDANTI LA CAPACITÀ DI CREDITO

Un cittadino della Comunità desidera comprare una casa per le vacanze in un paese A al di fuori della CE e chiede un prestito ad un'istituzione finanziaria di quel paese. Questa si rivolge ad un'agenzia d'informazioni commerciali per ottenere informazioni sulla solvibilità del cliente. L'agenzia non ha un dossier su questa persona, ma dispone che un suo curriculum finanziario completo sia trasferito dall'agenzia affiliata del Regno Unito. Il paese A è un paese altamente industrializzato, con istituzioni democratiche antiche e stabili. Il suo sistema giudiziario è ben organizzato ed efficiente. Ha una struttura costituzionale federale.

FASE 1: VALUTAZIONE DELL'ADEGUATEZZA DELLA TUTELA

Le norme applicabili pertinenti

Il responsabile del trattamento destinatario è soggetto alla legge federale che stabilisce norme sulle informazioni personali detenute per la valutazione dei rischi di credito. Il responsabile del trattamento s'impegna inoltre ad attenersi alla propria politica della privacy resa pubblica. Non è applicabile alcuna legge statale e non esiste un codice di autodisciplina settoriale.

Valutazione del contenuto delle norme applicabili

Innanzitutto va notato che la comunicazione effettuata dall'agenzia di informazioni commerciali situata nel Regno Unito sarebbe soggetta, come qualsiasi comunicazione a un responsabile del trattamento nel Regno Unito o in un altro Stato membro, agli obblighi previsti dalla legislazione del Regno Unito, che attua tutti gli articoli della direttiva fuorché gli articoli 25 e 26. Questo è importante perché evita la necessità di esaminare la legalità della comunicazione stessa e permette di concentrare l'attenzione sulla tutela di cui godranno i dati una volta trasferiti nel paese A.

La valutazione del contenuto delle norme dovrebbe, logicamente, iniziare dalla legislazione federale. In caso di lacune, si potrebbe considerare se la normativa meno «rigida» in materia di «privacy» permette di colmarle. Diamo qui

di seguito un elenco dei contenuti che si possono ritenere necessari e un giudizio circa la presenza di questo contenuto necessario nella legislazione o nella politica della privacy.

Il principio della finalità limitata, in questo contesto, può riguardare soltanto l'obbligo che tutti gli usi secondari e la comunicazione dei dati trasferiti siano compatibili con la finalità per cui sono stati trasferiti. L'inclusione dei dati in una «mailing list» destinata alla vendita o al noleggio sul mercato dev'essere considerata incompatibile, come anche la comunicazione dei dati a possibili datori di lavoro o a partner d'affari interessati alla solvenza della persona interessata. La comunicazione dei dati ad altri prestatori (banche, società di carte di credito) può comunque essere considerata compatibile.

In questo caso la legge federale stabilisce un numero limitato di finalità per le quali le informazioni commerciali personali possono essere comunicate legittimamente. Queste finalità comprendono «l'impiego» e «le legittime esigenze connesse ad un'operazione commerciale in cui la persona interviene». In questo concetto sono comprese anche talune utilizzazioni di dati a fini commerciali, tra cui la commercializzazione di beni o servizi diversi dal credito da parte di terzi. La legge federale non sembra quindi limitare sufficientemente la finalità e su questo punto la tutela non è adeguata. La politica della società in fatto di privacy non migliora la situazione.

Il principio della trasparenza dovrebbe comportare che l'interessato sia informato sull'identità dell'agenzia d'informazione commerciale del paese A e su ogni altra finalità del trattamento dei dati. Il modo esatto in cui questo avviene dovrebbe essere comparabile a quello stabilito nell'articolo 11 della direttiva. In questo caso la legge federale non contiene disposizioni specifiche sulla trasparenza che riguardino direttamente l'agenzia d'informazioni commerciali. Tuttavia, il prestatore del paese A è tenuto a comunicare all'interessato che saranno richieste informazioni ad un'agenzia d'informazioni commerciali, anche se non sarà necessario fornire il nome e l'indirizzo dell'agenzia. La persona interessata non ha quindi alcuna garanzia legale di essere informata del fatto che l'agenzia d'informazioni commerciali in questione procede a un trattamento di dati che lo riguardano. Poiché l'agenzia non ha contatti diretti con l'interessato, l'obbligo di contattarlo appositamente per informarlo sembra costituire uno «sforzo sproporzionato» ai sensi dell'articolo 11 della direttiva. Il livello di tutela per quanto riguarda la trasparenza pare quindi sufficiente.

Il principio della qualità e della proporzionalità comprende diversi elementi. La legge federale non prevede restrizioni alla raccolta e al trattamento di dati non necessari. Per quanto riguarda la durata della loro conservazione, ci sono norme che vietano la diffusione di informazioni obsolete (dichiarazioni di fallimento anteriori a 10 anni), e ne comportano di fatto la cancellazione. Non vi è alcun obbligo legale generale di conservare i dati con accuratezza, ma se una persona chiede di accedere alle informazioni commerciali che lo riguardano e contesta alcune di esse, i dati che non possono essere verificati vanno cancellati. Anche in questi casi la tutela non pare totalmente adeguata e la politica di privacy della società non va al di là della legge federale.

Il principio della sicurezza si traduce nella legge federale nell'obbligo di adottare misure appropriate per impedire una comunicazione illegale. La politica di privacy della società avverte che vengono effettuati severi controlli per impedire l'accesso non autorizzato alle informazioni commerciali e la loro mani-

polazione. Questi controlli consistono in dispositivi tecnici (parole chiave, ecc.) e in istruzioni ai dipendenti, la cui inosservanza può dar luogo a procedimenti disciplinari. Ciò sembra assicurare un livello adeguato di sicurezza.

I diritti di accesso e rettifica sono garantiti dalla legge federale e sono comparabili a quelli previsti dalla direttiva. Nel caso in cui a una persona sia rifiutato un credito, l'accesso alle informazioni che la riguardano è gratuito. Non esiste, comunque, un **diritto di opposizione**, anche se la persona può presentare ricorso presso un'agenzia federale specializzata oppure intentare un'azione legale (vedi sotto) se sono stati violati diritti di cui gode in forza della legge federale.

I dati riservati sulla salute dell'individuo fanno parte dei dati trasferiti. La legge federale comprende disposizioni più severe riguardanti il trattamento dei dati relativi a precedenti penali, sesso, razza, origine etnica, età e stato civile, ma non allo stato di salute. La politica di privacy dell'agenzia d'informazioni commerciali prevede che i dati sulla salute non siano utilizzati al fine di valutare la capacità di credito, ma solo per controlli sull'impiego o sull'assicurazione. In questi due casi l'uso dei dati sarà autorizzato dall'interessato nella domanda di assunzione o nel modulo d'assicurazione. Sembrerebbe dunque che per i dati sulla salute considerati in quest'esempio la tutela sia notevolmente maggiore, anche se non garantita per legge.

È qui in questione anche l'utilizzazione di dati per fini di commercializzazione diretta da parte dell'agenzia di informazioni commerciali (e la comunicazione dei dati ad altri per tali fini). Non esiste alcuna disposizione di legge che vieti tale utilizzazione né alcun obbligo giuridico di dare alla persona interessata la possibilità di opporvisi. Questa situazione è chiaramente inadeguata, in particolare perché i dati possono essere utilizzati dall'agenzia (per costituire «mailing lists» da offrire a istituti di credito) ma anche comunicati a terzi per la commercializzazione di prodotti attinenti a servizi finanziari o anche senza alcun rapporto con essi (per es. falciatrici da giardino o vacanze).

Il fine del trasferimento sembra essere quello di permettere una **decisione automatizzata** circa la concessione o meno di un credito alla persona interessata. In questo contesto, essa dovrebbe quindi beneficiare di un'ulteriore tutela. Sebbene la legge federale comprenda disposizioni che permettono alla persona di contestare le informazioni fornite da un'agenzia e, se necessario, di aggiungervi spiegazioni, non esistono norme che permettono di impugnare una decisione presa in base ad informazioni errate o incomplete, di riesaminarla e, se l'impugnazione è giustificata, di cambiarla. Il meccanismo permette di modificare un rapporto in modo da evitare problemi futuri, ma non risolve necessariamente il problema di una decisione di credito già presa. Questa tutela giuridica non retroattiva è insufficiente.

Restrizioni ai trasferimenti ulteriori di dati verso un altro paese terzo o verso organizzazioni di altri settori del paese A non soggetti alle norme della legge federale. Disposizioni in questo senso non esistono né nella legge federale né nella politica di privacy della società.

Campo d'applicazione della legge federale e della politica di privacy. Sarebbe necessario un altro controllo per accertare che la legislazione e la politica di privacy si applicano ai dati riguardanti tutte le persone e non soltanto i residenti o i cittadini del paese A. In tal caso, non esistono restrizioni del campo d'applicazione.

Valutazione dell'efficacia della tutela

La normativa federale in questione ha forza di legge ed istituisce anche un'autorità pubblica con alcuni poteri di controllo esterno. Per far valere i loro diritti, le persone possono inoltre promuovere privatamente un'azione legale. Tuttavia, l'autorità pubblica non ha l'obbligo preciso d'indagare su ogni singolo reclamo e, secondo taluni commentatori, non è sempre stata particolarmente attiva nel far rispettare la legge. Le cause private sono un metodo costoso e spesso lento per chi vuol far valere i propri diritti, soprattutto se vive in un paese diverso da quello in cui ha luogo il processo.

La politica di privacy interna della società non comprende un meccanismo indipendente che permetta alla persona di far valere i propri diritti, ma prevede sanzioni disciplinari per i dipendenti che non rispettano tale politica. Alcuni dipendenti hanno già subito provvedimenti disciplinari per passate violazioni.

La combinazione di legislazione e codice interno di privacy va valutata in base agli «obiettivi» che sono stati fissati per i meccanismi procedurali. Gli aspetti fondamentali a questo riguardo sono:

Un buon livello d'osservanza generale

Il miglior incentivo perché una società rispetti la propria politica di privacy è il rischio di pubblicità negativa sui giornali nel caso in cui non mantenesse le sue promesse. Inoltre, i dipendenti della società possono subire misure disciplinari se non si attengono alle regole di sicurezza.

Questi meccanismi non sembrano comunque sufficienti ad assicurare che la politica di privacy sia rispettata nella pratica.

La conclusione sarebbe stata diversa se:

1) la politica di privacy della società avesse rispecchiato un codice di condotta stabilito dall'associazione di categoria e valido per l'intero settore, che preveda l'immediata esclusione dall'associazione delle società che non rispettano tale codice; oppure

2) una norma di legge generale permettesse ad un organo pubblico di perseguire per pratiche «sleali ed ingannevoli»una società che non rispetta il proprio codice di privacy reso pubblico.

La legge federale incoraggia il rispetto delle norme in quanto prevede la possibilità di promuovere azioni legali private in caso di inosservanza. La prospettiva di finire in tribunale può avere un effetto deterrente sul responsabile del trattamento dei dati. Tuttavia, il controllo esterno diretto delle procedure di trattamento dei dati è molto limitato, dato che le autorità pubbliche reagiscono soltanto se un problema viene portato alla loro attenzione, ad esempio da un querelante o dalla stampa.

Sostegno ed aiuto alle persone interessate

Esiste un'agenzia pubblica a cui le persone possono rivolgersi per presentare i loro reclami circa le informazioni commerciali che li riguardano. L'esame del reclamo non comporta alcun costo per l'interessato.

Risarcimento adeguato

In caso di violazione degli obblighi previsti dalla legge federale, la persona può ottenere un risarcimento dal tribunale. Si tratta comunque di un processo relativamente costoso e spesso l'interessato non riceve in queste procedure il sostegno dell'agenzia pubblica. Il tribunale può imporre al responsabile del trattamento di risarcire gli eventuali danni, nonché di correggere le sue procedure di

trattamento dei dati ed il contenuto del dossier commerciale in questione. Non è invece possibile una riparazione in caso di inosservanza dei principi di tutela dei dati previsti soltanto dalla politica di privacy.

Il giudizio

1) Alcuni principi di tutela dei dati, definiti «principi fondamentali» nel documento di discussione, sono contenuti in certa misura nella legge federale applicabile alle informazioni commerciali. Altri si trovano invece nella politica di privacy. Anche considerando gli uni e gli altri, non si può dire, però, che tutti i «principi fondamentali» siano presenti; alcuni di essi (per es. il principio della finalità limitata) lo sono in forma assai blanda

2) Un problema più generale è se la politica di privacy di una società possa essere considerata in ogni caso un meccanismo abbastanza efficace. A meno che un'associazione di categoria o un organismo pubblico possa esercitare poteri di controllo esterno che ne permettono un'effettiva applicazione, tale politica risulta in larga misura inapplicabile e non può quindi essere presa in considerazione.

3) Sebbene l'organismo pubblico istituito per applicare la legge federale non abbia gli stessi poteri di un tipico organo europeo per la protezione dei dati, la legge garantisce una certa sicurezza giuridica, particolarmente nell'ambito di un sistema giudiziario efficiente e della «cultura processuale» esistente nel paese A. La legge contiene chiare disposizioni sul principio di protezione dei dati forse più importante di tutti, il diritto di accesso e di rettifica, e alcune limitazioni dei fini per i quali i dati possono essere utilizzati.

Conclusione

La tutela risulta inadeguata perché la legge include un numero insufficiente di «principi fondamentali» e la politica di privacy, di per sé, non è un mezzo di tutela efficace. Un giudizio di adeguatezza presupporrebbe che nella legge fossero inclusi principi come la trasparenza e la protezione dei dati sulla salute oppure che la politica di privacy fosse resa più efficace grazie a uno dei metodi suggeriti sopra (ossia fare del rispetto del codice di condotta una condizione per poter essere membro di un'associazione di categoria oppure dare a un organo pubblico il potere di ricorrere in giudizio contro la società per pratiche sleali e ingannevoli).

FASE 2: RICERCA DI UNA SOLUZIONE

Delle possibili deroghe indicate nell'articolo 26, paragrafo 1, soltanto la (a), il consenso della persona interessata, appare adeguata. La deroga (b), che riguarda i trasferimenti necessari per l'esecuzione di un contratto, non è applicabile perché la parte cedente, l'agenzia di informazioni commerciali situata nel Regno Unito, non ha un rapporto contrattuale con l'interessato. È difficile anche sostenere che il trasferimento sia necessario per la conclusione di un contratto «nell'interesse della persona interessata» come richiesto per la deroga (c).

Il consenso dell'interessato sembrerebbe essere una soluzione relativamente semplice del problema. Il consenso potrebbe essere ottenuto direttamente dall'agenzia situata nel Regno Unito oppure per conto dell'agenzia britannica dall'istituzione finanziaria del paese A, che potrebbe chiedere il consenso sul

modulo di domanda del credito. Qualsiasi metodo venga scelto, l'individuo dovrebbe essere informato del rischio particolare risultante dal fatto che i suoi dati devono essere trasferiti verso un paese che non garantisce una tutela adeguata.

Dato che questo tipo di trasferimento è ancora relativamente insolito, l'ottenimento del consenso di volta in volta è probabilmente la soluzione più pratica. Se le agenzie di informazioni commerciali di tutto il mondo inizieranno a scambiarsi dati in modo più sistematico, potranno essere trovate altre vie, come soluzioni contrattuali o un codice internazionale di condotta.

CASO (2): IL TRASFERIMENTO DI DATI RISERVATI NELL'INDUSTRIA AEREA

Un cittadino portoghese prenota un biglietto di volo di una compagnia aerea del paese B presso un'agenzia di viaggi di Lisbona. I dati raccolti contengono informazioni sul fatto che il cittadino è disabile e fa uso di una sedia a rotelle. Essi sono immessi in un sistema di prenotazione computerizzato internazionale e da qui sono trasferiti nella base di dati sui passeggeri della compagnia aerea situata nel paese B, dove vengono conservati fino a data indeterminata. La compagnia aerea intende utilizzare i dati per fornire un servizio migliore al passeggero se in futuro viaggerà ancora sui suoi voli, oltre che per scopi di programmazione della gestione interna [77].

FASE 1: VALUTAZIONE DELL'ADEGUATEZZA DELLA TUTELA

Le norme applicabili pertinenti

Sebbene esista un codice di condotta internazionale valido per i dati immessi nei sistemi di prenotazione computerizzati, non vi sono norme sulla tutela dei dati riguardo alle informazioni contenute nella base di dati della compagnia aerea nel paese B.

Valutazione del contenuto delle norme applicabili

Non esistono norme applicabili.

Valutazione dell'efficacia della tutela

Non applicabile.

Giudizio

I livelli di tutela nel paese B sono inadeguati, in particolare considerando la riservatezza dei dati in questione.

FASE 2: RICERCA DI UNA SOLUZIONE

Il trasferimento di dati verso il sistema di prenotazione computerizzato e la loro utilizzazione da parte della compagnia aerea allo scopo di fornire un servizio appropriato al passeggero disabile per il volo in questione è un trasferimento necessario per l'esecuzione del contratto fra il passeggero e la compa-

---

[77] Questo caso è simile a un caso realmente avvenuto sotto la giurisdizione svedese, che ha visto coinvolte American Airlines e Lufthansa. Il caso è ancora sotto giudizio.