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

DG XV D/5025/98
WP 12

Gruppo di lavoro "Tutela delle persone fisiche con riguardo al trattamento dei dati personali"

Documento di lavoro

Trasferimento di dati personali verso paesi terzi : applicazione degli articoli 25 e 26 della direttiva europea sulla tutela dei dati

Approvato dal gruppo di lavoro il 24 luglio 1998

Indice

Introduzione

Il presente documento, basato sui lavori del gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29 della direttiva sulla protezione dei dati (95/46/CE)[1], si propone di esaminare in modo organico tutte le principali questioni poste dal trasferimento di dati personali verso paesi terzi nel contesto dell'applicazione della direttiva europea sulla protezione dei dati. Il documento è strutturato secondo il sistema previsto dagli articoli 25 e 26 della direttiva per i trasferimenti internazionali di dati personali. (Il testo degli articoli è riportato nell'allegato 2).

L'articolo 25, paragrafo (1), stabilisce che gli Stati membri possono consentire il trasferimento verso un paese terzo di dati personali soltanto se il paese terzo in questione garantisce un livello di protezione adeguata. Il paragrafo (2) precisa che la 'adeguatezza' è valutata di volta in volta 'con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati'. Il paragrafo (6) prevede che la Commissione possa determinare che un paese terzo garantisce un livello di protezione adeguato. Il **capitolo 1** del presente documento esamina la questione centrale della protezione adeguata; si propone di chiarire che cosa si intenda per 'adeguata' e definisce una serie di criteri in base a cui valutare, in un caso specifico, l'adeguatezza della protezione.

I capitoli 2 e 3 sono dedicati all'applicazione di questi criteri. Il **capitolo 2** tratta dei trasferimenti verso i paesi che hanno ratificato la convenzione n. 108 del Consiglio d'Europa; il **capitolo 3** esamina le questioni attinenti ai trasferimenti per i quali la protezione dei dati personali è assicurata principalmente o esclusivamente da meccanismi di autodisciplina e non da norme di legge.

In caso di mancanza di una protezione adeguata ai sensi dell'articolo 25, paragrafo 2, la direttiva prevede all'articolo 26, paragrafo 2 la possibilità di provvedimenti *ad hoc*, in particolare di natura contrattuale, tali da fornire garanzie sufficienti per autorizzare un trasferimento di dati personali. Nel **capitolo 4** sono esaminate le circostanze in cui possono essere appropriate soluzioni contrattuali *ad hoc* e sono formulate alcune raccomandazioni quanto alla forma e al contenuto possibili di tali soluzioni.

Il **capitolo 5** tratta della terza ed ultima situazione contemplata dalla direttiva: i casi specifici, previsti dall'articolo 26, paragrafo (1), nei quali è possibile derogare ai

---

[1]Cfr **WP 4 (5020/97)** " Primi orientamenti relativi al trasferimento di dati personali verso paesi terzi - Possibili progressi nella valutazione dell'adeguatezza", documento di consultazione approvato dal gruppo di lavoro il 26 giugno 1997;
WP 7 (5057/97) Documento di lavoro: "Valutazione dell'autodisciplina settoriale: quando incide in modo significativo sul livello di tutela dei dati in un paese terzo?", approvato dal gruppo di lavoro il 14 gennaio 1998;
WP 9 (5005/98) 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.

principi della ‘tutela adeguata’. Viene esaminata l’esatta portata di tali deroghe, con alcune esemplificazioni di casi in cui tali deroghe potrebbero o no applicarsi.

Infine, il **capitolo 6** contiene alcuni commenti su questi procedurali relative alla valutazione dell’adeguatezza (o inadeguatezza) della protezione e all’adozione di un approccio comunitario coerente a tali questioni.

I casi esaminati nell’allegato 1 si propongono di esemplificare l’applicazione concreta dell’approccio illustrato nel presente documento.

CAPITOLO 1: VALUTAZIONE DELLA TUTELA ADEGUATA

(1) In che cosa consiste una 'tutela adeguata'?

Proteggere i dati significa proteggere la persona alla quale si riferiscono le informazioni trattate. A tal fine si associano in genere una serie di diritti di cui gode la persona interessata e una serie di obblighi a carico di chi tratta i dati e che controlla tale trattamento. Gli obblighi e i diritti istituiti dalla direttiva 95/46/CE si basano su quelli stabiliti nella convenzione n. 108 (1981) del Consiglio d'Europa, che a loro volta non si discostano da quelli contenuti negli orientamenti dell'OCSE (1980) o dell'ONU (1990). Sembra pertanto esistere un consenso circa il contenuto delle norme di tutela dei dati che si estende ben oltre i quindici Stati membri della comunità.

Tali norme, tuttavia, contribuiscono alla tutela dell'individuo solo se sono osservate nella pratica. È pertanto necessario considerare non soltanto il contenuto delle norme applicabili ai dati personali trasferiti verso un paese terzo, ma anche i meccanismi posti in essere per garantirne l'efficacia. In Europa è prevalsa storicamente la tendenza a dare forma di legge alle norme di protezione dei dati, il che ha consentito di sanzionare le violazioni e di riconoscere all'individuo il diritto ad un risarcimento. Tali leggi, inoltre, erano generalmente accompagnate da meccanismi procedurali supplementari, come la creazione di autorità di controllo con funzioni di vigilanza e di indagine in caso di denuncia. Questi aspetti procedurali sono ripresi nella direttiva 95/46/CE, con le sue disposizioni in materia di responsabilità, sanzioni, ricorsi, autorità di controllo e notificazione. Al di fuori della Comunità è meno frequente imbattersi in simili strumenti procedurali, per garantire l'osservanza delle norme di tutela dei dati. Le parti che hanno sottoscritto la convenzione n. 108 devono dare forma di legge ai principi di protezione dei dati, ma non hanno alcun obbligo quanto ai meccanismi supplementari (ad esempio un'autorità di controllo). Gli orientamenti dell'OCSE prevedono solo l'obbligo per la legislazione nazionale di 'prendere in considerazione' gli orientamenti medesimi, senza quindi offrire alcun mezzo procedurale atto a garantire una efficace tutela dell'individuo. I successivi orientamenti dell'ONU, invece, contengono alcune disposizioni relative al controllo e alle sanzioni, il che traduce la diffusa consapevolezza a livello internazionale della necessità di dare un'adeguata applicazione alle norme di tutela dei dati.

In questo contesto, un'analisi compiuta del significato di "tutela adeguata" deve tener conto di due elementi essenziali : il contenuto delle norme applicabili e gli strumenti per assicurarne un'efficace applicazione.

Prendendo come punto di partenza la direttiva 95/46/CE e tenendo presenti le disposizioni di altri testi normativi internazionali sulla protezione dei dati, dovrebbe essere possibile individuare un nucleo di principi di 'contenuto' e di prescrizioni di 'procedura/applicazione', la cui osservanza potrebbe essere considerata una condizione minima di adeguatezza della tutela. Si tratterebbe di una lista di riferimento duttile: eventualmente da integrare in alcuni casi, da ridimensionare quanto alle prescrizioni di altri. Il grado di rischio insito nel trasferimento per la persona interessata sarà un elemento importante ai fini della determinazione delle prescrizioni esatte di un caso

particolare. Pur con questa limitazione, la compilazione di una lista di condizioni minime costituisce un utile punto di partenza per qualsiasi analisi.

(i) Principi di contenuto

I principi fondamentali da includere sono i seguenti:

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 sole deroghe a tale norma sarebbero quelle necessarie in ogni società democratica per una delle ragioni elencate nell'articolo 13 della direttiva.[2]

2) **il principio della qualità e della proporzionalità :** i dati dovrebbero essere precisi e, se del caso, aggiornati. Essi dovrebbero essere adeguati, pertinenti e commisurati alle 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 e l'identità del responsabile del trattamento nel paese terzo, nonché qualunque altra informazione necessaria ad assicurare una procedura equa. Le sole deroghe consentite dovrebbero essere in linea con l'articolo 11, paragrafo 2[3] e con l'articolo 13 della direttiva.

4) **il principio della sicurezza :** il responsabile del trattamento dei dati dovrebbe adottare misure di sicurezza tecniche e organizzative commisurate ai rischi che il trattamento presenta. Chiunque operi sotto l'autorità del responsabile del trattamento, compresi gli incaricati del trattamento, procede al trattamento dei dati solo su istruzione del responsabile.

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

6) restrizioni ai successivi trasferimenti di dati personali da parte del destinatario del primo trasferimento dovrebbero essere consentite soltanto quando anche il secondo destinatario (ossia il destinatario del trasferimento successivo) è soggetto a norme che

[2] L'articolo 13 prevede la possibilità di limitare il 'principio della finalità', qualora tale restrizione costituisca una misura necessaria alla salvaguardia della sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate, di un rilevante interesse economico o finanziario, della protezione della persona interessata o dei diritti e delle libertà altrui.

[3] L'articolo 11, paragrafo (2) prevede che, nel caso in cui i dati non siano raccolti presso la persona interessata, a quest'ultima non debbano essere fornite informazioni quando ciò si rivela impossibile o richiede sforzi sproporzionati o la registrazione o la comunicazione è prescritta per legge.

assicurano un livello adeguato di tutela. Le sole deroghe consentite dovrebbero essere in linea con l'articolo 26, paragrafo (1) della direttiva. Tali deroghe sono esaminate nel capitolo 5e.

Di seguito sono riportati alcuni esempi di principi supplementari da applicare in casi specifici di trattamento.

1) **dati sensibili :** se il trattamento riguarda categorie di dati 'sensibili' (quelle elencate all'articolo 8 della direttiva[4]), 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.

3) **decisioni individuali automatizzate :** se la finalità del trasferimento consiste nell'adozione di una decisione automatizzata ai sensi dell'articolo 15 della direttiva, la persona dovrebbe avere il diritto di conoscere la logica a cui tale decisione risponde e dovrebbero essere adottati altri provvedimenti per garantire la salvaguardia del suo interesse legittimo.

(ii) Meccanismi di procedura/applicazione

Vi è in Europa un ampio consenso circa la necessità di dare forma di legge ai principi di tutela dei dati. Ugualmente riconosciuta è la necessità di un sistema di 'controllo esterno' sotto forma di autorità indipendente, atto ad assicurare l'osservanza delle norme di tutela. Non in tutti i paesi, tuttavia, questi elementi sono presenti.
Per fornire una base per la valutazione dell'adeguatezza della tutela offerta, è necessario individuare gli obiettivi di fondo di un sistema procedurale per la tutela dei dati e da qui procedere ad esaminare i diversi meccanismi procedurali giudiziari e non giudiziari applicati nei paesi terzi.

Gli obiettivi di un sistema di tutela dei dati sono essenzialmente tre :

1) assicurare un **buon livello di osservanza** delle norme (nessun sistema è in grado di garantire un'osservanza del 100%, ma alcuni sono migliori di altri). In un buon sistema, tra i responsabili del trattamento dei dati si può generalmente rilevare un elevato grado di consapevolezza dei propri obblighi e tra le persone interessate la medesima consapevolezza dei propri diritti e degli strumenti per esercitarli. Di particolare importanza, al fine di garantire il rispetto delle norme, è l'esistenza di sanzioni efficaci e dissuasive, al pari, ovviamente, di sistemi di verifica diretta da parte di autorità, revisori o addetti indipendenti alla tutela dei dati.

[4] Dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, dati relativi alla salute e alla vita sessuale e dati relativi a infrazioni, condanne penali o misure di sicurezza.

2) fornire **aiuto e sostegno alla persona interessata** nell'esercizio dei propri diritti. Ogni persona deve essere in grado di far rispettare i propri diritti in modo rapido ed efficace, ad un costo non proibitivo. A tal fine occorre porre in essere qualche meccanismo istituzionale che consenta di condurre un'indagine indipendente in caso di denuncia.

3) garantire un **risarcimento adeguato** alla parte lesa in caso di violazione delle norme. Si tratta di un elemento essenziale, che necessita di un sistema di arbitrato indipendente in grado di deliberare la corresponsione di un indennizzo e di imporre eventualmente sanzioni.

CAPITOLO 2: APPLICAZIONE DEI PRINCIPI AI PAESI CHE HANNO RATIFICATO LA CONVENZIONE N° 108 DEL CONSIGLIO D'EUROPA

Nel settore della protezione dei dati la convenzione n. 108 è l'unico strumento di diritto internazionale esistente oltre alla direttiva. La maggioranza dei firmatari è costituita da Stati membri dell'Unione europea (tutti i 15 hanno ormai ratificato la convenzione) o da paesi, come la Norvegia e l'Islanda, comunque vincolati dalla direttiva in forza dell'accordo sullo spazio economico europeo. Anche la Slovenia, l'Ungheria e la Svizzera hanno ratificato la convenzione e probabilmente altri paesi terzi lo faranno in futuro, tenuto conto in particolare del fatto che possono aderire alla convenzione anche paesi non membri del Consiglio d'Europa. Va quindi ben al di là di un interesse puramente accademico verificare se i paesi che hanno ratificato la convenzione si possono considerare in grado di garantire una tutela adeguata ai sensi dell'articolo 25 della direttiva.

Come punto di partenza è opportuno analizzare il testo della convenzione stessa alla luce del profilo teorico della 'tutela adeguata' definito nel capitolo uno del presente documento.

Per quanto riguarda il contenuto dei principi di base, si può affermare che la convenzione soddisfa le prime cinque delle sei 'condizioni minime'. [5] La convenzione prevede inoltre, a garanzia dell'adeguatezza della tutela dei dati particolarmente 'sensibili', l'obbligo di adottare misure di salvaguardia appropriate.

Per quanto riguarda il contenuto delle norme sostanziali della convenzione, una carenza è rappresentata dall'assenza di restrizioni al trasferimento verso paesi non firmatari. Questo comporta il rischio che un paese aderenti alla convenzione sia utilizzato come 'tappa intermedia' in un trasferimento di dati dalla Comunità verso un altro paese terzo in cui il livello di tutela è del tutto inadeguato.

Il secondo aspetto della 'tutela adeguata' riguarda i meccanismi procedurali atti a garantire un'applicazione efficace dei principi di base. La convenzione impone ai paesi firmatari l'obbligo di dare forma di legge nazionale ai principi in essa contenuti e di istituire un sistema appropriato di sanzioni e di ricorsi in caso di violazione di detti principi. Ciò dovrebbe bastare ad assicurare un livello ragionevole di osservanza delle norme e un risarcimento adeguato della persona interessata in caso di inadempienza (obiettivi (1) e (3) di un sistema di tutela dei dati). La convenzione, tuttavia, non impone alle parti contraenti di creare meccanismi istituzionali che permettano di condurre indagini indipendenti in caso di denuncia, anche se in pratica è quanto hanno fatto in genere i paesi firmatari. Si tratta di una lacuna della convenzione, dal momento che l'assenza di tali meccanismi istituzionali non consente di garantire alla singola persona interessata un sostegno adeguato nell'esercizio dei propri diritti (obiettivo (2)).

[5] Qualche dubbio può sussistere circa il 'principio di trasparenza'. L'articolo 8, lettera (a) della convenzione potrebbe non essere equivalente all'obbligo *attivo* di fornire informazioni, sancito dagli articoli 10 e 11 della direttiva. Inoltre, la convenzione non prevede in modo specifico il diritto di esclusione nel caso in cui i dati siano utilizzati a fini di commercializzazione diretta ne contiene disposizioni circa le decisioni individuali automatizzate.

Questa breve analisi sembra indicare che, nella maggioranza dei casi, i trasferimenti di dati personali verso paesi che hanno ratificato la convenzione n. 108 si possono ritenere ammissibili ai sensi dell'articolo 25, paragrafo (1) della direttiva, a condizione che :

- il paese in questione disponga di meccanismi istituzionali appropriati che garantiscano l'osservanza delle norme e consentano di prestare assistenza alle persone interessate e assicurarne il risarcimento (come ad esempio un'autorità di controllo indipendente dotata di potere adeguati);
- il paese in questione sia destinatario finale del trasferimento e non una tappa intermedia attraverso cui i dati transitano, tranne il caso in cui i trasferimenti successivi siano diretti verso i paesi dell'UE o verso un'altra destinazione che garantisca una tutela adeguata. [6]

Ovviamente questo esame della convenzione è abbastanza semplificato e superficiale. Casi specifici di trasferimenti di dati verso paesi firmatari della convenzione possono sollevare altri problemi che qui non sono stati presi in considerazione.

[6] La convenzione n.108 è attualmente oggetto di una revisione, che potrebbe dar luogo a modifiche introdotte per superare queste e altre difficoltà.

CAPITOLO 3 APPLICAZIONE DEI PRINCIPI ALL'AUTODISCIPLINA SETTORIALE

Introduzione

L'articolo 25, paragrafo 2, della direttiva sulla tutela dei dati personali (95/46/CE) statuisce che il livello di protezione garantito da un paese terzo deve essere valutato con riguardo a *tutte le circostanze* relative ad un trasferimento o ad una categoria di trasferimenti di dati. Si citano specificamente non solo le norme di diritto, ma anche "le regole professionali e le misure di sicurezza ivi osservate".

Il testo della direttiva impone quindi di tenere conto delle norme di carattere non giuridico che possono essere in vigore nel paese terzo in questione, a patto che dette norme *siano rispettate*. E' in questo contesto che va inquadrata la funzione dell'autodisciplina settoriale.

Che cos'è l'autodisciplina?

Il termine "autodisciplina" può assumere diversi significati. Nel presente documento per codice (o altro strumento) di autodisciplina s'intende qualsiasi complesso di norme per la tutela dei dati applicabili all'insieme dei responsabili del trattamento dei dati, appartenenti alla medesima professione od operanti nel medesimo settore economico, il cui contenuto è stato determinato essenzialmente da chi opera in tale settore o da chi esercita tale professione.

Si tratta di una definizione generale in cui può rientrare un'ampia gamma di strumenti, dal codice volontario di tutela dei dati elaborato dalla piccola associazione settoriale con solo pochi aderenti, fino al codice più articolato che fissa norme d'etica professionale applicabili a un'intera categoria professionale, ad es. medici o bancari, avente effetti pressoché analoghi a quelli giurisdizionali.

L'organismo responsabile del codice è rappresentativo del settore?

Come si chiarirà in questo capitolo, un importante parametro del valore di un codice è il grado di applicazione delle sue disposizioni. In questo contesto, la questione della rappresentatività dell'associazione o dell'organismo responsabile del codice, ossia se essi rappresentino tutti gli operatori del settore o solo una piccola percentuale di essi, è probabilmente meno importante rispetto alla determinazione del potere dell'associazione in termini di capacità, ad esempio, di applicare sanzioni agli aderenti che non rispettano il codice. Tuttavia, per varie altre ragioni, i codici applicabili a un intero settore o a un'intera professione, e aventi un campo d'applicazione definito in modo chiaro e dettagliato, sono degli strumenti di tutela più utili dei codici sviluppati da piccoli raggruppamenti di aziende all'interno dei vari settori. Anzitutto, dal punto di vista del consumatore, un settore non compatto e in cui operano molte associazioni rivali, ciascuna con un proprio codice di tutela dei dati, crea confusione. L'esistenza parallela di molti codici differenti crea un'immagine globale priva di trasparenza per la persona interessata. In secondo luogo, segnatamente per attività quali la vendita diretta, in cui è prassi corrente trasmettere i dati personali da una società all'altra, può succedere che la società che comunica i dati e la società ricevente non siano vincolate

dal medesimo codice di tutela. Ciò è una fonte di incertezza circa la natura delle norme applicabili e può rendere più difficile l'esame dei reclami presentati dalle persone interessate e la ricerca di una soluzione.

Valutazione dell'autodisciplina: criteri da seguire

Vista la grande varietà di strumenti compresi nel termine autodisciplina, è palese la necessità di differenziare le varie forme di autodisciplina in base al loro reale effetto sul livello di tutela offerto quando i dati personali sono trasferiti in un paese terzo.

Per valutare qualsiasi corpo specifico di norme per la tutela dei dati (che rientri nella categoria dell'autodisciplina o in quella della regolamentazione) è necessario fare riferimento ai principi generali enunciati nel capitolo 1. È di fondamentale importanza non limitare l'esame dello strumento al suo contenuto (che dovrà abbracciare una serie di principi di base) ma estenderlo alla sua efficacia nel conseguire:

- un buon livello generale di osservanza,
- sostegno e assistenza alle persone interessate dal trattamento dei dati,
- mezzi di riparazione adeguati (ivi incluso il risarcimento se necessario)

Valutazione del contenuto di uno strumento di autodisciplina

E' un compito relativamente facile. Si tratta di accertare la presenza dei necessari 'principi di contenuto' enumerati nel capitolo 1. Si tratta di una valutazione obiettiva, che verte sul contenuto del codice e non sulle modalità con cui è stato elaborato. Il fatto che un settore economico o una professione abbia avuto un ruolo chiave nell'elaborazione del contenuto del codice non è di per sé rilevante, benché sia evidente che se nella sua elaborazione si è tenuto conto del parere delle persone interessate e delle organizzazioni dei consumatori, è più probabile che esso rispecchi più rigorosamente i requisiti basilari di tutela dei dati.
La trasparenza del codice è un elemento determinante; soprattutto, è necessario che il codice sia redatto in un linguaggio semplice e offra esempi concreti, che ne illustrino le disposizioni. Il codice dovrebbe inoltre vietare la comunicazione dei dati a società che non abbiano sottoscritto il codice e che pertanto non vi siano assoggettate, a meno che non siano offerte altre garanzie adeguate.

Valutazione dell'efficacia dello strumento di autodisciplina

Valutare l'efficacia di un determinato codice o strumento di autodisciplina è un compito più arduo, che richiede la comprensione dei dispositivi che garantiscono il rispetto del codice e con i quali si regolano i problemi inerenti alle violazioni. Perché un codice di autodisciplina possa essere considerato atto a garantire una tutela adeguata, è necessario che siano soddisfatti i tre criteri funzionali su cui si basa la valutazione dell'efficacia della tutela.

Buon livello di osservanza

I codici settoriali o professionali sono di norma elaborati da un organo rappresentativo del settore o della professione e si applicano agli aderenti della categoria che fa capo a

tale organo rappresentativo. Il grado di osservanza del codice dipende verosimilmente dal fatto che i membri sappiano che esso esiste e ne conoscano il contenuto, dalle misure adottate per renderlo trasparente agli occhi dei consumatori, consentendo alle forze di mercato di dare un contributo concreto, dall'esistenza di un sistema di controllo esterno (quale ad esempio l'obbligo di accertamento periodico della sua osservanza) e, cosa forse più importante, dal genere di sanzioni contemplate in caso di violazione e dalla loro applicazione.

E' perciò importante chiedersi:

- Che cosa fa l'organo rappresentativo per garantire la conoscenza del codice tra i suoi aderenti?
- L'organo rappresentativo esige che i suoi aderenti dimostrino di aver applicato concretamente le disposizioni contemplate dal codice? Con che frequenza?
- Tale prova è fornita dall'impresa aderente stessa o da una fonte esterna (quale ad esempio un revisore riconosciuto)?
- L'organo rappresentativo esamina le violazioni, denunciate o presunte, del codice?
- L'osservanza del codice è una condizione per l'adesione all'organo rappresentativo o l'osservanza è puramente "facoltativa"?
- Qualora sia dimostrato che un aderente abbia violato il codice, di quali sanzioni disciplinari (espulsione o altro) può valersi l'organo rappresentativo?
- In caso di provvedimento d'espulsione da parte dell'organo rappresentativo, la società o l'individuo possono continuare ad operare nello stesso settore o ad esercitare la stessa professione?
- Il rispetto del codice può essere imposto in altro modo, ad esempio per via giudiziaria o mediante un organo avente giurisdizioni speciali? In taluni paesi i codici professionali o deontologici sono legalmente vincolanti. In alcuni casi ci si può persino valere delle norme di legge relative alle pratiche commerciali leali o addirittura alla concorrenza per far applicare i codici settoriali.

Allorché si esaminano i tipi di sanzioni comminate, è importante distinguere tra sanzioni "correttive", che, in caso di inosservanza, si limitano a esigere che il responsabile del trattamento dei dati modifichi le proprie pratiche adeguandole alle disposizioni del codice, e le sanzioni che vanno oltre e puniscono il responsabile del trattamento dei dati per la sua inadempienza. Solo questa seconda categoria di sanzioni "punitive" incide realmente sulla futura condotta dei responsabili del trattamento dei dati, incentivandoli a rispettare il codice in modo regolare.

La mancanza di sanzioni realmente dissuasive e punitive è, per un codice, una grave debolezza. Senza tali sanzioni è difficile immaginare come si possa ottenere un buon grado di osservanza generale, a meno che non esista un rigoroso sistema di controllo esterno (ad esempio un'autorità pubblica o privata abilitata ad intervenire in caso di inosservanza del codice, o l'obbligo di sottoporsi a una verifica esterna periodica).

Sostegno e assistenza alle persone interessate dal trattamento dei dati

Un requisito fondamentale a garanzia dell'adeguatezza e dell'efficacia del sistema di tutela dei dati è rappresentato dal fatto che chiunque abbia un problema circa il trattamento di dati che lo riguardano non sia abbandonato a se stesso, ma goda del

sostegno di una istanza prevista dal sistema di tutela medesimo, per poter risolvere il suo problema. Idealmente, questa istanza di sostegno dovrebbe essere imparziale, indipendente e dotata dei poteri necessari per indagare in merito a eventuali reclami sporti dalle persone interessate. Gli interrogativi riguardanti l'autodisciplina che si pongono sotto questo profilo sono i seguenti:

- Esiste un dispositivo che permetta di indagare in merito ai reclami presentati dalle singole persone interessate?
- Come sono informate le persone interessate dell'esistenza di detto dispositivo e delle decisioni prese nei singoli casi?
- Le persone interessate debbono sostenere dei costi?
- Chi conduce le indagini? Tale persona / organo dispone di sufficienti poteri al riguardo?
- Chi decide in merito ad un'asserita violazione del codice? Si tratta di persone indipendenti e imparziali?

L'imparzialità dell'arbitro o della persona investita della decisione in merito all'asserita violazione del codice è fondamentale. E' ovvio che tale persona od organo debbano essere indipendenti dal responsabile del trattamento dei dati. Tuttavia questo in sé non basta a garantire l'imparzialità. Idealmente l'arbitro dovrebbe essere estraneo alla professione o al settore in questione, poiché chi esercita la stessa professione od opera nel medesimo settore ha chiaramente interessi comuni al responsabile del trattamento dei dati accusato di violazione del codice. Se così non è, la neutralità dell'organo investito della decisione può essere garantita mediante l'inclusione (in pari numero) di rappresentanti dei consumatori e di rappresentanti del settore.

Riparazione adeguata

Qualora si dimostri che il codice di autodisciplina è stato violato, la persona interessata dovrebbe avere la possibilità di ottenere riparazione. Tale riparazione deve ovviare al problema (ad es. rettificare o eliminare i dati erronei, porre fine al trattamento dei dati per fini incompatibili) e, qualora la persona interessata abbia subito dei danni, deve permettere un adeguato risarcimento pecuniario. Va ricordato che il termine 'danno' ai sensi della direttiva concernente la tutela di dati non indica unicamente i danni materiali e finanziari, ma anche i danni psicologici e morali (noti come "distress" nel diritto del Regno Unito e degli Stati Uniti).

Molti dei quesiti relativi alle sanzioni, riportati nella sezione precedente intitolata "Buon livello di osservanza", sono pertinenti anche in questo contesto. Come precedentemente detto, le sanzioni hanno una duplice funzione: punire chi commette l'infrazione (stimolando quindi il trasgressore e gli altri aderenti a rispettare le norme) e rimediare alla violazione delle norme. È principalmente questa seconda funzione che prendiamo qui in considerazione. Ulteriori interrogativi potrebbero perciò essere:

- E' possibile verificare se un aderente, a carico del quale è stata accertata una violazione del codice, ha modificato le sue pratiche e rimediato al problema?
- Le persone interessate possono ottenere un risarcimento in base al codice, e come?
- La violazione del codice è equiparabile all'inadempienza contrattuale, o regolata dal diritto comune (ad es. tutela dei consumatori, concorrenza sleale),

e possono le autorità giudiziarie competenti accordare il risarcimento dei danni su tale base?

Conclusioni

- L'autodisciplina dovrebbe essere valutata in base ai criteri obiettivi e funzionale enunciati nel capitolo 1.
- Uno strumento di autodisciplina può essere considerato un valido elemento di "adeguata tutela" solo se è vincolante per tutti coloro che vi sono assoggettati, a cui sono trasferiti i dati personali, e se offre sufficienti garanzie qualora i dati siano trasmessi a terzi non aderenti.
- Lo strumento deve essere trasparente e incorporare nella sostanza i principi basilari relativi alla tutela dei dati.
- Lo strumento deve avere dispositivi che assicurino effettivamente un buon livello di osservanza generale. Un sistema di sanzioni dissuasive e punitive è una delle possibilità a tale fine. Un'altra sono i controlli esterni obbligatori.
- Lo strumento deve offrire sostegno e assistenza alle persone interessate che abbiano un problema relativo al trattamento dei loro dati personali. E' pertanto necessario istituire un organismo indipendente, imparziale e facilmente accessibile che esamini i reclami presentati dalle persone interessate e decida in merito alle violazioni del codice.
- Lo strumento deve garantire un'adeguata riparazione in caso di inosservanza. La persona interessata deve poter ottenere un provvedimento di riparazione e se del caso un risarcimento.

CAPITOLO 4 : IL RUOLO DELLE DISPOSIZIONI CONTRATTUALI

1. Introduzione

In base al principio stabilito 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. In questo capitolo sono esaminate le possibile deroghe al principio della "tutela adeguata" dell'articolo 25 previste dall'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 la Commissione può inoltre, 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 ricorrere a contratti come mezzo per regolamentare i trasferimenti internazionali di dati personali non è stata ovviamente introdotta dalla direttiva. Già nel 1992 il Consiglio d'Europa, la Camera di commercio internazionale e la Commissione europea avevano effettuato congiuntamente uno studio in merito[7]. In tempi più recenti un numero 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 dell'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 [8].

2. Utilizzazione di contratti come base per i trasferimenti 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 soggetto sia interessato

[7] '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.

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

al trattamento dei dati in questione. Ai sensi della direttiva un soggetto, il "responsabile del trattamento", deve assumere la responsabilità principale dell'osservanza dei principi essenziali di protezione dei dati. Il secondo soggetto, l'"incaricato del trattamento", è responsabile unicamente della sicurezza dei dati. Per responsabile del trattamento si intende un soggetto dotato di poteri di decisione circa le finalità e le modalità di trattamento dei dati, mentre l'incaricato del trattamento è unicamente il soggetto che fornisce fisicamente il servizio di trattamento dei dati. La relazione tra i due soggetti è definita all'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 dati personali, se non dietro istruzione del responsabile del trattamento oppure in virtù di obblighi di legge.

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 il soggetto che trasferisce i dati (il "cedente") e il soggetto 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. Il contratto deve però 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[9]) 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

[9] L'esercizio dei diritti in materia di tutela dei dati personali è facilitato nell'ambito della Comunità dal contesto giuridico generale, ad esempio dall'accordo di Strasburgo (1977) sulla trasmissione di richieste di assistenza giuridica.

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 delle "garanzie sufficienti" di cui all'articolo 26, paragrafo 2, è la nozione di "tutela adeguata", già esaminata nel capitolo 1, nel quale sono stati individuati alcuni principi fondamentali in materia di protezione dei dati e talune condizioni necessarie per assicurarne l'efficacia.

(i) Norme fondamentali 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 dei principi fondamentali in materia di protezione dei dati enunciati nel capitolo 1 al trattamento dei dati trasferiti verso il paese terzo. Tali principi fondamentali sono:

- il principio della finalità limitata
- il principio della qualità e della proporzionalità
- il principio della trasparenza
- il principio della sicurezza
- i diritti di accesso, rettifica e opposizione
- restrizioni ai successivi trasferimenti verso parti non firmatarie del contratto[10].

Inoltre, in alcune situazioni vanno applicati altri principi relativi ai dati sensibili, alla commercializzazione diretta e alle decisioni automatizzate.

Nel contratto andrebbe precisato in che modo il destinatario del trasferimento dei dati dovrà 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 garantita da norme analoghe a quelle previste dalla direttiva, è probabile che esistano altri meccanismi che precisano le modalità di applicazione pratica delle norme di protezione dei dati (codici di comportamento, notificazione, 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 fondamentali

Nel capitolo 1 sono enunciati tre criteri in base ai quali andrebbe valutata l'efficacia del sistema di protezione dei dati. Tali criteri si riferiscono alla capacità del sistema di:

[10] Non dovrebbero essere autorizzati ulteriori trasferimenti dei dati personali dal destinatario a terzi, a meno che non si trovi il modo di obbligare contrattualmente questi ultimi a fornire alle persone interessate le stesse garanzie di tutela dei dati.

- assicurare un **buon livello di osservanza** delle norme;

- fornire **sostegno e assistenza alle persone interessate dal trattamento dei dati** nell'esercizio dei propri diritti;

- elemento di importanza essenziale, garantire una **riparazione adeguata** alla parte lesa in caso di inosservanza delle norme.

Nel valutare l'efficacia di una soluzione contrattuale vanno applicati gli stessi criteri. Si tratta evidentemente 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.

Garantire una riparazione alla persona interessata

Garantire alla persona interessata la possibilità di un ricorso legame (ossia il diritto di presentare un reclamo ad un arbitro indipendente che possa giudicare in merito e di ottenere, se del caso, una riparazione) tramite un contratto tra il "cedente" 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 stabilita. 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 che 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 nel caso in cui i dati siano stati fisicamente trasferiti al di fuori dell'UE, il controllo decisionale sui dati spetta sempre al soggetto, stabilito nella Comunità, che ha effettuato il trasferimento. In tal modo il cedente resta il responsabile del trattamento, mentre il destinatario è semplicemente un subcontraente incaricato del trattamento. In questo caso, dato che il controllo dei dati è esercitato da un soggetto stabilito in uno Stato membro dell'UE, la legislazione dello Stato membro in questione continuerà ad essere applicabile al trattamento effettuato nel paese terzo[11] e inoltre il responsabile del trattamento continuerà, ai sensi della

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

legislazione di tale Stato membro, ad essere responsabile di eventuali danni cagionati da un trattamento illecito[12].

Disposizioni di questo tipo non sono dissimili da quelle previste 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[13].

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.

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

[13] 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.

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.

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[14]. 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[15]. 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[16] 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

[14] 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. E' quindi necessaria una procedura investigativa al di fuori delle procedure legali del diritto civile ufficiale.

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

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

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.

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[17]. 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.

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[18]. 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

[17] 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.

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

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.
- 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.

CAPITOLO 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.

CAPITOLO 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[19], 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

[19] 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.

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 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 premetterebbe 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 manipolazione. 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.[20]

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 compagnia aerea (articolo 26, paragrafo 1, lettera b). Tuttavia, la conservazione dei dati (compresi i dati riservati sulla salute dell'individuo) nella base di dati della compagnia aerea non può essere giustificata in base a questi motivi. Il trasferimento dei dati alla compagnia aerea deve quindi essere giustificato da una diversa deroga.

[20] 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.

Come nel caso (1), la soluzione migliore è il consenso dell'interessato, che potrebbe essere ottenuto dall'agenzia di viaggi di Lisbona per conto della compagnia aerea. L'interessato va informato dei rischi derivanti dal fatto che i dati saranno conservati nel paese B, nonché del fatto che il trasferimento e la conservazione dei dati nella base di dati della compagnia aerea non sono necessari per ragioni riguardanti il volo prenotato.

CASO (3) : Il trasferimento di dati di elenchi commerciali

Una società dei Paesi Bassi è specializzata nella creazione di "mailing lists". Utilizzando varie fonti di informazione pubblica disponibili nei Paesi Bassi e liste di clienti noleggiate da altre società olandesi, compila elenchi di persone che corrispondono a un particolare profilo socioeconomico. Questi elenchi sono poi venduti dalla società olandese a clienti nei Paesi Bassi e nell'UE, nonché in numerosi altri paesi terzi. Le società acquirenti utilizzano gli elenchi (che comprendono indirizzi postali, numeri di telefono e spesso indirizzi di posta elettronica) per contattare le persone e proporre loro l'acquisto di una vastissima gamma di prodotti e servizi. Numerose persone che figurano su questi elenchi hanno sporto reclamo presso le autorità olandesi di tutela dei dati a causa delle proposte commerciali che hanno ricevuto.

Le norme applicabili pertinenti

Alcune delle società che hanno acquistato le "mailing lists" offerte dalla società olandese hanno sede in paesi con leggi generali sulla tutela dei dati che prevedono il diritto di rifiutare queste proposte commerciali. Altre sono situate in paesi privi di tali leggi, ma sono membri di associazioni autoregolamentate che hanno introdotto codici di protezione dei dati. Altre ancora non sono soggette ad alcuna norma sulla tutela dei dati.

Valutazione del contento delle norme applicabili

Questo caso specifico richiede la valutazione di una serie di leggi e di codici diversi. Se la società con sede nei Paesi Bassi continua questo tipo di vendita e di noleggio di liste a società in vari paesi del mondo, si verificheranno inevitabilmente situazioni in cui il livello di tutela non è adeguato.

FASE 2 : RICERCA DI UNA SOLUZIONE

In questo caso, poiché i dati sono raccolti da fonti pubbliche e senza un contatto diretto con gli interessati, sarebbe molto problematico per la società situata nei Paesi Bassi chiedere il consenso di ogni persona alla sua inclusione nelle "mailing lists". È quindi improbabile che possa essere applicata una delle deroghe previste dall'articolo 26, paragrafo 1.

La società olandese ha due possibilità, che può utilizzare alternativamente oppure insieme. La prima è quella di limitare il suo commercio di mailing list a società soggette a giurisdizioni che garantiscono una tutela adeguata mediante leggi o strumenti efficaci di autodisciplina. In questa sua decisione la società potrebbe essere guidata da una qualsiasi "lista bianca". La seconda possibilità sarebbe quella di chiedere un impegno contrattuale a tutte le società acquirenti (o almeno a quelle soggette a giurisdizioni "non adeguate") circa la tutela dei dati trasferiti. Questi accordi contrattuali dovrebbero seguire le indicazioni contenute nel capitolo 4 del presente documento. In

virtù di tali accordi, in particolare, la società olandese dovrebbe rimanere responsabile, secondo la legislazione nazionale, di ogni violazione dei principi di tutela dei dati risultante da azioni della società cliente a cui sono stati trasferite le "mailing lists".

Una tale soluzione contrattuale, se applicata in modo appropriato, contribuirebbe a superare gli ostacoli al commercio creati dalla mancanza in vari paesi terzi di una tutela adeguata dei dati.

Fatto a Bruxelles, il 24 luglio 1998

Per il gruppo di lavoro

Il presidente

P.J. HUSTINX