grado di fornire a tutti un livello minimo e non negoziabile di protezione della vita privata. L'utilizzazione della P3P e dell'OPS senza questo quadro di riferimento rischia di scaricare principalmente sul singolo utente l'onere della protezione; si tratterebbe di un'evoluzione contraria alla norma ormai consolidata a livello internazionale secondo cui il «responsabile del trattamento» deve rispettare i principi della tutela dei dati (orientamenti OCSE del 1980, convenzione n. 108 del 1981 del Consiglio d'Europa, orientamenti ONU del 1990, direttive Ue 95/46/CE e 97/66/CE). Tale inversione di responsabilità presuppone peraltro un livello di conoscenza dei rischi per la vita privata posti dal trattamento dei dati che la maggioranza dei cittadini probabilmente non possiede.

– Esiste il rischio che la P3P, una volta applicata alla prossima generazione di software per il *browsing*, possa far erroneamente ritenere a taluni «incaricati del trattamento» con sede nell'Ue di poter essere esentati da determinati obblighi giuridici (per esempio, la concessione ai singoli utenti del diritto di accesso ai loro dati), qualora il singolo utente vi acconsenta nell'ambito della negoziazione «in linea». In realtà, le imprese, le organizzazioni e i singoli cittadini stabiliti nell'Ue e fornitori di servizi su Internet dovranno comunque osservare le norme fissate nella direttiva 95/46/CE sulla tutela dei dati (come recepita nella legislazione nazionale) per quanto riguarda la raccolta ed il trattamento dei dati personali. La P3P potrebbe pertanto essere fonte di confusione non solo tra gli incaricati del trattamento riguardo ai loro obblighi, ma anche tra gli utenti di Internet riguardo alla natura dei loro diritti in termini di protezione dei dati. Il software per il *browsing* venduto o distribuito nell'Ue deve pertanto essere progettato e configurato in modo tale da assicurare l'impossibilità di concludere accordi «in linea» che violino la normativa prevalente in materia di tutela dei dati.

– Per l'utente che ha sede nell'Ue ed entra in contatto con siti Web stabiliti in paesi non comunitari la preoccupazione principale deriva dal fatto che le organizzazioni a cui fornisce i suoi dati personali potrebbero non essere soggette alla direttiva Ue o a qualunque altra normativa che disciplini in modo efficace la protezione dei dati [57]. Per decidere se fornire o meno i dati a questi siti, sarà di fondamentale importanza sapere non solo quale sia il contenuto approssimativo di tutte le regole applicabili, ma anche se esistono sanzioni in caso di inosservanza, in particolare se è previsto uno strumento semplice ed efficace di ricorso nei casi di violazione. Una piattaforma «in linea» per le preferenze in materia di protezione della vita privata dovrebbe in teoria essere in grado di fornire tali informazioni agli utenti. Tuttavia, la configurazione attuale del vocabolario della P3P non richiede né prevede che agli utenti siano fornite informazioni circa le sanzioni o i ricorsi. Risulta pertanto necessario rivedere il vocabolario standard, affinché la P3P possa rivelarsi uno strumento utile per ottenere «in linea» dagli utenti Ue un consenso informato al trasferimento di dati personali (secondo quanto disposto dall'articolo 26, paragrafo 1, lettera *a)*, della direttiva).

– Essendo improbabile che la maggior parte degli utenti Internet cambi anche uno solo dei parametri predeterminati sul proprio *browser*, la configurazione predefinita (*default*) relativa alle preferenze dell'utente in materia di prote-

[57] Resta impregiudicata la possibilità di un esame dettagliato dell'articolo 4 della direttiva 95/46/CE, che potrebbe essere interpretato in maniera tale da rendere la direttiva applicabile a siti di paesi terzi che raccolgano dati da utenti con sede nell'Ue.

zione della vita privata avrà un'influenza decisiva sul livello complessivo della protezione della vita privata «in linea». La P3P e l'OPS devono essere applicate nella tecnologia dei *browser* con posizioni di *default* che rispecchino l'interesse dell'utente a beneficiare di un livello elevato di protezione della vita privata (compresa la possibilità di esplorare dei siti Web mantenendo l'anonimato) senza trovarsi bloccato o infastidito nei suoi tentativi di accedere ad un sito. Se l'incaricato del trattamento pone come condizione di accesso al proprio sito la fornitura di un profilo di dati identificabili, l'utente dovrebbe essere interrogato ogni volta se intende acconsentire alla fornitura di tali informazioni al sito in questione. Se il sito non richiede questi dati in via preliminare, l'accesso dovrebbe procedere senza interruzioni. I principali produttori di software per il *browsing* hanno la responsabilità di applicare la P3P e l'OPS in modo da rinforzare piuttosto che ridurre i livelli di protezione della vita privata.

Data l'importanza del processo di applicazione della P3P e dell'OPS, e alla luce dei diversi temi attualmente allo studio del gruppo relativamente alla funzionalità dei protocolli Web (HTTP), il gruppo è favorevole all'elaborazione di software Internet conformemente alla normativa sulla tutela dei dati applicabile nell'Unione europea e ritiene opportuna la messa a punto di meccanismi in grado di verificare la conformità del software Internet a tale riguardo.

Fatto a Bruxelles, il 16 giugno 1998

Per il Gruppo
Il Presidente P.J. HUSTINX

5.7.5 Trasferimento di dati personali verso Paesi terzi

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV
Mercato interno e servizi finanziari
Libera circolazione delle informazioni - Diritto delle società e 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

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) [58], 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 pre-

---

[58] 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.

sente 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 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 questioni 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.

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 notifica-

zione. 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. [59)]

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.

[59)] 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) **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 [60] 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 riguardano, 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 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 [61]), 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

---

[60] 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.

[61] 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.

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.

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.

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» [62]. La convenzione prevede inoltre, a garanzia dell'adeguatezza della tutela dei dati particolarmente «sensibili», l'obbligo di adottare misure di salvaguardia appropriate.

---

[62] 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 né contiene disposizioni circa le decisioni individuali automatizzate.

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 aderente 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).

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 [63].

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.

3. Applicazione dei principi all'autodisciplina settoriale

1. 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».

---

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

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*. È in questo contesto che va inquadrata la funzione dell'autodisciplina settoriale.

2. 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.

3. 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.

4. 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 fon-

damentale 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)

5. Valutazione del contenuto di uno strumento di autodisciplina

È 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.

6. 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.

È 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. È 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:

– È 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?

7. Conclusioni

– L'autodisciplina dovrebbe essere valutata in base ai criteri obiettivi e funzionali 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. È 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.

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 possibili 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 [64]. 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 [65].

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 al trattamento dei dati in questione. Ai sensi della

---

[64] «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.

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

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. Objettivo 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 [66]) verso un paese terzo in cui il livello generale di protezione non sia adeguato. Per soddisfare tale funzione, una disposizione contrattuale deve compensare in modo soddisfacente la mancanza di un livello generale di protezione adeguata e comportare gli elementi essenziali di tutela che possono mancare in una qualsiasi situazione particolare.

---

[66] 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.

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 [67].

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:

– 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

[67] 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.

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 legale (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 [68] e inoltre il responsabile del trattamento continuerà, ai sensi della legislazione di tale Stato membro, ad essere responsabile di eventuali danni cagionati da un trattamento illecito [69].

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 destina-

---

[68] Ai sensi dell'art. 4, paragrafo 1, lettera a), della direttiva 95/46/CE.
[69] Cfr. art. 23 della direttiva 95/46/CE.