Luiss
Libera Università
Internazionale
degli Studi Sociali
Guido Carli

CERADI
Centro di ricerca per il diritto d'impresa

Tutela della *privacy*: i trasferimenti transfrontalieri di dati personali

Massimiliano MASNADA

Maggio 2001

1. Quale *privacy* nella società della cd. *information tecnology*?

Lo sviluppo delle tecnologie informatiche ha prodotto un radicale mutamento della nostra società, trasformando i paradigmi classici dell'economia e dell'impresa, ed andando ad incidere profondamente sulle relazioni culturali e commerciali.

L'avvento di INTERNET ha messo in crisi la nozione stessa di "confine", creando quello che viene definito "villaggio globale", all'interno del quale gli individui entrano in contatto tra loro, in uno scambio continuo e costante di dati ed informazioni che infrange ogni barriera temporale, spaziale e culturale.

L'articolazione delle reti su base mondiale consente, con grande facilità, rapidità e con costi ridotti, la raccolta, la memorizzazione, l'elaborazione e lo scambio di enormi quantità di dati ed informazioni dei singoli utenti.

Ogni giorno si assiste al trattamento, da parte di privati, imprese, apparati ed enti pubblici, di una quantità infinita di dati personali, che si muovono sulle autostrade telematiche, al di là dei confini fisici degli Stati nazionali, spesso senza alcuna garanzia di riservatezza e di utilizzo lecito delle stesse.

Le tecniche di raccolta di tali informazioni, ad opera dei soggetti più vari, sono sempre più pervasive, capillari ed, in molti casi, invisibili (si pensi ad esempio al fenomeno dei cookies).

Nell'ambito delle relazioni commerciali, in particolare, le informazioni personali relative ai consumatori, reali o potenziali, sono considerate il vero "valore aggiunto", "l'alimento indispensabile" della società dell'information tecnology. Esse sono identificate, sempre più, come un "bene di consumo", oggetto di scambi e transazioni commerciali.

L'effetto di quanto descritto è una inevitabile erosione del potere dell'individuo sulle informazioni personali che lo riguardano, con evidenti ripercussioni sul diritto alla riservatezza ad esso riconosciuto.

Ne deriva, pertanto, la necessità di una riflessione sul valore attuale del diritto alla privacy e sugli strumenti idonei a tutelarlo.

Tale diritto, teorizzato alla fine del XIX secolo nei Paesi del Common Law come "right to be alone", ossia diritto ad essere lasciato solo, sembra aver progressivamente perso le caratteristiche di strumento di isolamento dagli altri, per assumere la dimensione di "spazio di libertà individuale", di diritto fondamentale che consente ai singoli individui, attraverso il controllo dei flussi delle informazioni personali che li riguardano, di partecipare, senza rischi di oggettivizzazioni e discriminazioni sociali, alla società dell'information tecnology (cfr. S. RODOTA', Relazione introduttiva alla 22^ Conferenza Internazionale sulla Privacy e Tutela dei dati personali, Venezia, 28-29-30 settembre 2000).

Nell'era telematica, infatti, la privacy appare configurarsi come uno strumento di comunicazione, ossia il mezzo attraverso il quale l'individuo può accedere ai beni e servizi offerti dal mercato globale, avendo la sicurezza che le sue informazioni personali non verranno utilizzate per fini diversi da quelli per le quali sono state fornite.

L'assetto globale dei rapporti economici e commerciali e la estrema velocità con cui le informazioni circolano liberamente (soprattutto tramite INTERNET, ma, anche mediante più tradizionali mezzi di comunicazione transnazionale), attraversando (rectius: rompendo) i confini fisici degli Stati, attribuiscono alla questione della tutela della privacy una portata mondiale.

Problema fondamentale è colmare il divario tra i livelli di protezione dei dati personali, garantiti dagli ordinamenti degli Stati, all'interno dei quali tali dati circolano.

Occorre, cioè, tutelare la riservatezza delle informazioni personali, laddove queste siano trasferite da uno Stato, il cui ordinamento garantisce un livello di protezione adeguato, ad un altro, in cui non siano in vigore norme (legislative o di autodisciplina) che tutelino sufficientemente la privacy individuale.

In tale contesto, la difesa del diritto alla privacy necessita, da un lato, dell'apporto di tecnologie "pulite", che tutelino ab origine la riservatezza delle informazioni personali, dall'altro, di accordi internazionali che fissino il quadro dei principi da rispettare.

Tali principi dovranno essere, poi, recepiti da legislazioni nazionali di ultima generazione, ovvero, laddove simili legislazioni non esistano, da codici di autoregolamentazione adottati dai titolari dei trattamenti di dati personali, nonché, nell'ipotesi di trasferimento transfrontaliero degli stessi, da modelli contrattuali standard che consentano ai singoli individui di agire direttamente contro le violazioni del proprio diritto alla privacy.

2. Il trasferimento transfrontaliero di dati personali nella disciplina comunitaria

La materia del trasferimento verso un Paese terzo di dati personali, oggetto di trattamento in uno Stato membro dell'UE ovvero destinati ad essere oggetto di trattamento dopo il trasferimento, è stata oggetto di specifica disciplina da parte della Direttiva Europea 95/46/CE, che ha provveduto ad armonizzare le legislazioni degli Stati membri in materia di privacy.

La disciplina comunitaria prende in esame tutti i tipi di trasferimento, indipendentemente dal fatto che tali flussi di dati avvengano per via informatica o telematica, nell'ambito di una rete INTRANET, tramite telex, telefax, trasmissioni satellitari o via cavo.

In base all'art. 25 della citata Direttiva, gli Stati membri devono impedire il trasferimento dei dati personali verso un Paese terzo, laddove quest'ultimo non presenti un "livello di protezione adeguata".

La valutazione di adeguatezza del livello di protezione garantito dal Paese terzo va fatta con riguardo a tutte le circostanze relative al trasferimento e, segnatamente: alla natura dei dati, alle finalità del o dei trattamenti previsti, al Paese di origine ed a quello di destinazione finale, alle

norme di diritto, generali o settoriali, vigenti nel Paese terzo, alle regole professionali ed alle misure di sicurezza adottate.

L'art. 26 della stessa Dir. 95/46/CE, tuttavia, prevede una serie di deroghe alla suesposta disciplina (cfr. art. 26, comma 1 Dir. 95/46/CE), stabilendo, inoltre, che il trasferimento transfrontaliero dei dati personali, anche verso Paesi che non garantiscono un livello di tutela adeguato, possa avvenire in presenza di determinate circostanze, come, ad esempio, quando il trasferimento medesimo sia accompagnato da clausole contrattuali appropriate, con le quali il responsabile del trattamento garantisca "la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone e l'esercizio dei diritti connessi" (cfr. art. 26, comma 2, Dir. 95/46/CE).

3. La disciplina italiana: art. 28 L. n. 675/96

Nell'ordinamento italiano, la Dir. 95/46/CE è stata recepita dalla L. 31 dicembre 1996 n. 675, la quale, all'art. 28 prende in esame sia le ipotesi di flussi di dati personali, oggetto di trattamento nel territorio nazionale, verso un Paese non appartenente alla Unione Europea, sia quelle di trasferimenti di dati sensibili verso un Paese terzo o verso uno Stato comunitario (per "dati sensibili", ai sensi degli artt. 22 e 24 della L. n. 675/96, si intendono tutti quei dati che sono idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, i dati personali idonei a rivelare lo stato di salute e la vita sessuale, nonché i dati personali contenuti nei casellari giudiziari o nei registri dei carichi pendenti. Ad essi viene accordato un livello di tutela particolarmente elevato, sia per quanto riguarda il trattamento vero e proprio, sia con riferimento alla comunicazione, diffusione e trasferimento degli stessi).

In conformità alle indicazioni contenute nella direttiva 95/46/CE, la norma in questione, nelle ipotesi esposte, vieta il trasferimento qualora l'ordinamento dello Stato di destinazione o di transito dei dati non assicuri un livello adeguato di tutela delle persone ovvero, se si tratta di dati sensibili, di grado pari a quello assicurato dall'ordinamento italiano.

La valutazione circa l'adeguatezza della protezione offerta dal Paese terzo è effettuata dall'Ufficio del Garante per la protezione dei dati personali,

sulla base delle modalità del trasferimento, delle relative finalità, della natura dei dati, e delle misure di sicurezza adottate dall'importatore.

Al fine di consentire tale valutazione di adeguatezza, è stato previsto, a carico del titolare del trattamento, l'obbligo di notificare previamente al Garante, il trasferimento medesimo, che potrà avvenire soltanto trascorsi quindici giorni dalla data della notificazione (venti giorni nell'ipotesi di dati sensibili).

Durante il termine indicato, l'Autorità garante, se ritiene che il Paese destinatario dei dati o quello di transito degli stessi non assicuri il livello di protezione richiesto dalla legge, può bloccare il trasferimento.

Infine, l'art. 28 L. n. 675/96, facendo proprie le deroghe contenute nell'art. 26 della Dir. 95/46/CE, indica una serie di ipotesi in cui il trasferimento transfrontaliero di dati personali è comunque consentito, tra le quali si prevede espressamente la possibilità del Garante di autorizzare il trasferimento "sulla base di adeguate garanzie per i diritti dell'interessato, prestate anche con un contratto".

4. Valutazione d'impatto della disciplina comunitaria sulle relazioni commerciali internazionali. Le principali attività poste in essere dalla Commissione europea

La disciplina comunitaria dei flussi transfrontalieri di dati personali ed il suo impatto sui rapporti commerciali delle imprese europee con quelle dei Paesi terzi (es. USA, Giappone, Paesi dell'Est Europeo, ecc…) sono oggetto di vivaci discussioni e di confronto, sia a livello istituzionale, sia tra gli studiosi della materia.

Le principali critiche muovono dal presupposto che, come accennato in premessa, la regolamentazione dei flussi di informazione attraverso i confini nazionali, indispensabili per lo sviluppo del commercio su scala mondiale, finisce per legarsi strettamente ed influenzare la libera circolazione di beni, servizi e capitali.

Da più parti, infatti, si è sostenuto che il potere di intervento e di blocco dei trasferimenti riservato alle Autorità Garanti dei singoli Stati membri potrebbe avere effetti disastrosi nel settore del commercio internazionale.

Il rischio che si corre non è soltanto un impoverimento delle relazioni commerciali con gli Stati Uniti, il Giappone o altri Paesi terzi, quanto, piuttosto, una emarginazione dell'economia europea rispetto all'espansione commerciale delle imprese USA e di altre realtà asiatiche.

Si pensi, ad esempio, alla ipotesi in cui una società multinazionale si veda vietare il trasferimento di dati personali, oggetto di trattamento nelle sedi europee, verso altre sedi negli Stati Uniti ovvero in altri Paesi terzi; trasferimento necessario ai fini dell'elaborazione contabile per il pagamento dei dipendenti, ovvero, con riferimento ai dati di consumatori ed utenti della società, per le analisi commerciali finalizzate ad offrire un servizio migliore o ad elaborare le strategie di marketing.

La disciplina comunitaria, inoltre, potrebbe avere effetti negativi anche nel settore delle banche di investimento, rendendo più difficile, o addirittura impossibile, l'analisi di imprese europee da parte di società non appartenenti all'UE e la preparazione di revisioni contabili su base unificata per conto di società di consulenza internazionali.

Al fine di evitare che la rigida applicazione della Dir. 95/46/CE produca gli effetti negativi suesposti, la Commissione UE, in virtù della competenza ad essa riservata dall'art. 25, comma 5 della direttiva, avvalendosi della collaborazione del "Gruppo di lavoro" istituito dall'art. 29 della Direttiva medesima, si è impegnata in una serie di negoziati con le Autorità competenti di alcuni dei principali Paesi terzi, volti, da un lato, a valutare il livello di protezione della privacy assicurato in tali Stati, dall'altro, a stipulare con essi, nel caso in cui le garanzie non siano ritenute sufficienti, accordi internazionali per la protezione dei dati personali dei cittadini europei, ivi trasferiti da istituzioni, imprese pubbliche e/o private, titolari dei trattamenti nel territorio della UE.

A ciò si aggiunga che la Commissione europea, in virtù della specifica competenza ad essa attribuita dall'art. 26, comma 4 della Dir. 95/46/CE, sta lavorando alla predisposizione di modelli contrattuali tipo, da adottare nell'ambito dei trasferimenti oltre frontiera di dati personali, per garantire una tutela adeguata della privacy dei titolari dei dati stessi.

5. Safe Harbor Privacy Principles e Frequently Asked Questions (FAQ)

La problematica relativa al trasferimento dei dati oltre frontiera ha assunto particolare rilievo con riferimento alle relazioni commerciali intrattenute da aziende pubbliche e/o private europee con le organizzazioni statunitensi, a causa dell'elevato flusso di dati personali che necessariamente si accompagnano ad esse.

Negli USA, infatti, non esiste una disciplina generale in materia di protezione della privacy come invece accade nell'UE, essendo tale protezione affidata ad un intreccio di disposizioni federali e statali, spesso di portata settoriale e, soprattutto, alla autoregolamentazione dei soggetti utilizzatori di dati personali (cfr. A. ETZIONI, The Limits of Privacy, Basic Books, N.Y., 1999).

Al fine di evitare un impatto traumatico della Dir. 95/46/CE sul flusso di dati tra Europa e Stati Uniti, la Commissione UE ha avviato un negoziato con il Governo USA, volto alla elaborazione di una serie di principi cui dovrebbero attenersi le organizzazioni statunitensi che trattano dati personali trasferiti dalla UE, e che garantirebbero, ove applicati, la protezione della privacy dei titolari dei dati medesimi.

Dopo circa due anni di negoziato, il 21 luglio 2000, il Dipartimento del Commercio USA ha provveduto alla pubblicazione del "Safe Harbor Privacy Principles", nonché delle "Frequently Asked Questions"(FAQ), che costituiscono la guida alla attuazione di detti principi, articolata in una serie di risposte alle "domande più frequenti" che vengono poste in materia di privacy.

Con decisione del 26 luglio 2000, adottata ai sensi dell'art. 25, comma 2 della Dir. 95/46/CE, la Commissione UE ha ritenuto che i principi del Safe Harbor in materia di riservatezza, applicati in conformità con le FAQ, "garantiscono un livello adeguato di protezione dei dati personali trasferiti dalla Comunità a organizzazioni aventi sede negli Stati Uniti (…)" (cfr. Decisione Comm. 2000/520/CE, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative "Domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti, in G.U. delle Comunità europee L. 215 del 25 agosto 2000).

L'accordo del "approdo sicuro", che combina elementi dell'approccio di self-regulation americano con la preferenza europea per la regolamentazione legislativa della materia, prevede l'adesione volontaria e non obbligatoria delle

imprese americane ad un sistema basato sul nucleo di principi alla base della Dir. 95/46/CE, recentemente riaffermati in ambito internazionale dalle Linee Guida dell'OCSE in materia di tutela dei dati personali e protezione della vita privata (cfr. OECD Guidelines on Protection of Privacy and Transborder Data Flow of Personal Data del settembre 1980, così come integrate a seguito della Conferenza ministeriale di Ottawa dell'ottobre 1998).

Le imprese americane che decideranno di qualificarsi per il Safe Harbor dovranno effettuare una "autocertificazione" mediante notifica al Dipartimento del commercio degli Stati Uniti, specificando, altresì, l'Ente Governativo USA all'autorità del quale esse sono sottoposte.

In particolare, secondo quanto indicato nei protocolli dell'accordo Safe Harbor, le autorità governative USA competenti a far rispettare gli impegni assunti dalle imprese statunitensi sono la Federal Trade Commission e, per le compagnie di trasporto, il Dipartimento dei trasporti USA. Tali enti, infatti, nell'ambito della competenza loro riconosciuta in materia di prevenzione e repressione di "attività e pratiche di concorrenza sleale o ingannevole", hanno la facoltà di comminare sanzioni, civili e penali, nei confronti delle imprese che, dopo aver autocertificato l'impegno a rispettare i principi dell'"approdo sicuro", abbiano violato gli obblighi assunti con tale pubblica certificazione.

A tal riguardo, appare opportuno tracciare le linee guida dell'accordo, al fine di fornire al lettore un quadro di riferimento adeguato. (l'analisi delle principali problematiche sottese all'applicazione del Safe Harbor e delle FAQ forma oggetto di una approfondita ricerca presso il Centro ricerche Ceradi dell'università degli studi sociali L.U.I.S.S. di Roma).

I principi del Safe Harbor possono essere sintetizzati come segue: informativa agli interessati, contenente, in particolare, l'indicazione della natura dei dati personali trasferiti, delle finalità per cui vengono trattati e degli utilizzi che ne seguiranno; scelta (opt-out choice) per i dati non sensibili, ossia la facoltà per gli interessati di opporsi a che tali dati siano rivelati a terzi ovvero siano utilizzati per scopi diversi da quelli per i quali sono stati originariamente forniti; consenso (opt-in choice) per i dati sensibili, ossia la richiesta di consenso esplicito agli interessati per la comunicazione dei dati a terzi ovvero per un diverso utilizzo degli stessi; diritto di accesso ai trattamenti di dati che li riguardano riconosciuto agli interessati e possibilità per quest'ultimi di chiederne ed ottenerne la rettifica, la correzione o la cancellazione; sicurezza dei dati, ossia l'obbligo per le organizzazioni statunitensi di adottare tutte le

misure di sicurezza idonee a garantire la riservatezza dei dati trattati; pertinenza dei dati agli scopi per i quali sono stati raccolti.

Componente di rilievo dell'accordo Safe Harbor è rappresentata dall'utilizzo di controlli, da parte del settore privato, per verificare e garantire la conformità ai principi delle imprese qualificate. Secondo quanto stabilito, tali controlli possono essere demandati ad organizzazioni separate che procederebbero, così, ad un monitoraggio di regolarità. (tra le organizzazioni facenti parte il primo blocco di organi di controllo sono incluse BBB on line e TRUSTe, la cui rete di compagnie partecipanti è costituita da AOL, Ernst & Young, Microsoft e Novell).

Al fine di garantire l'effettivo rispetto del Safe Harbor e di assicurare agli interessati uno strumento diretto di tutela della riservatezza dei propri dati personali, è stata prevista la possibilità, per quest'ultimi, di rivolgersi ad organismi privati per la risoluzione delle controversie nascenti dal mancato rispetto, da parte delle imprese americane, degli obblighi assunti con "l'approdo sicuro".

Ai citati organismi internazionali, pertanto, verrebbe attribuito, convenzionalmente, il potere di ricevere ricorsi, di istruire cause mediante ispezioni ed accertamenti, nonchè di chiedere la riparazione delle violazioni commesse.

Tale forma di tutela va ad aggiungersi a quella, in ogni caso, garantita, in tema di privacy, dalla autorità della Federal Trade Commission e del Dipartimento dei Trasporti USA, a cui potrebbero rivolgersi, sia direttamente le Autorità Garanti europee, sia gli organismi privati di risoluzione delle controversie, nell'ipotesi in cui le proprie decisioni non fossero rispettate.

Va, tuttavia, sottolineato che rimangono esclusi dal campo di applicazione dell'accordo Safe Harbor una vasta gamma di trasferimenti, in particolare nel settore delle telecomunicazioni, dei servizi finanziari e nel settore no profit; aree del commercio sottratte alla autorità governativa della Federal Trade Commission e del Dipartimento dei Trasporti USA.

6. Modelli contrattuali in materia di protezione dei dati personali

Come accennato in precedenza, il Safe Harbor è destinato a coprire solo una parte dei flussi di dati personali verso gli USA mentre non si applica

ad un'alta percentuale di trasferimenti in settori, peraltro, nevralgici dell'economia mondiale, quali quello finanziario e delle telecomunicazioni.

A ciò si aggiunga che esso, pur costituendo un modello di accordo internazionale estendibile anche ad altri Paesi terzi, riguarda esclusivamente i trasferimenti di dati personali che avvengono tra la Comunità europea e le organizzazioni USA, lasciando impregiudicato il problema relativo al flusso di dati verso altri Stati, soprattutto dell'Est europeo ed asiatici, che non garantiscono un livello adeguato di tutela della privacy.

A livello internazionale, si è sviluppata l'idea di ricorrere a "clausole contrattuali tipo" per vincolare, sia l'organizzazione che esporta i dati, sia quella che li utilizza nel Paese terzo privo di una legislazione adeguata, a condotte regolate più specificatamente, anche sotto il profilo della giurisdizione e della legge applicabile, sulla falsariga degli standards qualitativi europei e dell'esperienza maturata dagli Stati membri (es. schemi di clausole tipo elaborate dall'International Chamber of Commerce, dall'OCSE e dal Consiglio d'Europa).

In ambito comunitario, la Commissione UE, in ragione della specifica competenza, ad essa attribuita dall'art. 26, comma 4 della Dir. 95/46/CE, ha recentemente elaborato una bozza preliminare di contratto standard (di seguito, EU-draft model), che potrebbe diventare il principale strumento, utilizzato dalle imprese europee, per garantire la tutela della riservatezza dei dati personali trattati e trasferiti verso organizzazioni di Paesi terzi, nell'ambito delle loro relazioni commerciali a livello internazionale [cfr. "Preliminary Draft of a Commission decision under Art. 26 Dir. 95/46/CE on standard clauses for the trasfer of personal data to third contries tht do not provide an adeguate level of protection for the processing of personal data" (EU-draft model), consultabile sul sito www.europa.en.int/comm/internal_market.].

Attraverso il modello contrattuale elaborato dalla Commissione UE si vuole estendere al Paese importatore il livello di protezione garantito nel Paese esportatore, stabilendo, da un lato, a carico dell'organizzazione che importa i dati personali (cd."data importer"), regole certe in materia di protezione degli stessi, dall'altro, consentendo al titolare dei dati trasferiti (cd. "data subject") di imporre all'importatore il rispetto di tali regole, malgrado esse non abbiano il valore di norme di legge nel Paese terzo.

A tal fine, è stata inserita nel contratto una apposita clausola di terzo beneficiario, cd. “third-party beneficiary clause”, a favore dello stesso titolare dei dati personali oggetto del trasferimento.

Ciò consentirebbe, infatti, al data subject di esercitare i diritti ad esso riconosciuti in materia di privacy, agendo direttamente nei confronti, sia del data exporter, che del data importer, per il risarcimento dei danni derivanti dai loro inadempimenti contrattuali.

I problemi maggiori che tale soluzione contrattuale nasconde sono legati, più che altro, alla garanzia di effettività del contratto stesso ed alla facoltà per il terzo beneficiario di pretenderne, anche coattivamente, l’esecuzione.

La mera enunciazione dei diritti riconosciuti al titolare dei dati, infatti, non è, di per se, sufficiente a garantire la tutela della riservatezza delle informazioni personali trattate dall’importatore.

Affinchè la tutela sia effettiva, il contratto deve indicare con precisione, da un lato, le responsabilità, rispettivamente dell’esportatore e dell’importatore, nei confronti del data subject, per le violazioni degli obblighi contrattuali, ovvero se vi siano delle responsabilità comuni ad entrambi; dall’altro, gli organi giurisdizionali competenti a risolvere le controversie nascenti dal contratto, nonché la legge applicabile per integrare le regole contrattuali (es. validità del contratto, regole di interpretazione del contratto, ecc…).

Con riferimento alla prima questione, l’art. 7 del EU-draft model prevede, accanto alla separata responsabilità contrattuale delle parti per le obbligazioni reciprocamente assunte, una forma di responsabilità comune (“joint liable”) del data exporter e del data importer nei confronti del data subject, per i danni derivanti dal trattamento illecito dei dati, o da qualunque atto incompatibile con le previsioni di legge, adottate dallo Stato membro in esecuzione della Direttiva. La responsabilità comune è, inoltre, prevista per le violazioni degli obblighi contrattuali assunti dalle parti vis-à-vis con il soggetto titolare dei dati, se il contratto si riferisca ad alcune ipotesi di trasferimento (es. trasferimenti nell’ambito delle società multinazionali, o dei consorzi internazionali di imprese; ipotesi di licenza d’uso, affitto o vendita di dati personali) oppure riguardi il trasferimento di dati sensibili.

Con riferimento alla seconda questione, l’art. 8 del EU-draft model prevede che la scelta della giurisdizione competente a conoscere le eventuali controversie nascenti dall’esecuzione del contratto sia fatta dalle parti stesse (data exporter e data importer) al momento della stipulazione del contratto.

Esse dovranno dichiarare di accettare o la giurisdizione delle corti dello Stato membro in cui ha sede il data exporter, o quella di un corpo arbitrale situato nello Stato di appartenenza dell'esportatore, che sia autorizzato a riconoscere ed applicare la "third party beneficiary clause".

La questione relativa alla giurisdizione richiama il problema di come dare esecuzione, nel Paese terzo in cui ha sede il data importer, alle decisione adottate dalle corti europee o dal corpo arbitrale istituito per risolvere le controversie nascenti dal contratto.

Non sembra, infatti, essere sufficiente la soluzione adottata dalla Commissione europea di un preciso ed espresso impegno contrattuale, in tal senso, da parte del data importer, dal momento che tale volontaria sottomissione alla giurisdizione dello Stato membro cui appartiene l'esportatore (ovvero le pronunce del corpo arbitrale), non produce, di per se, l'effetto di rendere esecutive le decisione adottate da tali organi giurisdizionali nel Paese terzo in cui ha sede il data importer.

Affinchè ciò avvenga, infatti, è necessario uno specifico accordo bilaterale tra lo Stato del data exporter e quello dell'importatore, ovvero la ratifica, da parte degli Stati stessi, di convenzioni internazionali, ove si riconosca l'autorità giurisdizionale del corpo arbitrale adito.

L'analisi del contenuto delle clausole contrattuali tipo in materia di *privacy* elaborate dalla Commissione UE e delle principali problematiche relative all'*enforcement* dei diritti contrattualmente riconosciuti al titolare dei dati personali forma oggetto di una approfondita ricerca presso il Centro Studi Ceradi dell'università degli studi sociali L.U.I.S.S. di Roma.