Esiste inoltre una giurisprudenza che sviluppa le stesse argomentazioni con riguardo alla direttiva concernente gli agenti commerciali [12]. La Corte di giustizia europea ha stabilito [13] che allorché un agente commerciale che esercita la propria attività nella Comunità dipende da un mandante stabilito in un paese extracomunitario, quest'ultimo non può eludere le disposizioni della direttiva con l'espediente di una clausola contrattuale che afferma che alla relazione si applica il diritto di un paese terzo. La Corte ha stabilito che il diritto comunitario deve trovare applicazione "allorquando il fatto presenti un legame stretto con la Comunità".

Un ulteriore esempio pratico può essere citato con riguardo all'industria aeronautica. Il Consiglio ha approvato un regolamento relativo a un codice di comportamento in materia di sistemi telematici di prenotazione (CRS)[14]. Tale regolamento (che disciplina le modalità di utilizzo dei sistemi CRS) si applica "a tutti i sistemi telematici di prenotazione (...) qualora siano offerti per l'uso e/o utilizzati nel territorio della Comunità indipendentemente dallo status o dalla nazionalità del venditore del sistema (...) o dall'ubicazione della relativa unità centrale di elaborazione dati". Pertanto se a un sistema si può accedere dall'UE, anche nel caso in cui l'unità centrale del sistema non sia ubicata nell'UE (e i dati siano inseriti nel sistema attraverso terminali nell'UE o diversamente), il diritto comunitario si applica automaticamente.

Pertanto dall'esame dell'applicabilità del diritto comunitario a tali casi con una dimensione extraterritoriale si può concludere che sono generalmente applicati criteri simili. Pur essendo prescritto che la relazione abbia una "dimensione comunitaria" o un "legame stretto" con la Comunità, in talune situazioni la Corte di giustizia europea, il Parlamento europeo e il Consiglio nonché la Commissione europea ritengono opportuno imporre norme comunitarie a organismi stabiliti al di fuori dell'UE.

In altri paesi, ad esempio negli Stati Uniti d'America, la magistratura e i legislatori partono da premesse simili per assoggettare i siti Web stranieri alle norme locali. La legge statunitense sulla tutela della privacy dei bambini on-line del 1998 (Children's Online Privacy Protection Act - COPPA) si applica anche ai siti Web stranieri che raccolgono informazioni personali dai bambini sul territorio statunitense [15]. In virtù di tale legge federale, il gestore di un sito Web diretto verso bambini di meno di 13 anni (o di un sito con un pubblico più ampio, ma il cui gestore è effettivamente a conoscenza del fatto che il sito raccoglie informazioni da bambini) è obbligato a ottemperare alle disposizioni della COPPA. Tale legge stabilisce quali informazioni un gestore deve fornire nella sua privacy policy, quando e con quali modalità un gestore è obbligato a ottenere il consenso verificabile di un genitore e quali sono le responsabilità di un gestore ai fini della tutela della privacy dei bambini e della sicurezza in linea. Quel che è interessante ai fini della presente trattazione è che tale legge non si applica specificamente alle imprese statunitensi, bensì alle imprese "situate su Internet" e pertanto, in termini della sua giurisdizione, l'ubicazione fisica del sito Web non ha importanza nel caso in cui esso operi negli Stati Uniti. Se così avviene, il sito è assoggettato alla legge statunitense in materia.

Da un'indagine sul diritto internazionale emerge che gli Stati hanno la tendenza a utilizzare molteplici criteri alternativi per determinare estensivamente il campo d'applicazione del diritto nazionale al fine di coprire il maggior numero di casi possibile a beneficio della più ampia tutela dei consumatori e delle imprese nazionali. Inevitabilmente tale tendenza determina l'applicazione di molteplici diritti nazionali a una situazione che comporta un elemento di transnazionalità. Gli strumenti giuridici internazionali tentano pertanto di determinare i pertinenti criteri in modo neutro e non discriminatorio. Tuttavia il più recente tentativo di far avanzare il progetto di convenzione sul diritto applicabile ai contratti sotto gli auspici della "Conferenza dell'Aia" è fallito perché i paesi non hanno potuto accordarsi sul criterio decisivo. Questo evidenzia il nocciolo del problema in sede di discussione sul diritto applicabile: occorre trovare un giusto equilibrio tra i diversi interessi dei paesi implicati.

A questo riguardo va osservato che la direttiva comunitaria in materia di tutela dei dati contiene una disposizione esplicita riguardo al diritto applicabile che suggerisce un criterio. A prescindere che tale disposizione sia o no di facile comprensione o utilizzo, il fatto che la direttiva affronti questa questione fondamentale costituisce tuttavia un vantaggio per i privati e le imprese.

(12) Direttiva 86/653/CEE.

(13) Causa C-381/98, Ingmar GB Ltd contro Eaton Leonard Technologies Inc.

(14) Codice di comportamento in materia di sistemi telematici di prenotazione (versione combinata dei regolamenti (CEE) n. 2299/89 del Consiglio, come modificato dal regolamento (CEE) n. 3089/93 e dal regolamento (CE) n. 323/1999).

(15) 15 U.S.C., § 6502 (1)(A)(I), riferito da Joel R. Reidenberg, cfr. nota 5.

2. Articolo 4 della direttiva 95/46/CE in merito al diritto applicabile

L'articolo 4 della direttiva recita:
"Diritto nazionale applicabile

1. Ciascuno Stato membro applica le disposizioni nazionali adottate per l'attuazione della presente direttiva al trattamento di dati personali:

a)effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio dello Stato membro; qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, esso deve adottare le misure necessarie per assicurare l'osservanza, da parte di ciascuno di detti stabilimenti, degli obblighi stabiliti dal diritto nazionale applicabile;

b) il cui responsabile non è stabilito nel territorio dello Stato membro, ma in un luogo in cui si applica la sua legislazione nazionale, a norma del diritto internazionale pubblico;

c) il cui responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea.

2. Nella fattispecie di cui al paragrafo 1, lettera c), il responsabile del trattamento deve designare un rappresentante stabilito nel territorio di detto Stato membro, fatte salve le azioni che potrebbero essere promosse contro lo stesso responsabile del trattamento."

Tale articolo analizza i casi che fanno insorgere il problema del diritto applicabile alle operazioni di trattamento dei dati personali: si tratta di casi in cui almeno un aspetto del trattamento di dati personali oltrepassa le frontiere di uno Stato membro. Ad esempio, un'impresa di marketing diretto elabora mailing list di consumatori in più Stati membri e li utilizza in uno Stato membro per consentire l'invio di pubblicità a tali consumatori, oppure un sito Web statunitense inserisce un cookie sul personal computer di privati nell'UE al fine di rendere identificabile il PC al sito, in vista del collegamento di tale informazione con altre.

La direttiva distingue in termini generali tra le situazioni in cui gli elementi transnazionali sono limitati agli Stati membri dell'UE oppure a territori al di fuori delle frontiere geografiche dell'Unione europea in cui si applica tuttavia la legislazione di uno Stato membro a norma del diritto internazionale pubblico ("caso diplomatico")[16], da una parte, e le situazioni in cui il trattamento comprende elementi che travalicano le frontiere dell'Unione europea [17], dall'altra.

In merito alle situazioni all'interno della Comunità, l'obiettivo della direttiva è duplice: evitare vuoti legislativi (non applicazione di una normativa in materia di tutela dei dati) e evitare una duplice o molteplice applicazione delle normative nazionali. Poiché la direttiva affronta la questione del diritto applicabile e stabilisce un criterio ai fini della determinazione della legge idonea a fornire la soluzione al caso, la direttiva stessa assolve il compito di una cosiddetta "norma di conflitto" rendendo inutile ogni ricorso ad altri criteri esistenti di diritto internazionale privato.

Per fornire una risposta la direttiva utilizza il criterio o il "fattore di connessione" del "luogo di stabilimento del responsabile del trattamento" o, in altre parole, il principio del paese di origine usualmente applicato nel mercato interno. In concreto ciò significa quanto segue.

Allorché il trattamento è effettuato nel contesto delle attività di uno stabilimento del responsabile del trattamento nel territorio di uno Stato membro, si applica al trattamento la normativa in materia di protezione dei dati di tale Stato membro.

Qualora uno stesso responsabile del trattamento sia stabilito nel territorio di più Stati membri, ciascuno degli stabilimenti deve ottemperare agli obblighi fissati dalle rispettive normative di ciascuno degli Stati membri per il trattamento da essi effettuato nel corso delle proprie attività. Ciò non rappresenta un'ecce-

(16) Questo caso non viene analizzato nel presente documento. Va altresì rilevato come la direttiva e pertanto anche l'articolo 4 si applichino tanto al settore pubblico quanto al settore privato che trattano i dati personali assoggettati al diritto comunitario. Il presente documento di lavoro non tratta tuttavia dell'applicazione dell'articolo 4 ai casi del settore pubblico.

(17) Tale distinzione si applica principalmente al responsabile del trattamento. È opportuno tuttavia chiarire che l'applicabilità della direttiva non è influenzata dal fatto che per conto del responsabile del trattamento nell'UE agisca un incaricato operante al di fuori dell'UE. Anche in tale caso la direttiva si applica all'insieme delle operazioni di trattamento.

zione al principio del paese di origine, bensì rappresenta semplicemente una sua rigorosa applicazione: qualora il responsabile scelga di disporre non di un solo stabilimento bensì di molti stabilimenti non beneficia del vantaggio che l'osservanza di una normativa è sufficiente per le sue attività in tutto il mercato interno. Tale responsabile si trova a far fronte all'applicazione parallela delle pertinenti normative nazionali ai vari stabilimenti. Il gruppo potrebbe trattare tale questione in futuro.

L'applicazione del principio del paese d'origine è giustificata in un mercato interno in cui le normative nazionali in materia di tutela dei dati garantiscono una protezione equivalente in virtù dell'armonizzazione dei diritti alla tutela dei dati delle persone e degli obblighi delle imprese e degli altri responsabili del trattamento di dati personali. In tal modo il principio del paese d'origine, che rappresenta in qualche modo una restrizione del campo d'applicazione delle normative degli Stati membri in materia di tutela dei dati, non incide negativamente sui diritti e sugli interessi dei suoi residenti o delle imprese. Infatti anche se le legislazioni degli Stati membri non sono applicabili a tutti gli aspetti del trattamento concernente una persona interessata del paese o effettuato sul territorio nazionale, il fatto che sia applicabile solo la legislazione di un altro Stato membro presenta un impatto molto limitato, considerato che entrambe le normative sono armonizzate dalla direttiva e pertanto sono equivalenti. Inoltre la cooperazione tra le autorità nazionali preposte alla tutela dei dati dà fiducia e garantisce una reale esecuzione a prescindere dal diritto applicabile [18].

La situazione si presenta diversa per le operazioni di trattamento in cui interviene un responsabile di un paese terzo. Le leggi nazionali di questi paesi terzi non sono armonizzate, la direttiva non è applicabile in tali paesi e la tutela delle persone per quanto concerne il trattamento dei loro dati personali può pertanto risultare lacunosa o mancare del tutto. Il principio del paese d'origine, connesso allo stabilimento del responsabile del trattamento, non può essere più utilizzato ai fini della determinazione del diritto applicabile. È necessario scegliere un altro fattore di connessione. Il Parlamento europeo e il Consiglio hanno deciso di ritornare a uno dei fattori di connessione classici nel diritto internazionale, ossia al legame fisico tra l'azione e un sistema giuridico. Il legislatore comunitario ha scelto il paese dell'ubicazione territoriale degli strumenti utilizzati [19]. La direttiva si applica pertanto allorché il responsabile non stabilito nel territorio della Comunità decide di trattare dati personali a fini specifici e ricorre a strumenti, automatizzati o non automatizzati, situati nel territorio di uno Stato membro.

L'obiettivo di tale disposizione contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE è quello di garantire che una persona non sia priva di tutela per quanto riguarda il trattamento effettuato nel suo paese per il solo fatto che il responsabile non è stabilito sul territorio comunitario. Il motivo potrebbe essere semplicemente che il responsabile non ha, in linea di principio, nulla a che vedere con la Comunità, ma è immaginabile anche che i responsabili trasferiscano il loro stabilimento al di fuori dell'UE al fine di eludere l'applicazione della normativa comunitaria.

È opportuno notare come non sia necessario che la persona sia un cittadino comunitario o sia fisicamente presente o residente nell'UE. La direttiva non opera alcuna distinzione sulla base della nazionalità o della residenza in quanto armonizza le normative degli Stati membri in materia di diritti fondamentali riconosciuti a tutti gli esseri umani, indipendentemente dalla loro nazionalità. Pertanto nei casi che verranno discussi in appresso la persona in questione potrebbe essere un cittadino tanto statunitense quanto cinese. In termini di applicazione della normativa comunitaria in materia di tutela dei dati, tale persona è protetta allo stesso modo di qualsiasi cittadino comunitario. Ciò che conta è l'ubicazione degli strumenti del trattamento.

La decisione del legislatore comunitario di assoggettare il trattamento tramite strumenti ubicati nell'UE alla sua normativa in materia di tutela dei dati riflette pertanto una reale preoccupazione di proteggere le persone sul proprio territorio. A livello internazionale è riconosciuto che gli Stati possono fornire tale protezione. L'articolo XIV del GATS consente di stabilire eccezioni alle norme in materia di libera circolazione al fine di tutelare le persone con riguardo al loro diritto alla tutela della privacy e dei dati personali e di applicare tali normative.

Qui di seguito vengono spiegati i termini pertinenti ai fini della determinazione del diritto applicabile.

(18) Si veda l'articolo 28, paragrafo 6, primo comma, della direttiva 95/46/CE: "Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare, nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3" e l'ultimo comma dello stesso paragrafo in merito al loro obbligo di cooperazione.

(19) *Ciò non vale nel caso in cui gli strumenti siano utilizzati ai soli fini di transito nel territorio della Comunità europea.*

2.1 Stabilimento

La nozione di stabilimento è contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva nel senso che il responsabile non è stabilito nel territorio della Comunità. Il luogo in cui è stabilito il responsabile implica l'esercizio effettivo e reale dell'attività mediante un'organizzazione stabile e deve essere determinato in conformità con la giurisprudenza della Corte di giustizia delle Comunità europee. Secondo la Corte la nozione di stabilimento implica l'esercizio effettivo di un'attività economica per una durata di tempo indeterminata mediante l'insediamento in pianta stabile [20]. Tale condizione è soddisfatta anche nel caso in cui una società sia costituita a tempo determinato.

Il luogo di stabilimento, per le società che forniscono servizi tramite siti Internet, non è là dove si trova la tecnologia di supporto del sito né là dove esso è accessibile, bensì il luogo in cui tali società esercitano la loro attività [21]. Si consideri il caso di una società di marketing diretto registrata a Londra che sviluppa da lì le sue campagne a livello europeo: anche se utilizza server a Berlino e a Parigi resta sempre stabilita a Londra.

2.2. Il responsabile del trattamento

Il responsabile del trattamento è secondo la nozione generale contenuta nella direttiva la persona fisica o giuridica che, da sola o insieme ad altre, determina le finalità e gli strumenti del trattamento di dati personali (articolo 2, lettera d), della direttiva 95/46/CE). La definizione è neutra per quanto riguarda il luogo di stabilimento del responsabile. È generale perché tutto il trattamento deve essere attribuibile ad uno o più responsabili. Nel contesto dell'articolo 4, paragrafo 1, lettera c), della direttiva, ciò significa che è imprescindibile l'esistenza di un responsabile nel senso della direttiva. Sembra inoltre necessario che il trattamento sia effettuato nel corso di un'attività che rientri nell'ambito del diritto comunitario e a cui si applichi quindi la direttiva. Il trattamento da parte di una persona fisica nel corso di un'attività puramente personale o familiare non rientra nell'ambito della direttiva.

Ai fini dell'applicazione dell'articolo 4, paragrafo 1, lettera c), della direttiva, il responsabile deve far ricorso, ai fini del trattamento di dati personali (e non ai soli fini di transito) a strumenti situati nel territorio di uno Stato membro [22]. Ciò sembra suggerire che il responsabile deve essere attivo e perseguire uno scopo particolare. La sua decisione in merito alle finalità e agli strumenti di trattamento comprende pertanto tale aspetto.

2.3. Strumenti

La direttiva non contiene una definizione di tale termine. Il dizionario inglese Collins definisce il termine "equipment" come un complesso di strumenti o dispositivi riuniti per un fine specifico.

Ne sono un esempio i personal computer, i terminali e i server, che possono essere utilizzati per quasi ogni tipo di operazione di elaborazione.

La direttiva chiarisce che gli strumenti in quanto tali possono essere automatizzati o non automatizzati, purché non siano utilizzati ai soli fini di transito delle informazioni sul territorio della Comunità europea.

Un tipico esempio in cui gli strumenti in questione sono utilizzati ai soli fini di transito è costituito dalle reti di telecomunicazioni (reti dorsali, cavi, ecc.), che formano parte di Internet e attraverso le quali le comunicazioni viaggiano dal punto di spedizione al punto di destinazione.

2.4. Ricorso agli strumenti

La determinazione del momento in cui il responsabile ricorre a strumenti ai fini del trattamento di dati personali di cui all'articolo 4, paragrafo 1, lettera c), della direttiva costituisce un elemento decisivo per quanto riguarda l'applicazione della normativa in materia di tutela dei dati nell'UE.

(20) Causa C-221/89 Factortame [1991] Raccolta della giurisprudenza I-3905, paragrafo 20.

(21) Direttiva 2000/31/CE, diciannovesimo considerando.

(22) Va osservato che esiste una differenza tra il termine "equipment" utilizzato nella versione inglese dell'articolo 4, paragrafo 1, lettera c), e i termini, più vicini al vocabolo inglese "means" (strumenti), utilizzati in altre versioni dell'articolo 4, paragrafo 1, lettera c). La terminologia utilizzata in altre versioni dell'articolo 4, paragrafo 1, lettera c), è coerente con la formulazione dell'articolo 2, lettera d), per definire il responsabile del trattamento: la persona che determina le finalità e gli strumenti ("means") del trattamento di dati personali. Va tuttavia riconosciuto che il testo inglese della direttiva nelle versioni precedenti (ad esempio, nella proposta emendata del 1992) utilizzava anch'esso il termine "means", modificato successivamente nel corso dei negoziati, a uno stadio assai avanzato, nel termine "equipment" come emerge dal testo della posizione comune del marzo 1995.

Il gruppo raccomanda cautela in sede di applicazione ai casi concreti di tale norma della direttiva sulla tutela dei dati. Il suo obiettivo è quello di garantire che i privati beneficino della tutela delle normative nazionali in materia e della supervisione del trattamento dei dati da parte delle competenti autorità nazionali in quei casi in cui è necessario, è giustificato ed esiste un grado ragionevole di attuabilità tenuto conto del connesso elemento di transnazionalità.

Premesso questo, il gruppo è del parere che non tutte le interazioni tra un utente di Internet nell'UE e un sito Web stabilito al di fuori dell'UE portino necessariamente all'applicazione della normativa comunitaria in materia di tutela dei dati. Il gruppo ritiene che gli strumenti debbano essere a disposizione del responsabile per il trattamento dei dati personali.

Nel contempo non è necessario che il responsabile eserciti un pieno controllo sugli strumenti. La misura in cui essi sono a sua disposizione può variare. Il necessario grado di disposizione è raggiunto se il responsabile, determinando le modalità di funzionamento degli strumenti, prende le pertinenti decisioni in merito alla sostanza dei dati e alla procedura della loro elaborazione: in altre parole, se il responsabile determina quali dati sono rilevati, archiviati, trasferiti, modificati, ecc., con quali modalità e con quali finalità.

Il gruppo ritiene che il concetto di "ricorrere" presuppone due elementi: una qualche forma di attività esercitata dal responsabile e l'intenzione dello stesso di trattare dati personali. Ciò significa che la direttiva non si applica a qualsiasi "ricorso" a "strumenti" nell'Unione europea.

Il potere di disposizione del responsabile non va tuttavia confuso con la proprietà degli strumenti da parte del responsabile o della persona. In effetti la direttiva non attribuisce alcuna rilevanza alla proprietà di uno strumento.

L'interpretazione avanzata dal gruppo è perfettamente conforme alla motivazione della disposizione contenuta nell'articolo 4, paragrafo 1, lettera c), della direttiva fornita dal legislatore comunitario. Il ventesimo considerando spiega che *"la tutela delle persone prevista dalla presente direttiva non deve essere impedita dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; che, in tal caso, è opportuno che i trattamenti effettuati siano disciplinati dalla legge dello Stato membro nel quale sono ubicati i mezzi utilizzati per il trattamento in oggetto e che siano prese le garanzie necessarie per consentire l'effettivo rispetto dei diritti e degli obblighi previsti dalla presente direttiva"*. Si tratta del corollario necessario per conseguire l'obiettivo più ampio della direttiva, consistente nell'evitare *"che una persona venga privata della tutela cui ha diritto in forza della presente direttiva"*.

3. Esempi pratici

Il presente capitolo è inteso a tradurre in soluzioni concrete gli orientamenti contenuti nell'articolo 4. Un elemento comune ai casi esaminati qui di seguito è che l'utente di Internet non è sempre necessariamente a conoscenza del fatto se il sito Web da lui visitato o a cui fornisce dati (coscientemente o meno) sia situato nell'UE o no. La determinazione dell'ubicazione fisica per i domini privi di suffissi geografici non è possibile in mancanza di informazioni aggiuntive e persino per quelli per cui esistono elementi geografici non esiste alcuna garanzia che il sito Web sia effettivamente ospitato su un server nel paese indicato.

Caso A: cookie

Il responsabile decide di rilevare dati personali con l'ausilio di un file di testo (cookie) posto sul disco rigido del personal computer di un utente, mentre una copia può essere tenuta dal sito Web o da un terzo [23]. In caso di ulteriori comunicazioni, il sito Web accede alle informazioni memorizzate nel cookie (e pertanto nel PC dell'utente) al fine di rendere identificabile tale PC al responsabile del trattamento. Quest'ultimo è quindi in grado di collegare tutte le informazioni raccolte nel corso delle precedenti sessioni con le informazioni rilevate durante le sessioni successive. In tal modo è possibile creare profili assai dettagliati degli utenti.

I cookie rappresentano una componente standard del traffico HTTP e, in quanto tali, possono essere trasportati senza ostacoli con il traffico IP. Contengono informazioni sull'individuo che possono essere rilette dal sito Internet che li ha creati. Un cookie può contenere tutte le informazioni che il sito desidera includervi: pagine visualizzate, annunci pubblicitari selezionati, numero di identificazione dell'utente, ecc.[24].

Il SET-COOKIE si trova nell'intestazione di risposta HTTP [25], segnatamente nei collegamenti ipertestuali invisibili. Se viene stabilita una scadenza [26], il cookie verrà memorizzato sul disco rigido dell'utente e ritrasmesso al sito Web che lo ha originato (o ad altri siti Web dello stesso sottodominio) per la durata prefissata. Questa ritrasmissione assumerà la forma di un campo COOKIE, che farà parte del browser chattering descritto in precedenza e avverrà senza alcun intervento dell'utente.

Come precisato in precedenza il PC dell'utente può essere considerato uno strumento ai sensi dell'articolo 4, paragrafo 1, lettera c), della direttiva 95/46/CE. È situato sul territorio di uno Stato membro. Il responsabile del trattamento ha deciso di utilizzare tale strumento ai fini del trattamento di dati personali e, come spiegato nei precedenti paragrafi, numerose operazioni tecniche si svolgono senza il controllo della persona interessata. Il responsabile dispone dello strumento dell'utente e tale strumento non è utilizzato ai soli fini di transito nel territorio della Comunità europea.

Il gruppo è pertanto del parere che il diritto nazionale dello Stato membro in cui è ubicato il personal computer dell'utente sia applicabile con riguardo alla domanda in quali condizioni i suoi dati personali possono essere rilevati collocando cookie sul suo disco rigido.

Come indicato in una precedente raccomandazione del gruppo [27], l'utente dovrebbe essere informato quando un cookie viene ricevuto, memorizzato o spedito dal software Internet. Il messaggio fornito all'utente dovrebbe specificare, in termini chiari, quali informazioni si intendono memorizzare nel cookie e a quale fine, nonché il periodo di validità del cookie stesso. L'utente dovrebbe quindi poter scegliere se accettare o respingere la trasmissione o la memorizzazione di un cookie nel suo insieme e dovrebbe anche potere scegliere di decidere quali informazioni dovrebbero essere conservate o eliminate da un cookie, in funzione ad esempio del periodo di validità dello stesso o dei siti Web che lo spediscono e lo ricevono [28].

Caso B: JavaScript, banner e altre applicazioni simili

I JavaScripts sono applicazioni software inviate da un sito Web al computer di un utente e consentono ai server remoti di far girare applicazioni sul PC dell'utente. In funzione del contenuto del software, i JavaScripts possono essere utilizzati per visualizzare informazioni su una pagina Web, ma anche per introdurre virus nei computer (i cosiddetti Java maligni) e/o per raccogliere e trattare dati personali memorizzati nel computer. Se decide di utilizzare tali strumenti ai fini della raccolta e del trattamento dei dati personali, il responsabile ricorre a strumenti nel senso della direttiva e dovrà ottemperare alle disposizioni della normativa comunitaria.

Una società di pubblicità, in virtù di un accordo con i proprietari di siti (ad esempio, i siti di motori di ricerca) ordina al browser (più in generale al computer) della persona interessata di collegarsi non soltanto con il motore di ricerca che intende visitare, ma anche con il server della società di pubblicità. In tal modo a tale società viene consentito non soltanto di inviare banner [29] sullo schermo della persona interessata, ma anche, utilizzando il browser dell'utente, di rilevare l'indirizzo e le informazioni che la persona invia al motore di ricerca. I banner vengono inseriti nel sito Web richiesto mediante un collegamento ipertestuale invisibile con la società di pubblicità [30]. Il responsabile del trattamento controlla pertanto, dal luogo in cui

(23) I cookie sono dati creati da un server che possono essere memorizzati in file di testo sul disco rigido di un utente di Internet, mentre una copia può essere conservata dal sito Web. Costituiscono una componente standard del traffico HTTP e, in quanto tali, possono essere trasportati senza ostacoli con il traffico IP. Un cookie può contenere un numero esclusivo (GUI, Global Unique Identifier) che consente una migliore personalizzazione rispetto agli indirizzi IP dinamici. I cookie permettono al sito Web di essere al corrente dei comportamenti e delle preferenze dell'utente. I cookie contengono una serie di URL (indirizzi) per i quali sono validi. Allorché il browser incontra nuovamente tali URL, spedisce gli specifici cookie al server. I cookie possono avere natura diversa: possono essere permanenti, ma possono anche avere una durata limitata (session cookies).

(24) Cfr. HAGEL III, J. e SINGER, M., Net Worth: the emerging role of the informediary in the race for customer information, Harvard Business School Press, 1999, pag. 275.

(25) In termini tecnici è possibile anche implementare cookie in JavaScript o nei campi <META-http EQUIV> presenti nel codice HTML.

(26) I cookie privi di scadenza fissa sono denominati "session cookies" e scompaiono quando il browser viene scaricato o al termine della sessione.

(27) Raccomandazione 1/99 (WP 17) "Trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware".

(28) Per ulteriori informazioni sulla natura dei cookie e sulle migliori modalità del loro trattamento si rinvia al documento di lavoro WP 37 (doc. 5063/00) "Tutela della vita privata su Internet - Un approccio integrato dell'UE alla protezione dei dati on-line". Alla pagina 16 è fornita una descrizione generale: "i cookie sono dati che possono essere memorizzati in file di testo sul disco fisso dell'utente Internet e conservati in copia dal sito Web". Alla pagina 79 sono fornite informazioni sui "cookie killer" analizzando sia la risposta dell'industria ai problemi di tutela della privacy comportati dai cookie (il meccanismo di opposizione ai cookie) sia la risposta dei vari attivisti in materia di tutela della vita privata (programmi indipendenti, quali cookie washer, cookie cutter e cookie master).

(29) I banner sono piccole caselle grafiche che appaiono in testa alle pagine Web oppure sono integrate nel loro contenuto.

(30) Per maggiori informazioni si rinvia al capitolo 8 "Cybermarketing" del documento WP 37 "Tutela della vita privata su Internet".

si trova, il funzionamento del browser in modo da metterlo in connessione con terzi e di trasmettere a questi informazioni.

Inoltre, al fine di fornire al cliente il banner più "adeguato", i pubblicitari in rete creano profili utilizzando cookie posti attraverso collegamenti ipertestuali invisibili. In funzione della configurazione del browser, l'utente può essere a conoscenza del fatto che viene copiato un cookie e può fornire o meno il suo consenso. Il profilo del cliente è collegato al numero identificativo del cookie della società di pubblicità in modo tale che può essere arricchito ogni volta che il cliente visita un sito Web legato contrattualmente con il pubblicitario. In tal modo si verifica una rilevazione aggiuntiva di dati personali dell'utente, attraverso il suo computer e senza il suo intervento, ogni volta che egli visita il sito Web contenente il banner.

La direttiva si applicherebbe anche alle informazioni rilevate attraverso spyware, ossia software segretamente installati in un computer ad esempio in occasione del downloading di un software più vasto (come un software per ascoltare musica) al fine di inviare informazioni personali riguardo alla persona interessata (ad esempio, i titoli delle canzoni che la persona preferisce ascoltare). I programmi software di questo tipo sono comunemente conosciuti come applicazioni E.T. *"perché dopo aver alloggiato nel computer dell'utente e aver appreso quel che gli interessa sapere, fanno ciò che faceva l'extraterrestre di Steven Spielberg: chiamano casa"*[31].

Queste nuove applicazioni software di monitoraggio utilizzano spesso JavaScript e altre tecniche simili e fanno chiaramente ricorso agli strumenti della persona interessata (computer, browser, disco rigido, ecc.) per rilevare dati e inviarli ad un altro sito. Poiché sono per definizione utilizzate senza informare l'utente (il nome spyware non lascia dubbi in proposito), tali tecnologie rappresentano una forma di trattamento invisibile e illegittimo.

***

Il gruppo "articolo 29" è consapevole del fatto che, in aggiunta ai due esempi citati in precedenza, esistono altri casi pratici connessi a Internet che potrebbero sollevare difficoltà di interpretazione, in parte a causa della complessità tecnica di alcuni dei sistemi utilizzati.

Il gruppo continuerà la sua riflessione sulla materia e potrebbe prendere in considerazione altri casi pratici alla luce dell'esperienza nazionale e degli sviluppi tecnici che potrebbero assumere rilievo in futuro.

Il gruppo desidera sottolineare che anche nei casi in cui l'applicazione della direttiva non è perfettamente chiara esso è impegnato a continuare il dialogo con le imprese e le organizzazioni dei paesi terzi che raccolgono dati personali nell'Unione europea al fine di promuovere adeguati standard di tutela dei dati per le persone interessate.

4. Cosa significa questo nella pratica?

a) Applicazione dei principi disciplinanti la rilevazione di dati personali

In tutti questi casi l'applicazione della normativa comunitaria in materia di tutela dei dati significa tra l'altro quanto segue:

- al fine di rendere la rilevazione dei dati personali corretta e lecita, il responsabile del trattamento deve definire chiaramente le finalità di tale trattamento;
- il responsabile deve anche garantire che i dati sono adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali vengono rilevati;
- la rilevazione deve essere fondata su motivi legittimi (consenso inequivocabile, esecuzione di un contratto, adempimento di un obbligo legale, perseguimento di interessi legittimi del responsabile, ecc.) e all'interessato è riconosciuto il diritto di accesso, rettifica o cancellazione dei propri dati personali;
- l'interessato deve essere come minimo informato in merito all'identità del responsabile del trattamento e del suo eventuale rappresentante, alle finalità della rilevazione, ai destinatari e ai propri diritti [32];

(31) Si veda la storia di copertina della rivista Time di Adam COHEN del 31 luglio 2000: How to protect your privacy: who's watching you? They're called E.T. programs. They spy on you and report back by "phoning home". Millions of people are unwittingly downloading them.

(32) L'articolo 10 della direttiva stabilisce che vengano fornite informazioni aggiuntive qualora necessario per garantire un trattamento leale nei confronti della persona interessata. Nel caso dei cookie, alla persona deve essere offerta la possibilità di accettare o rifiutare il cookie e inoltre di determinare quali dati desidera siano trattati dal cookie e quali no.

- un altro importante aspetto è costituito dalla sicurezza del trattamento dei dati che può richiedere al responsabile, fin dalla rilevazione, di adottare specifiche misure tecniche ed organizzative al fine di garantire la protezione dei dati personali dalla distruzione accidentale o illecita, dalla perdita accidentale o dall'alterazione, dalla diffusione o dall'accesso non autorizzati, segnatamente quando il trattamento comporta trasmissioni di dati all'interno di una rete; tali misure devono garantire un livello di sicurezza appropriato rispetto ai possibili rischi e alla natura dei dati da proteggere;
- per quanto concerne i dati sensibili, la loro rilevazione è disciplinata da disposizioni specifiche riguardanti in particolare i requisiti di sicurezza [33].

Maggiori informazioni circa il modo in cui le direttive in materia di tutela dei dati si applicano al trattamento dei dati da parte dei siti Web sono fornite nella raccomandazione 2/2001 del gruppo relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea [34].

b) Aspetti procedurali

Ai sensi dell'articolo 4, paragrafo 2, della direttiva 95/46/CE, il responsabile del trattamento deve designare un rappresentante stabilito nel territorio dello Stato membro in cui sono situati gli strumenti utilizzati.

Le informazioni in merito all'identità del responsabile del trattamento e all'identità del suo rappresentante potrebbe essere facilmente incluse nella privacy policy del sito Web o nelle informazioni generali che permettono l'identificazione del responsabile del sito in modo che il responsabile per il trattamento responsabile anche per il sito Web possa essere facilmente individuato e contattato.

Si potrebbe raccomandare di fare ampiamente ricorso alla possibilità che un solo rappresentante agisca per conto di numerosi responsabili del trattamento o di cercare altre soluzioni pragmatiche.

Per quanto riguarda la notificazione della prevista operazione di trattamento (segnatamente la raccolta) alle autorità nazionali di tutela dei dati, la direttiva prevede alcune scelte. L'articolo 18, paragrafo 1, primo comma, contempla a carico del responsabile del trattamento o del suo rappresentante un obbligo di notificazione presso l'autorità di controllo prima di procedere alla realizzazione di un trattamento o di un insieme di trattamenti. L'articolo 19, paragrafo 1, lettera a), stabilisce che la notificazione deve includere tra gli altri elementi il nome e l'indirizzo del responsabile del trattamento e del suo rappresentante.

Conformemente all'articolo 18, paragrafo 2, secondo trattino, gli Stati membri possono prevedere una semplificazione o l'esonero dall'obbligo di notificazione in due casi: qualora si tratti di categorie di trattamento che non siano tali da recare pregiudizio ai diritti e alle libertà della persona interessata o qualora il responsabile del trattamento designi un incaricato della protezione dei dati a cui è demandato di assicurare in maniera indipendente l'applicazione interna della legislazione in materia di tutela dei dati [35].

Il gruppo è consapevole del fatto che l'applicazione di tali disposizioni può sollevare problemi pratici e potrebbe approfondire ulteriormente tali temi in futuro.

c) Applicazione

È evidente che l'applicazione di norme in un contesto internazionale non è altrettanto semplice della loro esecuzione in un solo paese. Il cittadino deve essere (reso) consapevole di questo. Esistono tuttavia diverse possibilità che possono essere sviluppate nell'intento di ottenere un ragionevole grado di applicazione.

Un buon livello di ottemperanza richiede in primo luogo una sensibilizzazione delle organizzazioni sia

(33) Alcuni Stati membri richiedono un controllo preventivo prima che possa essere avviato il trattamento di dati sensibili.
(34) Si veda il documento WP 43 "Raccomandazione 2/2001 relativa ai requisiti minimi per la raccolta di dati on-line nell'Unione europea". Resta da verificare se tutti gli elementi citati in tale documento si applichino anche alla raccolta di dati on-line nell'UE da parte di responsabili non stabiliti nell'UE.
(35) Per le specifiche misure nazionali di esecuzione di tale articolo della direttiva si veda il sito: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm.

europee sia internazionali circa le prescrizioni della direttiva per quanto riguarda la raccolta di dati nell'Unione europea. La più ampia diffusione di tale raccomandazione può rappresentare soltanto il primo passo: sarebbero necessarie anche soluzioni tecnologiche che forniscano una struttura prestabilita per la raccolta di dati personali, incorporante negli strumenti di software utilizzati per tale raccolta le prescrizioni descritte. Il gruppo ha già fatto riferimento alla possibilità di concepire procedure di autorizzazione di prodotti implicanti un controllo del rispetto delle prescrizioni giuridiche per la tutela dei dati personali. Un sistema europeo di etichette/marchi Web aperto anche a siti Web extracomunitari, potrebbe rappresentare la base di tale azione.

Inoltre, nella pratica, un cittadino dell'Unione europea che abbia problemi con un sito Web non comunitario può segnalare il suo caso alla competente autorità nazionale di controllo in materia di tutela dei dati. Tale autorità determina se è applicabile la direttiva, oppure la normativa nazionale in materia di tutela dei dati. In caso affermativo, l'autorità potrebbe contattare il sito Web straniero al fine di risolvere il problema. Nel caso in cui sia adita l'autorità giudiziaria nello Stato membro in cui l'interessato è residente, questa decide se sia competente in materia (ciò che è possibile in conformità al diritto di procedura internazionale in quanto la parte più interessata è la persona che vive nello stesso territorio su cui ha la giurisdizione l'autorità giudiziaria). Una volta verificata tale competenza, l'autorità giudiziaria applica l'articolo 4 della direttiva 95/46/CE o la pertinente normativa nazionale di attuazione e può constatare che il sito Web straniero tratta in maniera illecita e non corretta i dati personali dell'interessato. Molti paesi terzi già prevedono il riconoscimento e l'attuazione della sentenza, ma anche in caso contrario esistono esempi che lasciano intendere che il sito Web straniero si adeguerà comunque alla sentenza e apporterà modifiche al proprio trattamento dei dati al fine di sviluppare buone prassi commerciali e di salvaguardare una buona immagine commerciale.

Nei paesi terzi in cui sono previste autorità e norme in materia di tutela dei dati l'applicazione è ovviamente meno problematica.

5. Conclusioni

• Il gruppo per la tutela dei dati personali ("articolo 29") è del parere che un'interpretazione delle leggi nazionali, così come indicato nel presente documento di lavoro, sarebbe di grande beneficio in vista del conseguimento della certezza del diritto per i siti Web stabiliti al di fuori dell'Unione europea. Il gruppo è convinto che un elevato livello di protezione delle persone può essere assicurato soltanto se i siti Web non stabiliti nell'Unione europea che utilizzano strumenti nell'UE come spiegato nel presente documento di lavoro rispettano le garanzie in merito al trattamento dei dati personali, segnatamente la raccolta, e i diritti delle persone riconosciuti a livello europeo e applicabili comunque a tutti i siti Web stabiliti nell'Unione europea.

• Il gruppo per la tutela dei dati personali ("articolo 29") ritiene che lo sviluppo di un programma per la promozione in modo pragmatico di norme europee in materia di tutela dei dati contribuirebbe a permettere ai responsabili del trattamento in paesi terzi di essere maggiormente sensibilizzati, nonché di rispettare e dimostrare attenzione per la privacy. Un sistema europeo di etichette/marchi Web, aperto anche a siti extracomunitari, potrebbe costituire la base di una siffatta azione.

• Il gruppo per la tutela dei dati personali ("articolo 29") invita la Commissione a tener conto del presente documento di lavoro nell'adozione di future iniziative.

Fatto a Bruxelles, il 30 maggio 2002

Per il gruppo
Il presidente
Stefano RODOTÀ

118 Parere 1/2002 riguardo alla relazione CEN/ISSS sulla standardizzazione delle modalità di tutela della vita privata in Europa (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

10761/02/IT/def.
WP 57

Parere 1/2002 riguardo alla relazione CEN/ISSS sulla standardizzazione delle modalità di tutela della vita privata in Europa

Adottato il 30 maggio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp57_it.pdf

119 Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6 (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

10750/02/IT/def.
WP 58

Parere 2/2002 sull'uso di identificativi esclusivi negli apparecchi terminali di telecomunicazione: l'esempio dell'IPv6.

Adottato il 30 maggio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp58_it.pdf

120 Parere 3/2002 sulle prescrizioni in merito alla tutela dei dati contenute nella proposta della Commissione di una direttiva relativa all'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di credito al consumo (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

11190/02/IT/def.
WP 61

Parere 3/2002 sulle prescrizioni in merito alla tutela dei dati contenute nella proposta della Commissione di una direttiva relativa all'armonizzazione delle disposizioni legislative, regolamentari e amministrative degli Stati membri in materia di credito al consumo.

Adottato il 2 luglio 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp61_it.pdf

121 Documento di lavoro sul funzionamento dell'Accordo di approdo sicuro (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

11194/02/IT
WP 62

IL GRUPPO DI LAVORO SULLA TUTELA DELLE PERSONE FISICHE PER QUANTO RIGUARDA IL TRATTAMENTO DEI DATI PERSONALI

costituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [1],
considerando gli articoli 29 e 30, paragrafi 1, lettera (a) e 3 di tale direttiva,
considerando le sue norme procedurali ed in particolare gli articoli 12 e 14,
ha approvato il presente documento di lavoro:

Data la prossima conclusione del primo periodo d'attuazione della decisione della Commissione del 26 luglio 2000 riguardante l'accordo d'Approdo sicuro, il gruppo di lavoro ha ritenuto necessario iniziare a considerare lo stato di attuazione di detto accordo [2].

Il gruppo di lavoro ha preso nota, innanzitutto, del documento di lavoro della Commissione recentemente pubblicato [3], nel quale si forniscono ragguagli circa la presenza di tutti gli elementi dell'Approdo sicuro, così come le prime esperienze note sulle disposizioni riguardanti la trasparenza, il funzionamento dei meccanismi di risoluzione delle controversie e la protezione dei diritti.

Successivamente il gruppo di lavoro ha fatto una visita a Washington, il 13 e 14 marzo 2002, dove una delegazione ha effettuato un'approfondita analisi in collaborazione con svariate autorità competenti, organizzazioni non governative e organi di risoluzione delle controversie.

Le informazioni raccolte attraverso questo primo insieme di iniziative è alquanto utile ad evidenziare la necessità di collaborazione di tutte le autorità competenti a dare piena esecuzione all'accordo.

Il gruppo di lavoro contribuirà brevemente all'analisi della questione assolvendo i propri compiti di controllo sull'applicazione delle leggi nazionali riguardanti flussi di dati transfrontalieri ed il livello di tutela in paesi terzi, nonché di consigliere per quanto attiene ai provvedimenti da adottare per la tutela dei diritti e delle libertà delle persone fisiche [4], oltre alle linee guida fornite nei sei pareri emessi prima dell'adozione della decisione da parte della Commissione il 26 luglio 2000 [5].

(*) *Gruppo per la tutela dei dati personali - Articolo 29*
Il Gruppo di lavoro è stato costituito ex articolo 29 della direttiva 95/46/EC. È un organo europeo consultivo indipendente per la tutela dei dati e la privacy. Le sue funzioni sono descritte nell'articolo 30 della direttiva 95/46/CE e nell'articolo 14 della direttiva 97/66/CE.
La segreteria è fornita dalla direzione A (Funzionamento ed impatto del mercato unico - Coordinamento - Protezione dei dati) della Direzione generale della Commissione europea, DG Mercato interno, B-1049 Bruxelles, Belgio, ufficio C100-6/136.
Sito Web: www.europa.eu.int/comm/privacy

(1) Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm.
(2) Decisione della Commissione 520/2000/CE del 26 luglio 2000 in applicazione della direttiva 95/46 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 GU 215 del 28 agosto 2000, pagina 7.
(3) Documento di lavoro SEC(2002)196 del 13.02.2002.
(4) Articolo 30, paragrafo 1, direttiva 95/46/CE.
(5) Parere 4/2000, parere 3/2000, parere 7/1999, parere 4/1999, parere 2/1999, parere 1/1999.

In particolare, il gruppo di lavoro desidera studiare in maniera costruttiva se si possano superare eventuali divergenze nei pareri riguardanti l'attuazione di determinati provvedimenti dell'Approdo sicuro, ed in che modo colmare possibili divari tra i principi stabiliti nell'Accordo e la prassi esecutiva. Si prenderanno in seria considerazione anche i requisiti di trasparenza cui le organizzazioni devono adempiere, sia per quanto riguarda la loro autocertificazione di conformità all'Approdo sicuro, sia per quanto attiene alle loro politiche sulla privacy.

Il gruppo di lavoro è di conseguenza dell'opinione che è opportuno gli vengano fornite informazioni aggiornate con particolare attenzione alle poche questioni collegate all'attuazione dell'accordo. Il gruppo di lavoro si riserva, in base a tali informazioni, di richiamare tutti gli enti, organizzazioni ed imprese coinvolti affinché compiano rinnovati sforzi per adempiere ai principi e ai prerequisiti di un accordo prossimo alla scadenza del proprio periodo di avvio – iniziato l'1 novembre 2000, al momento dell'entrata in vigore dell'Approdo sicuro. Ciò è altresì opportuno alla luce della possibile applicazione di tale accordo, strettamente legato alla peculiare esperienza statunitense, ad altre operazioni di trattamento di dati personali negli Stati Uniti.

Stanti le summenzionate premesse, il gruppo di lavoro ritiene necessaria una rapida analisi dei passi da effettuare al fine di aumentare la consapevolezza in Europa sulle possibili violazioni dei principi salienti.

Inoltre il gruppo di lavoro ritiene opportuno valutare la consapevolezza dei soggetti di dati, dell'uso dei propri dati personali per ulteriori scopi.

Conformemente alla richiesta fatta dal Parlamento europeo nella sua risoluzione del 5 luglio [6], il gruppo di lavoro richiama le autorità, organizzazioni ed associazioni coinvolte a collaborare per raccogliere - in particolare attraverso le autorità nazionali per la protezione dei dati e la Commissione europea - informazioni aggiornate, con particolare attenzione

- ad accordi per l'aumento della trasparenza nei confronti delle organizzazioni firmatarie, in particolare se una dichiarazione di adesione ad AS non è accompagnata da adeguate politiche per la privacy,
- alla possibilità di fornire meccanismi di controllo addizionali nei confronti della procedura d'adesione all'accordo, la conformità di condotta degli aderenti allo stesso con le proprie politiche di privacy e l'eventuale perdita dei benefici dell'Approdo sicuro,
- alle iniziative da adottare al fine di aumentare la conoscenza dei prerequisiti per l'adesione all'Approdo sicuro, anche attraverso documenti brevi, facilmente comprensibili e l'eventuale integrazione nel Safe Harbor Workbook,
- ai provvedimenti da adottare per mettere a punto meccanismi di risoluzione delle controversie, aumentare l'uniformità e la conoscenza dei criteri salienti, aumentare la trasparenza circa l'esito delle controversie e semplificarne i meccanismi di pubblicazione,
- alle eventuali difficoltà derivanti dall'esistenza di molteplici politiche di privacy dichiarate dal medesimo operatore,
- ai criteri di priorità ed alle possibili ulteriori iniziative intraprese dalle competenti autorità statunitensi ed agli accordi per una rinnovata cooperazione tra il comitato europeo per la protezione dei dati, gli organi di risoluzione delle controversie e la Federal Trade Commission.

Il gruppo di lavoro ritiene che sarebbe auspicabile raccogliere le summenzionate informazioni entro il prossimo 31 ottobre e si riserva il diritto di esprimere un parere su tale questione non appena entri in possesso di dati aggiornati.

Fatto a Bruxelles, 2 luglio 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

(6) Risoluzione del Parlamento europeo su progetto di decisione della Commissione sull'adeguatezza della protezione ..., pubblicata nella GU C121 del 24.04.2001, pagina 152.

122 Parere 4/2002 sul livello di tutela dei dati personali in Argentina (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

11081/02/IT/def.
WP 63

Parere 4/2002 sul livello di tutela dei dati personali in Argentina

Adottato il 3 ottobre 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp63_it.pdf

123 Parere 5/2002 sulla dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni (*)

Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali
(art.29 direttiva 95/46/CE)

11818/02/IT/def.
WP 64

IL GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI PERSONALI

istituito in virtù della direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 1 ,
visti gli articoli 29 e 30, paragrafi 1 (a) e 3 della direttiva,
visto il regolamento di procedura del comitato , e in particolare gli articoli 12 e 14,
considerando la dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni
approva incondizionatamente tale dichiarazione.

Fatto a Bruxelles, 11 ottobre 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

Dichiarazione dei Commissari europei per la protezione dei dati alla conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni

I Commissari europei per la protezione dei dati rilevano con preoccupazione che, nell'ambito del cosiddetto "terzo pilastro" dell'UE, sono state avanzate proposte che comporterebbero l'obbligo sistematico di mantenimento dei dati di traffico concernenti tutti i tipi di telecomunicazioni (ossia luogo, data, e numeri utilizzati per comunicazioni telefoniche, fax, posta elettronica, e altri usi di Internet) per un periodo di un anno o anche oltre, allo scopo di consentire la possibilità di accesso a tali dati da parte delle autorità di polizia e di sicurezza.

(*) Gruppo per la tutela dei dati personali - Articolo 29
Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. Esso costituisce l'organismo consultivo indipendente dell'UE in materia di riservatezza e protezione dei dati. Le funzioni del gruppo sono stabilite dall'articolo 30 della diretttiva 95/46/CE e dell'articolo 14 della direttiva 97/66/CE. La segreteria è assicurata dalla Direzione A (Funzionamento e impatto del mercato unico - Coordinamento - Protezione dei dati) della Commissione europea, Direzione generale del Mercato interno,, B-1049 Bruxelles, Belgio, Ufficio C100-6/136.
Indirizzo Internet: www.europa.eu.int/comm/privacy