

tutela dei dati personali, denominato “habeas data”. Si tratta di una sottocategoria della procedura prevista dalla costituzione per la tutela dei diritti costituzionali che eleva quindi la tutela dei dati personali a diritto fondamentale. A norma dell'articolo 43, paragrafo 3 della costituzione argentina, ciascuno ha il diritto, a norma dell'“habeas data” di prendere conoscenza del contenuto di tutti i dati che lo riguardano e della loro finalità, che figurino in banche dati o archivi pubblici, o in quelli privati destinati a fornire dei rapporti informativi. In base a detto articolo, in caso di informazioni false o utilizzate a scopo discriminatorio, l'interessato può richiedere la cancellazione, la correzione, la qualificazione dei dati come riservati o l'aggiornamento dei dati contenuti negli archivi di cui sopra. Tale articolo non concerne la segretezza delle fonti d'informazione giornalistiche. La giurisprudenza argentina riconosce l'“habeas data” come diritto fondamentale e direttamente applicabile.

(8) La legge sulla tutela dei dati personali 25 326 del 4 ottobre 2000 (in prosieguo “la legge”) sviluppa ed approfondisce le disposizioni costituzionali. Essa contiene disposizioni relative ai principi generali di tutela dei dati, ai diritti delle persone interessate, agli obblighi dei responsabili del trattamento dei dati e degli utilizzatori, all'autorità o organo di controllo, alle sanzioni e al regolamento interno concernenti il ricorso giurisdizionale all'“habeas data”.

(9) Il regolamento approvato con decreto n. 1558/2001 del 3 dicembre 2001 (in prosieguo “il regolamento”) stabilisce le modalità d'applicazione della legge, ne completa le disposizioni e chiarisce i punti che possono essere oggetto di interpretazioni divergenti.

(10) La legislazione argentina concerne la tutela dei dati personali registrati in archivi, registri, basi di dati o altri strumenti tecnici gestiti da enti pubblici, così come la tutela dei dati personali registrati in archivi, registri, banche di dati o altri strumenti tecnici gestiti da privati, destinati a fornire dei rapporti informativi. Si tratta degli strumenti non limitati all'uso esclusivamente personale e di quelli destinati alla cessione o al trasferimento dei dati personali, indipendentemente dal fatto che la circolazione dei rapporti o delle informazioni prodotte sia gratuita o a pagamento.

(11) Alcune disposizioni della legge si applicano uniformemente a tutto il territorio nazionale. Si tratta di provvedimenti generali e provvedimenti relativi alla tutela generale dei dati, principi, diritti degli interessati e obblighi dei responsabili del trattamento dei dati e degli utilizzatori di archivi, registri e banche di dati, sanzioni penali, nonché dell'esistenza e delle modalità principali del ricorso giurisdizionale all'“habeas data” definito nella Costituzione.

(12) Altre disposizioni della legge riguardano i registri, gli archivi, le basi o le banche di dati che siano collegati in reti diffuse a livello intergiurisdizionale (ossia “interprovinciale”), nazionale o internazionale e considerati di competenza della giurisdizione federale. Dette disposizioni riguardano il controllo esercitato dalle autorità di controllo, le sanzioni che possono essere imposte dall'autorità di controllo e le norme di procedura che disciplinano il ricorso giurisdizionale in materia di “habeas data”. Altri tipi di registri, archivi, basi o banche di dati devono essere considerati di competenza della giurisdizione provinciale. Le province possono emanare disposizioni normative nelle dette materie.

(13) Disposizioni relative alla tutela dei dati figurano anche in numerosi strumenti giuridici relativi a diversi settori, quali le transazioni tramite carta di credito, le statistiche, le operazioni bancarie o la sanità.

(14) La legislazione argentina contempla tutti i principi basilari necessari per un adeguato livello di tutela delle persone fisiche, anche se prevede eccezioni e restrizioni al fine di salvaguardare importanti interessi pubblici. L'applicazione di tali norme è garantita da uno specifico ricorso giurisdizionale, semplificato e veloce, relativo alla tutela dei dati personali, denominato “habeas data”, così come dai ricorsi giurisdizionali generali. La legge prevede l'istituzione di un organo di controllo della tutela dei dati incaricato di prendere tutte le misure necessarie al rispetto delle disposizioni e degli obiettivi previsti ed è dotato di poteri d'indagine e d'intervento. Conformemente al regolamento, la Direzione nazionale per la tutela dei dati personali è stata istituita come organo di controllo. La legislazione argentina prevede sanzioni

efficaci e dissuasive, sia amministrative che penali. Inoltre le disposizioni della legislazione argentina concernenti la responsabilità civile (contrattuale ed extra-contrattuale) sono applicate in caso di trattamento illegale dei dati che reca pregiudizio alle persone interessate.

(15) Il governo argentino ha fornito spiegazioni e garanzie relative all'interpretazione della legislazione argentina ed ha assicurato che le norme concernenti la tutela dei dati sono applicate conformemente a tale interpretazione. La presente decisione si basa su tali spiegazioni e garanzie, dalle quali di conseguenza dipende. La presente decisione si riferisce segnatamente alle spiegazioni e alle garanzie fornite dalle autorità argentine in merito all'interpretazione della legislazione argentina, nonché alle situazioni che rientrano nel campo d'applicazione della legislazione argentina relativa alla tutela dei dati.

(16) Si ritiene pertanto che l'Argentina fornisca un adeguato livello di tutela dei dati personali di cui alla direttiva 95/46/CE.

(17) Nell'interesse della trasparenza e al fine di salvaguardare la capacità delle autorità competenti negli Stati membri di garantire la tutela delle persone fisiche per quanto concerne il trattamento dei dati personali che li riguardano, è necessario specificare nella decisione le circostanze eccezionali in cui, nonostante la constatazione di un livello di protezione adeguato, può essere giustificata la sospensione di trasferimenti di dati specifici.

(18) Il gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE ha fornito un parere sul livello di protezione dei dati personali in Argentina di cui si è tenuto conto nella preparazione della presente decisione⁽³⁾.

(19) Le misure previste dalla presente decisione sono conformi al parere del comitato di cui all'articolo 31, paragrafo 1 della direttiva 95/46/CE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Ai fini dell'articolo 25, paragrafo 2, della direttiva 95/46/CE, si ritiene che l'Argentina fornisca un adeguato livello di tutela dei dati personali trasferiti dalla Comunità.

Articolo 2

La presente decisione riguarda soltanto l'adeguatezza della protezione fornita in Argentina al fine di soddisfare i requisiti di cui all'articolo 25, paragrafo 1 della direttiva 95/46/CE e non produce alcun effetto su altre condizioni o restrizioni conseguenti all'attuazione di altre disposizioni della direttiva riguardanti il trattamento dei dati personali all'interno degli Stati membri.

Articolo 3

1. Fatti salvi i poteri di intervento al fine di garantire il rispetto dei provvedimenti nazionali adottati in applicazione di disposizioni diverse dall'articolo 25 della direttiva 95/46/CE, le autorità competenti degli Stati membri hanno facoltà di sospendere i trasferimenti di dati verso destinatari in Argentina, al fine di proteggere i cittadini nell'ambito del trattamento dei loro dati personali nei casi in cui:

- a) un'autorità competente argentina abbia constatato che il destinatario non rispetta le norme applicabili relative alla protezione;
- b) sia fortemente probabile una violazione delle norme relative alla protezione; vi siano motivi ragionevoli di ritenerne che le autorità competenti argentine non adottino o non intendano adottare misure adeguate e tempestive per risolvere il caso in questione; la continuazione del trasferimento dei dati comporti un rischio imminente di grave pregiudizio per le persone interessate e le autorità competenti degli Stati membri abbiano fatto il possibile, date le circostanze, per avvertire il responsabile del trattamento in Argentina e dargli la possibilità di replicare.

(3) Parere 4/2002 sul livello di protezione dei dati personali in Argentina - WP 63 del 3 ottobre 2002 disponibile al seguente indirizzo:
www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

La sospensione cessa non appena sia garantito il rispetto delle norme di protezione e ne sia informata l'autorità competente della Comunità.

2. Gli Stati membri informano immediatamente la Commissione dell'adozione di provvedimenti in base al paragrafo 1.

3. Gli Stati membri e la Commissione si informano reciprocamente dei casi in cui l'azione degli organismi argentini responsabili per il rispetto delle norme di protezione non sia sufficiente a garantire tale rispetto.

4. Ove risulti provato, dalle informazioni di cui ai paragrafi 1, 2 e 3, che gli organismi argentini incaricati di garantire il rispetto delle norme di protezione non svolgono la loro funzione in modo efficace, la Commissione avverte le autorità argentine competenti e, se necessario, presenta progetti di misure, con la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE, al fine di abrogare o sospendere la presente decisione o di limitarne il campo d'applicazione.

Articolo 4

1. La presente decisione può essere modificata in qualsiasi momento, per tener conto delle esperienze relative alla sua applicazione o di cambiamenti intervenuti nella legislazione argentina, nella sua applicazione ed interpretazione.

La Commissione verifica l'applicazione della presente decisione e comunica qualsiasi informazione utile al comitato istituito dall'articolo 31 della direttiva 95/46/CE, in particolare ogni elemento rilevante ai fini della valutazione di cui all'articolo 1 della presente decisione circa l'adeguatezza della protezione argentina ai sensi dell'articolo 25 della direttiva 95/46/CE e ogni elemento che dimostri che la presente decisione è applicata in modo discriminatorio.

2. Se necessario, la Commissione presenta progetti di misure con la procedura di cui all'articolo 31, paragrafo 2, della direttiva 95/46/CE.

Articolo 5

Gli Stati membri adottano le misure necessarie per conformarsi alla presente decisione entro centoventi giorni dalla notifica della stessa.

Articolo 6

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il 30 giugno 2003

Per la Commissione
Frederik Bolkestein
Membro della Commissione

70

Risoluzione del Parlamento europeo sul trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici (*)



P5_TA(2003)0097
B5-0187/2003

Trasmissione dei dati personali da parte delle compagnie aeree in occasione di voli transatlantici

Il Parlamento europeo,

— visti la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati⁽¹⁾ e il regolamento del Consiglio CEE n. 2299/89 del 24 luglio 1989 su un codice di condotta per i sistemi telematici di prenotazione⁽²⁾,

A. consapevole del fatto che dopo l'11 settembre 2001 gli Stati Uniti hanno riformato profondamente la legislazione al fine di garantire la propria sicurezza interna anche nel settore dei trasporti e che, il 19 novembre 2001, hanno adottato "l'Aviation and Transportation Security Act (ATSA)"⁽³⁾, e il 5 maggio 2002 "l'Enhanced Border Security and Visa Entry Reform Act of 2002 (EBSV)"⁽⁴⁾ nonché altre misure connesse che riguardano, per i soli voli transatlantici, circa 10/11 milioni di passeggeri l'anno,

B. considerando che inizialmente l'amministrazione degli Stati Uniti si era limitata a richiedere alle compagnie aeree la trasmissione dei dati relativi ai passeggeri e ai membri dell'equipaggio ("Passenger Manifest Information") (nota finale1) attraverso "l'Advance Passenger Information System (APIS)", che in seguito

[...]

(*) Prima pagina del documento, rinvenibile in [www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=P5_TA\(2003\)0097it.pdf&LANGUE=IT](http://www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=P5_TA(2003)0097it.pdf&LANGUE=IT)

(1) GU L 281 del 23.11.1995, pag. 31.

(2) GU L 220 del 29.7.1989, pag. 1.

(3) "Aviation and Transportation Security Act" del 19 novembre 2001 (107-71), norme provvisorie del Dipartimento del tesoro (dogane) - dati relativi a passeggeri e equipaggi richiesti per i voli passeggeri nel trasporto aereo dall'estero verso gli Stati Uniti (registro federale, 31 dicembre 2001) e trasmissione del registro dei nomi dei passeggeri richiesta per i passeggeri di voli internazionali da o verso gli Stati Uniti (registro federale, 25 giugno 2002).

71

Risoluzione del Parlamento europeo sul trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici: stato dei negoziati con gli Stati Uniti (*)



P5_TA(2003)0429
B5-0411/2003

Trasferimento di dati personali da parte delle compagnie aeree in occasione di voli transatlantici

Il Parlamento europeo,
– visto l'articolo 42, paragrafo 5, del suo regolamento,

A. considerando la sua risoluzione del 13 marzo 2003 sulla trasmissione di dati personali da parte delle compagnie aeree in occasione di voli transatlantici¹,

B. considerando che, dopo l'11 settembre 2001, gli USA hanno attuato differenti misure volte a rafforzare i controlli alle proprie frontiere; rilevando, in particolare, che dal 1° ottobre 2003 soltanto i passeggeri provvisti di un "passaporto leggibile a macchina" possono entrare senza visto e che nel prossimo futuro i passeggeri dovranno presentare un passaporto contenente dati biometrici,

C. considerando le verifiche svolte dalla Commissione nel corso degli ultimi mesi, sia a livello amministrativo che politico, al fine di accertare se le misure adottate e previste dalle autorità statunitensi garantiscono un'adeguata protezione dei dati, in conformità delle disposizioni della direttiva 95/46/CE² nonché dei principi sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dalla Carta dei diritti fondamentali dell'Unione europea,

D. considerando le informazioni fornite dalla Commissione e il fatto che attualmente non è possibile ritenere adeguata la protezione dei dati assicurata dalle autorità statunitensi perché:

- (a) l'obiettivo che giustificherebbe l'acquisizione e la conservazione dei dati permane oscuro e non è limitato alla lotta contro il terrorismo; di conseguenza, sussiste il rischio che i dati possano essere utilizzati per altri scopi, ivi compreso il loro trasferimento ad altri servizi dell'amministrazione statunitense oppure a terzi,
- (b) il numero di dati richiesti (39 elementi diversi del codice di prenotazione del passeggero) appare eccessivo ed è in ogni caso sproporzionato rispetto all'obiettivo perseguito,
- (c) la conservazione dei dati (6/7 anni) appare ingiustificata, in particolare rispetto ai dati riguardanti persone che non costituiscono una minaccia per la sicurezza del [...]

(*) Prima pagina del documento, rinvenibile in [www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=P5_TA\(2003\)0429it.pdf&LANGUAGE=IT](http://www3.europarl.eu.int/omk/omnsapir.so/calendar?APP=PDF&TYPE=PV2&FILE=P5_TA(2003)0429it.pdf&LANGUAGE=IT)

72

Risoluzione del Parlamento europeo sulla prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) del 9 marzo 2004 (COM(2003) 265 - C5- 0375/2003 - 2003/2153(INI)) (*)

P5_TA-PROV(2004)0141
A5-0104/2004

Il Parlamento europeo,

- vista la Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE) (COM(2003) 265 - C5-0375/2003),

- visti i testi di diritto internazionale a tutela del diritto alla vita privata e, in particolare, l'articolo 12 della dichiarazione universale dei diritti dell'uomo del 10 dicembre 1948, l'articolo 17 del patto internazionale relativo ai diritti civili e politici del 16 dicembre 1966, l'articolo 8 della convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950(1), la convenzione per la protezione delle persone rispetto al trattamento automatico dei personali del 28 gennaio 1981(2) e le raccomandazioni adottate dal Consiglio d'Europa,

- visti l'articolo 6 del trattato UE sul rispetto dei diritti dell'uomo e delle libertà fondamentali nell'Unione, l'articolo 286 del trattato CE, nonché gli articoli 7 e 8 della Carta europea dei diritti fondamentali dell'Unione dedicati rispettivamente al rispetto della vita privata e della vita familiare e alla protezione dei dati di carattere personale,

- viste le disposizioni del diritto comunitario a tutela del diritto alla vita privata e alla protezione dei dati, in particolare la direttiva 95/46/CE, 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati(3), e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)(4),

- visti gli altri strumenti UE relativi alla protezione dei dati nell'ambito del terzo pilastro, in particolare il progetto di documento di lavoro della Presidenza greca su norme comuni per la protezione dei dati personali nel quadro del terzo pilastro e l'annuncio del Commissario Vitorino relativo alla presentazione, nel 2004, di uno strumento giuridico in proposito(5),

- visti i pareri del gruppo di lavoro sulla privacy istituito dall'articolo 29 della direttiva 95/46/CE (gruppo 'Articolo 29'),

[...]

(*) Prima pagina del
documento, rinvenibile in
www3.europarl.eu.int

73

**Risoluzione del Parlamento europeo
sul progetto di decisione della
Commissione che prende atto del
livello di protezione adeguato dei
dati a carattere personale contenuti
nelle pratiche passeggeri (PNR-
Passenger Name Records) trasferite
all'Ufficio delle dogane e della
protezione di frontiera degli Stati
Uniti del 31 marzo 2004
(2004/2011(INI)) (*)**



P5_TA-PROV(2004)0245

Protezione dei dati personali dei passeggeri aerei

Il Parlamento europeo,

— visti la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche don riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ⁽¹⁾, e in particolare il suo articolo 25, nonché il regolamento (CE) n. 2289/99 del Consiglio, del 24 luglio 1989, relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione ⁽²⁾,

— visto il progetto di decisione della Commissione che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR-Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (C5-0124/2004),

— visti il parere espresso il 29 gennaio 2004 dal gruppo di lavoro di cui all'articolo 29 della direttiva 95/46/CE sulla tutela dei dati personali e quello espresso il 17 febbraio 2004 dal comitato di cui all'articolo 31 della direttiva sopra citata,

— vista la sua risoluzione del 9 marzo 2004 ⁽³⁾ sull'applicazione della direttiva 95/46/CE,

— vista la posizione espressa dai parlamenti nazionali al riguardo,

— visti il parere della commissione belga per la privacy su due casi relativi al trasferimento da parte di tre compagnie aeree dei dati personali di alcuni passeggeri transatlantici - tra cui quelli di un deputato europeo - secondo il quale sono stati violati il diritto nazionale ed europeo in materia di privacy; la constatazione del Consiglio secondo la quale le misure USA confliggono potenzialmente con la legislazione comunitaria e degli Stati membri sulla protezione dei dati (2562^a sessione del Consiglio Affari Generali - Bruxelles, 23 febbraio 2004); il documento interno della Commissione che conferma l'effettiva esistenza di tale conflitto; la condanna da parte del Parlamento europeo della flagrante violazione della legislazione sulla privacy; il fatto che le maggiori responsabilità incombono alla Commissione, agli Stati membri nonché a talune autorità garanti della privacy,

(*) p. 198-205

(1) G.U. L 281 del 23

novembre 1995, p. 31

Direttiva modificata dal
regolamento (CE)

n. 1882/2003 (G.U. L 284
del 31 ottobre 2003, p. 1).

(2) G.U. L 220 del 29 luglio
1989. Regolamento
modificato da ultimo dal
regolamento (CE)

n. 323/1999 (G.U. L 40 del
13 febbraio 1999, p. 1).

(3) P5_TA(2004)0141.

— visto l'articolo 8 della decisione 1999/468/CE del Consiglio, del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione⁽³⁾,

— visto l'articolo 88 del suo regolamento,

(3) G.U. L 184 del 17 luglio 1999, p. 23.

(4) FEDERAL REGISTER 68 FR 2101 "il TSA intende utilizzare questo sistema di registrazioni per agevolare il passeggero TSA e il programma di verifica della sicurezza aerea ai sensi dell'Aviation and Transportation Security Act. Il TSA intende usare il sistema CAPPS II per effettuare valutazioni dei rischi al fine di garantire la sicurezza dei passeggeri e dei voli.

(5) CEDU, sentenza Amann contro Svizzera del 16 febbraio 2000, raccolta delle sentenze e decisioni 2000-II, par. 65, e Rotaru contro Romania del 4 maggio 2000, raccolta delle sentenze e delle decisioni 2000-V, par. 43).

(6) Il ricorso a una "legge" è tanto più giustificato quando si tratta della protezione di un diritto fondamentale e tale protezione non può essere lasciata a misure di tipo amministrativo o a semplici provvedimenti di attuazione. Una "legge" deve inoltre essere elaborata con precisione sufficiente per consentire ai destinatari delle sue disposizioni di conformarvi la propria condotta e rispondere all'esigenza di prevedibilità che deriva dalla giurisprudenza della Corte europea dei diritti dell'uomo (vedasi in particolare CEDU, sentenza Rekvényi contro Ungheria del 20 maggio 1999, raccolta delle sentenze e decisioni 1999-III, par. 34).

•/• segue

A. ricordando che l'amministrazione USA, in applicazione del Transport Security Act (Legge sulla sicurezza dei trasporti) e dei relativi provvedimenti di attuazione, come l'Aviation Security Screening Records⁽⁴⁾ (Registri di controllo della sicurezza aerea) ha imposto alle compagnie aeree che operano in Europa di consentire l'accesso ai dati commerciali contenuti nelle pratiche passeggeri (PNR), al fine di stabilire preventivamente la minaccia potenziale che ogni passeggero potrebbe rappresentare e di garantire che terroristi o individui responsabili di gravi crimini siano identificati e arrestati o che sia loro negato l'ingresso negli Stati Uniti,

B. constatando che è necessario un chiaro quadro giuridico se si vuole consentire tale accesso è illegale secondo il diritto nazionale ed europeo sulla privacy, e che ciononostante né la Commissione, né gli Stati membri, né le autorità garanti della privacy e dotate di poteri vincolanti hanno operato per assicurare l'applicazione della legge,

C. ricordando che, nel settore dei trasporti aerei, la pratica passeggeri (PNR) è un archivio contenente una serie di informazioni commerciali che riguardano in particolare:

- a) i dati che consentono di individuare il passeggero, le persone che lo accompagnano e coloro che hanno chiesto la prenotazione per suo conto, l'agenzia o il dipendente che l'hanno effettuata e/o che hanno emesso il biglietto, ecc.,
- b) i dati concernenti il percorso per il quale è stato emesso il biglietto, ma anche tutti gli altri segmenti che costituiscono l'itinerario completo di un percorso composto a diverse tratte che implicano quindi più biglietti,
- c) i dati concernenti i mezzi di pagamento, il numero di carta di credito del passeggero, le condizioni speciali concesse a categorie particolari (frequent flyers, membri di categorie speciali), gli indirizzi e-mail nonché gli indirizzi fisici e i numeri di telefono privati e/o professionali dichiarati al momento della prenotazione, le persone da avvisare, ecc.,
- d) i dati relativi ad un servizio particolare connesso alle condizioni di salute della persona, alle sue preferenze alimentari, ecc.,
- e) le osservazioni specifiche effettuate dal personale della compagnia aerea,
- f) se del caso, dettagli sulle prenotazioni di un'automobile a noleggio e stanze d'albergo,

D. considerando che i dati PNR variano a seconda delle pratiche commerciali seguite da ogni compagnia aerea e sono trattati da centri di prenotazione e che, di conseguenza, le compagnie aeree dovrebbero mettere a punto programmi adeguati per estrarre i dati che potrebbero legittimamente essere trasferiti,

Quanto ai principi di tutela dei dati da parte dell'Europa

E. considerando che l'articolo 8, paragrafo 2 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, come viene interpretato dalla Corte europea dei diritti dell'uomo (CEDU)⁽⁵⁾, ammette un'ingerenza nella vita privata solo quando "... sia prevista dalla legge⁽⁶⁾, sia necessaria⁽⁷⁾ in una società democratica⁽⁸⁾ per perseguire scopi legittimi e non sia sproporzionata⁽⁹⁾ in rapporto all'obiettivo perseguito",

F. consapevole che, in questa fase, non esiste una base giuridica nell'Unione europea che consenta di utilizzare a fini di sicurezza pubblica i dati commerciali PNR e che tale base giuridica è indispensabile per modificare la finalità per cui i dati sono stati originariamente raccolti e per autorizzare l'utilizzazione di questi dati a scopi di sicurezza pubblica,

G. ricordando che questa base giuridica deve definire esattamente i dati da raccogliere, le norme da seguire per la loro elaborazione e le responsabilità di tutte le parti interessate

(passeggeri, compagnie aeree e autorità pubbliche),

H. considerando che il Consiglio ha di recente approvato il mandato negoziale della Commissione per un accordo internazionale in questo settore ,

...e da parte degli Stati Uniti

I. considerando che negli Stati Uniti la protezione della vita privata, pur essendo citata dal quarto emendamento alla Costituzione, non è considerata come un diritto fondamentale,

- a) ma è disciplinata da disposizioni specifiche (che tuttavia non contemplano il settore dei trasporti) e dal Freedom of Information Act (Legge sulla libertà di informazione),
- b) permette ai soli cittadini USA e ai residenti legali di beneficiare di una protezione dei dati e, in particolare, del diritto di accesso e di rettifica relativamente ai soli dati detenuti dalle autorità pubbliche federali (Privacy Act del 1974), in modo che
- c) nessuna tutela giuridica è attualmente garantita per i dati dei passeggeri non americani e in particolare europei, né alcun diritto di ricorso giurisdizionale contro eventuali abusi delle misure restrittive della libertà di circolazione,

Quanto all'impatto giuridico di una decisione in materia di adeguatezza a norma dell'articolo 25 della direttiva 95/46/CE

J. consapevole del fatto che il progetto di decisione presentato dalla Commissione:

- a) è una misura di semplice esecuzione della direttiva 95/46/CE che non può avere l'effetto di ridurre i criteri di protezione dei dati garantiti nella UE come stabilito dalla direttiva 95/46/CE,
- b) riguarda una situazione caratterizzata ancora da un limbo giuridico sia negli Stati Uniti (poiché gli "impegni" presi dagli Stati Uniti non in tutti i casi hanno effetti giuridici) che in Europa (poiché non è stata ancora adottata nessuna base giuridica che consenta il legittimo trasferimento di dati PNR ad autorità pubbliche),
- c) una volta adottato, priverà in pratica gli Stati membri (attualmente responsabili di garantire la protezione delle persone quanto ai dati PNR) di ogni possibilità di bloccare i trasferimenti per garantire i diritti dei loro cittadini,

K. deplorando che, per tutto il 2003, la Commissione non abbia tenuto conto delle ripetute richieste del Parlamento europeo e delle autorità di controllo dei dati che la invitavano:

- a) a definire i dati che potrebbero essere trasferiti legittimamente senza rischi (vedasi l'elenco dei 19 punti proposti il 13 giugno 2003 dal Gruppo di cui all'articolo 29 della direttiva 95/46/CE)⁽¹⁰⁾,
- b) a sostituire immediatamente il sistema "PULL" (utilizzato senza base giuridica dall'amministrazione USA e senza filtri per i dati sensibili o per i voli non transatlantici) col sistema "PUSH" (che permette a ogni compagnia aerea di trasferire solo i dati legittimi e per i soli voli con destinazione USA),
- c) a negoziare un accordo internazionale con gli USA che preveda garanzie reali per i passeggeri o quantomeno la stessa protezione di cui beneficiano i cittadini USA,

L. facendo proprie gran parte delle riserve formulate all'unanimità dalle autorità di controllo dei dati riunite in seno al gruppo di lavoro previsto dall'articolo 29 della direttiva 95/46/CE, precisamente il 29 gennaio 2004⁽¹¹⁾,

1. ritiene che la decisione della Commissione del ... , che prende atto del livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche passeggeri (PNR - Passenger Name Records) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti, esuli dalle competenze di esecuzione conferite alla Commissione, in quanto:

•/• segue nota (8)

Nel caso in questione, la legge deve anche comportare disposizioni esplicite e dettagliate sulle persone autorizzate a consultare i fascicoli, la natura di tali fascicoli, la procedura da seguire e l'uso che può essere fatto delle informazioni così ottenute (vedasi CEDU, sentenza Rotaru contro Romania, 4 maggio 2000).

(7) Il concetto di "necessità" implica l'esigenza sociale imperiosa che la misura adottata sia proporzionata allo scopo legittimo perseguito (vedasi in particolare CEDU, sentenza Gillow contro Regno Unito del 24 novembre 1986, Serie A n. 109, par. 55) e che, in questa prospettiva, il legislatore usufruisca di un margine di valutazione "la cui ampiezza non dipende solo dalla finalità ma anche dal carattere proprio dell'ingerenza" (vedasi CEDU, sentenza Leander contro Svezia del 26 marzo 1987, Serie A n. 116, par. 59).

(8) Il criterio di società "democratica" si applica alle relazioni tra poteri pubblici e cittadini ed è da considerare tanto più presente quando sono i cittadini a controllare le istituzioni e non il contrario. Evidentemente, qualunque sia la natura di tali relazioni, in ogni democrazia è essenziale valutare con molta cautela ogni forma di raccolta e di stoccaggio sistematico dei dati, soprattutto qualora tali dati riguardino persone che non rappresentano un pericolo per la collettività.

(9) Il criterio di proporzionalità si applica a tutti i parametri

•/• segue

Per quanto riguarda la base giuridica e la forma

1.1. il progetto di decisione non è (e non potrebbe essere):

- a) una **base giuridica** che possa, in seno all'Unione europea, modificare le finalità per cui sono stati raccolti dati nel PNR e permetterne il trasferimento totale o parziale a terzi da parte delle compagnie aeree⁽¹²⁾; esso può avere però quale probabile risultato una riduzione dei criteri di protezione dei dati previsti dalla direttiva 95/46/CE all'interno dell'UE o la creazione di nuovi criteri d'intesa con paesi terzi;
- b) un accordo internazionale in applicazione del quale la Commissione sarebbe tenuta ad autorizzare il trasferimento di tali dati; non si può che deplofare l'ambigua formulazione di alcune clausole della decisione e degli impegni corrispondenti (come quelle relative alla durata, ai meccanismi di controllo, ai casi di sospensione o revoca della decisione, alle condizioni di intervento degli Stati membri, ecc.) che potrebbero indurre falsamente a ritenere che tale testo sia suscettibile di creare alcuni obblighi in quanto sono esplicitamente esclusi dalla clausola 47 la quale stipula che "tali impegni non creano alcun diritto o vantaggio per alcuna persona o parte, privata o pubblica";

Per quanto riguarda il contenuto

1.2. il progetto di decisione si fonda su "impegni" la cui obbligatorietà è lungi dall'essere evidente:

- a) sia per la fonte che è puramente amministrativa (e quindi soggetta a possibili ristrutturazioni interne al Departement of Home Security (DHS - Ministero della sicurezza interna) che renderebbero obsolete le separazioni tra strutture interne);
- b) sia per il contenuto in quanto, da una parte, si fa riferimento a garanzie che non sono ancora una base giuridica negli USA e, dall'altra, si mantiene la possibilità di modificare la regolamentazione in qualsiasi momento, in particolare per quanto riguarda le modalità di utilizzazione e riutilizzazione dei dati;

1.3. il sistema "pull" di accesso ai dati PNR mette a repentaglio eventuali limitazioni che possano essere state convenute e deve essere sostituito da un sistema "push" dotato di filtri adeguati;

2. ritiene che l'importanza della questione sia tale che l'Unione europea debba regolarla con gli Stati Uniti sulla base di un vero accordo internazionale che, nel pieno rispetto dei diritti fondamentali, definisce:

- a) i dati che possono essere trasferiti in modo automatizzato (APIS) e i dati che possono essere trasferiti caso per caso;
- b) l'elenco dei reati gravi per cui è possibile avanzare una richiesta supplementare;
- c) l'elenco delle autorità e delle agenzie che potrebbero condividere i dati e le condizioni di tutela dei dati da rispettare;
- d) il periodo di conservazione per i due tipi di dati, fermo restando che i dati relativi alla prevenzione di reati gravi devono essere scambiati sulla base dell'accordo UE/USA sulla cooperazione giudiziaria e l'estradizione;
- e) il ruolo che le compagnie aeree devono svolgere nel trasferire i dati dei passeggeri e gli strumenti previsti (APIS, PNR, ecc.) a fini di sicurezza pubblica;
- f) le garanzie da fornire ai passeggeri per consentire loro di correggere i dati che li riguardano o fornire spiegazioni in caso di discordanze tra i dati connessi a un contratto di viaggio e i dati figuranti nei documenti di identità, nei visti e nei passaporti;
- g) le responsabilità delle compagnie aeree nei confronti dei passeggeri e delle autorità pubbliche in caso di errori di trascrizione o di codificazione e per quanto concerne la tutela dei dati trattati;
- h) il diritto di far ricorso ad un'autorità indipendente e a meccanismi di rimedio in caso di violazione dei diritti dei passeggeri;

3. si dichiara disposto a esaminare in base alla procedura d'urgenza un accordo internazionale che rispetti i suddetti principi; ritiene che, se fosse adottato tale accordo, la

•/• segue nota (9)

del trattamento dei dati (ad esempio in che momento i dati vengono trasferiti, quali dati sono trasferiti, a chi, per fare cosa, durata della conservazione, durata della deroga). Nel quadro del diritto europeo tali valutazioni devono anche essere fatte tenendo presente le esigenze di sussidiarietà che disciplinano i rapporti tra gli Stati membri e l'Unione europea. Ciò è tanto più necessario nel caso in cui gli Stati membri venissero privati della possibilità di intervenire da un atto di un'Istituzione (10) "I dati dovrebbero includere le informazioni seguenti: "PNR record locator code", dati di prenotazione, data/e prevista/e del viaggio, nome del passeggero, altri nomi presenti nel PNR, l'itinerario di viaggio, le coordinate dei biglietti gratuiti, biglietti di sola andata, "ticketing field information", dati "ATFQ (Automatic Ticket Fare Quote)", numero del biglietto, data in cui il biglietto è stato emesso, "no show history", numero di bagagli, numero identificativo dei bagagli, "no show information", numero di bagagli per ogni segmento, modifiche volontarie o involontarie di classe, dettagli delle modifiche effettuate sui dati PNR e riguardanti gli elementi precedentemente menzionati".

(11) www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87-fr.pdf.

(12) Peraltro, l'obbligo imposto alle compagnie aeree dalla legislazione

•/• segue

Commissione potrebbe legittimamente dichiarare che i dati sarebbero adeguatamente protetti negli USA;

4. invita la Commissione a presentare al Parlamento una nuova decisione in materia di adeguatezza, a chiedere al Consiglio il mandato per un nuovo e rigoroso accordo internazionale nel rispetto dei principi enunciati nella presente risoluzione;

5. invita, in attesa di una soluzione legislativa definitiva o della conclusione di uno o più accordi internazionali:

- a) gli Stati membri a imporre immediatamente il rispetto del diritto nazionale ed europeo sulla privacy, richiamando in particolare l'attenzione sull'obbligo fatto, a norma dell'articolo 26, paragrafo 1, lettera a) della direttiva 95/46/CE, alle compagnie aeree e alle agenzie di viaggio di ottenere dai passeggeri il consenso per il trasferimento dei dati; tale consenso deve essere concesso spontaneamente e i passeggeri devono essere informati in merito alle possibilità di scelta per influenzare il contenuto del proprio PNR, alle conseguenze di un mancato consenso e all'assenza di un livello adeguato di protezione negli Stati Uniti;
- b) la Commissione ad intervenire per assicurare l'applicazione del regolamento (CE) n. 2289/99 e, nella fattispecie, a verificare che i dati non siano trasferiti, in particolare attraverso i sistemi telematici di prenotazione (CRS), senza il consenso del passeggero e che le amministrazioni di paesi terzi non abbiano accesso a tali sistemi;

6. invita la Commissione a bloccare:

- a) il sistema "PULL" a partire dal 1° luglio 2004 e, dopo tale data, ad applicare il sistema "PUSH" con i 19 punti proposti il 13 giugno 2003 dal gruppo di lavoro di cui all'articolo articolo 29 della direttiva 95/46/CE;
- b) le iniziative concernenti l'istituzione di una gestione centralizzata europea dei dati PNR come delineato nella Comunicazione COM(2003) 826 e come è stato recentemente confermato dal Commissario competente alla commissione parlamentare, in quanto tali iniziative violano per il momento i principi di proporzionalità e di sussidiarietà;

7. si riserva comunque il diritto di adire la Corte di giustizia qualora il progetto di decisione venga adottato dalla Commissione; ricorda alla Commissione l'obbligo di cooperazione leale tra istituzioni previsto all'articolo 10 del Trattato e la invita a non adottare, durante il periodo elettorale, una decisione come quella esaminata dalla presente risoluzione;

8. si riserva il diritto di adire la Corte di Giustizia per verificare la legalità del previsto accordo internazionale e, in particolare, la sua compatibilità con la tutela di un diritto fondamentale;

9. ritiene estremamente importante che l'esito dei negoziati non sia adottato come modello per le ulteriori attività dell'UE in ordine al varo delle proprie misure finalizzate alla lotta contro la criminalità, alla memorizzazione dei dati nonché alla tutela della privacy;

10. invita la Commissione a ritirare il progetto di decisione;

* * *

11. incarica il suo Presidente di trasmettere la presente risoluzione al Consiglio e alla Commissione, ai parlamenti e ai governi degli Stati membri, nonché al Congresso degli Stati Uniti.

•/• segue nota (12)
americana non può essere considerato come un obbligo legale sufficiente ai sensi dell'articolo 7, lettera c) della direttiva 95/46/CE che va interpretato alla luce dei diritti fondamentali i quali, secondo una giurisprudenza costante, fanno parte integrante dei principi generali del diritto di cui la Corte di giustizia delle Comunità europee assicura il rispetto (cfr. in particolare sentenza del 6 marzo 2001, Connolly/Commissione, C-274/99 P, Rec. p. I-1611, punto 37).

74**Ethical Aspects of Genetic Testing in the Workplace (*)**

OPINION OF THE EUROPEAN GROUP ON ETHICS
IN SCIENCE AND NEW TECHNOLOGIES
TO THE EUROPEAN COMMISSION

No 18**Final – 28th July 2003****Original in English****ETHICAL ASPECTS OF GENETIC TESTING IN THE WORKPLACE**

Reference: Initiative of the Group

Rapporteurs: Peter Whittaker and Nicos C. Alivizatos

The European Group on Ethics in Science and New Technologies (EGE),

Having regard to the Treaty on European Union as amended by the Treaty of Nice, and in particular Article 6 of the common provisions, concerning the respect for fundamental rights;

Having regard to the EC Treaty and in particular Article 137 concerning the working conditions and health and safety at work;

Having regard to the Charter on Fundamental Rights of the European Union, approved by the European Council in Biarritz on October 14th 2000 and proclaimed solemnly in Nice by the European Parliament, the Council and the Commission on December 7th 2000, in particular Article 8 on the "Protection of personal data", Article 15 on the "Freedom to choose an occupation and right to engage in work", Article 21 prohibiting discrimination based, among others, on genetic features, and Article 31 on "Fair and just working conditions";

Having regard to the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data;

Having regard to the Directive 2000/78/EC of the European Council of 27 November 2000 establishing a general framework for equal treatment in employment and occupation;

(*) Prima pagina del documento, rinvenibile in http://europa.eu.int/comm/european_group_ethics/docs/avis18EN.pdf

75

Sentenza della Corte di giustizia delle Comunità europee del 20 maggio 2003, *Österreichischer Rundfunk e.a. (*)*

“Tutela delle persone fisiche con riguardo al trattamento di dati personali - Direttiva 95/46/CE - Tutela della vita privata - Divulgazione dei dati sui redditi di dipendenti di enti sottoposti al controllo del Rechnungshof”

Nei procedimenti riuniti C-465/00, C-138/01 e C-139/01,

aventi ad oggetto tre domande di pronuncia pregiudiziale proposte alla Corte, a norma dell'art. 234 CE, rispettivamente dal Verfassungsgerichtshof (C-465/00) e dall'Oberster Gerichtshof (C-138/01 e C-139/01) (Austria) nelle cause dinanzi ad essi pendenti tra

[...]

domande vertenti sull'interpretazione della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31),

[...]

LA CORTE,

pronunciandosi sulle questioni sottoposte dal Verfassungsgerichtshof, con ordinanza 12 febbraio 2000, e dall'Oberster Gerichtshof, con ordinanze 14 e 28 febbraio 2001, dichiara:

- 1) Gli artt. 6, n. 1, lett. c), e 7, lett. c) ed e), della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, non ostano ad una normativa nazionale come quella di cui trattasi nelle cause principali, a condizione che sia provato che l'ampia divulgazione non solo dell'importo dei redditi annui, laddove questi superino un certo limite, delle persone impiegate presso enti soggetti al controllo del Rechnungshof, ma anche dei nomi dei beneficiari di tali redditi, è al contempo necessaria ed appropriata all'obiettivo di buona gestione delle risorse pubbliche perseguito dal costituente. La verifica di ciò spetta ai giudici del rinvio.
- 2) Gli artt. 6, n. 1, lett. c), e 7, lett. c) ed e), della direttiva 95/46 sono direttamente applicabili, nel senso che essi possono essere fatti valere da un singolo dinanzi ai giudici nazionali per evitare l'applicazione delle norme di diritto interno contrarie a tali disposizioni.

(*) Estratto del documento, rinvenibile in
www.europa.eu.int/servlet/portail/CuriaServlet?curiaLink=%26lang%3DIT%26ident%3D79969479C19010139%26model%3Ddoc_curia

76

Sentenza della Corte di giustizia delle Comunità europee del 6 novembre 2003, *Bodil Lindquist* (*)

“Direttiva 95/46/CE - Ambito di applicazione -Pubblicazione dei dati personali su Internet - Luogo della pubblicazione - Nozione di trasferimento di dati personali verso paesi terzi - Libertà d'espressione - Compatibilità con la direttiva 95/46 di una protezione più ampia dei dati personali da parte della normativa di uno Stato membro”

Nel procedimento C-101/01,

avente ad oggetto la domanda di pronuncia pregiudiziale proposta alla Corte, a norma dell'art. 234 CE, dalla Göta Hovrätt (Svezia), nel procedimento penale dinanzi ad essa pendente contro

Bodil Lindqvist,

domanda vertente, in particolare, sull'interpretazione della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281, pag. 31),

LA CORTE

[...]

pronunciandosi sulle questioni sottoposte dalla Göta Hovrätt con ordinanza 23 febbraio 2001, dichiara:

- 1) L'operazione consistente nel fare riferimento, in una pagina Internet, a diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce un «trattamento di dati personali interamente o parzialmente automatizzato», ai sensi dell'art. 3, n. 1, della direttiva del Parlamento europeo e del Consiglio 24 ottobre 1995, 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.
- 2) Un siffatto trattamento di dati personali non rientra in alcuna delle eccezioni che figurano nell'art. 3, n. 2, della direttiva 95/46.
- 3) L'indicazione del fatto che una persona si è ferita ad un piede e si trova in congedo parziale per malattia costituisce un dato personale relativo alla salute ai sensi dell'art. 8, n. 1, della direttiva 95/46.
- 4) Non si configura un «trasferimento verso un paese terzo di dati» ai sensi dell'art. 25 della direttiva 95/46 allorché una persona che si trovi in uno Stato membro inserisce in una pagina Internet - caricata presso una persona fisica o giuridica che ospita («web hosting») il sito Internet nel quale la pagina può essere consultata e che è stabilita nello Stato stesso o in un altro Stato membro - dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in paesi terzi.
- 5) Le disposizioni della direttiva 95/46 non pongono, di per sé, una restrizione incompatibile con il principio generale di libertà di espressione, o con altri diritti e libertà vigenti all'interno dell'Unione europea e che trovano corrispondenza,

(*) Estratto del documento,
rinvenibile in
www.europa.eu.int/servlet/portail/CuriaServlet?curiaLink=%26lang%3DIT%26ident%3D7996893C19010101%26model%3Ddoc_curia

tra l'altro, nell'art. 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, firmata a Roma il 4 novembre 1950. Spetta alle autorità e ai giudici nazionali incaricati di applicare la normativa interna che traspone la direttiva 95/46 garantire il giusto equilibrio tra i diritti e gli interessi in gioco, ivi compresi i diritti fondamentali tutelati dall'ordinamento giuridico comunitario.

- 6) Le misure adottate dagli Stati membri per garantire la protezione dei dati personali devono essere conformi tanto alle disposizioni della direttiva 95/46 quanto al suo obiettivo, consistente nel mantenere un equilibrio tra la libera circolazione dei dati personali e la tutela della vita privata. Per contro, nulla impedisce che uno Stato membro estenda la portata della normativa nazionale di attuazione della direttiva 95/46 a settori non compresi nell'ambito di applicazione di quest'ultima, qualora non vi osti alcun'altra disposizione del diritto comunitario.

X - Consiglio d'Europa

77

Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance (20-23 May 2003)

INTRODUCTION

The Council of Europe's data protection committees wished to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe therefore asked a consultant, Dr Giovanni BUTTARELLI (Secretary General of the Italian Data Protection Authority), to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context. It was therefore agreed to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account in relation to video surveillance.

After examination of Mr Buttarelli's report and guiding principles, the CJ-PD agreed to re-elaborate and specify some of these guiding principles, and prepared the following text.

Many public and private entities have increasingly been using surveillance systems in different sectors for various purposes, in particular in order to control the movement of persons and goods and access to property, as well as events, situations and conversations - whether by telephone, over electronic networks or at a physical location.

Surveillance systems often result in the collection of personal data even though their collection and/or storage is sometimes not the aim of the surveillance data controller.

A considerable portion of these activities is performed by means of video surveillance devices, which raises specific issues as regards data protection.

Information collected during video surveillance activities often includes data (in the form of images and sounds) which directly or indirectly permit the identification of individuals, and the monitoring of their conduct. Moreover, video surveillance systems are increasingly converging with other technologies that raise new privacy and data protection concerns. These include the recording of sounds, wireless and high-speed computer networks used to transfer images; facial recognition systems integrated with computerised databases which can identify and track individuals; and devices that search under clothing and through walls, for example heat recognition devices or infra-red devices.

Video surveillance activities entailing the processing of personal data fall within the scope of application of the Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data [ETS No.108] (hereinafter Convention 108) -which was prepared when it became apparent that in order to ensure the effective legal protection of personal data it would be necessary to develop more specifically and systematically the general reference to respect for private life in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (hereinafter ECHR).