I Commissari europei per la protezione dei dati nutrono gravi dubbi sulla legalità e legittimità di misure di così vasta portata. Inoltre, essi desiderano richiamare l'attenzione sull'eccessivo livello dei costi di tali provvedimenti per l'industria di Internet e delle telecomunicazioni, e sull'assenza di provvedimenti siffatti negli Stati Uniti.

I Commissari europei per la protezione dei dati hanno ripetutamente sottolineato che simili provvedimenti costituirebbero un'impropria lesione dei diritti fondamentali garantiti ai cittadini dall'articolo 8 della Convenzione europea sui diritti dell'uomo, come ulteriormente specificato dalla giurisprudenza della Corte europea dei diritti dell'uomo (vedi parere 4/2001 del gruppo di lavoro di cui all'articolo 29 istituito in virtù della direttiva 95/46/CE e Dichiarazione di Stoccolma dell'aprile 2000).

La protezione dei dati di traffico delle telecomunicazioni è adesso prevista anche dalla direttiva 2002/58/CE del Parlamento europeo e del Consiglio relativa alla vita privata e alle comunicazioni elettroniche (Gazzetta ufficiale L 201/37), in base alla quale, in linea di principio, il trattamento dei dati di traffico è consentito a fini di contabilità e di riscossione dei canoni di collegamento. Dopo lungo e approfondito dibattito, è stato deciso che il mantenimento dei dati di traffico a fini di pubblica sicurezza debba essere strettamente subordinato alle condizioni di cui all'articolo 15 della direttiva, ossia, sempre e comunque, soltanto per un periodo limitato e qualora strettamente necessario, opportuno e proporzionato nell'ambito di una società democratica.

Perché i dati di traffico possano essere mantenuti in casi specifici, è quindi necessario che sussista una necessità dimostrabile in tal senso, che il periodo in cui vengono mantenuti sia più breve possibile e che tale attività venga esplicitamente regolata dalla legge, in maniera da garantire un'adeguata salvaguardia in caso di illecito accesso e qualsiasi altro abuso. L'archiviazione sistematica di tutti i tipi di dati di traffico per un periodo di un anno o più sarebbe chiaramente sproporzionata e quindi inaccettabile comunque.

I Commissari europei per la protezione dei dati si aspettano che il Gruppo di lavoro di cui all'articolo 29 venga consultato sui provvedimenti che potrebbero emergere dalle discussioni sul "terzo pilastro" prima della loro adozione.

(2) GU L 281 del 23/11/1995, pag. 31, disponibile presso: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

124 Documento di lavoro sulle "liste nere" (*)

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

11118/02/IT/def.
WP 65

Documento di lavoro sulle liste nere

Adottato il 3 ottobre 2002

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp65_it.pdf

125 Parere 6/2002 relativo alla trasmissione da parte delle compagnie aeree d'informazioni sugli elenchi dei passeggeri e di altri dati agli Stati Uniti (*)

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

11647/02/IT/def.
WP 66

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

costituito in base alla direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 [1],

visto l'articolo 29 e l'articolo 30, paragrafo 1, lettera a) e paragrafo 3 di tale direttiva,

visto il proprio regolamento interno, in particolare gli articoli 12 e 14,

ha adottato il seguente parere:

1. OGGETTO DI DISCUSSIONE

1.1 Contesto e finalità

In seguito agli avvenimenti dell'11 settembre 2001 [2] gli Stati Uniti hanno adottato il 19 novembre 2001 la legge sulla sicurezza del trasporto aereo (Aviation and Transportation Security Act) [3] la quale prescrive che le compagnie aeree che si trovano a volare in territorio statunitense debbano comunicare alle autorità competenti dati personali relativi ai passeggeri ed ai membri dell'equipaggio (Informazioni sugli elenchi dei passeggeri) [4]. Tale comunicazione deve avvenire per via elettronica ed essere completata prima del decollo dell'aereo, al più tardi 15 minuti dopo la partenza per quanto riguarda i dati personali dei passeggeri. Quantunque il "Commissario alle dogane" sia il destinatario dei dati inoltrati agli Stati Uniti, siffatti dati sono successivamente messi a disposizione di tutte le autorità federali statunitensi. La trasmissione dei dati personali non riguarda unicamente la sicurezza aerea ma negli Stati Uniti rappresenta altresì una questione d'ordine pubblico.

Il 14 maggio 2002 gli Stati Uniti hanno adottato un'altra legge per aumentare la sicurezza delle fron-

(*) Gruppo di lavoro sulla protezione dei dati - Articolo 29
Il Gruppo di lavoro è stato istituito a norma dell'articolo 29 della direttiva 95/46/CE. È un organismo consultivo europeo indipendente per la protezione dei dati personali e della vita privata. Le finalità dell'organismo sono stabilite all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. La segreteria ha la propria sede presso: Commissione europea, DG Mercato interno, "Funzionamento ed impatto del mercato interno; coordinamento; protezione dei dati". B-1049 Bruxelles - Belgio - Ufficio: C100-6/136
Telefono : linea diretta (+32 2) 299.27.19, centralino 299.11.11. Fax : 296.80.10
Indirizzo Internet: http://europa.eu.int/comm/privacy

(1) La Gazzetta Ufficiale n. L 281 del 23.11.1995, pag. 31 è consultabile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

(2) Prima dell'11 settembre 2001 le compagnie aeree trasmettevano già su base volontaria alcune informazioni agli Stati Uniti.

(3) Legge sulla sicurezza del trasporto aereo (Aviation and Transportation Security Act) del 19 novembre 2001 (107-71), Norme transitorie ("Interim Rules") del Dipartimento del Tesoro (Dogana) statunitense – Informazioni sugli elenchi dei passeggeri e dell'equipaggio richieste nell'ambito dei voli con passeggeri nel trasporto aereo internazionale verso gli Stati Uniti (Registro federale, 31 dicembre 2001) e Informazioni sui dati relativi ai nomi dei passeggeri richiesti nell'ambito dei voli passeggeri nel trasporto aereo internazionale da e verso gli Stati Uniti (Registro federale, 25 giugno 2002).

(4) I medesimi obblighi sono stati introdotti per il trasporto marittimo.

tiere, la quale dispone che le compagnie aeree trasmettano all'ufficio americano per l'immigrazione e la naturalizzazione le informazioni relative ai passeggeri e all'equipaggio dei loro voli in arrivo e in partenza dagli Stati Uniti [5]. Per i passeggeri e gli equipaggi che arrivano negli Stati Uniti, gli obblighi di comunicazione dei dati sono identici a quelli stabiliti dalle autorità doganali statunitensi. Per i passeggeri e gli equipaggi che partono dagli Stati Uniti tale comunicazione deve invece avvenire per via elettronica ed essere completata al più tardi 15 minuti dopo il decollo, con la possibilità di correggere ed aggiornare la lista dei passeggeri non oltre i 15 minuti successivi alla partenza. All'occorrenza l'ufficio per l'immigrazione e la naturalizzazione americano si riserva il diritto di richiamare a terra l'aereo entro un'ora dalla partenza.

Tutti i dati vanno trasmessi ad una banca di dati centralizzata [6] gestita congiuntamente dalle autorità doganali e dall'ufficio per l'immigrazione e la naturalizzazione. In un secondo momento essi sono messi a disposizione di altre agenzie federali e non sono più oggetto di una tutela specifica.[7]

1.2 Categorie di dati trasmessi

L'APIS (un acronimo di "Advanced Passenger Information System" - sistema avanzato d'informazione sui passeggeri) è stato oggetto di una serie di cambiamenti di rilievo che riguardano in particolare l'ampliamento della lista di dati. Inizialmente le informazioni richieste erano specificamente correlate al tipo di volo in oggetto, al visto o al permesso di soggiorno valido per gli Stati Uniti, nonché a dati a carattere identificativo contenuti, ad esempio, nei passaporti.

In particolare le più recenti disposizioni statunitensi in merito alla sicurezza delle frontiere prescrivono che per i voli in partenza ed in arrivo dagli Stati Uniti, vengano comunicati i seguenti dati all'ufficio per l'immigrazione americano: nome, data di nascita, nazionalità, sesso, numero di passaporto e luogo di rilascio, stato di residenza, numero del visto americano, data e luogo di rilascio (all'occorrenza), numero di registrazione estero (all'occorrenza), indirizzo durante la permanenza negli Stati Uniti ed ogni altro dato ritenuto significativo per l'identificazione dei viaggiatori e per l'applicazione delle disposizioni in tema d'immigrazione e protezione della sicurezza nazionale e dell'incolumità personale [8].

È altresì prescritto che vengano a richiesta comunicati anche i dati trattati nei sistemi di prenotazione e controllo delle partenze (Departure control systems - DCS), in particolare quelli contenuti nei registri dei nomi dei passeggeri (Passenger Name Records - PNR) [9]. Tali dati non si limitano ai soli passeggeri in arrivo nel territorio statunitense e possono variare notevolmente da compagnia a compagnia. Essi riguardano: dati d'identificazione [10] (cognome, nome, data di nascita, numero di telefono); numero di prenotazione PNR, giorno della prenotazione, al caso l'agenzia di viaggio, informazioni presenti sul biglietto; informazioni di natura finanziaria (numero della carta di credito, data di scadenza, indirizzo di fatturazione ecc.); itinerario, informazioni sul volo fornite dal vettore (numero del volo ecc.), numero del posto assegnato nonché precedenti dati del sistema PNR. Tra questi ultimi possono rientrare non solo viaggi precedentemente effettuati ma anche informazioni a carattere religioso ed etnico (scelta del pasto ecc.), affiliazione ad un particolare gruppo, informazioni concernenti il luogo di residenza o contatti personali (indirizzo di posta elettronica, dettagli su un amico, luogo di lavoro ecc.), informazioni mediche (qualsiasi richiesta di assistenza sanitaria, ossigeno, problemi di vista, udito, mobilità o di ogni altra sorta la cui comunicazione è necessaria per garantire un volo soddisfacente) ed altri tipi di dati connessi, ad esempio, a programmi per clienti abituali (numero d'identificazione corrispondente) [11].

(5) Legge per aumentare la sicurezza delle frontiere (Enhanced Border Security) e legge sulla riforma dei visti d'ingresso (Visa Entry Reform Act) del 2002; si veda anche la legge sull'immigrazione e le nazionalità (Immigration and Nationality Act).

(6) Il sistema interagenzie di ispezione delle frontiere (IBIS - Interagency Border Inspection System).

(7) Alcune di queste informazioni possono all'occorrenza essere rese pubbliche conformemente alla legge in tema di accesso all'informazione in possesso del settore pubblico.

(8) Decisione del procuratore generale di concerto con il segretario di stato ed il segretario del tesoro.

(9) Norma transitoria (Registro federale, 25 giugno 2002), Registro dei nomi dei passeggeri richiesto nell'ambito dei voli con passeggeri nel trasporto aereo internazionale da e verso gli Stati Uniti.

(10) E' espressamente indicato che tale lista "intende illustrare unicamente i dati cui le autorità doganali possono richiedere di avere accesso".

(11) Questi dati, contenuti nelle norme transitorie ("interim rules") e pubblicati dal Dipartimento delle dogane (Department of Customs), non sono pero' presenti in quanto tali nella legge 107-71.

Per tutti i paesi che aderiscono al programma per l'esenzione dall'obbligo del visto (Visa Waiver Program) diverrà inoltre obbligatorio a partire da ottobre 2004 la trasmissione dei dati biometrici [12].

1.3 Sanzioni

La mancata trasmissione delle informazioni richieste o una loro trasmissione non corretta o incompleta è punibile con severe sanzioni, quali la perdita dei diritti di atterraggio ed il pagamento di pesanti ammende [13].

A questo riguardo il gruppo di lavoro s'interroga sulla compatibilità di tali provvedimenti unilaterali con gli accordi e le convenzioni internazionali in merito al trasporto e al traffico aereo nonché con le disposizioni applicabili a livello nazionale nel rispetto per quanto riguarda i paesi in cui le compagnie aeree operano in modo permanente.

1.4 Estensione ad altri paesi

Altri paesi quali Canada, Messico [14], Australia, Nuova Zelanda, Sudafrica e Regno Unito hanno già applicato o prevedono di porre in essere provvedimenti simili atti a soddisfare le proprie esigenze.

2. COMPATIBILITÀ' CON LA DIRETTIVA 95/46/CE

2.1 Attuazione della direttiva

I dati trasmessi dalle compagnie aeree si riferiscono a persone fisiche identificate ed in seno all'Unione europea il loro trattamento, è affidato in alle varie compagnie aeree (raccolta, registrazione, modificazione, archiviazione, rettificazione, estrazione, utilizzo, comunicazione ecc.). In quanto tali, siffatti dati sono soggetti alle disposizioni contenute nella direttiva 95/46/CE.

Lo sviluppo del sistema APIS solleva inoltre questioni specifiche, presentate nel seguito di cui molte trascendono la sfera di competenza delle singole compagnie aeree. Queste ultime si trovano spesso dinanzi ad un dilemma poiché, se da un canto sono tenute ad osservare le misure nazionali di esecuzione della direttiva 95/46/CE in tema di protezione dei dati personali, dall'altro la legislazione statunitense le obbliga alla comunicazione di questi stessi dati per mezzo di sanzioni severe.

2.2 Informazione degli interessati

Le persone interessate dal trasferimento dei propri dati personali devono esserne necessarie a garantirne un trattamento adeguato. Nel novero di tali informazioni dovrebbero rientrare le finalità specifiche del trattamento nonché i destinatari di tali dati.

Non è giustificabile un ricorso all'articolo 13 della direttiva 95/46/CE al fine di limitare quest'obbligo quando la comunicazione avviene in modo sistematico e le categorie di dati richieste sono state già parzialmente rese note al pubblico degli Stati Uniti mediante la pubblicazione della normativa. Più specificamente, tali informazioni dovrebbero essere fornite agli interessati nel momento stesso in cui i dati vengono rilevati e concernere tra l'altro le finalità ultime di trattamento negli Stati Uniti e i destinatari di siffatti dati [15].

2.3 Misure di sicurezza

A norma della direttiva 95/46/CE le compagnie aeree sono tenute ad applicare misure di sicurezza idonee per la protezione dei dati personali. Tale obbligo non contempla eccezioni. Si ritiene che le misure di natura tecnica imposte alle compagnie aeree dagli Stati Uniti consentano l'accesso ai dati da parte di terzi non autorizzati.

2.4 Osservanza del principio di finalità

Dati gli sviluppi recenti del sistema, la comunicazione dei dati personali descritta al precedente para-

(12) Sezione 203 della legge per aumentare la sicurezza delle frontiere (Enhanced Border Security), e della legge sulla riforma dei visti d'ingresso (Visa Entry Reform Act) del 2002.

(13) Circa 5000 dollari per errore da corrispondere alle autorità doganali statunitensi (in casi, ad esempio, di errore riguardante il nome del passeggero o altre categorie di dati al di sotto della media settimanale accettata) e di circa 1000 per comunicazione erronea del nome all'ufficio per l'immigrazione e la naturalizzazione.

(14) Anche il Messico trasmetterà tutti i dati in suo possesso sui voli in arrivo dagli Stati Uniti verso il proprio territorio.

(15) Tale disposizione non si applica se gli interessati sono sospetti sotto inchiesta.

grafo 1.2 (che va oltre la tipologia limitata di dati forniti normalmente dai passeggeri in occasione dell'organizzazione di un viaggio) non può considerarsi compatibile con le finalità originarie di raccolta dei dati personali da parte di compagnie aeree ed agenzie di viaggi, in particolare nell'ambito del rispetto degli obblighi contrattuali nei confronti dei passeggeri. L'articolo 6, paragrafo 1, lettera b) della direttiva 95/46/CE vieta che vengano successivamente trattati dati raccolti per finalità determinate, esplicite e legittime, in modo incompatibile con tali finalità.

Tenuto conto della grande e multiforme quantità di dati in gioco, è impossibile ritenerli adeguati, pertinenti e non eccedenti rispetto alle finalità per cui vengono rilevati e/o successivamente trattati a norma dell'articolo 6, paragrafo 1, lettera c) della direttiva 95/46/CE.

Rimane tuttavia la possibilità di ricorrere all'articolo 13 della direttiva 95/46/CE, il quale autorizza gli Stati membri ad adottare provvedimenti legislativi miranti a circoscrivere la portata di questi due obblighi nella misura in cui tale restrizione si renda necessaria per la salvaguardia degli interessi elencati nella stessa direttiva (prevenzione e inchieste penali, sicurezza pubblica, ecc.). È ovviamente auspicabile che gli Stati membri seguano un'impostazione comune in materia.

2.5 Flussi transfrontalieri di dati

La direttiva 95/46/CE dispone che il trasferimento di dati personali in un paese terzo sia consentito solo se ed in quanto il paese in questione è in grado di assicurare un adeguato livello di protezione. Lo sviluppo del sistema APIS solleva a questo proposito, alcune perplessità. Il trattamento di dati trasmessi dalle compagnie aeree da parte delle autorità federali statunitensi non ottempera pienamente a tale condizione [16]. L'ambito ristretto di applicazione dell' "approdo sicuro" (Safe Harbor) non consente una sua applicazione a salvaguardia della protezione del trasferimento dei dati in favore delle autorità governative.

Le deroghe contemplate all'articolo 26 della direttiva 95/46/CE non sembrano altresì applicabili.

– Attualmente, il requisito del consenso inequivocabile non costituisce una soluzione adeguata perché giacché per molti versi continuano a sussistere forti perplessità. Non sembra infatti che il consenso del passeggero venga richiesto in ogni caso a differenza di quanto previsto dalla normativa in vigore. La direttiva 95/46/CE definisce il consenso come qualsiasi manifestazione di volontà libera, specifica ed informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento. Tale consenso può' risultare difficile da ottenere non da ultimo a causa delle difficoltà pratiche da affrontare quando si vogliano comunicare chiaramente tutte le informazioni necessarie ai passeggeri che acquistano un biglietto aereo nell'ambito di sistemi globali i quali consentono di prenotare un volo dall'Unione europea verso gli Stati Uniti a partire da quasi tutti i paesi del mondo, attraverso molteplici canali (diverse compagnie aeree, agenzie di viaggio, ecc.). Le informazioni fornite agli interessati devono includere le indicazioni stabilite agli articoli 10 e 11 della direttiva in oggetto, compresa, all'occorrenza, l'inadeguatezza della tutela nei paesi terzi.

– È difficile invocare la necessità del trasferimento ai fini dell'esecuzione di un contratto tra gli interessati e il responsabile del trattamento dei dati vista la portata dei dati trasmessi. La comunicazione di grandi quantità di dati non può infatti essere considerata "necessaria" ai fini dell'esecuzione di un contratto. L'impossibilità fisica per le compagnie aeree di adempiere ai propri obblighi contrattuali in seguito alla perdita ei diritti non rappresenta in questo caso una condizione sufficiente. È inoltre impossibile applicare siffatta eccezione a tutela della comunicazione di dati attinenti a persone non dirette verso gli Stati Uniti.

– Risulta parimenti impossibile la comunicazione di dati invocata in nome della salvaguardia d'importanti interessi pubblici. In primo luogo non è dimostrata la necessità di tale comunicazione; secondariamente, non è accettabile che una decisione unilaterale adottata da un paese terzo nel proprio interesse pubblico debba portare al trasferimento in massa d'informazioni tutelate a norma della presente direttiva.

(16) La normativa sulla vita privata, applicabile alle autorità federali statunitensi, tutela solo i dati relativi ai cittadini americani.

– E' infine difficile legittimare la liceità della comunicazione di siffatti dati per finalità connesse alla tutela degli interessi vitali delle persone coinvolte.

La direttiva 95/46/CE autorizza nondimeno il trasferimento dei dati personali in presenza di un adeguato livello di protezione all'interno del paese terzo quando il responsabile del trattamento (destinatario) è in grado di fornire garanzie sufficienti per la tutela dei dati personali.

Sarebbe pertanto auspicabile un negoziato tra Stati membri dell'Unione ed autorità statunitensi per trovare una soluzione atta ad assicurare livelli adeguati di protezione per i dati trasmessi.

2.6 Problemi specifici attinenti alla comunicazione ed all'accesso ai dati PNR trattati nell'ambito di sistemi telematici di prenotazione e di controllo delle partenze

Le osservazioni fatte a questo riguardo integrano quelle già presentate.

2.6.1 Collegamenti elettronici diretti tra il servizio doganale statunitense e i sistemi di prenotazione e controllo delle partenze

Nei casi in cui sia preferibile che il servizio doganale americano possa accedere direttamente ai sistemi informativi ubicati sul territorio europeo, per selezionare e raccogliere i dati, invece di essere il destinatario convenzionale di flussi transfrontalieri d'informazione, tutte le disposizioni contenute nella direttiva possono essere direttamente e pienamente applicate. L'articolo 4, paragrafo 1, lettera c) dispone le modalità d'applicazione della direttiva nei casi in cui il responsabile del trattamento non sia stabilito nel territorio della comunità e ricorra, ai fini del trattamento di dati personali, a strumenti, automatizzati o no situati sul territorio di uno Stato membro [17]. La piena applicazione di questa direttiva presenta ancora molti aspetti controversi.

2.6.2 Informazioni riguardanti viaggiatori non diretti negli Stati Uniti

Le informazioni riguardanti viaggiatori non diretti negli Stati Uniti non sono rilevanti e possono quindi non essere trasmesse, fatto salvo un eventuale impiego nell'ambito di specifici accordi in tema di giustizia e affari interni (assistenza reciproca).

2.6.3 Dati sensibili

Il registro PNR può contenere dei dati in grado di rivelare l'origine etnica o razziale, il credo religioso, o altri dati sensibili a termini dell'articolo 8 della direttiva 95/46/CE. Tale direttiva vieta in linea di massima qualsiasi tipo di trattamento dei dati sensibili fatto salvo il caso di autorizzazioni specifiche (consenso esplicito al trattamento per un determinato fine, informazioni di ovvia natura pubblica, ecc.) Come già visto, il ricorso al consenso crea molti problemi che dovrebbero essere tenuti in maggior considerazione data la natura estremamente delicata di siffatte informazioni [18].

L'articolo 8, paragrafo 4 della direttiva autorizza gli Stati membri o le autorità di controllo a stabilire ulteriori deroghe per seri motivi di interesse pubblico purché siano previste le opportune garanzie. In tali condizioni gli Stati membri potrebbero conseguentemente autorizzare il trasferimento di dati sensibili contenuti nel registro PNR [19].

2.6.4 Trattamento dei dati in sistemi di prenotazione e controllo delle partenze (DCS)

Il problema dell'accesso al registro PNR su richiesta delle autorità statunitensi solleva immediatamente la questione della legittimità del trattamento dei dati all'interno dei sistemi di prenotazione e con-

(17) Il ventesimo considerando della direttiva 95/46/CE rileva che la tutela delle persone disposta dalla presente direttiva non è ostacolata dal fatto che il responsabile del trattamento sia stabilito in un paese terzo; 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. In un parere recentemente espresso in merito all'interpretazione del campo di applicazione dell'articolo 4, paragrafo 1, lettera c) della direttiva (Documento di lavoro sulla determinazione dell'applicazione internazionale della normativa comunitaria in materia di tutela dei dati al trattamento dei dati personali su Internet da parte di siti Web non stabiliti nell'UE - 30 maggio 2002), il gruppo di lavoro (ex articolo 29) ha fatto notare come non occorra che il responsabile del trattamento eserciti un pieno controllo sugli strumenti ma sia importante che egli determini quali dati sono rilevati, archiviati, trasferiti, modificati, ecc., e con quali finalità.

(18) Conformemente all'articolo 8, paragrafo 2, lettera a) della direttiva, le normative degli Stati membri possono disporre che il divieto di trattamento dei dati personali di cui all'articolo 8, paragrafo 1 della direttiva in questione non debba applicarsi nel caso in cui l'interessato abbia dato il proprio consenso esplicito.

(19) Continua ad applicarsi l'articolo 13 della direttiva.

trollo delle partenze [20]. Tali dati possono essere utilizzati se ritenuti adeguati, rilevanti e non eccessivi rispetto alle finalità in base alle quali vengono trattati. I dati personali non dovrebbero più essere inseriti nei sistemi di prenotazione poiché il loro impiego non è più finalizzato al viaggio in occasione del quale vengono registrati.

2.7 Comunicazione di dati biometrici

La comunicazione di dati biometrici è disciplinata dalla direttiva 95/46/CE. Occorre notare che tale direttiva obbliga gli Stati membri a determinare a quali condizioni un mezzo identificativo di portata generale può essere oggetto di trattamento. Gli identificatori biometrici consentono unicamente l'identificazione d'individui e potrebbero pertanto formare l'oggetto di questa stessa norma [21].

Conclusioni

1. Il gruppo di lavoro riconosce che Stati sovrani possono decidere circa le categorie di dati da richiedere a chi intende accedere al loro territorio. Le proposte attuali attinenti al sistema APIS, benché legittimate da un contesto storico di nefandezze terroristiche, comporterebbero tuttavia una diffusione sproporzionata e sistematica di dati da parte delle compagnie aeree la cui attività è soggetta alle disposizioni della direttiva 95/46/CE. Tali dati potrebbero essere usati quotidianamente per fini doganali e legati all'immigrazione e, più in generale, per motivi di sicurezza nazionale americana e potrebbero così essere diffusi quanto meno tra tutte le agenzie federali.

2. Alla luce della recente evoluzione del sistema APIS il gruppo di lavoro ritiene che il rispetto delle prerogative statunitensi crei difficoltà nell'applicazione della direttiva 95/46/CE. Molti dei problemi in questione trascendono la sfera delle singole compagnie aeree e ricadono nella sfera di competenza degli Stati membri e, conseguentemente, della Commissione.

3. In definitiva, stando al parere del gruppo di lavoro la comunicazione di dati relativi a viaggiatori non diretti verso gli Stati Uniti non dovrebbe essere autorizzata fatto salvo il loro impiego nell'ambito di specifici accordi di cooperazione in tema di giustizia ed affari interni.

4. Qualsiasi altro tipo di trasferimento di dati effettuato a partire da sistemi di prenotazione e di controllo delle partenze relativi ai passeggeri ed ai membri dell'equipaggio è possibile solo nel rispetto delle normative in vigore negli Stati membri.

Tali normative devono disporre che le necessarie restrizioni su diritti ed obblighi soggetti alla direttiva 95/46/CE siano conformi all'articolo 13 di tale direttiva, e che siano poste in essere le garanzie a tutela delle persone interessate.

È auspicabile che si persegua un approccio comune a livello comunitario.

5. Occorre ponderare attentamente la comunicazione di dati che possono essere considerati alla stregua di dati sensibili. Tali comunicazioni necessitano infatti all'occorrenza di prove atte a dimostrare l'esistenza di 1) motivi di interesse pubblico rivelante per gli Stati membri, 2) garanzie appropriate e 3) talvolta di una legislazione nazionale in materia o di una decisione dell'autorità di controllo.

6. Qualora si ritenga inoltre necessario l'accesso diretto da parte del servizio doganale o del servizio per l'immigrazione e la naturalizzazione statunitense ai dati contenuti nei sistemi di prenotazione e controllo delle partenze, tali autorità sono tenute a garantire il pieno rispetto della direttiva.

7. Il sistema dovrebbe essere concordato con le autorità statunitensi. Il negoziato dovrebbe vertere specificamente sul chiarimento e la definizione di obiettivi, finalità e destinatari dei dati nonché sulle categorie di dati che possono essere trasferiti, tenuto conto delle presenti osservazioni nonché dell'in-

(20) Si veda la raccomandazione 1/98 in materia di sistemi telematici di prenotazione nel trasporto aereo che dispone, per regolare le controversie e trattare i dati relativi ai clienti abituali, una loro archiviazione limitata ad un determinato arco temporale, previo ottenimento del consenso delle persone interessate. Il gruppo di lavoro ex articolo 29 ritiene che l'archiviazione dei dati reperiti on-line debba essere limitata a sole 72 ore e che la loro distruzione avvenga ai più tardi entro i tre anni successivi (con un accesso ristretto per richieste di indagini) o in tempi ancor più lunghi (solo ai fini dell'adempimento di un obbligo legale).

(21) Il dibattito sui dati biometrici è attualmente in corso presso il gruppo di lavoro.

sieme delle condizioni e garanzie che caratterizzano il processo di trattamento dei dati personali, con particolare riguardo ad una loro diffusione presso le autorità federali statunitensi (ed in tal caso una comunicazione limitata alle sole autorità incaricate dell'applicazione della legge).

8. Nei casi di comunicazione di dati personali da parte delle compagnie aeree agli Stati Uniti è preferibile un'impostazione di tipo globale. Occorrerebbe in primo luogo tenere conto di altre comunicazioni programmate o in corso verso gli Stati Uniti. A tal proposito di particolare interesse potrebbe risultare l'introduzione del concetto del terzo pilastro. Ciò significa che i trasferimenti alle autorità pubbliche di paesi terzi di dati richiesti per motivi d'ordine pubblico all'interno di questi stessi paesi andrebbero analizzati nel più ampio contesto dei meccanismi di cooperazione fissati nell'ambito del terzo pilastro (cooperazione giudiziaria e di polizia). Questi ultimi dovrebbero inoltre andare di pari passo con le garanzie a tutela delle informazioni comunicate.[22] Tali meccanismi di cooperazione concordati nell'ambito del terzo pilastro non devono essere elusi ricorrendo al primo pilastro. La soluzione elaborata per comunicare i dati verso gli Stati Uniti potrebbe infine rivelarsi utile anche per i trasferimenti APIS verso altri paesi terzi.

Fatto a Bruxelles, 24 ottobre 2002

Per il gruppo di lavoro
Il presidente
Stefano RODOTA

(22) I dati personali sono esportati dagli Stati membri ai fini della cooperazione giudiziaria e di polizia. Tali dati sono stati trasferiti da Europol per analizzare gli avvenimenti dell'11 settembre 2001 come parte di una procedura eccezionale. E' attualmente in corso un dibattito per creare una cooperazione stabile conformemente alle disposizioni della convenzione Europol (articolo 18). Si veda altresì la decisione Eurojust (articolo 27) ed i negoziati in corso sull'articolo 38 del trattato.

126 Documento di lavoro sul trattamento di dati personali tramite videosorveglianza (*)

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

11750/02/IT
WP 67

IL GRUPPO DI LAVORO PER LA TUTELA DELLE PERSONE RIGUARDO AL TRATTAMENTO DI DATI PERSONALI

istituito dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995 [1],
visti gli articoli 29 e 30, paragrafo 1, lettera a), e paragrafo 3, di detta direttiva,
visto il regolamento interno, in particolare gli articoli 12 e 14,

HA ADOTTATO IL PRESENTE DOCUMENTO DI LAVORO:

1. INTRODUZIONE

Negli ultimi anni, gli organismi pubblici e privati in Europa hanno fatto sempre maggior ricorso ai sistemi di acquisizione di immagini. Tale circostanza ha suscitato un acceso dibattito tanto a livello comunitario quanto a quello dei singoli Stati membri al fine di identificare presupposti e restrizioni applicabili all'installazione di attrezzature di videosorveglianza, nonché le necessarie garanzie per le persone interessate.

Dall'esperienza acquisita negli ultimi anni, anche a seguito del recepimento, a livello nazionale, della direttiva 95/46/CE, si constata un'enorme proliferazione di sistemi a circuito chiuso, videocamere e altri strumenti più sofisticati utilizzati nei settori più diversi.

Inoltre, lo sviluppo delle tecnologie disponibili, digitalizzazione e miniaturizzazione, aumentano notevolmente le possibilità offerte dai dispositivi di registrazione di immagini e suoni, anche in relazione con la loro utilizzazione in intranet e Internet.

Oltre alle operazioni di trattamento nel contesto dell'occupazione, trattate dal gruppo di lavoro in un documento particolare (parere 8/2001 sul trattamento di dati personali nell'ambito dell'occupazione [2]), la crescente proliferazione delle tecniche di videosorveglianza può essere facilmente rilevata da tutti i cittadini.

Un'analisi non esaustiva delle principali applicazioni dimostra che la videosorveglianza può servire a

(*) Gruppo di lavoro per la tutela dei dati personali - Articolo 29
Il gruppo di lavoro è stato istituito ai sensi dell'articolo 29 della direttiva 95/46/CE. È un organo europeo indipendente a carattere consultivo in materia di tutela dei dati e della vita e della vita privata. I suoi compiti sono illustrati all'articolo 30 della direttiva 95/46/CE e all'articolo 14 della direttiva 97/66/CE. Le funzioni di segretariato sono espletate dalla Direzione E (Servizi, Proprietà intellettuale e industriale, Media e Protezione dei dati) della Commissione europea, Direzione generale mercato interno, B-1049 Bruxelles, Belgio, Ufficio n. C100-6/136.
Website: www.europa.eu.int/comm/privacy
(1) Gazzetta ufficiale n. L 281 del 23/11/1995, pag. 31, disponibile su: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm
(2) WP 48, adottato il 13 settembre 2001, disponibile su: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

fini molteplici [3], che possono essere raggruppati peraltro in alcuni settori principali:

1) protezione degli individui,
2) protezione della proprietà,
3) interesse pubblico,
4) scoperta, prevenzione e controllo delle infrazioni,
5) presentazione di prove,
6) altri interessi legittimi.

Requisiti di vario genere si applicano inoltre agli impianti di videocamere e dispositivi simili.

In alcuni casi, l'utilizzazione di un sistema di videoregistrazione può essere effettivamente obbligatoria, sulla base di disposizioni specifiche degli Stati membri – ciò è stato il caso, ad esempio, in alcuni casinò - oppure per fini ai quali i familiari delle persone in causa attribuiscono speciale importanza – ad esempio ricerca di bimbi e adulti dispersi. D'altro canto, si possono menzionare casi di utilizzo stravagante – principalmente in paesi terzi – nei quali sono stati usati sistemi di riconoscimento facciale per evitare la bigamia oppure quando un'autorità di polizia ha deciso di divulgare immagini della vita difficile condotta nelle prigioni, senza il consenso dei detenuti.

Di conseguenza, se da un lato la videosorveglianza può apparire in certo qual modo giustificata in particolare circostanze, esistono però casi in cui impulsivamente si ricerca la protezione per mezzo di videocamere senza considerare adeguatamente le condizioni e le disposizioni applicabili. Talvolta questo è dovuto tanto ai benefici economici concessi su larga scala dagli organismi pubblici quanto all'offerta di condizioni assicurative migliori in relazione all'utilizzo di attrezzature di videosorveglianza.

Si tratta quindi di un settore diversificato, in continua evoluzione, nel quale molte tecniche sono già disponibili.

Obiettivo del presente documento di lavoro è quello di fornire un'analisi iniziale, partendo dall'esistenza di regolamenti parzialmente diversi nonché dall'esistenza di disposizioni esageratamente particolareggiate nelle varie legislazioni nazionali, per cui è necessario un approccio più sistematico ed armonizzato.

Il presente documento di lavoro riguarda la sorveglianza mirante al controllo a distanza di eventi, situazioni e avvenimenti, mentre non considera direttamente altri casi in cui certi avvenimenti vengono pubblicizzati su base occasionale e/o abituale, ad esempio in relazione con la trasparenza delle attività di enti locali e/o organismi parlamentari.

Ogni operatore sarà quindi in grado di specificare ulteriormente le indicazioni qui fornite, sia nel rispettivo settore sia per quanto riguarda i futuri sviluppi tecnologici che il gruppo di lavoro intende analizzare.

Inoltre, i principi di cui si tiene conto in questa sede si applicano all'acquisizione di immagini, even-

(3) Sistemi di videosorveglianza di vario genere sono installati:
a) all'interno e in prossimità di edifici di accesso pubblico e/o privato, ad esempio musei, luoghi di culto o monumenti, al fine di evitare infrazioni e/o atti minori di vandalismo,
b) presso stadi e impianti sportivi, specialmente in relazione con determinate manifestazioni,
c) nel settore dei trasporti e in relazione con il traffico stradale, al fine di sorvegliare il traffico delle autostrade, oppure per rilevare infrazioni per eccesso di velocità e/o infrazioni del regolamento del traffico in zone urbane, oppure ancora per controllare locali sotterranei che danno accesso alle linee della metropolitana, controllare stazioni di rifornimento e l'interno dei taxi,
d) per evitare e/o rilevare comportamenti illegali in prossimità delle scuole, anche in relazione con l'adescamento dei minori,
e) presso installazioni mediche durante operazioni chirurgiche e/o, ad esempio, per prestare cure a distanza o controllare pazienti nelle unità di rianimazione e/o in zone in cui sono ricoverati pazienti gravemente malati e/o in quarantena,
f) negli aeroporti, a bordo di imbarcazioni e in prossimità delle zone di frontiera, al fine di controllare le entrate clandestine di stranieri, come pure per facilitare la ricerca di minori e di altre persone disperse,
g) dagli investigatori privati,
h) all'interno e in prossimità di supermercati e di negozi, specialmente di articoli di lusso, al fine di presentare prove in caso di infrazioni, come pure per promuovere prodotti e/o elaborare un profilo dei clienti,
i) presso condomini privati e zone adiacenti, sia per ragioni di sicurezza sia per presentare prove in caso di infrazione,
j) a fini giornalistici e pubblicitari, mediante webcam o videocamere on-line utilizzate per la promozione turistica e pubblicitaria, anche relativamente a stazioni balneari e locali da ballo, filmando su base regolare clienti e visitatori senza alcun preavviso.

tualmente in associazione con dati sonori e/o biometrici, ad esempio le impronte digitali [4].

I principi sopra menzionati possono essere altresì presi in considerazione, ove concretamente applicabili, in relazione al trattamento di dati personali non effettuato da attrezzature video ma tramite altri tipi di sorveglianza, ad esempio controllo a distanza, com'è il caso, ad esempio, con i sistemi GPS via satellite.

Il presente documento di lavoro mira anzitutto ad attirare l'attenzione sulla vasta gamma di criteri di valutazione della legittimità e dell'adeguatezza in materia di installazione di vari sistemi di videosorveglianza.

Si è peraltro tenuto conto degli aspetti seguenti:

a) occorre che le istituzioni competenti degli Stati membri valutino la videosorveglianza da un punto di vista generale, anche al fine di promuovere un approccio globalmente selettivo e sistematico della questione. L'eccessiva proliferazione di sistemi di acquisizione di immagini in zone pubbliche e private non dovrà tradursi nell'applicazione di ingiustificate restrizioni dei diritti e delle libertà fondamentali dei cittadini; in caso contrario, i cittadini sarebbero effettivamente obbligati a sottoporsi a procedure sproporzionate di raccolta di dati, il che li renderebbe identificabili in massa in numerosi posti pubblici e privati.

b) Le tendenze che riguardano l'evoluzione delle tecniche di videosorveglianza potrebbero essere valutate utilmente per evitare che lo sviluppo di applicazioni di software basate sia sul riconoscimento facciale sia sullo studio e sulla previsione del comportamento umano si traducano avventatamente in una sorveglianza dinamico-preventiva, al contrario della sorveglianza statica convenzionale, che si prefigge principalmente di documentare avvenimenti specifici e i loro autori. Questa nuova forma di sorveglianza si basa sull'acquisizione automatica dei lineamenti degli individui, come pure sulla loro condotta "anormale" in associazione con la disponibilità di allarmi e avvisi automatizzati, che potrebbero implicare pericoli di discriminazione.

2. STRUMENTI GIURIDICI INTERNAZIONALI.

a) Convenzione per i diritti umani e le libertà fondamentali

La protezione della vita privata è garantita dall'articolo 8 della Convenzione sui diritti umani.

b) Convenzione n. 108/1981 del Consiglio d'Europa per la protezione delle persone relativamente al trattamento automatizzato di dati a carattere personale.

L'ambito di questa Convenzione non è limitato, come la direttiva 95/46/CE, alle attività di primo pilastro (vedi sotto). Le attività di videosorveglianza che comportano il trattamento di dati personali rientrano nel campo d'applicazione di tale Convenzione. Il comitato consultivo istituito da tale convenzione ha affermato che voci e immagini sono considerate dati personali, ove esse forniscano informazioni su un individuo rendendolo, anche se indirettamente, identificabile.

Il Consiglio d'Europa sta attualmente elaborando una serie di principi di orientamento per la protezione degli individui rispetto alla raccolta e al trattamento di dati tramite videosorveglianza. Tali principi dovrebbero specificare ulteriormente le garanzie applicabili alle persone interessate, contemplate nelle disposizioni degli strumenti del Consiglio d'Europa.

c) Carta dei diritti fondamentali dell'Unione europea

La Carta dei diritti fondamentali dell'Unione europea dispone, all'articolo 7, la protezione della vita privata e familiare, del domicilio e delle comunicazioni, mentre l'articolo 8 riguarda la protezione di dati di carattere personale.

3. SORVEGLIANZA AI SENSI DELLA DIRETTIVA 95/46/CE.

Le caratteristiche specifiche del trattamento delle informazioni personali incluse in dati sonori e visivi sono state espressamente sottolineate dalla direttiva 95/46/CE (di seguito denominata "la direttiva") che le menziona espressamente in vari punti.

(4) L'aspetto più generale dell'applicazione della direttiva 95/46/CE alla biometria sarà trattato dal gruppo di lavoro in un documento a parte.

La direttiva garantisce la protezione della vita privata nonché la protezione più ampia di dati personali relativamente alla tutela dei diritti e delle libertà fondamentali delle persone fisiche (articolo 1, paragrafo 1).

Una parte notevole delle informazioni raccolte per mezzo della videosorveglianza riguarda persone identificate e/o identificabili filmate quando frequentavano locali pubblici e/o di accesso pubblico. Persone del genere, in transito, potrebbero sì prevedere un minore livello di riserbo, ma non di essere private totalmente dei propri diritti e libertà anche riguardo alla propria sfera ed immagine privata.

In questo contesto occorre anche considerare il diritto alla libera circolazione delle persone che si trovano legalmente nel territorio di uno Stato, diritto tutelato dall'articolo 2 del protocollo n. 4 addizionale della Convenzione europea per la protezione dei diritti dell'uomo e delle libertà fondamentali.

Tale libertà di circolazione può essere oggetto di restrizioni necessarie in una società democratica, e proporzionate al raggiungimento di fini specifici. Le persone interessate hanno il diritto di esercitare la propria libertà di circolazione senza dover essere soggette ad eccessivi condizionamenti psicologici quanto ai loro movimenti e comportamento e senza dover essere sottoposte ad un controllo particolareggiato, come quello del loro comportamento a seguito dell'applicazione sproporzionata della videosorveglianza in vari locali pubblici e/o di accesso pubblico.

Nelle parti iniziali della direttiva vengono sottolineate la specificità e la sensibilità del trattamento di dati in forma di suoni e immagini relative alle persone fisiche. Oltre alle considerazioni che verranno formulate di seguito quanto al campo d'applicazione, tali assunti ed i rispettivi articoli della direttiva chiariscono che:

a) la direttiva si applica, in linea di massima, a questo caso tenendo conto altresì dell'importanza degli sviluppi delle tecniche utilizzate per captare, manipolare o altrimenti utilizzare la categoria specifica di dati personali raccolti in questo modo (cfr. considerando n. 14),

b) i principi di protezione della direttiva si applicano a qualsiasi informazione – incluse quelle sotto forma di suoni e immagini – concernenti una persona identificata o identificabile, prendendo in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona (cfr. articolo 2, lettera a), e considerando n. 26).

Oltre ai riferimenti specifici sopra menzionati, la direttiva ovviamente produce tutti i suoi effetti nel quadro delle sue disposizioni individuali riguardanti, in particolare:

1) Qualità dei dati. Le immagini devono essere trattate lealmente e lecitamente per finalità determinate, esplicite e legittime. Le immagini debbono essere utilizzate conformemente al principio che i dati debbono essere adeguati, pertinenti e non eccedenti e non trattati successivamente in modo incompatibile con tali finalità; essi vanno conservati per un periodo limitato, ecc. (cfr. articolo 6),

2) Principi relativi alla legittimazione del trattamento dei dati. In base a tali principi, il trattamento di dati personali tramite videosorveglianza va fondato almeno su uno dei requisiti preliminari di cui all'articolo 7 – consenso inequivocabile, necessità per obblighi contrattuali, per osservanza ad un obbligo legale, per la protezione degli interessi vitali della persona interessata, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, equilibrio degli interessi,

3) Trattamento di categorie particolari di dati, soggetto alle garanzie applicabili all'utilizzazione di dati sensibili o di dati concernenti infrazioni nell'ambito della videosorveglianza (conformemente all'articolo 8),

4) Informazioni da fornire alla persona interessata (cfr. articoli 10 e 11),

5) Diritti delle persone interessate, in particolare diritto di accesso e diritto di opposizione per motivi preminenti e legittimi (cfr. articoli 12 e 14, lettera a),

6) Garanzie applicabili in relazione alle decisioni individuali automatizzate (conformemente all'articolo 15),

7) Sicurezza dei trattamenti (articolo 17),

8) Notificazione delle operazioni di trattamento (conformemente agli articoli 18 e 19),

9) Controllo preliminare delle operazioni di trattamento che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone (ai sensi dell'articolo 20), e

10) Trasferimenti di dati verso paesi terzi (conformemente agli articoli 25 e seguenti.).

La specificità e la sensibilità del trattamento di dati sotto forma di suoni e immagini sono infine riconosciuti nel penultimo articolo della direttiva, in cui la Commissione si impegna ad esaminare, in particolare, l'applicazione della direttiva in questione e di presentare opportune proposte di modifica, tenuto conto dell'evoluzione della tecnologia dell'informazione e alla luce dei progressi della società dell'informazione (cfr. articolo 33).

4. DISPOSIZIONI NAZIONALI APPLICABILI ALLA VIDEOSORVEGLIANZA

In vari Stati membri sono già stati svolti studi analitici riguardo alla videosorveglianza, in base a disposizioni costituzionali [5] o legislazioni specifiche, ordinanze o altre decisione promulgate dalle competenti autorità nazionali [6] [7].

In alcuni paesi esistono anche disposizioni specifiche applicabili indipendentemente dal fatto che la videosorveglianza possa comportare il trattamento di dati personali. Ai sensi di tali regolamentazioni, l'installazione e l'uso di televisioni a circuito chiuso e attrezzature simili di sorveglianza debbono essere autorizzati preventivamente da un ente amministrativo, che può essere rappresentato, in tutto o in parte, dall'autorità nazionale per la protezione dei dati. Tali regolamentazione possono differire a seconda della natura pubblica o privata dell'ente responsabile del funzionamento delle attrezzature in questione.

In altri paesi, la videosorveglianza non forma attualmente oggetto di legislazioni specifiche; peraltro, le autorità per la protezione dei dati hanno svolto lavori per garantire la corretta applicazione delle disposizioni generali in materia di protezione dei dati, tra l'altro elaborando pareri, orientamenti o codici di comportamento, che sono già state adottati nel Regno Unito e che sono ad esempio in corso di elaborazione in Italia.

Belgio - Pareri dell'autorità per la protezione dei dati, in particolare parere 34/99 del 13 dicembre 1999, relativo al trattamento di immagini, in particolare attraverso l'utilizzazione di sistemi di videosorveglianza; parere 3/2000 del 10 gennaio 2000 relativo all'utilizzazione di sistemi di videosorveglianza nei vestiboli dei condomini.

Danimarca - Testo unico n. 76 del 1° febbraio 2000 relativo al divieto della videosorveglianza.

La decisione dell'autorità per la protezione dei dati, del 3 giugno 2002, relativa alla videosorveglianza da parte di un grande gruppo di supermercati e la trasmissione in diretta su Internet da un pub.

Francia - Legge n.78-17, del 6 gennaio 1978 relativa al trattamento dei dati, agli archivi e alle libertà (CNIL)

Raccomandazione n. 94-056 dell' autorità per la protezione dei dati, del 21 giugno 1994

Orientamento dell'autorità per la protezione dei dati relativo alla videosorveglianza sul posto di lavoro: http://www.cnil.fr/thematic/index.htm; su altri aspetti (ad esempio. webcam)

Legge specifica riguardante la videosorveglianza per la sicurezza pubblica in luoghi pubblici: legge n. 95-73, del 21 gennaio 1995, sulla sicurezza (modificata dall'ordinanza 2000-916 del 19 settembre 2000)

Decreto n. 96-926, del 17 ottobre 1996, e circolare del 22 ottobre 1996 sull'attuazione della legge n. 95-73

Grecia - Decisione dell'autorità per la protezione dei dati del 28 gennaio 2000 (metropolitana di Atene)

(5) Cfr. decisione 255/2002 del tribunale costituzionale portoghese. Il tribunale ha concluso che "l'utilizzazione di attrezzature elettroniche di sorveglianza e il controllo dei cittadini da parte di enti di sicurezza privati costituiscono una limitazione o una restrizione al diritto di tutelare la vita privata, contemplato nell'articolo 26 della Costituzione".

(6) Quanto meno in un paese (Belgio – causa Gaia), la non osservanza della legislazione in materia di protezione dei dati nel quadro della raccolta di immagini ha comportato un rifiuto di prove ammissibili in tribunale.

(7) Cfr. le relazioni annuali della "Commission Nationale de l'Informatique et des Libertés" francese.

Germania - Sezione 6, b della legge federale del 2001.

Irlanda - Studio analitico n. 14/1996 (utilizzazione di televisioni a circuito a chiuso)

Italia. Sezione 20 del decreto legge n. 467 del 28.12.2001 (che prevede l'adozione di codici di comportamento)
Decisione del garante n. 2, del 10 aprile 2002 (che promuove l'adozione di codici di comportamento), 28 settembre 2001 (biometria e tecniche di riconoscimento facciale applicate dalle banche) e 29 novembre 2000 (denominata "decalogo della videosorveglianza")
Decreto presidenziale n. 250, del 22.06.1999 (che regola l'accesso di veicoli al centro città e alle zone ad accesso limitato)
Decreto n. 433 del 14.11.1992 e legge n. 4/1993 (applicabile a musei, biblioteche e archivi di stato)
Decreto legislativo n. 45 del 04.02.2000 (navi passeggeri su rotte nazionali)
Sezione 4 della legge n. 300 del 20.05.1970 (denominata "statuto dei lavoratori")

Lussemburgo - Articoli 10 e 11 della legge del 02.08.2002 sulla protezione delle persone riguardo al trattamento dei dati personali

Paesi Bassi - Relazione dell'autorità per la protezione dei dati pubblicata nel 1997, che contiene orientamenti in merito alla videosorveglianza specialmente per la protezione delle persone e delle proprietà in luoghi pubblici.
La Camera bassa ha recentemente approvato un progetto di legge che estenderà l'ambito di atto criminale alla ripresa di fotografie di luoghi accessibili al pubblico senza informare le persone interessate.
Tra breve sarà presentato al Parlamento un progetto di legge che attribuirà esplicitamente alle giunte comunali la competenza di utilizzare sistemi di videosorveglianza a certe condizioni.

Portogallo - Decreto legge 231/98, del 22 luglio 98 (attività di sicurezza private e sistemi di autoprotezione)
Legge 38/98 del 4 agosto 98 (misure da adottare in caso di violenza connessa con manifestazioni sportive)
Decreto legge 263/01, del 28 settembre 2001 (luoghi destinati alle danze)
Decreto legge 94/2002, del 12 aprile 2002 (manifestazioni sportive)

Spagna - Legge organica n. 4/1997 (videosorveglianza da parte di agenzie di sicurezza in luoghi pubblici)
Real decreto n. 596/1999 in applicazione della legge n. 4/1997

Svezia - La videosorveglianza è specificatamente regolamentata nella legge (1998:150) sulla videosorveglianza generale e dalla legge (1995:1506) sulla videosorveglianza segreta (nelle indagini criminali)[8].

(8) In Svezia la videosorveglianza richiede in generale l'autorizzazione degli organi di amministrazione locale quantunque vi siano varie esenzioni, ad esempio per quanto riguarda la sorveglianza di uffici postali, filiali bancarie e negozi. La videosorveglianza segreta deve essere autorizzata da un tribunale. Una decisione degli organi di amministrazione locali secondo la legge sulla videosorveglianza generale può essere oggetto di ricorso da parte del Cancelliere di giustizia, al fine di tutelare gli interessi pubblici. La registrazione video con l'utilizzo di camere digitali è stata ritenuta come trattamento di dati personali ai sensi della legge sui dati personali svedese ed ha quindi successivamente formato oggetto della supervisione dell'autorità per la protezione dei dati. Una commissione inquirente sta attualmente analizzando l'utilizzazione della videosorveglianza da una prospettiva di prevenzione della criminalità. Tra l'altro, la commissione valuterà la legge sulla videosorveglianza generale e appurerà se sono necessarie modifiche. La commissione inquirente esaminerà altresì il campo di applicazione della legge svedese sui dati personali rispetto alla videosorveglianza e alla eventuale necessità di una legislazione specifica in materia di trattamento di dati personali in relazione alla videosorveglianza.

Regno Unito - Codice di comportamento 2000 per televisioni a circuito chiuso (Commissario per l'informazione)

Altri importanti strumenti normativi sono stati anche adottati in Islanda (sezione 4, legge n. 77/2000), Norvegia (titolo VII della legge n. 31, del 14.04.2000), Svizzera (raccomandazione del Commissario federale) e Ungheria (raccomandazione dell'autorità per la protezione dei dati, del 20.12.2000).

5. SETTORI IN CUI LA DIRETTIVA 95/46/CE È INAPPLICABILE, IN TUTTO O IN PARTE

La direttiva non si applica al trattamento di dati sotto forma di suoni e immagini per fini connessi con la sicurezza pubblica, la difesa, la sicurezza dello Stato e le attività dello Stato relative al diritto penale e/o nell'esercizio di altre attività che rientrano nel campo di applicazione della legislazione comunitaria [9]. Nonostante ciò, molti Stati membri, nel recepire la direttiva 95/46/CE, hanno contemplato tali aspetti in modo generale, disponendo peraltro esenzioni specifiche.

A) In alcuni paesi, le operazioni di trattamento effettuate per i fini sopra menzionati sono altresì soggette, in ogni caso, alle garanzie in conformità della convenzione n. 108/1981 e alle relative raccomandazioni del Consiglio d'Europa come pure a certe disposizioni nazionali (cfr. articolo 3, paragrafo 2, e il considerando n. 16 della direttiva 95/46/CE). Tenendo conto della sua peculiare natura e dell'esistenza di disposizioni specifiche connesse con attività di indagine di polizia e delle autorità giudiziarie, anche per fini di sicurezza dello Stato [10]- che possono includere la videosorveglianza "occulta", ossia effettuata senza fornire informazioni nei luoghi interessati - tale categoria di operazioni di trattamento non verrà trattata in dettaglio nel presente documento.

Il gruppo di lavoro vorrebbe far rilevare comunque che, al pari di altre simili operazioni di trattamento di dati personali anch'esse non rientranti nel campo d'applicazione della direttiva, la videosorveglianza effettuata per motivi di reale necessità di sicurezza pubblica o per la ricerca, prevenzione e controllo di atti criminali deve rispettare i requisiti fissati dall'articolo 8 della convezione dei diritti umani e delle libertà fondamentali e, nel contempo, essere disciplinata da disposizioni specifiche rese note al pubblico e connesse e proporzionate alla prevenzione di rischi concreti e reati specifici – ad esempio, in luoghi esposti a tali rischi o in relazione a manifestazioni pubbliche con probabilità ragionevole di tradursi in tali reati [11]. Vanno considerati gli effetti prodotti dai sistemi di videosorveglianza, ad esempio il fatto che attività illecite potrebbero spostarsi in altre aree o settori, mentre il responsabile del trattamento dei dati va sempre chiaramente specificato, affinché le persone interessate possano esercitare i loro diritti.

Quest'ultimo requisito è altresì connesso con il fatto che la videosorveglianza è sempre più utilizzata dalla polizia e da altre autorità pubbliche (ad esempio, gli enti locali) e/o da enti privati (banche, associazioni sportive, imprese di trasporti), con il rischio di rendere indistinti i ruoli e le responsabilità individuali per quanto riguarda i compiti da eseguire [12].

B) In secondo luogo, la direttiva non si applica alle operazioni di trattamento effettuate da una persona fisica nell'esercizio di attività a carattere esclusivamente personale o domestico (cfr. articolo 3, paragrafo 2, e considerando n. 12).

Mentre le circostanze sopra menzionate possono applicarsi, ad esempio, alla videovigilanza effettuata per il controllo a distanza oppure per vedere cosa succede in casa propria – ad esempio, per prevenire furti, oppure in relazione con la gestione della cosiddetta "famiglia elettronica" - ciò non è il caso qualora l'impianto di videosorveglianza sia installato all'esterno o in prossimità di luoghi privati, al fine di proteggere la proprietà e/o di garantire la sicurezza.

(9) Cfr. considerando 16.

(10) A questo proposito si potrebbe fare riferimento ai princípi fissati dal tribunale europeo dei diritti dell'uomo nella causa Rotaru /. Romania, esaminato il 4 maggio 2000. Vedi sopra.

(11) Ad esempio, una circolare pubblicata in Francia il 22.10.1996 faceva riferimento a luoghi isolati e a negozi aperti fino a tardi.

(12) Un esempio significativo di questo rischio è rappresentato dalle attività svolte da un certo numero di comuni in Italia al fine di controllare, mediante videosorveglianza, aree pubbliche frequentate di notte da prostitute. Un certo numero di comuni avevano argomentato, in passato, di essere – discutibilmente – competenti per la prevenzione di questo fenomeno, mentre altri comuni avevano emesso ordinanze che proibivano unicamente ai clienti delle prostitute di parcheggiare e/o di guidare in tali aree e avevano minacciato di inviare un fotografo al loro domicilio in caso di non osservanza dell'ordine. L'autorità italiana ha pubblicato una decisione al fine di chiarire le adeguate disposizioni per punire la violazione delle disposizioni pertinenti.