In questi casi, potrebbe trattarsi, anzitutto, di un sistema non utilizzato da singoli proprietari per controllare le porte che danno accesso alla loro residenza, ma piuttosto da vari proprietari in base ad un accordo oppure da un consorzio o da un condominio al fine di controllare varie entrate e zone del caseggiato – il che rende la direttiva applicabile a dette attività.

Laddove il sistema è gestito a beneficio di una famiglia e per controllare una sola porta, pianerottolo, parcheggio, ecc., il fatto che la direttiva non sia applicabile a motivo dell'utilizzazione esclusivamente personale nonché della non disponibilità dei dati per terzi non esenta il responsabile del trattamento dal rispetto dei diritti e interessi legittimi dei suoi vicini e di altre persone di passaggio. Negli Stati membri dell'UE, tali diritti e interessi sono effettivamente protetti indipendentemente dai principi della protezione dei dati da disposizioni generali (diritto civile) che tutelano i diritti personali, l'immagine, la vita familiare e la sfera privata – basta pensare, ad esempio, all'angolo visuale di una videocamera installata fuori dalla porta di un appartamento, che potrebbe permettere sistematicamente la registrazione dei pazienti di una clinica medica e/o i clienti di uno studio legale che si trova sullo stesso piano e causare quindi un'indebita interferenza con il segreto professionale.

Sarà necessario prestare particolare attenzione all'orientamento dell'attrezzatura video, alla necessità di affiggere avvisi ed informazioni e alla tempestiva eliminazione delle immagini, da effettuare entro poche ore – nel caso non si siano verificati effrazioni o reati.

C) Infine, l'articolo 9 della direttiva prevede che gli Stati membri debbono fissare esenzioni e deroghe da alcune delle disposizioni qualora il trattamento fosse effettuato unicamente a fini giornalistici o di espressione artistica o letteraria, in particolare nel campo audiovisivo (cfr. considerando n. 17). Vanno fissate unicamente le eccezioni necessarie per conciliare il diritto alla vita privata con le norme sulla libertà di espressione [13]. A tal riguardo, sarà necessaria una speciale attenzione in particolare nell'installazione di webcam e/o di videocamere on-line, al fine di evitare vizi e lacune nella protezione delle persone oggetto di videosorveglianza con fini che possono essere di pubblicità e/o di attività di promozione turistica [14].

6. VIDEOSORVEGLIANZA E TRATTAMENTO DI DATI PERSONALI

Alla luce delle varie situazioni sopra menzionate, il gruppo di lavoro è del parere che occorra attirare l'attenzione sul fatto che la direttiva 95/46/CE si applica al trattamento di dati personali, inclusi i dati sotto forma di immagini e suoni tramite circuiti chiusi di televisione o altri sistemi di videosorveglianza, in totalità o in parte tramite mezzi automatici, e al trattamento diverso da quello automatico di dati personali che formano parte di un sistema di archivio o che sono destinati a formar parte di un sistema di archivio.

I dati in forma di immagini e suoni relativi a persone fisiche identificate o identificabili rappresentano dati personali:

a) anche se le immagini sono utilizzate nel quadro di un sistema di circuito chiuso e non sono connesse con caratteristiche specifiche di una persona,

b) anche se non riguardano individui i cui volti sono stati filmati, anche se contengono altre informazioni, ad esempio numeri di targa di automobili o numeri di codice PIN acquisiti nel contesto della sorveglianza di sportelli automatici,

c) indipendentemente dal supporto utilizzato per il trattamento, ad esempio, sistemi fissi e/o mobili quali ricevitori videoportatili, immagini a colori e/o in bianco e nero, dalle tecniche utilizzate, ad esempio apparecchi con cavi o fibre ottiche, dal tipo di attrezzatura, ad esempio fissa, rotativa, mobile, dalle caratteristiche applicabili all'acquisizione di immagini, ad esempio continua (all'opposto di discontinua), il che potrebbe essere il caso se l'acquisizione di immagini occorre unicamente in caso del superamento del limite di velocità e non ha alcuna relazione con immagini video captate in forma interamente casuale e frammentaria e dagli strumenti di comunicazione utilizzati, ad esempio collegamento con un "centro" e/o trasmissione di immagini a terminal remoti, ecc. .

(13) Cfr. raccomandazione 1/97 del gruppo di lavoro sulla legislazione in materia di protezione di dati e media.

(14) Una webcam installata di nascosto presso le scale di una stazione di metropolitana a Milano mostrava direttamente nel Net immagini delle parti intime delle donne di passaggio, per fini solo apparentemente connessi ad attività giornalistiche. Il fatto che le persone coinvolte non potevano essere identificate non ha consentito all'autorità nazionale per la protezione dei dati di intraprendere iniziative in merito.

L'identificabilità, nel senso della direttiva, potrebbe essere anche determinata dalla combinazione di dati con informazioni detenute da terzi oppure dall'applicazione, in casi individuali, di tecniche e/o dispositivi specifici.

Di conseguenza, una delle prime precauzione che il responsabile del trattamento deve prendere è quella di controllare se la videosorveglianza implica il trattamento di dati personali nella misura in cui si riferisca a persone identificabili. In questo caso, la direttiva è applicabile indipendentemente dalle disposizioni nazionali che richiedono, inoltre, autorizzazione a fini di sicurezza pubblica.

Ciò può essere il caso, ad esempio, di attrezzature situate all'entrata oppure all'interno di una banca per consentire l'identificazione dei clienti; al contrario, in talune circostanze l'applicabilità della direttiva può essere esclusa per immagini di rilevamento aereo che non possono essere ingrandite o non includono informazioni connesse con persone fisiche – immagini raccolte, ad esempio, per rilevare fonti idriche o aree di eliminazione dei residui – come pure per attrezzature che forniscono immagini generiche del traffico in autostrada.

7. OBBLIGHI E PRECAUZIONI ADEGUATE APPLICABILI AL RESPONSABILE DEL TRATTAMENTO DEI DATI

A) Legittimità del trattamento

Anche tenendo conto che il trattamento deve essere lecito (conformemente all'articolo 6, lettera a), della direttiva), il responsabile del trattamento deve verificare in anticipo se la sorveglianza è conforme alle disposizioni generali e specifiche applicabili al settore, ad esempio leggi, regolamenti, codici di comportamento con significato giuridico. Tali disposizioni possono altresì essere fissate in relazione a fini di sicurezza pubblica nonché a fini diversi da quelli connessi con la protezione dei dati personali – ad esempio, la necessità di ottenere autorizzazioni ad hoc da organi amministrativi specifici e di attenersi alle loro istruzioni.

Occorre adottare tutte le misure necessarie per garantire che la videosorveglianza sia conforme ai principi di protezione dei dati, e devono essere evitati riferimenti inappropriati alla vita privata [15].

In proposito, occorre tener conto delle migliori prassi che potrebbero essere stabilite in raccomandazioni pubblicate da autorità di supervisione e in altri strumenti di autoregolamentazione.

È necessario altresì verificare le restanti disposizioni di diritto nazionale – inclusi i principi costituzionali, disposizioni di diritto civile e di diritto penale – per quanto riguarda, in particolare, quelle applicabili al "droit à l'image"[16] o alla protezione del domicilio di una persona; va tenuto conto della giurisprudenza in materia che potrebbe aver deciso che luoghi diversi da quelli connessi con il domicilio di una persona – ad esempio stanze d'albergo, uffici, bagni pubblici, vestiari, cabine telefoniche interne, ecc. – debbono considerarsi come luoghi privati.

Se l'attrezzatura è stata installata da enti privati o pubblici, in special modo enti locali, presumibilmente per fini di sicurezza o per la ricerca, la prevenzione e il controllo di reati, occorrerà prestare speciale attenzione, nella determinazione e informazione di tali fini, ai compiti che potrebbero essere lecitamente eseguiti dal responsabile del trattamento – dato che talune funzioni pubbliche possono essere esercitate legalmente da organismi specifici non amministrativi, come ad esempio, in particolare, organi di polizia.

Tale questione è stata sollevata in special modo a proposito di alcune autorità locali che non hanno alcuna diretta competenza in questioni di ordine pubblico e di sicurezza pubblica ma che svolgono comunque attività ausiliarie a fini di sorveglianza. Allo stesso modo, la sorveglianza spesso giustificata per motivi di controllo della criminalità è destinata invece, ad ottenere prove in caso di perpetrazione di atti criminali.

(15) Di recente, una banca e una locale stazione di polizia non hanno soddisfatto la richiesta di un cliente di estrarre, dalle immagini registrate da una videocamera che filmava anche uno sportello automatico, le immagini di un ladro che, dopo aver rubato la carta bancaria del cliente, l'aveva utilizzata illegalmente per ritirare denaro da uno sportello automatico – allegando motivi di "vita privata".

(16) In Francia e in Belgio questo diritto richiede un "consenso preliminare".

B) Specificità, specificazione e legittimità delle finalità

Il responsabile del trattamento dei dati deve garantire che le finalità non siano poco chiare né ambigue, anche per poter disporre di un criterio preciso al momento di valutare la compatibilità delle finalità del trattamento (cfr. articolo 6, lettera b), della direttiva).

Tale chiarimento è altresì necessario per illustrare le finalità tanto nelle informazioni da fornire alle persone interessate, tanto nella rispettiva notifica, quanto in relazione all' eventuale controllo preliminare da effettuare eventualmente conformemente all'articolo 20 della direttiva.

Deve essere chiaramente specificato che le immagini raccolte non possono essere utilizzate per altre finalità, in particolare per quanto riguardo le possibilità di riproduzione tecnica – ad esempio vietandone espressamente la copia.

Le finalità specificate debbono essere menzionate in un documento in cui dovrebbero essere anche ricapitolate altre caratteristiche importanti della politica della "vita privata" – fondamentali quali la documentazione del momento di cancellazione delle immagini, eventuali richieste di accesso da parte delle persone interessate e/o consultazione legittima dei dati.

C) Criteri per rendere il trattamento legittimo

Il responsabile del trattamento dei dati deve verificare che la videosorveglianza soddisfi le disposizioni specifiche di cui al punto A), ed almeno uno dei criteri che rendono il trattamento legittimo ai sensi dell'articolo 7 della direttiva – per quanto riguarda in modo particolare la protezione di dati personali.

Oltre ai casi meno frequenti in cui un obbligo giuridico va rispettato – si è fatto riferimento alle attività in un casinò, dove il trattamento è necessario per proteggere interessi vitali – ad esempio per il controllo a distanza di pazienti in unità di rianimazione – accade spesse volte che un responsabile del trattamento dei dati debba svolgere una missione di interesse pubblico o nell'esercizio di autorità pubblica di cui è investito, possibilmente in conformità di regolamentazioni specifiche – ad esempio, per individuare violazioni del codice stradale o un comportamento violento su mezzi di trasporto pubblici in zone di alta criminalità – conformemente all'articolo 7, lettera e), della direttiva; alternativamente, il responsabile del trattamento dei dati può perseguire interessi legittimi, in cui non prevalgono l'interesse o i diritti e le libertà fondamentali della persona interessata (cfr. articolo 7, lettera f)).

In entrambi i casi, specialmente nell'ultimo caso, la natura sensibile dell'operazione di trattamento richiede un'attenta considerazione della portata dei compiti, dei poteri e degli interessi legittimi del responsabile del trattamento. In tale analisi devono essere eliminate in assoluto superficialità e ampliamento senza fondamenti della portata di tali compiti e poteri.

Per quanto riguarda, in particolare, l'equilibrio dei vari interessi, si dovrà prestare un'attenzione particolare anche ascoltando in via preliminare le parti interessate, sulla possibilità che un interesse da proteggere può essere in conflitto con l'installazione del sistema oppure con taluni accordi di conservazione dei dati o con altre operazioni di trattamento [17].

Infine, per quanto riguarda l'ottenimento del consenso della persona interessata, quest'ultimo dovrà essere inequivocabile e basato su informazioni ben definite. Il consenso dovrà essere concesso separatamente e specificamente per attività di sorveglianza riguardanti luoghi in cui la persona passa la sua vita privata [18].

La legittimità del trattamento va anche valutata tenendo conto delle disposizioni della direttiva che fissano garanzie specifiche per i dati relativi alle infrazioni (cfr. articolo 8, paragrafo 5) della direttiva) [19]

(17) Ai sensi della sezione 6b della nuova legge federale tedesca sulla protezione dei dati, che è entrata in vigore il 23 maggio 2001, l'osservazione di aree di accesso pubblico per mezzo di dispositivi ottici ed elettronici è permessa se, tra l'altro, non sussistono motivi di credere che prevalgano gli interessi delle persone in causa, da proteggere.

(18) Occorre prestare un'attenzione specifica alla reale possibilità di esprimere un consenso valido nel senso dell'articolo 2, lettera h) della direttiva 95/46/CE ("qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento") in caso di installazione di sistemi di videosorveglianza in coproprietà (condomini, etc.).

(19) In proposito si può fare riferimento alla sezione 8 della legge portoghese relativa ai dati riguardanti persone sospette di attività illecite e/o criminali.

Le operazioni di trattamento per mezzo della videosorveglianza devono basarsi sempre su disposizioni giuridiche espresse, ove vengano eseguite da organismi pubblici.

D) Proporzionalità del ricorso alla videosorveglianza

Il principio in base al quale i dati debbono essere adeguati e proporzionati alle finalità da raggiungere significa, in primo luogo che la televisione a circuito chiuso e altre attrezzature simili di videosorveglianza possono essere utilizzate unicamente in via sussidiaria, cioè: per fini che giustifichino effettivamente il ricorso a tali sistemi.

Occorre evitare, ad esempio, che un organo amministrativo installi un'attrezzatura di videosorveglianza in relazione a infrazioni minori – ad esempio, per rafforzare il divieto di fumare nelle scuole ed in altri luoghi pubblici oppure il divieto di lasciare mozziconi di sigarette e rifiuti in luoghi pubblici.

In altre parole, è necessario applicare, caso per caso, il principio di adeguatezza alle finalità perseguite, il che implica un specie di dovere di minimizzazione dei dati da parte del responsabile del trattamento.

Mentre un sistema proporzionato di videosorveglianza e di allarme può essere ritenuto legittimo in caso di attacchi ripetuti a bordo di autobus in zone periferiche o in prossimità delle fermate di autobus, ciò non è il caso con un sistema destinato a impedire insulti ai conducenti di autobus e l'imbrattamento di veicoli – conformemente ad una descrizione fornita ad un'autorità per la protezione dei dati – oppure a identificare cittadini responsabili di infrazioni amministrative minori, quali l'abbandono di sacchetti di rifiuti fuori dai rispettivi contenitori e/o in zone in cui non si debbono lasciare rifiuti.

La proporzionalità deve essere valutata sulla base di criteri ancora più rigorosi per quanto riguarda luoghi non accessibili al pubblico.

In questo contesto potrebbe rivelarsi utile lo scambio di informazioni e di esperienza tra le competenti autorità dei vari Stati membri [20]; inoltre, tali sistemi possono essere applicati qualora altre misure di protezione di sicurezza che non comporta l'acquisizione di immagini – ad esempio l'utilizzazione di porte blindate contro il vandalismo, l'installazione di cancelli automatici e dispositivi per l'autorizzazione a passare, sistemi congiunti di allarmi, migliore e più forte illuminazione delle strade di notte, etc. – si rivelino chiaramente insufficienti e/o inapplicabili nell'ottica delle finalità legittime sopra menzionate.

Tali considerazioni si applicano, in particolare, all'utilizzazione sempre più frequente della videosorveglianza a fini di autodifesa e di protezione della proprietà – soprattutto in prossimità di edifici pubblici e uffici, incluse le aree circostanti. Questo tipo di applicazione richiede una valutazione, da un punto di vista più generale, degli effetti indiretti prodotti dal ricorso massiccio alla videosorveglianza – ad esempio, se un'installazione di vari dispositivi sia un elemento effettivamente dissuasivo, oppure se i trasgressori e/o vandali passano semplicemente in altre aree ed attività.

E) Proporzionalità delle attività di videosorveglianza

Il principio secondo il quale i dati debbono essere adeguati, pertinenti e non eccessivi implica un'attenta valutazione della proporzionalità delle disposizioni applicabili al trattamento dei dati, una volta accertata la legittimità di tale trattamento.

Le modalità relative alla ripresa di immagini dovranno essere considerate in particolare riguardo ai seguenti aspetti:

a) l'angolo visuale in relazione alla finalità prevista [21]– ad esempio se la sorveglianza è effettuata in un

(20) Ciò consentirebbe altresì una migliore armonizzazione degli approcci regolamentari e delle decisioni amministrative, talvolta divergenti – come è stato il caso, ad esempio, per le sale di Bingo.

(21) In due disposizioni formulate dall'autorità italiana per la protezione dei dati si possono trovare esempi di precauzioni specifiche da prendere riguardo all'angolo visuale. Un ente sanitario, che intendeva introdurre un servizio che consentisse ai familiari di osservare continuamente, a distanza, pazienti in coma, quarantena e/o gravemente malati in una unità di pronto soccorso è stato informato della necessità di adottare adeguate misure per impedire la visualizzazione simultanea di altri pazienti. In un altro caso, l'autorità ha fatto presente alle autorità amministrative di polizia che, per un sistema di rilevamento del superamento dei limiti di velocità era necessario unicamente filmare le targhe piuttosto che l'interno dei veicoli.

luogo pubblico, l'angolo non dovrà consentire la visualizzazione di dettagli e/o di tratti somatici irrilevanti ai fini prefissi, oppure aree all'interno di luoghi privati situati nelle vicinanze, soprattutto se vengono utilizzate funzioni di "zoom",

b) il tipo di attrezzatura utilizzato per filmare, ad esempio fisso o mobile,

c) le disposizioni effettive di installazione, ad esempio la localizzazione delle videocamere, l'utilizzazione di videocamere ad immagine fissa e/o mobile, etc.,

d) la possibilità di ingrandire e/o ravvicinare (funzioni di zoom) immagini nel momento in cui esse sono filmate o successivamente, ad esempio riguardo ad immagini memorizzate,

e) funzioni di blocco di immagini,

f) collegamento con un "centro" per inviare allarmi sonori e/o visivi,

g) misure adottate a seguito della videosorveglianza, a esempio chiusura delle vie d'accesso, intervento del personale di sorveglianza, etc. .

In secondo luogo, è necessario considerare la decisione da prendere per quanto riguarda la conservazione delle immagini e il periodo di conservazione – quest'ultimo deve essere di breve durata e conforme alle caratteristiche specifiche del caso in questione.

Mentre in alcuni casi potrebbe essere sufficiente un sistema che consente unicamente la visualizzazione di immagini a circuito chiuso, senza registrazione – ad esempio nel caso della casse di un supermercato –, in altri casi – ad esempio per proteggere luoghi privati – potrebbe essere giustificato registrare le immagini durante un certo numero di ore ed eliminarle automaticamente, entro la fine della giornata e quanto meno alla fine della settimana. Una eccezione a questa regola sarà ovviamente il caso in cui sia stato lanciato un allarme o inoltrata una richiesta meritevole di attenzione particolare; in tali casi sussistono motivi ragionevoli per aspettare, per un breve periodo di tempo, la decisione eventualmente adottata dalla polizia oppure dalle autorità giudiziarie.

Per citare un altro esempio, un sistema destinato a rilevare accessi non autorizzati a veicoli nei centri città e in zone di traffico limitato dovrebbe registrare immagini unicamente ove fossero commesse infrazioni.

La questione della proporzionalità dovrebbe essere altresì tenuta in considerazione ove siano ritenuti necessari periodi di conservazione meno lunghi che non devono comunque superare una settimana [22] – ad esempio per quanto riguarda immagini ottenute tramite videosorveglianza che potrebbero essere utilizzate per identificare le persone presenti in una banca prima di una rapina.

In terzo luogo occorrerà fare attenzione ai casi in cui l'identificazione di una persona è facilitata dall'associazione di immagini del viso della persona con altre informazioni relative al comportamento e/o alle attività osservate – ad esempio, nel caso di associazione tra immagini e attività di clienti in una banca in un momento facilmente identificabile.

In questo contesto, si dovrà tener conto della chiara differenza tra la conservazione temporanea delle immagini di videosorveglianza ottenute per mezzo di attrezzature situate all'entrata di una banca e l'elaborazione decisamente più invadente di banche dati che includono fotografie e impronte digitali fornite dai clienti della banca con il loro consenso.

Infine, occorrerà tener conto delle decisioni da adottare riguardo all'eventuale comunicazione dei dati a terzi – che, di massima, non devono coinvolgere organismi senza relazioni con le attività di videosorveglianza – e la loro divulgazione, totale o parziale, addirittura all'estero o on-line – anche alla luce delle disposizioni relative ad un'adeguata protezione, cfr. articolo 25 e seguenti della direttiva.

Ovviamente, la necessità che le immagini siano pertinenti e non eccessive si applica altresì alla combinazione di informazioni detenute da vari responsabili dei sistemi di videosorveglianza.

Le garanzie sopra citate sono destinate ad applicare, anche a livello operativo, il principio menzio-

(22) Le autorità per la protezione di dati danesi e svedesi hanno espresso il parere che la videoregistrazione può essere conservata unicamente per un breve periodo e che tale periodo non deve essere superiore a 30 giorni.

nato nelle legislazioni nazionali di alcuni paesi come il principio di moderazione nell'utilizzazione di dati personali – che mira ad evitare o a ridurre, nei limiti del possibile, il trattamento di dati personali.

Questo principio deve essere applicato in tutti i settori tenendo inoltre conto del fatto che molte finalità possono essere effettivamente raggiunte senza dover ricorrere a dati personali, oppure utilizzando dati realmente anonimi, anche se inizialmente sembrino richiedere l'utilizzazione di informazioni personali.

Le considerazioni di cui sopra si applicano inoltre in presenza di un'esigenza motivata di razionalizzare le risorse commerciali [23] oppure di migliorare i servizi offerti agli utenti [24].

F) Informazione delle persone interessate

L'apertura e l'adeguatezza dell'utilizzazione di attrezzature di videosorveglianza comporta la trasmissione di informazioni adeguate alle persone interessate, conformemente agli articoli 10 e 11 della direttiva.

Le persone interessate debbono essere informate, conformemente agli articoli 10 e 11 della direttiva. Le persone debbono essere consapevoli del fatto che viene effettuata una videosorveglianza, anche se quest'ultima si riferisce a manifestazioni e spettacoli pubblici oppure ad attività pubblicitarie (web cam); esse devono essere informate in dettaglio circa i luoghi sotto vigilanza.

Non è necessario specificare la localizzazione esatta dell'attrezzatura di sorveglianza, peraltro il contesto della sorveglianza va chiarificato inequivocabilmente.

Le informazioni dovrebbero essere affisse ad una ragionevole distanza dai luoghi sotto vigilanza – al contrario di quanto si è fatto in alcuni casi, in cui si era ritenuta accettabile la collocazione a 500 metri dalle zone sotto sorveglianza dei cartelli informativi – anche a seconda del tipo di ripresa di immagini.

Le informazioni debbono essere visibili e possono essere fornite in forma sommaria, a condizione che sia efficace; tali informazioni possono includere simboli che si sono già dimostrati utili in relazione con la videosorveglianza e informazioni circa il divieto di fumare – che possono differire a seconda che le immagini siano registrate o meno. Le finalità della videosorveglianza e il responsabile del trattamento devono essere specificati in tutti i casi. Il formato delle informazioni dovrà adeguarsi alle varie ubicazioni.

Potranno essere permesse limitazioni specifiche e ben motivate ai requisiti di informazione unicamente nei casi di cui agli articoli 10, 11 e 13 della direttiva – ad esempio, può essere applicata una limitazione temporanea a dati raccolti nel corso di indagini effettuate legalmente da un avvocato della difesa, oppure al fine di esercitare il diritto di difesa durante il periodo in cui ciò potrebbe mettere a rischio le finalità specifiche perseguite.

Infine particolare attenzione deve essere rivolta al modo appropriato di fornire informazioni alle persone non vedenti.

G) Requisiti supplementari

Per quanto riguarda i requisiti, le precauzione e le garanzie supplementari menzionate nella legislazione relativa alla protezione dei dati e ricapitolate al punto 3) precedente – anche rispetto l'esigenza di notificare il trattamento di dati personali e di sottoporlo alla supervisione di un'autorità indipendente, conformemente agli articoli 18, 19 e 28 della direttiva – , il gruppo di lavoro gradirebbe attirare l'attenzione, in particolare, sugli aspetti seguenti:

a) Un numero limitato di persone fisiche, da specificare, deve poter visualizzare o accedere all' eventuali immagini registrate esclusivamente per le finalità prefisse tramite videosorveglianza o al fine di pro-

(23) Ciò può essere il caso, ad esempio, della necessità di calcolare il numero di casse che devono restare aperte simultaneamente in un supermercato a seconda dell'affluenza dei clienti, nonché della creazione di un "percorso d'acquisti" ottimale per i consumatori in un supermercato.

(24) Per facilitare l'accesso in un luogo di lavoro e/o a bordo di un mezzo di trasporto specifico che richieda controlli di identità, è sufficiente utilizzare carte di identità con foto della persona interessata, eventualmente su supporto informatico, evitando l'installazione di un sistema di riconoscimento facciale.

cedere alla manutenzione delle attrezzature in questione per verificarne il corretto funzionamento; in alternativa, il caso può scaturire della richiesta di una persona interessata ed avere accesso ai dati o da un ordine legale emesso da una autorità di polizia o giudiziaria per la scoperta di atti criminali.

Ove la videosorveglianza sia destinata unicamente ad evitare, scoprire e controllare infrazioni, la soluzione dell' utilizzazione di due chiavi di accesso – una detenuta dal responsabile del trattamento e l'altra dalla polizia – potrebbe essere utile per garantire che le immagini siano viste soltanto dal personale di polizia e da nessun altro personale non autorizzato – fatto salvo l'esercizio legittimo della persona interessata dei suoi diritti di accesso, tramite richiesta espressa durante il breve periodo di conservazione delle immagini.

b) Devono essere applicate adeguate misure di sicurezza al fine di prevenire il verificarsi di eventi di cui all'articolo 17 della direttiva, inclusa la diffusione dell'informazione che potrebbe essere utile a proteggere un diritto della persona interessata, di un terzo o dello stesso responsabile del trattamento – anche per evitare la manipolazione, l'alterazione o la distruzione di prove.

c) È anche fondamentale la qualità delle eventuali immagini registrate – in particolare se lo stesso supporto di registrazione viene utilizzato ripetutamente; incorre il rischio di non poter cancellare interamente le immagini registrate in precedenza.

d) Infine, è indispensabile che gli operatori concretamente coinvolti nelle attività di videosorveglianza siano adeguatamente formati e resi consapevoli delle iniziative da adottare per soddisfare interamente i requisiti.

H) Diritti della persona interessata

Le caratteristiche peculiari dei dati personali raccolti non escludono l'esercizio, da parte della persona interessata, dei diritti di cui agli articoli 13 e 14 della direttiva, in particolare riguardo al diritto di opporsi al trattamento. La direttiva 95/46 permette effettivamente che la persona interessata si opponga, in qualsiasi momento, al trattamento di dati a lei relativi [25] per motivi preponderanti e legittimi relativi alla sua situazione particolare.

Il diritto della persona interessa all'oblio e il periodo di conservazione relativamente breve delle immagini riduce effettivamente il campo di applicazione del diritto della persona interessata all'accesso di dati personali che la rendono identificabile; tuttavia, tale diritto va garantito specialmente in caso di richiesta particolareggiata che consenta di ritrovare le immagini facilmente, tenuto conto altresì della necessità di salvaguardare l'interesse di terzi in modo temporaneo.

Qualsiasi limitazione fondata sugli sforzi per recuperare le immagini, e nel caso in cui tali sforzi siano chiaramente sproporzionati, tenuto conto del breve periodo di conservazione delle immagini, deve essere fissata esclusivamente tramite diritto secondario (cfr. articolo 13, paragrafo 1, della direttiva) con il debito rispetto del diritto della persona interessata alla difesa nel contesto di eventi specifici che possono essere occorsi nel periodo considerato.

I) Garanzie supplementari relative ad operazioni specifiche di trattamento

Deve essere proibita la videosorveglianza esclusivamente basata sull'origine etnica delle persone osservate, il loro credo religioso o opinioni politiche, la loro appartenenza a sindacati o alle loro abitudini sessuali (articolo 8 della direttiva).

Senza pretendere di elaborare un elenco esaustivo delle varie applicazione della videosorveglianza, il gruppo di lavoro gradirebbe rilevare la necessità di prestare maggiore attenzione – di massima, se del caso, nel contesto del controllo preliminare delle operazioni di trattamento di cui all'articolo 20 della direttiva – e specifici contesti in cui sono raccolte immagini relative a persone identificate o identificabili, dato che tali contesti dovrebbero essere valutati caso per caso.

Si fa riferimento, in particolare, ai casi seguenti, risultanti da esperienze e/o prove in corso:

a) interconnessione permanente di sistemi di videosorveglianza gestiti da più responsabili del trattamento,

b) possibile associazione di immagini e di dati biometrici, quali impronte digitali (ad esempio, all'en-

(25) Tranne quando disposto altrimenti dalla legislazione nazionale.

trata delle banche),

c) utilizzazione di sistemi di identificazione vocale,

d) applicazione, conformemente ai principi di proporzionalità e basata su disposizioni specifiche, di sistemi di indicizzazione applicabili ad immagini registrate e/o sistemi per il loro recupero simultaneo automatico, specialmente attraverso dati di identificazione,

e) utilizzazione di sistemi di riconoscimento facciale che non si limitano all'identificazione del camuffamento di persone in transito, (ad esempio barbe o parrucche false) ma che si basano su tecniche che consentono di segnalare le persone sospette – cioè la capacità del sistema di identificare automaticamente certi individui, in base a modelli e/o identikit standard risultanti da talune caratteristiche esterne (ad esempio colore della pelle di una persona, occhi, zigomi sporgenti, etc.), oppure sulla base di un comportamento anomalo predefinito (movimenti bruschi, passaggi successivi ad intervalli determinati, modo di parcheggiare l'autovettura, etc.). A questo riguardo, l'intervento umano è adeguato anche alla luce di errori che possono succedere in tali casi, come anche menzionato al punto f) seguente,

f) possibilità di seguire automaticamente percorsi e tragitti e/o ricostruire o prevedere il comportamento di una persona,

g) adozione di decisioni automatizzate basate sul profilo di una persona o su sistemi intelligenti d'analisi e d'intervento non connessi con allarmi standard – ad esempio, accesso senza identificazione o allarme d'incendio.

8. VIDEOSORVEGLIANZA NEL CONTESTO DELL'OCCUPAZIONE

Nel suo parere n. 8/2001 sul trattamento di dati personali nel contesto dell'occupazione, adottato il 13 settembre 2001 e nel suo documento di lavoro sulla sorveglianza delle comunicazioni elettroniche sul posto di lavoro, adottato il 29 maggio 2002 [26], il gruppo di lavoro ha già richiamato l'attenzione, in termini più generali, su alcuni principi destinati a salvaguardare i diritti, le libertà e la dignità delle persone interessate, nell'ambito dell'occupazione.

Oltre alle considerazioni formulate nei documenti sopra menzionati, nella misura in cui essi sono effettivamente applicabili alla videosorveglianza, è opportuno rilevare che i sistemi di videosorveglianza miranti direttamente a controllare da un luogo remoto la qualità e la quantità delle attività lavorative, implicando di conseguenza il trattamento di dati personali in questo contesto, non dovrebbero essere di regola permesse.

La situazione è diversa per quanto riguarda i sistemi di videosorveglianza utilizzati con le debite garanzie, per soddisfare requisiti di sicurezza della produzione e/o dell'occupazione e che, sebbene indirettamente [27], comportano il controllo a distanza.

L'esperienza di applicazione ha dimostrato inoltre che la sorveglianza non deve includere locali riservati all'uso privato dei dipendenti o non destinati allo svolgimento dei compiti connessi con l'occupazione – ad esempio bagni, docce, armadietti e zone di ricreazione; che le immagini raccolte esclusivamente per tutelare la proprietà e/o per scoprire, prevenire e controllare infrazioni gravi non devono essere utilizzate per incolpare un dipendente di infrazioni disciplinari minori, che i lavoratori dipendenti debbano poter sempre presentare una domanda riconvenzionale utilizzando il contenuto delle immagini raccolte.

Le informazioni vanno fornite ai dipendenti e ad ogni persona che lavori nei luoghi in questione. Le informazioni dovrebbero includere l'identità del responsabile del trattamento e la finalità della sorveglianza, nonché altre informazioni necessarie per garantire un trattamento reale nei confronti della persona interessata, ad esempio in quali casi le registrazioni vengono esaminate dall'amministrazione delle imprese, il periodo di registrazione e quando la registrazione è trasmessa alle autorità giudiziarie. La fornitura di informazioni, ad esempio attraverso un simbolo, non può essere ritenuta sufficiente nel contesto dell'occupazione.

(26) Entrambi i documenti sono disponibili al seguente indirizzo: www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index/htm.

(27) In questi casi, oltre alle considerazioni espresse nel presente documento, occorre anche tener conto in modo speciale dell'esigenza di rispettare i diritti menzionati negli accordi collettivi, che talvolta si basano su informazioni collettive dei dipendenti e/o dei loro sindacati – ossia, oltre alle informazioni da fornire individualmente in osservanza delle legislazioni sulla protezione dei dati; in altri casi, va ricercato un accordo preliminare con i rappresentanti dei dipendenti o con le organizzazioni sindacali riguardo disposizioni in merito all'installazione, anche per quanto concerne la durata della sorveglianza ed altre disposizioni di ripresa di immagini. In alcuni paesi, può essere necessario l'intervento dello Stato qualora non si raggiungano accordi tra le parti interessate.

9. CONCLUSIONE

Il gruppo di lavoro ha elaborato il presente documento per contribuire all'applicazione uniforme delle misure nazionali adottate ai sensi della direttiva 95/46/CE nel campo della videosorveglianza.

In questo contesto, è anche indispensabile che gli Stati membri forniscano orientamenti quanto all'attività dei produttori, prestatori di servizi e distributori, nonché ricercatori in vista dello sviluppo delle tecnologie, dei software e dei dispositivi tecnici conformi ai principi illustrati nel presente documento.

Fatto a Bruxelles, il 25 novembre 2002

Per il gruppo di lavoro
Il Presidente
Stefano RODOTÀ

127 Documento di lavoro relativo ai servizi di autenticazione *on-line* (*)

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

10054/03/IT
WP 68

Documento di lavoro relativo ai servizi di autenticazione on-line

Adottato il 29 gennaio 2003

(*) http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_it.pdf

128 Parere 1/2003 sulla memorizzazione dei dati relativi al traffico a fini di fatturazione

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

12054/02/IT
WP 69

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

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

visti l'articolo 29 e l'articolo 30, paragrafo 1, lettera a), e paragrafo 3, di tale direttiva e l'articolo 14, paragrafo 3, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997,

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

HA ADOTTATO IL PRESENTE PARERE:

1. Introduzione

1.1 Il presente parere verte sul periodo di tempo durante il quale i dati relativi al traffico, originati dall'effettuazione delle comunicazioni elettroniche, possono essere sottoposti a trattamento ai fini della fatturazione.

Nel suo parere 7/2000 sulla proposta della Commissione che ha portato all'adozione della direttiva 2002/58/CE [2], il gruppo osservava che il progetto di direttiva non prevedeva alcuna armonizzazione del periodo durante il quale può essere legalmente contestata la fattura. Il presente parere intende ritornare sulla raccomandazione 3/99 [3] che ha già fornito alcuni orientamenti in materia, in particolare nei casi in cui le bollette sono state pagate e non sono contestate, al fine di contri-

(1) G.U L 281 del 23.11.1995, pag. 31, disponibile al sito: http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm
(2) Proposta della Commissione europea di una direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000, COM (2000) 385.
(3) Raccomandazione 3/99 sulla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari: http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wpdocs_99.htm

buire all'uniforme applicazione delle direttive comunitarie in materia di tutela dei dati, nell'intento di essere di ausilio alle società di telecomunicazioni, alle autorità nazionali [4] e agli interessati.

1.2 In seno all'Unione europea la direttiva 95/46/CE armonizza le disposizioni che disciplinano la tutela delle persone fisiche con riguardo al trattamento dei dati personali.

L'articolo 6 di tale direttiva stipula che:

> *« 1. Gli Stati membri dispongono che i dati personali devono essere:*
> *(a) trattati lealmente e lecitamente;*
> *(...)*
> *(e) conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati. Gli Stati membri prevedono garanzie adeguate per i dati personali conservati oltre il suddetto arco di tempo per motivi storici, statistici o scientifici.»*

2. Applicazione delle direttive comunitarie in tema di telecomunicazioni e di tutela dei dati

2.1 La direttiva 97/66/CE è finalizzata all'armonizzazione delle normative nazionali degli Stati membri atte a garantire un livello equivalente di tutela dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle telecomunicazioni, nonché a garantire la libera circolazione di tali dati e delle apparecchiature e dei servizi di telecomunicazione all'interno della Comunità. L'articolo 6 di tale direttiva stabilisce che:

> *«1. I dati sul traffico relativi agli abbonati e agli utenti, trattati per inoltrare chiamate e memorizzati dal fornitore di una rete pubblica e/o di un servizio di telecomunicazione offerto al pubblico, devono essere cancellati o resi anonimi al termine della chiamata, fatte salve le disposizioni dei paragrafi 2, 3 e 4.*
>
> *2. Ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento i dati indicati nell'allegato. Il trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. »*

2.2 Tale direttiva sarà sostituita nel novembre 2003 dalla direttiva 2002/58/CE, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche [5].

L'articolo 6 della direttiva 2002/58/CE conferma la scelta fatta nella direttiva 97/66/CE e ne estende l'ambito al contesto più generale delle comunicazioni elettroniche. Esso stabilisce che:

(4) Il presente parere dovrebbe essere di ausilio alle autorità competenti in materia di tutela dei dati allorché verificano l'applicazione delle disposizioni adottate dagli Stati membri in virtù delle direttive sulla tutela dei dati o allorché sono consultate in sede di redazione da parte degli Stati membri di misure o disposizioni amministrative in tema di trattamento dei dati sul traffico. Dovrebbe anche essere di ausilio agli Stati membri in sede di elaborazione delle disposizioni nazionali di attuazione della direttiva 2002/58/CE.
(5) Pubblicato nella G.U.C.E. L 201 del 31 luglio 2002

« 1. I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1.

2. I dati relativi al traffico che risultano necessari ai fini della fatturazione per l'abbonato e dei pagamenti di interconnessione possono essere sottoposti a trattamento. Tale trattamento è consentito solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento. »

2.3 Nella sua raccomandazione 3/99, il gruppo "articolo 29" ha ricordato l'obbligo previsto all'articolo 6 della direttiva 97/66/CE di cancellare i dati relativi al traffico o di renderli anonimi al termine della comunicazione (articolo 6, paragrafo 1). Il gruppo spiegava che "ciò si deve alla delicatezza di tali dati, che possono consentire l'elaborazione di profili individuali di comunicazione, ivi comprese le fonti delle informazioni e la località geografica dell'utente di telefoni fissi o mobili, e ai pericoli per la riservatezza che derivano dalla raccolta, trasmissione o ulteriore utilizzazione di tali dati". Infine il gruppo ricordava che l'articolo 6, paragrafo 2, stabiliva un'eccezione in merito al trattamento dei dati relativi al traffico ai fini delle attività di fatturazione agli abbonati e della riscossione dei canoni di interconnessione "ma *solo sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento*".

2.4 L'articolo 6, paragrafo 2, della direttiva 97/66/CE (così come l'articolo 6, paragrafo 2, della direttiva 2002/58/CE) deve essere interpretato in conformità agli obiettivi delle direttive generali e specifiche. A questo proposito il decimo considerando della direttiva 95/46/CE ricorda che:

«(10) considerando che le legislazioni nazionali relative al trattamento dei dati personali hanno lo scopo di garantire il rispetto dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, riconosciuto anche dall'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e dai principi generali del diritto comunitario; che pertanto il ravvicinamento di dette legislazioni non deve avere per effetto un indebolimento della tutela da esse assicurata ma deve anzi mirare a garantire un elevato grado di tutela nella Comunità; »

2.5 L'articolo 6, paragrafo 5, della direttiva 2002/58/CE (articolo 6, paragrafo 4, della direttiva 97/66/CE) stabilisce che "il trattamento dei dati relativi al traffico ai sensi dei paragrafi da 1 a 4 (...) deve essere limitato a quanto è strettamente necessario per lo svolgimento di tali attività". Il diciassettesimo considerando della direttiva 97/66/CE fornisce un ausilio interpretativo rispetto all'articolo 6, paragrafo 2 *(si veda anche il ventiseiesimo considerando della direttiva 2002/58/CE)*:

«(17) considerando che i dati relativi agli abbonati, trattati per stabilire le chiamate, contengono informazioni sulla vita privata delle persone fisiche e riguardano il loro diritto al rispetto della propria corrispondenza o i legittimi interessi delle persone giuridiche; che ***tali dati possono essere memorizzati solo nella misura necessaria per la fornitura del servizio ai fini di fatturazione e di pagamenti di interconnessione, nonché per un periodo di tempo limitato****; che un ulteriore trattamento che il fornitore di un servizio di telecomunicazione offerto al pubblico volesse effettuare per*

la commercializzazione dei suoi servizi di telecomunicazione può essere permesso unicamente se l'abbonato ha dato il proprio consenso sulla base di informazioni esaurienti ed accurate date dal fornitore del servizio di telecomunicazione offerto al pubblico riguardo al genere dei successivi trattamenti che egli intende effettuare; »

2.6 Risulta evidente da tali considerando che i dati memorizzati ai fini della fatturazione e dei pagamenti di interconnessione possono esserlo soltanto per un periodo di tempo limitato e non devono essere conservati su base routinaria per lunghi periodi come indicato anche nella raccomandazione 3/99 del Gruppo.

Data questa situazione si pone la domanda per quanto tempo i dati personali relativi al traffico possano essere memorizzati "ai fini della fatturazione e dei pagamenti di interconnessione" **in particolare in quei casi in cui la fattura è stata pagata e non è oggetto di contestazioni.**

2.7 I diversi sistemi giuridici degli Stati membri contemplano varie disposizioni in merito all'estensione del periodo durante il quale possono essere avviate iniziative nell'ambito del diritto contrattuale. Tali periodi sono talvolta utilizzati per stabilire il termine massimo di memorizzazione in caso di contestazione di una fattura o di richiesta di pagamento. Tali disposizioni devono tuttavia essere applicate in conformità al principio per cui il trattamento dei dati personali deve essere limitato a quanto è strettamente necessario per conseguire i fini per i quali i dati sono stati rilevati e successivamente trattati. Nella grande maggioranza dei casi una fattura è pagata entro i termini prescritti.

A parere del gruppo, l'applicazione del principio di proporzionalità e il fatto che, conformemente all'articolo 6, paragrafo 2, della direttiva 97/66/CE (e dell'articolo 6, paragrafo 2, della direttiva 2002/58/CE), i dati relativi al traffico possono essere sottoposti a trattamento "sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento" dovrebbero normalmente essere intesi come segue:

I dati relativi al traffico dovrebbero essere conservati per il periodo necessario a consentire il pagamento delle fatture e la composizione delle controversie. Normalmente ciò implica un periodo di memorizzazione massimo di 3-6 mesi e non più lungo in quei casi in cui le fatture sono state pagate e non sembrano essere state oggetto di contestazione o di richieste di delucidazioni (tenuto conto del diritto alla tutela della vita privata dei singoli abbonati) [6].

In casi particolari di contestazioni o di richiesta di delucidazioni, i dati possono essere memorizzati per un periodo più lungo al fine di facilitare il pagamento della fattura. Anche dopo il pagamento di una fattura un periodo di memorizzazione più lungo potrebbe eventualmente essere giustificato in particolari casi eccezionali allorché esistano indicazioni concrete di una possibile contestazione o richiesta di delucidazioni. In ognuna di tali situazioni i periodi di memorizzazione dei dati devono essere valutati tenendo conto delle particolari circostanze di ogni singolo caso onde permettere la composizione delle controversie in corso. Il limite massimo di questi periodi più lunghi coincide con il termine di prescrizione stabilito nel diritto nazionale [7].

Il periodo di riferimento dovrebbe decorrere dal momento in cui i dati relativi al traffico non sono più necessari ai fini della trasmissione di una comunicazione, conformemente all'articolo 6 della diret-

(6) Si veda al riguardo in particolare la situazione in Grecia. In forza di una decisione del comitato nazionale greco per le poste e le telecomunicazioni (EETT) (cui ha fatto seguito una decisione positiva del garante della tutela dei dati greco), gli abbonati possono avvalersi della possibilità di chiedere al fornitore la cancellazione dei dati sul traffico che li riguardano a condizione di escludere ogni successiva contestazione del pagamento. In tal caso il fornitore è obbligato a cancellare i dati sul traffico indipendentemente dal periodo di tempo stabilito dalla legge.(7) In paesi quali l'Irlanda e il Regno Unito tale periodo è di sei anni.

tiva 97/66/CE (o della direttiva 2002/58/CE) [8]*. Il momento esatto del completamento della trasmissione di una comunicazione può dipendere dal tipo di servizio di comunicazione elettronica prestato* [9].

2.8. Il gruppo desidera mettere in evidenza che, come già affermato, conformemente all'articolo 6 della direttiva 95/46/CE e all'articolo 6, paragrafo 4, della direttiva 97/66/CE (e all'articolo 6, paragrafo 5, della direttiva 2002/58/CE), i dati relativi al traffico memorizzati devono limitarsi ai dati « necessari ». Possono essere sottoposti a trattamento soltanto i dati che sono adeguati, pertinenti e non eccedenti in relazione alle finalità di fatturazione e dei pagamenti di interconnessione (principio di proporzionalità dei dati sottoposti a trattamento). Ciò implica, tra l'altro, che se non si procede a fatturazione per taluni tipi di comunicazioni, i dati relativi al traffico non possono essere sottoposti a trattamento per le suddette finalità.

Il gruppo richiama l'attenzione sul fatto che la direttiva 2002/58/CE ha previsto un regime unificato per tutti i dati che rientrano nella definizione di "dati relativi al traffico" (cfr. articolo 2, lettera b), della direttiva). Conformemente al principio di proporzionalità dei dati sottoposti a trattamento di cui al precedente paragrafo, è responsabilità degli Stati membri e, a seconda delle circostanze, delle autorità nazionali di controllo nell'ambito delle proprie competenze, in sede di applicazione della direttiva 2002/58/CE, adottare le misure necessarie con riguardo alle diverse categorie di dati relativi al traffico. A questo proposito è opportuno prestare particolare attenzione per impedire la memorizzazione prolungata dei dati relativi al traffico non necessari ai fini della fatturazione o dei pagamenti di interconnessione. Specifica attenzione dovrebbe essere inoltre rivolta alle implicazioni dei sistemi di comunicazione interamente basati su tariffe forfettarie.

3. Trattamento dei dati personali a fini fiscali

Il gruppo è a conoscenza del fatto che, per giustificare periodi lunghi di memorizzazione dei dati, i responsabili del trattamento si appellano talvolta alle finalità di natura fiscale. Le finalità di natura fiscale sono effettivamente connesse alle finalità di fatturazione. Tuttavia, sebbene possa essere necessario per i responsabili del trattamento serbare per diversi anni a fini fiscali la prova dei pagamenti, compresi gli importi aggregati delle fatture, tale obbligo non dovrebbe essere esteso ai corrispondenti dati sul traffico su cui si basano le bollette telefoniche. Conformemente all'articolo 6 della direttiva 97/66/CE (e all'articolo 6 della direttiva 2002/58/CE), tale obbligo può giustificare soltanto il trattamento di importi aggregati di fatturazione, ma non il trattamento di dati relativi al traffico su cui sono basate le fatture relative alle comunicazioni.

4. Raccomandazione

4.1 Sono emerse indicazioni dell'esistenza di divergenze nella prassi seguita dalle società di comunicazioni elettroniche negli Stati membri riguardo ai periodi di memorizzazione dei dati relativi al traffico. Il Gruppo è del parere che qualsiasi prassi non conforme ai principi stabiliti ai paragrafi 2.7 e 2.8 di cui sopra e non chiaramente autorizzata da disposizioni legislative ai sensi dell'articolo 14 della direttiva 97/66/CE (e dell'articolo 15 della direttiva 2002/58/CE)[10] sia, prima facie, incompatibile con le disposizioni della normativa comunitaria in materia di tutela dei dati.

4.2 È quindi importante adottare misure per interpretare in maniera armonizzata il **periodo limitato** durante il quale i fornitori di servizi di telecomunicazioni sono autorizzati a trattare i dati

(8) La formulazione utilizzata nella direttiva 97/66/CE è stata modificata nella direttiva 2002/58/CE al fine di tener conto dei diversi tipi di servizi di comunicazione elettronica.

(9) Cfr. ventisettesimo considerando della direttiva 2002/58/CE.

(10) L'articolo 14 della direttiva 97/66/CE autorizza gli Stati membri ad adottare disposizioni legislative volte a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni della direttiva, incluso l'articolo 6 relativo ai dati sul traffico. Tuttavia tali restrizioni devono essere « necessarie » alla salvaguardia di uno degli interessi elencati (sicurezza dello Stato, difesa, pubblica sicurezza, prevenzione, ricerca, accertamento e perseguimento di reati, ovvero uso non autorizzato del sistema di telecomunicazione). [segue]

relativi al traffico a fini di fatturazione e di pagamenti di interconnessione. Conformemente al principio di cui al paragrafo 2.7, il gruppo ritiene che un'interpretazione ragionevole delle direttive in tema di tutela dei dati è quella secondo la quale un periodo di memorizzazione normale ai fini della fatturazione dura un massimo di 3-6 mesi, **fatta eccezione** per casi particolari di controversie in cui i dati possono essere sottoposti a trattamento per un periodo più lungo. Inoltre possono essere sottoposti a trattamento soltanto i dati relativi traffico che sono adeguati, pertinenti e non eccedenti ai fini della fatturazione e dei pagamenti di interconnessione. Gli altri dati relativi al traffico devono essere cancellati.

Fatto a Bruxelles, lì 29 gennaio 2003

Per il gruppo
Il Presidente
Stefano RODOTÀ

[segue] L'articolo 15 della direttiva 2002/58/CE non modifica tali disposizioni in maniera sostanziale. Esso precisa che le restrizioni devono essere « necessarie, opportune e proporzionate » « all'interno di una società democratica » e aggiunge anche che gli Stati membri possono, tra l'altro, adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati all'articolo 15, paragrafo1, e che le misure di cui a tale paragrafo devono essere conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.
Si veda al riguardo il parere 5/2002 del gruppo sulla dichiarazione dei Commissari europei per la protezione dei dati alla Conferenza internazionale di Cardiff (9-11 settembre 2002) sull'obbligo di conservazione sistematica dei dati di traffico delle telecomunicazioni, in particolare laddove si afferma che la conservazione sistematica di tutti i tipi di dati di traffico per un periodo di un anno o più sarebbe chiaramente sproporzionata e quindi inaccettabile in una società democratica.