11750/02/IT
WP 67

Documento di lavoro sul trattamento di dati personali tramite videosorveglianza

Adottato il 25 novembre 2002

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

---

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

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

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.

---

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.

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, eventualmente 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

[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.

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.

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].

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.

---

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.

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)[7] 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)
Germania	Sezione 6, b della legge federale del 2001.
Irlanda	Studio analitico n. 14/1996 (utilizzazione di televisioni a circuito a chiuso)

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

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].
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 connese con attività di indagine di polizia e delle autorità giudiziarie, anche

[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.

[9] Cfr. considerando 16.

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

---

10 A questo proposito si potrebbe fare riferimento ai principi 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.

prossimità di luoghi privati, al fine di proteggere la proprietà e/o di garantire la sicurezza.

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

---

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.

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. .

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

---

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".

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.

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]

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

---

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'artico 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.

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 conto 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 luogo pubblico, l'angolo non dovrà

[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

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.

---

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.

[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.

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 menzionato 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 migliore i servizi offerti agli utenti[24].

F) Informazione delle persone interessate

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

---

[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.

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 procedere 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 ricuperare 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 secundario (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.

[25] Tranne quando disposto altrimenti dalla legislazione nazionale.

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'entrata 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

[26] Entrambi i documenti sono disponibili al seguente indirizzo:

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 chi 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 questioni. 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.

9. CONCLUSIONE

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

* * *

---

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.

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