Commissione europea

107 Dichiarazione del Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie in merito alla pubblicizzazione di test genetici via Internet - 24 febbraio 2003 (*)

Questa dichiarazione intende sensibilizzare la società civile ed i soggetti chiamati a ruoli decisionali rispetto ai problemi suscitati dalla pubblicizzazione di test genetici via Internet.

Si stanno moltiplicando le offerte via Internet di test genetici relativi soprattutto all'accertamento di paternità, ma anche alla predisposizione a diverse malattie (cardiache, diabete, ecc.). La pubblicità diventa sempre più aggressiva e capillare, anche in Europa: in alcuni Paesi compare, ad esempio, anche in popolari catene di negozi, nelle stazioni di servizio, negli autogrill lungo le autostrade, in televisione.

La commercializzazione di massa dei test genetici pone molti e gravi problemi etici, sociali, giuridici, sui quali il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie ritiene urgente richiamare l'attenzione. Le informazioni attualmente offerte tendono ad essere fuorvianti ed incomplete, soprattutto alla luce della bassa prevedibilità dell'insorgere di patologie sulla base dei risultati di test genetici qualora vi siano caratteri multigenici. Spesso non vi sono sufficienti garanzie che i dati genetici inviati per i test siano stati raccolti rispettando le norme sul consenso degli interessati, in particolare per i test di paternità. I test genetici possono avere conseguenze negative se non si accompagnano ad un'adeguata consulenza. L'Articolo 12 della Convenzione sui diritti dell'uomo e la biomedicina del Consiglio d'Europa condiziona la legittimità dei test genetici anche ad una "consulenza genetica appropriata". Nel Parere n. 6 sugli aspetti etici delle diagnosi prenatali (20 febbraio 1996), il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie affermava che "un'attenta consulenza genetica prima e dopo il test costituisce parte integrante del test e non dovrebbe essere disgiunta dall'attività di campionatura e dai test". Le banche dati contenenti i risultati di test genetici potrebbero essere utilizzate a fini discriminatori nei confronti di alcuni gruppi di individui.

Le conseguenze individuali e sociali dei test genetici devono essere rigorosamente valutate. Alla luce delle particolari caratteristiche dei dati genetici, è possibile che si verifichi la violazione di diritti fondamentali, in particolare l'eguaglianza. Possono essere messe a rischio sia la salute delle persone sia la riservatezza dei dati sanitari. La pubblicità dei test genetici tende a trasformarli in merce ed a produrre una domanda di test genetici che può avere effetti di disgregazione delle relazioni sociali ed interpersonali.

Il Gruppo europeo sull'etica nelle scienze e nelle nuove tecnologie intende lavorare su questi temi in futuro. È in preparazione un Parere sugli aspetti etici dei test genetici sul luogo di lavoro

(*)Traduzione non ufficiale.
http://www.europa.eu.int/comm/european_group_ethics/docs/statgentest-en.pdf

Consiglio d'Europa

108 Raccomandazione R(2002)9 del Comitato dei ministri agli Stati membri sulla protezione dei dati personali raccolti e trattati per scopi assicurativi (*)

CONSIGLIO D'EUROPA
Comitato dei Ministri

Preambolo

Il Comitato dei Ministri, ai sensi dell'Articolo 15.b dello Statuto del Consiglio d'Europa,

1. considerato che scopo del Consiglio d'Europa è di raggiungere un'unione più stretta fra i suoi membri,

2. richiamandosi ai principi generali relativi alla protezione dei dati contenuti nella Convenzione per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali (ETS n. 108), ed in particolare all'Articolo 6 della stessa, il quale afferma che i dati personali classificati come sensibili non possono essere oggetto di trattamento se il diritto interno non prevede garanzie adeguate,

3. consapevole del fatto che il trattamento automatizzato di dati personali per scopi assicurativi è sempre più diffuso, non solo per la preparazione, conclusione, attuazione e cessazione di assicurazioni, ma anche per facilitare la gestione razionale ed economica delle assicurazioni, e per la lotta contro le frodi,

4. consapevole del fatto che le assicurazioni sono fornite da diversi soggetti economici, ed in particolare da compagnie assicurative,

5. convinto dell'importanza che la qualità, l'integrità e la disponibilità dei dati personali rivestono per le persone assicurate,

6. rilevando che la quasi totalità della popolazione degli Stati membri è interessata da uno o più contratti assicurativi, e che, per tale motivo, gli operatori del settore assicurativo sono in possesso di una quantità considerevole di dati personali, alcuni dei quali sono dati sensibili,

7. convinto che sia auspicabile regolamentare la raccolta ed il trattamento di dati personali per scopi assicurativi, garantirne la riservatezza e la sicurezza, e assicurare che l'utilizzo di tali dati rispetti diritti umani e libertà fondamentali, in particolare il diritto alla vita privata,

8. alla luce del fatto che la mobilità delle persone e la globalizzazione dei mercati e delle attività commerciali rendono indispensabile lo scambio transfrontaliero di informazioni anche nel settore assicurativo, e richiedono un'equivalente protezione dei dati in tutti gli Stati membri del Consiglio d'Europa,

Raccomanda che i governi degli Stati membri

1. prendano provvedimenti in modo da garantire che i principi contenuti nell'Appendice alla presente Raccomandazione si riflettano nella legislazione e nelle prassi interne,

(*) Traduzione non ufficiale
http://cm.coe.int/stat/E/Public/2002/adopted_texts/recommendations/2002r9.htm

2. assicurino un'ampia diffusione dei principi contenuti nell'Appendice alla presente Raccomandazione fra le persone, le pubbliche autorità e gli organismi pubblici o privati che raccolgono e trattano dati personali per scopi assicurativi, nonché fra gli organismi competenti in materia di protezione dati,

3. promuovano l'accoglimento e l'attuazione dei principi contenuti nell'Appendice alla presente Raccomandazione, in particolare attraverso l'adozione di norme di legge oppure stimolando la redazione di codici deontologici.

Appendice alla Raccomandazione R(2002)9

1. Definizioni

Ai fini della presente Raccomandazione:

a. per "dato personale" si intende ogni informazione relativa ad una persona fisica identificata o identificabile ("interessato"). Una persona fisica non dovrebbe essere ritenuta "identificabile" se l'identificazione richiede tempi e attività irragionevoli.

b. per "dato sensibile" si intende un dato personale che riveli l'origine razziale, le opinioni politiche, le convinzioni religiose o di altra natura, nonché un dato personale relativo allo stato di salute e alla vita sessuale. Anche i dati relativi a procedimenti penali e condanne, ed altri dati definiti sensibili dal diritto interno, si considerano dati sensibili.

c. l'espressione "per scopi assicurativi" si riferisce ad ogni operazione che comporti la raccolta e il trattamento di dati personali con riguardo alla copertura di un rischio, in particolare sulla base di una polizza o di un contratto assicurativo.

d. per "trattamento" si intende ogni operazione o complesso di operazioni effettuate in tutto o in parte con l'ausilio di procedure automatizzate e riguardanti dati personali, come la registrazione, la conservazione o la modifica, l'estrazione, la consultazione, l'utilizzazione, la comunicazione, l'incrocio o l'interconnessione e la cancellazione o la distruzione.

e. per "comunicazione" si intende l'atto con cui dati personali sono resi accessibili a terzi, indipendentemente dallo strumento o dal supporto utilizzato.

f. per "titolare" si intende la persona fisica o giuridica, la pubblica autorità, il servizio o ogni altro organismo che, da solo o congiuntamente ad altri, definisce gli scopi e gli strumenti utilizzati nella raccolta e nel trattamento di dati personali.

g. per "responsabile" si intende la persona fisica o giuridica, la pubblica autorità, il servizio o ogni altro organismo che tratti dati personali per conto del titolare.

2. Ambito di applicazione

2.1. La presente Raccomandazione si applica ai dati personali raccolti e trattati per scopi assicurativi. Essa non si applica alla raccolta ed al trattamento di dati personali utilizzati per scopi di previdenza sociale.

2.2. Gli Stati membri sono invitati ad estendere l'applicazione della presente Raccomandazione al trattamento non automatizzato di dati personali per scopi assicurativi.

2.3. Nessun dato personale dovrebbe essere sottoposto ad un trattamento non automatizzato per evitare l'applicazione dei principi della presente Raccomandazione.

2.4. Gli Stati membri possono estendere l'applicazione dei principi fissati nella presente Raccomandazione alla raccolta ed al trattamento di dati relativi a gruppi di persone, associazioni, fondazioni, società, imprese ed ogni altro organismo costituito direttamente o indirettamente da persone fisiche, dotato o meno di personalità giuridica.

2.5. Gli Stati membri possono estendere i principi fissati nella presente Raccomandazione alla protezione di dati personali utilizzati per scopi di previdenza sociale.

3. Rispetto della vita privata

3.1. Nella raccolta e nel trattamento di dati personali per scopi assicurativi è necessario salvaguardare il rispetto di diritti e libertà fondamentali, in particolare del diritto alla vita privata.

3.2. Coloro che hanno accesso a dati personali, nel corso di un'attività assicurativa, devono essere soggetti a vincoli di riservatezza conformemente al diritto ed alle prassi interne. Inoltre, la raccolta ed il trattamento di dati sanitari devono essere effettuati esclusivamente da operatori del settore sanitario, oppure secondo vincoli di riservatezza paragonabili a quelli cui soggiacciono gli operatori del settore sanitario o nel rispetto di garanzie di pari efficacia previste dal diritto interno.

4. Raccolta e trattamento di dati personali per scopi assicurativi

Presupposti essenziali per la raccolta ed il trattamento di dati personali

4.1. La raccolta ed il trattamento (compresa la comunicazione) di dati personali dovrebbero essere effettuati in modo leale e lecito, e per scopi specifici e leciti.

I dati personali dovrebbero essere
- adeguati, pertinenti e non eccedenti in rapporto agli scopi per i quali sono raccolti o ulteriormente trattati,
- accurati e, se necessario, aggiornati.

Fonti dei dati personali

4.2. In linea di principio, i dati personali raccolti e trattati per scopi assicurativi dovrebbero essere raccolti presso l'interessato o il suo legale rappresentante.

Liceità

4.3. La raccolta ed il trattamento di dati personali per scopi assicurativi sono consentiti
a. se previsti per legge;
b. per l'esecuzione di un contratto assicurativo concluso con l'interessato, nonché per la preparazione di un contratto di questo tipo su richiesta dell'interessato;
c. se l'interessato o il suo legale rappresentante o un'autorità od ogni altra persona o soggetto previsto per legge ha dato il proprio consenso come previsto al Capo 6, oppure
d. se i dati sono necessari per il perseguimento degli interessi legittimi del titolare, purché su questi ultimi non prevalgano gli interessi della persona interessata.

Finalità

4.4. Salvo quanto previsto dai Principi 4.6, 4.7 e 4.8, 8.1 e 13.1, la raccolta ed il trattamento di dati personali sono consentiti esclusivamente per i seguenti scopi:
a. predisposizione e fornitura di assicurazioni;
b. raccolta di premi e presentazione di altre fatturazioni;
c. risoluzione di controversie in materia di indennizzo o pagamento di altri benefici;
d. riassicurazione;
e. co-assicurazione;
f. prevenzione, individuazione e/o perseguimento di frodi assicurative;
g. riconoscimento, esercizio o difesa di un diritto in sede giudiziaria;
h. adempimento di altri specifici obblighi legali o contrattuali;
i. indagini su nuovi mercati assicurativi;
j. attività gestionali interne;
k. attività attuariali.

I dati in questione non possono essere sottoposti a trattamenti ulteriori per scopi incompatibili con quelli per cui sono stati inizialmente raccolti.

Nascituri

4.5. I dati personali relativi a nascituri dovrebbero godere di una tutela paragonabile a quella riservata ai dati personali di un minore.

Salvo diversa disposizione del diritto interno, chi detiene la potestà genitoriale può agire da soggetto che ha legalmente il diritto di agire per conto del nascituro, nella misura in cui quest'ultimo sia l'interessato.

Dati sensibili

4.6. La raccolta ed il trattamento di dati sensibili dovrebbero essere proibiti salvo che, per una delle finalità di cui ai Principi 4.1, 4.8, 8.1 e 13.1,

a. l'interessato o il suo legale rappresentante o un'autorità o ogni altra persona od ente nominato per legge abbia dato il proprio consenso esplicito secondo quanto disposto al Capo 6, oppure

b. siano consentiti dalla legge e

i. salva l'esistenza di adeguate garanzie, il trattamento sia necessario per l'adempimento di altri obblighi legali o contrattuali del titolare, oppure

ii. il trattamento sia necessario per far valere, esercitare o difendere un diritto in sede giudiziaria, oppure

iii. il trattamento sia necessario per tutelare gli interessi vitali della persona interessata o di un terzo, e l'interessato non sia in grado di prestare il proprio consenso per incapacità fisica o giuridica.

c. la raccolta ed il trattamento siano consentiti, salva l'esistenza di adeguate garanzie, per motivi di interesse pubblico rilevante e sulla base di una disposizione di legge o di una decisione dell'autorità ai sensi del Principio 15.1.

Dati di natura penale

4.7. In deroga al Principio 4.6., la raccolta ed il trattamento di dati relativi a procedimenti penali e condanne possono essere effettuati per scopi assicurativi esclusivamente sulla base di adeguate e specifiche garanzie previste dal diritto interno, e purché i dati siano necessari per la lotta alle frodi assicurative, per la concessione di assicurazioni o per il pagamento di indennizzi o di altri benefici assicurativi.

Marketing diretto

4.8. Il titolare può utilizzare i dati raccolti e registrati per scopi assicurativi al fine di commercializzare e promuovere la propria offerta di servizi, purché l'interessato ne sia stato informato e non vi si sia opposto. Tuttavia, se il trattamento riguarda dati sensibili, occorre il consenso esplicito dell'interessato, salvo che ciò contrasti con il diritto interno.

L'interessato dovrebbe essere informato del fatto che la mancata prestazione del consenso o la sua opposizione rispetto all'impiego dei propri dati per scopi di marketing non influirà sulla decisione di concedergli copertura assicurativa o di consentirgli di continuare ad usufruire della copertura assicurativa già concessa.

5. Informazione della persona interessata

5.1. Gli interessati dovrebbero essere informati di quanto segue:

a. la o le finalità per cui i dati sono o saranno sottoposti a trattamento;

b. l'identità del titolare del trattamento;

c. ogni altra informazione necessaria a garantire che il trattamento sia effettuato in modo leale, come ad esempio

- le categorie di dati raccolti o dei quali si prevede la raccolta;
- le categorie di individui o organismi esterni ai quali i dati possono essere comunicati, e per quali scopi;
- l'eventuale possibilità per gli interessati di rifiutare il consenso o di ritirarlo, e le conseguenze di tale ritiro;
- le condizioni per l'esercizio dei diritti di accesso e di rettifica;
- le persone o gli organismi presso i quali i dati sono o saranno raccolti;
- la natura obbligatoria o facoltativa delle risposte alle domande che costituiscono oggetto della raccolta, e le conseguenze per la persona in caso di risposta parziale.

5.2. Qualora i dati siano raccolti presso l'interessato, il titolare dovrebbe fornire a quest'ultimo le informazioni di cui al punto 5.1. al più tardi al momento della raccolta, salvo che l'interessato sia già stato informato.

5.3. Qualora i dati personali non siano raccolti presso l'interessato, il titolare dovrebbe fornire a quest'ultimo le informazioni di cui al punto 5.1. al momento in cui i dati sono registrati, oppure, se si prevede di comunicare i dati ad un soggetto terzo, al più tardi al momento della prima comunicazione di tali dati.

L'obbligo di informare l'interessato non sussiste se
a. l'interessato ha già ricevuto le informazioni;
b. risulta impossibile fornire le informazioni, oppure se ciò comporta uno sforzo sproporzionato;
c. il trattamento o la comunicazione dei dati per scopi assicurativi sono previsti espressamente dal diritto interno.

Nei casi di cui alle lettere b. e c. devono essere previste adeguate garanzie.

5.4. Le informazioni destinate all'interessato devono essere adeguate e adatte alle singole circostanze.

5.5. Qualora l'interessato versi in stato di incapacità giuridica e non sia in grado di decidere liberamente, e il diritto interno gli vieti di agire in modo autonomo, le informazioni devono essere fornite a chi ha legalmente il diritto di agire per conto dell'interessato.

5.6. Sono ammesse limitazioni alle informazioni da fornire agli interessati purché esse siano previste per legge e siano necessarie ai fini della prevenzione, delle indagini o del perseguimento di reati penali oppure allo scopo di garantire i diritti e le libertà altrui.

6. Consenso

6.1. Qualora sia richiesto il consenso degli interessati, deve trattarsi di un consenso fornito liberamente, in modo specifico e informato. Inoltre, il consenso deve essere inequivocabile e, se riguarda dati sensibili, esplicito.

Tuttavia, possono darsi situazioni nelle quali il diritto interno non ammette il consenso come fondamento sufficiente della liceità della raccolta o del trattamento.

6.2. Qualora i dati personali riguardino persone in stato di incapacità giuridica, e il diritto interno non consenta all'interessato di agire in modo autonomo, è necessario il consenso del legale rappresentante oppure di un'autorità o di un'altra persona o un altro organismo nominato per legge.

6.3. Se, ai sensi del Principio 5.5., un interessato che sia giuridicamente incapace è stato informato dell'intenzione di raccogliere e trattare dati che lo riguardano, se ne dovrebbero tenere in considerazione i desideri [le volontà espresse] purché ciò non contrasti con il diritto interno.

7. Raccolta e trattamento da parte di responsabili

7.1. Ai sensi delle disposizioni del diritto interno, i titolari possono affidare ad altri la raccolta ed il trattamento di dati personali per uno scopo specifico, nella misura in cui essi siano autorizzati a raccogliere e trattare tali dati ed il responsabile si impegni ad agire esclusivamente sulla base delle indicazioni del titolare ed a rispettare le disposizioni di diritto interno che danno attuazione al Capo 11 dell'Appendice alla presente Raccomandazione.

7.2. I titolari dovrebbero scegliere come responsabili soggetti che offrano adeguate garanzie relativamente agli aspetti tecnici ed organizzativi del trattamento da effettuare. Devono accertarsi dell'osservanza di tali garanzie e, in particolare, della conformità del trattamento alle indicazioni da loro fornite.

7.3. La raccolta e il trattamento di dati personali da parte di responsabili dovrebbero avvenire sulla base di un contratto o di un atto legale che vincoli il responsabile al titolare e specifichi che il responsabile può agire esclusivamente secondo le indicazioni fornite dal titolare e le disposizioni del diritto interno relative agli obblighi dei responsabili.

8. Comunicazione di dati per altri scopi

8.1. I dati personali possono essere comunicati per scopi diversi da quelli indicati nel Principio 4.4. esclusivamente se

a. ciò è previsto dal diritto interno e costituisce una misura necessaria, in una società democratica, ai fini della prevenzione, delle indagini e del perseguimento di reati penali oppure per garantire un altro importante interesse pubblico, oppure

b. gli interessati o i loro legali rappresentanti o un'autorità o un'altra persona o ente nominati per legge hanno prestato il consenso secondo quanto previsto dal Capo 6, oppure

c. la comunicazione è effettuata per scopi di marketing diretto, purché l'interessato ne sia stato informato e non vi si opponga. Tuttavia, dovrebbe essere richiesto il consenso espresso dell'interessato qualora i dati oggetto di comunicazione siano di natura sensibile, secondo quanto indicato al Capo 6, oppure

d. i dati sono necessari per il perseguimento di interessi legittimi del titolare, purché non prevalgano gli interessi della persona interessata. Tuttavia, dovrebbe essere richiesto il consenso espresso dell'interessato qualora i dati oggetto di comunicazione siano di natura sensibile, secondo quanto indicato al Capo 6.

9. Decisioni individuali automatizzate

9.1. Non si dovrebbero prendere decisioni in materia assicurativa che abbiano effetti giuridici per gli interessati, o comunque effetti significativi, qualora esse si basino esclusivamente sul trattamento automatizzato di dati finalizzato a valutare determinati aspetti personali concernenti gli interessati secondo criteri predefiniti o risultati statistici.

9.2. Tuttavia, tali decisioni possono essere prese se soddisfano una richiesta formulata dagli interessati ai fini della conclusione o dell'esecuzione di un contratto assicurativo, oppure se gli interessati hanno la possibilità di far valere il proprio punto di vista al fine di garantire la tutela dei propri interessi legittimi. Tali decisioni possono essere prese anche qualora siano autorizzate da una legge che tuteli gli interessi legittimi delle persone interessate.

10. Diritti di accesso e di rettifica

10.1. Tutti gli interessati dovrebbero avere la possibilità di ottenere, su richiesta, conferma dell'esistenza o meno di trattamenti di dati personali che li riguardano, e di ottenere, in forma intelligibile, tutti i dati che li riguardano nonché di essere informati almeno rispetto agli scopi del trattamento, alle categorie di dati oggetto di trattamento, ai destinatari o alle categorie di destinatari della comunicazione dei dati, ed all'origine dei dati. Inoltre, essi dovrebbero essere informati, su richiesta, in merito alla logica posta a fondamento del trattamento automatizzato di dati che li riguardano, almeno in caso di decisioni individuali automatizzate.

10.2. Il diritto degli interessati di ottenere i dati che li riguardano non dovrebbe trovare limitazioni, salvo che ciò sia previsto per legge e risulti necessario

a. per la prevenzione, le indagini o il perseguimento di reati penali;

b. per garantire i diritti e le libertà degli interessati o di terzi.

In tal caso, il diritto di accesso può essere limitato solo fin quando sussistano le motivazioni che ne hanno imposto la limitazione.

10.3. Gli interessati dovrebbero avere il diritto di ottenere la correzione, il blocco o la cancellazione dei propri dati, a seconda dei casi, qualora tali dati siano stati raccolti o trattati in difformità dalle disposizioni del diritto interno che danno attuazione ai principi della presente Raccomandazione e, in particolare, qualora essi risultino non accurati, non pertinenti o eccedenti.

10.4. Le motivazioni della limitazione del diritto di accesso, rettifica, cancellazione e blocco dovrebbero essere specificate per iscritto. In caso di limitazione del diritto dell'interessato di ottenere l'accesso a, la rettifica, la cancellazione e il blocco dei propri dati, l'interessato dovrebbe essere informato del diritto di chiedere all'autorità competente di verificare la liceità del trattamento.

10.5. I terzi destinatari della comunicazione dei dati dovrebbero essere informati della rettifica, della cancellazione o del blocco effettuati a meno che ciò risulti manifestamente irragionevole o irrealizzabile.

10.6. I titolari dovrebbero comunicare a intervalli ragionevoli e senza ritardi eccessivi con le persone che esercitano il diritto di accesso ai dati personali che le riguardano, anche per quanto concerne le informazioni di cui al Principio 10.1 rispetto alle quali sia formulata una richiesta di accesso.

11. Sicurezza dei dati

11.1 Dovrebbero essere adottate opportune misure tecniche e organizzative per tutelare i dati personali, che devono essere trattati conformemente alle disposizioni di diritto interno adottate in attuazione dei principi della presente Raccomandazione, contro la distruzione accidentale o illecita, la perdita accidentale, l'accesso, l'alterazione o la comunicazione non autorizzati e contro ogni altra forma di illecito trattamento.

Tali misure dovrebbero assicurare un livello adeguato di sicurezza tenendo conto, da un lato, dei più recenti sviluppi tecnici e, d'altro lato, della natura sensibile dei dati raccolti e trattati per scopi assicurativi e per la valutazione di rischi potenziali. Le misure in questione dovrebbero essere oggetto di un riesame periodico.

11.2. Al fine di garantire, in particolare, la riservatezza, l'integrità e la disponibilità dei dati oggetto di trattamento, nonché la tutela degli interessati, il titolare dovrebbe adottare opportune misure

a. per impedire a soggetti non autorizzati di accedere alle installazioni utilizzate per il trattamento di dati personali (controllo all'ingresso delle installazioni);

b. per impedire la lettura, la copiatura, l'alterazione o l'asportazione di supporti informazionali da parte di soggetti non autorizzati (controllo dei supporti informazionali);

c. per impedire l'inserimento non autorizzato di dati nel sistema informatico, nonché ogni consultazione, modifica o cancellazione non autorizzata dei dati personali memorizzati (controllo di memoria);

d. per impedire che sistemi per il trattamento automatizzato di dati siano utilizzati da soggetti non autorizzati attraverso dispositivi di trasmissione dati (controllo di utilizzazione);

e. allo scopo di consentire, da un lato, l'accesso selettivo ai dati e, d'altro lato, la sicurezza dei dati personali, per fare in modo che il trattamento sia strutturato, in linea di principio, così da consentire la separazione fra

- identificatori e dati relativi all'identità delle persone,
- dati amministrativi,
- dati sensibili (controllo degli accessi);

f. per garantire la possibilità di verificare e accertare a quali persone o enti sia consentita la comunicazione di dati personali attraverso dispositivi per la trasmissione dei dati (controllo delle comunicazioni);

g. per garantire la possibilità di verificare e stabilire, a posteriori, chi abbia avuto accesso al sistema e quali dati personali siano stati inseriti nel sistema informativo, quando e da chi (controllo dell'inserimento dati);

h. per impedire la lettura, la copiatura, l'alterazione o la cancellazione non autorizzate di dati personali durante la comunicazione di tali dati ed il trasporto di supporti informazionali (controllo del trasporto);

i. per salvaguardare i dati attraverso la realizzazione di copie di sicurezza (controllo della disponibilità).

11.3. I titolari dovrebbero redigere gli opportuni regolamenti interni, ai sensi del diritto nazionale, onde rispettare i principi pertinenti di cui alla presente Raccomandazione.

11.4. Se necessario, i titolari dovrebbero nominare un soggetto indipendente quale responsabile della sicurezza dei sistemi informatici e della protezione dati, con competenze estese alla consulenza in materia.

12. Flussi transfrontalieri di dati

12.1. I principi della presente Raccomandazione si applicano al flusso transfrontaliero di dati personali raccolti e trattati per scopi assicurativi.

12.2. Il flusso transfrontaliero di dati personali verso uno Stato che ha ratificato la Convenzione per la protezione delle persone fisiche rispetto al trattamento automatizzato di dati personali (ETS N. 108), e che dispone di norme di legge tali da garantire quantomeno un'equivalente protezione dei dati, non dovrebbe essere soggetto a condizioni speciali riferite alla tutela della privacy.

12.3. Non dovrebbero essere previste limitazioni al flusso transfrontaliero di dati verso uno Stato che non ha ratificato la Convenzione ma garantisce un livello adeguato di tutela.

12.4. Salvo diversa disposizione del diritto interno, il flusso transfrontaliero di dati verso uno Stato che non garantisce un livello adeguato di tutela non dovrebbe avere luogo, a meno che

a. l'interessato vi abbia acconsentito ai sensi del Capo 6, oppure

b. siano state adottate misure, anche di natura contrattuale, necessarie a rispettare le disposizioni del diritto interno che danno attuazione ai principi della Convenzione e della presente Raccomandazione, e l'interessato abbia la possibilità di opporsi al trasferimento.

13. Conservazione dei dati

13.1. Qualora i dati personali cessino di essere necessari per la realizzazione delle finalità per cui sono stati raccolti e trattati dal titolare, dovrebbero essere cancellati. Tale principio vale anche qualora si decida di rifiutare la copertura assicurativa. Tuttavia, se i dati devono essere conservati per scopi di ricerca scientifica o di statistica, o per altri scopi previsti dalla legge, dovrebbero essere conservati in forma separata ed essere accessibili esclusivamente per tali scopi, salva l'esistenza di opportune garanzie.

13.2. Nello stabilire il periodo di conservazione dei dati, si dovrebbe tenere conto, in particolare, della necessità di conservare i dati per il periodo necessario alla difesa di un diritto in sede giudiziaria, oppure per comprovare transazioni avvenute, o per giustificare la decisione di rifiutare la copertura assicurativa.

14. Rimedi giuridici

Il diritto interno dovrebbe prevedere opportune sanzioni e rimedi giuridici in caso di violazione delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente Raccomandazione.

15. Garantire il rispetto dei principi

15.1. Gli Stati membri dovrebbero incaricare una o più autorità di garantire, in piena indipendenza, l'applicazione delle disposizioni di diritto interno che danno attuazione ai principi fissati nella presente Raccomandazione.

15.2. Le informazioni di seguito indicate dovrebbero essere pubblicizzate nei modi opportuni e rese facilmente accessibili a chiunque:

a. nominativo e indirizzo del titolare e dell'eventuale rappresentante;

b. la o le finalità del trattamento;

c. la categoria o le categorie di interessati e dei dati;

d. il destinatario o le categorie di destinatari della comunicazione dei dati;

e. i trasferimenti di dati previsti verso Paesi terzi.

109 Protection of personal data with regard to surveillance (2000) and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance

Notice

The importance of the phenomenon of surveillance and surveillance activities by technical means which are becoming increasingly sophisticated demands serious thought at both national and international level with regard to the advantages and risks for democratic societies and individuals.

Several states have undertaken work in this field, even considering it necessary to draft specific legislative provisions on data protection in the field of (video-)surveillance.

In this context, the Council of Europe wishes to draw attention to certain particular aspects of surveillance. The Project Group on Data Protection (CJ-PD) of the Council of Europe asked a consultant, Dr Giovanni BUTTARELLI, to write a report on data protection in relation to surveillance activities. This Report acknowledged that any study of surveillance is linked to technological developments in the means of control and should thus be situated in the historical context.

It was therefore wished to highlight a list of Guiding Principles specifically for video surveillance, which ought to be taken into account when preparing specific legislative provisions on data protection with relation to video surveillance. These principles could, where appropriate, be applied to other forms or technical means of surveillance after making any necessary adjustments to them.

The report and guiding principles prepared by Mr Buttarelli were published on the Council of Europe's website in December 2000 for public consultation. Comments on the text were received only from the International Communications Round Table (ICRT) who considered that the principles should be restricted to video surveillance and not extend to all other sectors of surveillance. On the basis of the report and guiding principles prepared by Mr Buttarelli, the CJ-PD decided to prepare a draft containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance. Members of the CJ-PD have been asked to send final written comments on the guiding principles prepared by the Co-ordination Group of the CJ-PD (June 2002). The Co-ordination Group will submit the guiding principles to the CJ-PD at its meeting in October 2002 for examination and approval. It is also preparing the third evaluation of Recommendation R (87) 15 regulating the use of personal data in the police sector.

1) FOREWORD

Any research and/or report on surveillance is related to the technological development of control systems and is therefore to be considered in connection with the relevant historical context.

This is confirmed by a summary overview of the development of surveillance techniques, which initially focused (especially starting from the 1970s) on the monitoring of road traffic or else on the prevention of theft and robberies in banks and shops selling luxury items.

However, the relationship between surveillance and personal rights had long been pointed out, in particular concerning labour relations - so much so that the use of audiovisual and other devices for con-

trolling employees in the workplace was prohibited or specifically regulated by various countries (see, for instance, Italy's Act no. 300/1970).

In subsequent years surveillance techniques were especially refined in respect of the workplace: indeed, it became possible to control better the security of equipment, the quality and regularity of labour performance as well as productivity. The opportunity was also created for monitoring facts and circumstances having no relevance in terms of skill assessment.

During the 1980s there was also an increased use of surveillance techniques in the transportation sector - in particular on subways and in nearby areas - as well as within certain public buildings (in order to prevent vandalism) and in recreational areas.

The growing use of surveillance techniques by an increasing number of highly patronized shops resulted in facilitating the assessment of customer habits and behaviour with regard to the arrangement of the products on sale. In this specific sector, surveillance systems (especially video surveillance systems) became a valuable tool for commercial purposes even though they had been initially (or seemingly) deployed for the prevention of theft and robberies; in turn, this made it possible to rationalize business resources both within a given shop (for example, by determining the number of tills to be opened in accordance with the time of day and the monitoring of entrances) and from a more general standpoint (for example, by devising "shopping routes" that could be found more stimulating by consumers).

Surveillance techniques have been subsequently developing uninterruptedly and have been applied to the most diverse sectors.

In the transportation sector, there has been a continued increase in the number of controlled roads - both motorways and highways - with a view to the monitoring of traffic misdemeanours (even by means of infrared devices) and, more recently, the access to town centres - both big and small.

For instance, video surveillance devices have been installed :
- in stadiums [1] and sports facilities;
- in petrol stations;
- in casinos;
- in health care centres (in particular, emergency or reanimation rooms and during surgical operations)
- in sewage and waste disposal plants.

Museums and cathedrals have been the subject of this surveillance, which has also been applied to air or satellite observation activities (in connection with regular filming, with a view to geographic research, for air traffic management and for urban planning purposes).

Similar remote control techniques based on signal transmission are being used in respect of the electronic bracelets for convicts either paroled or released on licence or under house arrest.

Additional applications are related to the following sectors:
- the fight against illegal migrants;
- security of domestic units and residential districts (in this regard, there is a significant trend towards setting up, in the industrial and commercial sectors, "fortress units" as a way of preventing thefts, burglaries and vandalism);
- taxi services (for example, in New York a few cabs have been equipped with infrared cameras filming either clients when they get on the cab or the meter as it starts operating; the relevant images are recorded on digital media and automatically erased unless either the driver or the car owner decides otherwise);
- use of web-cams or online cameras for broadcasting images in connection with tourist promotion

(1) In the Recommendation on Stewarding (99/1), adopted on 9-10 June 1999 by the Standing Committee of the European Convention on Spectator Violence and Misbehaviour at Sports Events and in particular at Football Matches, attention is drawn to the surveillance of all potentially dangerous areas and the prevention of overcrowding as well as, though in general, to providing spectators with information on all the security devices deployed by organisers.

activities or else for advertising public places such as bars or night-clubs, or even for showing living conditions in prisons;

- banking institutions, where hidden devices are frequently installed allowing the taking of fingerprints and photographs so as to identify, visually and based on the relevant fingerprints, all visitors - whether they are clients or not, including possible robbers and individuals reconnoitring the place with a view to a robbery.

The voluntary use of remote control techniques for managing the so-called e-family should also be pointed out; it has even been suggested that statistical surveys could be performed on the images recorded in order to establish the behavioural patterns of members of a given community/group.

Finally, reference should be made to the economic interests related to the production of the relevant equipment and devices and to the reduction in insurance premiums granted by insurance companies if surveillance systems or satellite anti-burglar devices are installed in a vehicle.

2) A SHORT OVERVIEW OF THE AVAILABLE TECHNIQUES

As already pointed out, the increasing pace of technological evolution makes it absolutely necessary to set the surveillance issue against the relevant background.

Based on the technical development of these systems, it has progressively become possible :

- to transmit images to a "control centre" from terminals connected either via cable, optic fibres or digital network;
- to record images that in the past were only visible via CCTV (closed circuit television);
- to obtain images with higher resolution and reproduce them in colour;
- to associate images and sound;
- to expand the visual field up to a 360° vision;
- to use fixed and/or mobile, stationary and/or rotational cameras;
- to use zooming functions and therefore, magnify - even to a considerable extent - individual areas in a photogram.

Thus, there is the actual risk that any overview in this sector will rapidly become obsolete.

On the whole, it can be argued that the most significant contribution was not made so much by the enhancement of transmitting equipment (only think of the recently developed subcutaneous transmitters that are used for the surveillance of paroled convicts) or by the possibility of recording and keeping images instead of simply watching them, but rather by the introduction of "intelligent systems" for assessment and intervention. [2]

Indeed, the latest surveillance systems do not simply include an image-freezing (and printing) function nor are they exclusively connected to a control centre whence sound or visual alarm signals can be issued or else the closing of entrances to and/or exits from places and shops can be ordered, or where the intervention of staff or even helicopters can be requested. Nowadays, surveillance systems can be equipped or associated with software for automated image retrieval. There are systems allowing the recognition of persons by means of techniques for the targeting of suspected offenders - for instance, based on automatic facial recognition techniques (facial mapping computers).

It is increasingly feasible to issue various types of alarm (including the signalling to watchmen) regarding persons suspected either on account of specific descriptions or based on behavioural patterns that are automatically classified as "abnormal" by the software (for example, in a parking place or at the entrance to a stadium).

This points to the possible identification in future of alleged misbehaviour based either on the outward appearance (physical features, clothing, skin colour) or on actions and events that are regarded as especially interesting (sudden movements, smoke, opening of doors).

(2) Only think of the DcxNet system which - allegedly - is capable of facilitating driving when coupled with radar systems by operating brakes, steering wheel, etc. or even by guiding the driver in the presence of bad weather (for example, fog). This is an example of electronic networks applied to road traffic.

Whereas in the past there was just the exchange among supermarkets of videotapes including images of consumers either "suspected" or caught in the act, the most sophisticated systems available nowadays allow identifying the voice or conversation of the persons filmed - or, at the very least, significant words spoken by such persons - and even searching for a voice or face in an indexed file. For instance, a test system implemented in 1998 allowed retrieving over 1000 images per second, in real time, in order to find a given face; the system could not be fooled by the fact that the person in question was growing a beard or moustache as camouflage.

Recent tests have also allowed tracking the route presumably followed by a person or vehicle within complex scenarios or else identifying persons who frequently or at given intervals follow a certain route.

All the above techniques can obviously be implemented not only for the prevention and control of offences, but also for different purposes - such as finding missing persons or children - and in connection with the public interest; this is why the Council of Europe recommended their utilisation in some cases. [3]

Facial recognition systems have been used even with a view to preventing false marriages and - based on consensus - in order to allow access to workplaces or buildings (for example, by providing for the automatic opening of doors and gates in respect of the members of a given family) and for purchasing air tickets and using ATMs (automated teller machines).

There are ceaseless technological innovations in this sector. [4]

3) OVERVIEW OF THE EFFECTS OF SURVEILLANCE

In evaluating the effects of surveillance it is necessary, again, to take account of the relevant background.

This type of assessment is usually carried out with delay and is committed to experts, without any information to the public as a whole. Whenever it is decided that the relevant results should be disclosed to the public, the technology is found to have developed further and new considerations and analyses are required. [5]

For instance, the use of facial recognition techniques is currently far from widespread and the considerations mentioned above have been made exclusively by enlightened scholars and journalists. Meanwhile the growing diffusion of surveillance techniques and the increased number of entities keeping recorded images would require a different, more advanced type of analysis. It is time for legal scholars not to limit themselves to stressing the dangers of surveillance, but rather pay greater attention to the issue of the real-time interconnection of images obtained via surveillance which are kept by different entities (for example, motorway management companies, banks, town councils, etc.).

Given the above premises, the issue of the effects of surveillance should not only be the province of legal scholars, as the development of control mechanisms in the public sector makes it necessary for Parliament and the relevant institutions to carry out a political analysis.

In the first place, there is the need for assessing the proportional relationship between security and privacy requirements.

Indeed, surveillance systems may have positive effects in terms of security; however, there is no uniformity in the extent to which this effect can be regarded as positive. In a few cases there has been

(3) In Recommendation No. R(96)6 of the Committee of Ministers to Member States on the Protection of the Cultural Heritage against Unlawful Acts (adopted on 19 June 1996), under item 4 (concerning "Protective strategies for preventing and responding to unlawful acts") it is said that the preventive measures applying to museums, cathedrals, etc. should also include electronic surveillance measures (detection, control centre, transmission, closed circuit TV, monitoring access, video surveillance, and so forth).

(4) See, for instance, the recently published advertisement by Visionics Corporation (http://www.visionics.com) concerning the new version of the FaceIt Sentinel/Surveillance System 2.0 produced by Visionics.

(5) Consider, for instance, that the launching of an "Echelon2" system has been already reported when, in fact, the full picture of the Echelon1 system has not been highlighted yet.

undoubtedly a decrease in the number of criminal offences in public places; in other cases this surveillance has proved ineffective or caused criminals to move to other nearby areas, or else it has simply allowed obtaining evidence against the persons filmed.

Additionally, it should be considered that facial or behavioural recognition systems may frequently result in mistakes to the detriment of "innocent bystanders" - as they are based on the reduction of a face to a few dozen building elements and on the measurement of distances between key parts.

Since surveillance systems are likely to attain wider diffusion, their beneficial effects are also likely to decrease on account of their becoming rather commonplace. Finally, there is the risk that surveillance is implemented to an excessive extent as a handy way to cope with basic flaws in organisational and/or law enforcement matters rather than in order to meet actual requirements. As an example, consider that in Italy it has been proposed by a town council that video surveillance devices be installed under the wide vaulted passages of a few downtown streets since the police patrolling those streets in a car are unable to keep such passages under visual control.

It has even been suggested that a distinction should be drawn between:
- surveillance for control purposes (i.e., aimed at allowing the taking of measures in case of misconduct), and
- surveillance for prevention purposes (i.e., aimed at establishing a relationship with citizens in order to get them to behave in accordance with a given pattern).

In other words, it is feared that modern society may inadvertently tend to replace or supplement control with the incitement to self-control and the repression of impulses.

This consideration cannot but lead to expanding the scope of the assessment concerning surveillance, instead of limiting the analysis - as is often the case - to establishing whether control mechanisms cause a disproportionate damage to individual freedom as compared with the need for preventing and controlling crime. [6]

From this standpoint there can be no doubt as to the need in future for a definitely more selective approach to the use of surveillance systems: the public as a whole should not suffer excessive limitations on account of the need to prevent the misbehaviour of a minority.

The scope of discussion should therefore be expanded by going beyond the issue of the beneficial effects on security for persons and property: it would be more appropriate to evaluate also the effects, if any, on citizens' freedom and conduct.

In other words, in addition to considering the extent to which surveillance causes a breach of privacy, one should evaluate the effects resulting from the widespread use of surveillance as regards citizens' freedom of movement and behaviour.

As to the former issue, one should actually argue whether the freedom of movement which is referred to in many constitutional charters (as well as in Article 2 of Additional Protocol no. 4 to the European Human Rights Convention) means the freedom to move not only in a physical sense, but also in a more fundamental sense - that is to say, the freedom to move without having inevitably to leave continued and/or frequent traces of one's movements for the benefit of permanent "optic informers".

As to the latter issue, it has been suggested that the fact of "being seen without seeing" may influence a person's conduct and activity. On the one hand, hidden filming and/or control devices do not promote openness for citizens; on the other hand, cameras and other devices that are known to have been installed at a given location might lead to "submissive" behaviour on the citizens' part.

It is undoubtedly true that one should expect less privacy in public places; still, the concept that no

(6) In a meeting with Italy's Minister of Justice, it was recently reported alarmingly by 220 Italian chaplains that prison inmates no longer go to confession because they are afraid that bugs may be present in the confessionals.

privacy exists in public places is to be rejected.

Indeed, reference should be made in this regard :
- to domestic laws applying to non-economic rights in connection with copyright matters, which provide for safeguards even in respect of the dissemination/broadcasting of images related to facts, events and ceremonies either of public interest or occurring in public;
- to the national measures implementing Directive 95/46/EC, under which data subjects are entitled to object, on legitimate grounds, to the processing of their personal data even though the processing is ultimately lawful.

Additionally, it should be noted that the openness requirement is sometimes complied with exclusively by providing notification of the fact that cameras or other control devices have been installed and are in operation: citizens are "compelled" to provide personal data (often consisting of images) and no information is given as to their use, even though the data or images are included in data files or used for identification purposes. Citizens may thus be turned into information "subjects", without respecting the right to information self-determination. [7]

The lack of openness deprives citizens of the right to know that certain items of evidence included in the relevant data and/or images can be used against them.

If the concern for the possible discrimination against minorities and/or the sexual orientation of persons may be regarded by some as excessive in modern democratic societies, there is the actual risk of an all-pervasive control: indeed, technology should not be an obstacle to retaining the possibility of anonymity or privacy - all the more so if images are reproduced for private purposes or else for purposes less directly related to the public interest (see the recently reported use of advertising web cams in seaside resorts, which regularly perform close-ups of persons without their being aware of it).

4) THE INSTRUMENTS ADOPTED SO FAR BY THE COUNCIL OF EUROPE

It is probably unnecessary to point out here that the principles of Convention No. 108/1981 are based on the provisions of the Human Rights Convention [8]; by the same token, there is no need to stress that the processing of any personal data relating to natural persons that have been collected in connection with surveillance activities falls - as a rule - within the scope of application of Convention No. 108.

Indeed, this type of processing is performed in part by means of automated procedures on account of the tools used (for example, video cameras, bugs, computers, microphones, satellites, GPS equipment, etc.) (see Article 2(c) of Convention No. 108).

With regard to those Parties which - as is the case with Italy - have made use of the possibility of applying the Convention to the processing of data concerning groups, associations, foundations, societies, etc. as well as to manual processing operations (see Article 3(2), litt. b) and c) of Convention No. 108), the safeguards provided in the Convention also apply to the latter sectors.

Additionally, a few Parties have also provided for the above-mentioned safeguards in respect of collection; by so doing, they have in practice applied Article 11 of the Convention in line with Directive 95/46/EC, which includes collection in the definition of processing - unlike Convention No. 108.

This entails that the processing of data for surveillance purposes falls within the scope of application of Article 5 (quality of data), 7 (security), 8 (right of access), 10 (penalties and remedies) and 12 (transborder data flows) of the Convention - without prejudice to the derogations provided by domestic law in accordance with Article 9 of the Convention.

The application of the above-mentioned provisions to surveillance raises a few issues that will be

(7) The risks related to the widespread use of video surveillance in respect of the right to information self-determination and free movement in public places are highlighted in the resolution adopted by the 59th Conference of German Data Protection Authorities of the Federation and Länder, which convened in Hannover on 14-15 March 2000 ("Risks and Limitations of Video Surveillance").
(8) Mme Marie-Odile Wiederkehr, Discours d'ouverture, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 10.

addressed subsequently in connection with possible new initiatives by the Council of Europe.

It should be pointed out, however, that the application of Article 5 to surveillance activities results in the obligation for any entity processing the data to comply with safeguards that - if domestic legislation also takes account of collection operations and the strict observance of Article 5 is ensured - markedly influence the technical mechanisms underlying data collection. Only think, for instance, of the orientation and visual field of cameras, of the sensitivity of microphones, of the choice as to recording the data or not, and so on.

As to Article 6 in the Convention, it should be noted that certain data collected for surveillance purposes fall definitely outside the scope of this article: this may be the case, for instance, of surveillance for some commercial purposes or else performed in respect of direct marketing trainees, or even for some surveillance activities carried out by private detectives in connection with civil litigations, etc. There are, however, other data categories that are undoubtedly the subject of Article 6 provisions: reference can made in this regard to the surveillance in operating or emergency rooms, or else to the targeted surveillance activities performed by the police in respect of political and/or trade-union manifestations or small areas in which racial or ethnic minority groups are resident, or else in connection with prostitution activities.

It is currently debated whether Article 6 can also apply to the data collected (in particular by law enforcement agencies) with regard to persons suspected, but not yet convicted of an offence. Based on the wording of the second sentence in Article 6, one might argue that the answer should be negative as it only refers to criminal convictions; however, it has also been pointed out that even the data related to crime should be considered sensitive data, also where there is not yet a criminal conviction, but merely suspicion. [9]

Apart from the possibility for the Parties to extend the protection by applying Article 11, this interpretation issue is quite important: with regard to the processing of sensitive data, or data equated to sensitive data pursuant to Article 6, there must be suitable safeguards as provided for by a law, specific regulations or administrative directives [10] . Conversely, pursuant to Article 9, any derogations from individual principles in the Convention should be provided for exclusively by a law which also takes account of the "necessity" principle as defined by the European Court of Human Rights. [11]

This summary overview of the Convention is based on the following preliminary considerations:

- the Parties to the Convention can exclude certain processing operations from the scope of application of the Convention, as may be the case for the processing of data in connection with State security (a declaration to this effect has been made by Ireland) or else the processing of data for personal or domestic purposes (which has been excluded by various Parties);
- the data and information collected via surveillance are subjected to the Convention insofar as they relate to an individual that is identified or identifiable by reference to other information, irrespective of whether such information concerns linguistic data, static or dynamic images or sound. In this regard, the Consultative Committee of the Convention has rejected the opinion according to which voices and images are not to be regarded as personal data if they are unaccompanied by nominal information: in fact, it is sufficient for voices and images to provide information on an individual by making him/her identifiable even though indirectly. [12]

5) CONCEPT OF SURVEILLANCE UNDER CONSIDERATION

The scope of the surveillance concept is wide-ranging by nature and goes well beyond the control via video equipment - which constitutes nevertheless a major issue at stake. It can actually include the control of phone and computerised conversations as well as of the circulation of documents. It may even apply to the distance control of specific users of a service (see, for instance, the location of mobile pho-

(9) A. Patjin, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 17.
(10) Explanatory report on the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, para. 46.
(11) A. Patjin, Data Protection in the Police Sector, Council of Europe, Strasbourg, 13-14 December 1999, p. 18.
(12) In particular, the Consultative Committee has considered the digital processing of voices and images to always represent "automatic processing", whereas the analogue processing should only be regarded as such if voices and images undergo automatic processing in order to identify data subjects or else contribute to their identification.