

BPH/div.

SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont (97) 55, 2a rev.
Traduzione: orig./DE

Parere n. 98/1 dell'Autorità di controllo comune destinato al Comitato esecutivo.

Oggetto: Conservazione dei dossier ad avvenuta cancellazione di una segnalazione.

In occasione della riunione del 3 febbraio 1998, l'Autorità di Controllo comune (di seguito denominata ACC) ha adottato, sulla base dell'articolo 115, 3° comma della Convenzione di Schengen (di seguito denominata CSCH), il seguente parere:

Consapevole del fatto che servizi di polizia nazionali di determinate Parti contraenti continuano a conservare dossier anche ad avvenuta cancellazione di segnalazioni ex art. 95 e segg. CSCH e che ne fanno l'oggetto di fascicoli penali,

che le Autorità di polizia interessate si basano, in tale contesto, sulle disposizioni previste dal diritto nazionale in materia di protezione dei dati cfr. punto 2.1.3, lett. b), del Manuale SIRENE) e che si applicano anche le disposizioni di cui al Titolo VI della Convenzione di Schengen,

l'ACC ha esaminato questa prassi e al riguardo rinvia soprattutto alle seguenti esigenze attinenti al diritto in materia di protezione dei dati.

L'Autorità di controllo comune conferma i principi ed i diritti fondamentali in materia di protezione dei dati di cui alla Convenzione di Schengen, in particolare:

a) i dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (artt. 102, 1° comma, e 94, 1° comma, CSCH). Una deroga a tale principio generale è ammessa soltanto se giustificata dalla necessità di prevenire una minaccia grave imminente per l'ordine pubblico e la sicurezza pubblica dello Stato, per gravi ragioni di sicurezza dello Stato o ai fini della prevenzione di un fatto punibile grave (art. 10, 3° comma, CSCH);

b) qualsiasi utilizzo dei dati non conforme ai commi da 1 a 4 dell'art. 102 sarà considerato uno sviamento di finalità (art. 102, 5° comma);

c) in conformità dell'articolo 112 CSCH, i dati personali inseriti nel Sistema d'Informazione Schengen ai fini della ricerca di persone sono conservati esclusivamente per il periodo necessario ai fini per i quali sono stati forniti;

d) questi principi si applicano, nel quadro di un'interpretazione integrativa della Convenzione, a ogni tipo di trattamento dell'informazione relativo a segnalazioni contenute nel Sistema d'informazione Schengen o basato sulle stesse.

L'Autorità di controllo comune considera pertanto che si debbano adottare le seguenti misure:

a) in caso di soppressione di una segnalazione ai fini della ricerca di persone, ciascuna Parte contraente Schengen, in conformità dell'art. 112 CSCH, è tenuta a cancellare tale segnalazione e a distruggere senza indugio la corrispondente documentazione,

b) le Autorità Schengen devono procedere ad una revisione del Manuale SIRENE allo scopo di cancellare le disposizioni contrarie di cui al suo punto 2.1.3 lett. b).

BPH/div.

SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998
SCH/Aut-cont(97) 42, 2^a rev.
Traduzione: orig./PT

Parere n. 98/2 dell'Autorità di controllo comune destinato al Comitato esecutivo.

Oggetto: Segnalazione nel Sistema d'informazione Schengen di persone la cui identità è stata usurpata.

L'ACC ha esaminato i problemi posti dall'utilizzazione abusiva di alias di persone segnalate nel SIS (vedasi le note SCH/Aut-cont (95) 46, SCH/Aut-cont (97) 41 e SCH/Aut-cont (97) 42), alla luce dei principi di protezione dei dati di natura personale previsti dalla Convenzione di Schengen.

La segnalazione del titolare legittimo la cui identità è stata usurpata viene conservata nel SIS dalla maggioranza degli Stati. Attualmente non sembra possibile precisare nel SIS, quanto meno in testo libero, che si tratta di un caso d'identità usurpata.

L'ACC riafferma, in particolare, i seguenti principi e diritti fondamentali in materia di protezione dei dati:

a) I dati possono essere forniti ed utilizzati soltanto ai fini enunciati per ciascuna delle segnalazioni (articolo 102, primo comma e articolo 94, primo comma). Si tratta di un principio generale a cui si può derogare in via eccezionale se necessario per prevenire una minaccia grave o un reato grave (articolo 102, terzo comma).

b) Qualunque utilizzazione dei dati non conforme ai commi da 1 a 4 dell'articolo 102 sarà considerata uno sviamento di finalità (articolo 102, quinto comma).

c) Chiunque ha diritto di esigere la rettifica o la cancellazione dei dati che lo riguardano contenenti errori di fatto o di diritto (articolo 10).

d) Chiunque ha il diritto di promuovere un'azione dinanzi alla giurisdizione o all'autorità competente in base alla legislazione nazionale, finalizzata ad assicurare il diritto di rettifica o di cancellazione (articolo 111, primo comma).

e) Chiunque ha il diritto di verifica dei dati, esercitato presso l'autorità di controllo nazionale (articolo 114, secondo comma).

L'ACC, tenendo conto in modo proporzionale ed equilibrato dei diritti della persona la cui identità è stata usurpata, previsti dalla Convenzione di Schengen, nonché della necessità di individuare l'usurpatore, formula il seguente parere:

1) Alle segnalazioni nel SIS relative a persone la cui identità è stata usurpata si applica il diritto nazionale, fatte salve norme più rigorose previste dalla Convenzione (articolo 104, primo comma).

2) Spetta alla Parte contraente autrice della segnalazione garantire che i dati siano registrati per gli scopi enunciati e mantenerli attuali ed esatti (articolo 102, primo comma; articolo 106, primo comma; articolo 110; disposizioni in materia di protezione dei dati della Convenzione 108 del Consiglio d'Europa vincolanti per gli Stati Schengen, in particolare quelle dell'articolo 5).

3) In conformità della procedura prevista dall'articolo 106 della Convenzione, spetta alla Parte contraente autrice della segnalazione garantire l'esercizio del diritto di rettifica e di cancellazione dei dati registrati.

4) La conservazione nel SIS della segnalazione di una persona la cui identità è stata usurpata deve essere valutata secondo il principio della proporzionalità, tenuto conto, da un lato, dei diritti della persona la cui identità è stata usurpata e, dall'altro, della necessità di individuare l'usurpatore.

5) Nell'attesa che il SIS II sia messo in funzione, occorre studiare e adottare una soluzione adeguata e se possibile comune che consenta di indicare che si tratta di una segnalazione con identità usurpata. L'ACC esprime la sua volontà di collaborare per trovare tale soluzione.

BPH/CP

SCHENGEN IT

Autorità di controllo comune

Bruxelles, 3 dicembre 1997
Sch/Aut-cont (97) 50, 2^a rev.
Traduzione: orig. FR**Parere n. 98/3 dell'autorità di controllo comune all'attenzione del comitato esecutivo**

Relativo alle eventuali relazioni tra il Sistema d'informazione Schengen e il progetto ASF - veicoli rubati (Automated Search Facility) di Interpol (97) 81.

L'ACC è stata invitata ad esaminare una nota della delegazione tedesca del Comitato di orientamento SIS (doc. SCH/OR.SIS (97) 81) del 30 aprile 1997 nella quale si presenta il progetto "ASF - veicoli rubati (Automated Search Facility)" in vista di una presa di posizione in ambito Schengen nei confronti di Interpol. Il progetto in questione spinge l'ACC a chiedersi se i dati SIS relativi alle persone e ai veicoli rubati possano essere trasmessi a Interpol.

La nota in oggetto descrive sommariamente il progetto: "Stando alle informazioni di cui dispone la delegazione tedesca, solo quattro Stati (Svezia, Lussemburgo, Russia e Slovacchia) partecipano attualmente alla parte del progetto relativa ai veicoli rubati. Sono disponibili attualmente record relativi a circa 80.000 veicoli rubati. (...) non solo per quanto riguarda in particolare le parti del progetto già in funzione relative alle persone e ai veicoli rubati, ma anche (...)".

E' inoltre prevista l'estensione del progetto ad altre categorie di dati (opere d'arte, carte di credito, documenti e passaporti falsificati, navi/aerei rubati). Considerata l'importanza che possono assumere in futuro progetti di questo tipo, l'ACC ha deciso di formulare un parere in merito a questo progetto e di rispondere al quesito relativo alla possibilità di trasmettere a Interpol nell'ambito del progetto ASF i dati del SIS relativi alle persone e ai veicoli rubati.

Limitandosi ai soli aspetti relativi alla protezione dei dati di natura personale, l'ACC

considerando che:

a) in virtù dell'articolo 101, quarto comma della Convenzione, solo le autorità competenti sono autorizzate a consultare direttamente i dati inseriti nel SIS. A tal fine, ciascuna Parte contraente comunica al Comitato esecutivo l'elenco delle autorità competenti autorizzate a consultare direttamente i dati inseriti nel Sistema d'Informazione Schengen. L'elenco indica per ciascuna autorità i dati che essa può consultare e per quali missioni;

b) in virtù dell'articolo 102, primo comma della Convenzione, le Parti contraenti possono utilizzare i dati soltanto ai fini enunciati per ciascuna categoria di segnalazioni;

— in virtù dell'articolo 102, secondo comma, della Convenzione, la duplicazione dei dati è vietata (salvo per motivi tecnici necessari per l'interrogazione diretta da parte delle autorità competenti);

— in virtù dell'articolo 102, quarto comma, della Convenzione, i dati non possono essere utilizzati per fini amministrativi;

— infine, in virtù dell'articolo 102, quinto comma, della Convenzione, qualsiasi utilizzazione dei dati non conforme ai summenzionati commi di tale articolo sarà considerata uno sviamento di finalità;

c) in virtù dell'articolo 104, primo comma, della Convenzione, fatte salve condizioni più rigorose previste dalla Convenzione, ai dati inseriti nella sezione nazionale de SIS si applica la legislazione nazionale;

d) in virtù dell'articolo 126, primo e secondo comma, della Convenzione, le trasmissioni di dati di natura personale potranno avvenire solo verso le Parti contraenti che hanno adottato le disposizioni nazionali necessarie per ottenere un livello di protezione dei dati personali almeno pari a quello derivante dai principi della Convenzione del Consiglio d'Europa del 28 gennaio 1981;

e) in virtù dell'articolo 118, lettera d), della Convenzione, ogni Parte contraente si impegna ad impedire che persone non autorizzate utilizzino i sistemi di elaborazione automatizzata di dati mediante apparecchiature per la trasmissione di dati;

f) i dati relativi alla marca, al tipo, al colore e alle caratteristiche tecniche dei veicoli non sono dati di natura personale a condizione che non sia possibile stabilire un collegamento con un dato che consenta di identificare una persona in relazione con il veicolo come, ad esempio, il numero di targa o di telaio, e di risalire all'identità del proprietario o del conducente del veicolo;

g) le autorità di polizia di ogni paese partecipante al sistema ASF possono scambiare informazioni (nella fattispecie dati di natura personale) provenienti da basi dati nazionali, nella misura in cui, mediante meccanismi di cooperazione di polizia bilaterale o multilaterale, questo scambio di informazioni sia autorizzato o non sia vietato dalla legislazione nazionale in materia di protezione dei dati;

h) si deve tener conto del parere dell'ACC del 7 marzo 1997 relativo al progetto pilota sui veicoli rubati (v. doc. SCH/Aut-cont (97) 2 riv.). In tale parere si trattava di determinare se i paesi non ancora integrati nel Sistema di Informazione Schengen possono avere accesso ai dati del SIS riguardanti i veicoli rubati;

BPH/div.

SCHENGEN

IT

Autorità di controllo comune

Bruxelles, 3 febbraio 1998

SCH/Aut-cont (97) 70 riv.

Traduzione: orig.\DE

Parere n. 98/4 dell'Autorità di controllo comune destinato al Comitato esecutivo

Oggetto: Registrazione delle consultazioni di cui all'articolo 103 della Convenzione

L'Autorità di controllo comune,

visto l'articolo 115 della Convenzione di applicazione dell'accordo di Schengen,

consapevole del fatto che il Sistema d'informazione Schengen (SIS) è un sistema di ricerca automatizzato che richiede un'efficace protezione contro l'accesso non autorizzato da parte di terzi,

che la registrazione di una media rappresentativa delle consultazioni del sistema effettuate costituisce un mezzo di protezione adeguato contro l'accesso non autorizzato,

che l'articolo 103 CSCH impone a ciascuna Parte contraente di provvedere affinché una trasmissione in media su dieci di dati personali sia registrata nella sezione nazionale del Sistema d'informazione Schengen dall'organo di gestione dell'archivio, ai fini del controllo dell'ammissibilità dell'interrogazione,

ritiene necessarie le seguenti esigenze minime per quanto concerne una regolare registrazione ai sensi dell'art. 103 CSCH:

1) Deve essere registrata una media sufficientemente rappresentativa di tutte le consultazioni, a prescindere dal fatto che alla relativa interrogazione venga data una risposta positiva o negativa. L'esigenza minima della registrazione del 10% può essere rispettata anche mediante una registrazione ad intervalli regolari.

2) Fanno parte degli elementi essenziali di un'adeguata registrazione:

- a) generalità trasmesse dalla persona oggetto della consultazione,
- b) identificazione del terminale utilizzato o dell'Autorità che ha proceduto all'interrogazione, badando a che siano adottate tutte le misure utili per consentire l'identificazione dell'utente,
- c) luogo, data e ora della consultazione,
- d) motivo della consultazione, per es. indicazione del fondamento giuridico di una segnalazione.

3) Ai fini di un controllo, in singoli casi, dell'ammissibilità della consultazione sarebbe inoltre auspicabile indicare il riferimento del dossier o il numero di protocollo della polizia per poter risalire al dossier di base, se disponibile.

4) I dati sono utilizzati esclusivamente ai fini previsti dall'art. 103.

5) I dati registrati vanno cancellati entro 6 mesi.

L'ACC insiste affinché si tenga conto dell'obbligo previsto dall'art. 103 in conformità del presente parere.

6.4. UNIONE EUROPEA - GRUPPO PER LA TUTELA DELLE PERSONE IN RELAZIONE AL TRATTAMENTO DEI DATI PERSONALI.

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV

6.4.1. Raccomandazioni.

Mercato interno e servizi finanziari

Libera circolazione delle informazioni, diritto delle società e informazione finanziaria

Libera circolazione delle informazioni, protezione dei dati e relativi aspetti finanziari

XV/5012/97-IT

Gruppo per la tutela delle persone
con riguardo al trattamento dei dati personali

RACCOMANDAZIONE 1/97

Norme in materia di protezione dei dati e mezzi di comunicazione

Adottata dal gruppo il 25 febbraio 1997.

SOMMARIO**1. INTRODUZIONE****2. ASPETTI GENERALI**

2.1. Libertà di espressione e tutela della vita privata.

2.2. Genesi legislativa dell'articolo 9 della direttiva.

2.3. Sintesi dell'attuale situazione in diritto nazionale.

3. CONCLUSIONI**IL GRUPPO PER LA TUTELA DELLE PERSONE
CON RIGUARDO AL TRATTAMENTO DEI 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 3 della direttiva,

Visto il suo regolamento interno, in particolare gli articoli 12 e 14, ha adottato la presente raccomandazione:

1. INTRODUZIONE

L'articolo 9 della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati ("la direttiva"), dispone che:

"Gli Stati membri prevedono, per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica e letteraria, le esenzioni o le deroghe alle disposizioni del presente capo e dei capi IV e VI solo qualora si rivelino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà di espressione".

Il gruppo, conformemente al mandato disposto dall'articolo 30 paragrafo 1, lettera a) della direttiva, nel corso della prima riunione ha iniziato a discutere la possibile attuazione dell'articolo 9. Le delegazioni britannica e tedesca hanno presentato dei documenti di lavoro. Il dibattito

1) GU n. L 281 del 23 novembre 1995, pag. 31.

tito ha evidenziato le differenze attualmente esistenti nelle legislazioni nazionali per quanto riguarda l'applicazione ai media²⁾ delle disposizioni sulla protezione dei dati.

Si è riconosciuto che il gruppo potrebbe dare utili orientamenti sull'interpretazione dell'articolo 9 della direttiva. Come prima iniziativa è stato deciso che il segretario raccolga informazioni sull'attuale situazione giuridica ed elabori una relazione tenendo conto del rapporto pubblicato dal Consiglio d'Europa nel 1991 "Data Protection and the Media" (La protezione dei dati e i media).³⁾

Il 21 febbraio 1996 è stato distribuito un questionario elaborato dal gruppo.

Nel corso della terza riunione il gruppo ha esaminato un documento di lavoro e ha tratto alcune conclusioni che sono state discusse in dettaglio nel corso della quarta riunione. Alla luce di dette conclusioni è emerso un consenso a favore dell'adozione del documento in forma di raccomandazione ai sensi dell'articolo 30, paragrafo 3, della direttiva. La raccomandazione è stata adottata dal gruppo il 25 febbraio 1997.

La parte che segue sottolinea alcuni aspetti generali dell'applicazione ai media delle norme sulla protezione dei dati compreso il contesto legislativo in cui s'inquadra l'articolo 9 della direttiva. La parte terza riassume alcune delle principali caratteristiche dell'attuale situazione normativa a livello nazionale.⁴⁾ La parte quarta contiene le conclusioni della discussione del gruppo sull'applicazione ai media delle norme sulla protezione dei dati.

L'articolo 9 prevede esenzioni e deroghe all'applicazione di alcune disposizioni della direttiva al trattamento di dati personali a scopi giornalistici o di espressione artistica e letteraria. Il dibattito del gruppo si è concentrato sul trattamento dei dati da parte dei media a scopi giornalistici. La presente raccomandazione riguarda quindi le esenzioni e deroghe in relazione a tale trattamento dei dati⁵⁾

2. ASPETTI GENERALI

2.1 Libertà di espressione e tutela della vita privata

L'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) stabilisce che:

"Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o comunicare informazioni o idee senza ingerenza alcuna da parte delle Autorità pubbliche e senza considerazioni di frontiera [...]".

Si tratta di uno dei diritti umani fondamentali derivante dalle tradizioni costituzionali comuni a tutti gli Stati membri e di uno degli elementi peculiari del patrimonio giuridico delle società democratiche. Storicamente è stato questo uno dei primi diritti dell'uomo ad essere riven-

2) Salvo diversamente indicato, il termine "media" è riferito a tutti i diversi mezzi di comunicazione di massa come la stampa, l'emissione radiofonica e televisiva, ecc.

3) Data protection and the media, studio elaborato dal comitato di esperti sulla protezione dei dati (CJ-PD) sotto l'autorità del Comitato europeo per la cooperazione giuridica (CDCJ), Consiglio d'Europa, Strasburgo 1991.

4) Ulteriori dettagli sulla situazione nazionale in ogni Stato membro figurano nel documento XV D 502/96.

5) La delegazione svedese precisa che la presente raccomandazione non pregiudica la libertà costituzionale garantita in Svezia ad ogni persona di esprimere le proprie opinioni attraverso i media.

dicato e di fatto garantito dalla legge. La stampa soprattutto ha ottenuto garanzie giuridiche e costituzionali specifiche, in particolare contro la censura preventiva.

Il diritto al rispetto della vita privata è ugualmente garantito dall'articolo 8 della CEDU. La protezione dei dati rientra nel rispetto della vita privata garantito da tale articolo. Le deroghe ai principi della protezione dei dati e all'articolo 8 della CEDU devono essere conformi alla legge e rispettare il principio di proporzionalità.⁶⁾ Ugualmente i limiti alla libertà di espressione, quali potrebbero derivare dall'applicazione dei principi in materia di protezione dei dati, devono essere conformi alla legge e rispettare il principio di proporzionalità.⁷⁾

I due diritti fondamentali non devono tuttavia essere considerati in sé contraddittori. In assenza di sufficienti garanzie di tutela della vita privata le persone possono essere restie ad esprimere liberamente le proprie idee. Analogamente il fatto di identificare lettori ed utenti dei servizi di informazione e di tracciarne il profilo rischia di disincentivare le persone a ricevere e dare informazioni.

2.2 Genesi legislativa dell'articolo 9 della direttiva

Conformemente all'articolo K, paragrafo 2 del trattato sull'Unione europea, l'Unione rispetta i diritti fondamentali quali sono garantiti dalla CEDU e quali risultano dalle tradizioni costituzionali comuni degli Stati membri.

Il legislatore comunitario ha riconosciuto il caso particolare dei media e la necessità di conciliare il rispetto della vita privata con la tutela della libertà d'espressione.⁸⁾

L'articolo 19 della proposta originaria della Commissione⁹⁾ prevedeva che gli Stati membri potessero accordare deroghe alle disposizioni della direttiva a favore degli organismi di stampa e audiovisivi. La relazione precisava che la principale caratteristica dell'articolo consisteva nell'esigenza di conciliare gli interessi in gioco e che a tal fine si poteva tener conto della possibilità di altri mezzi di ricorso o di un diritto di replica, dell'esistenza di un codice deontologico, dei limiti fissati dalla CEDU e dei principi generali del diritto.

L'articolo 9 della proposta modificata dalla Commissione¹⁰⁾ ha reso obbligatoria la concessione di deroghe a favore dei media. Il testo è stato inoltre modificato per includervi i giornalisti e limitare le deroghe alle attività giornalistiche.

L'articolo è stato ulteriormente modificato affinché le deroghe non possano applicarsi indiscriminatamente a tutte le disposizioni sulla tutela dei dati: nel testo attuale le deroghe sono sì obbligatorie, ma "soltanto se necessarie", nel senso che le deroghe ad ogni principio specifico della direttiva devono essere concesse soltanto laddove (in francese

6) P. es. European Court of Human Rights (CHR) Sunday Times, Series A, N. 30.

7) Vedere da ultimo CHR Goodwin c. Regno Unito, 27 marzo 1996, non ancora pubblicata.

8) La necessità di conciliare gli interessi tutelati da queste norme è stata riconosciuta anche dalla Convenzione 108/81 ("la Convenzione"). Nella relazione (rapporto esplicativo sulla convenzione relativa alla tutela delle persone fisiche con riguardo al trattamento automatico dei dati personali, Consiglio d'Europa, Strasburgo 1991) la libertà d'espressione è considerata come uno dei "diritti e libertà di altri" per la cui tutela i legislatori nazionali, conformemente all'articolo 9, paragrafo 2, lettera b) della Convenzione, possono derogare ai principi fondamentali della protezione dei dati.

9) COM(90) 314 def.-SYN 287.

10) COM(92) 422 def.-SYN 287.

"dans la seule mesure où", in tedesco "nur insofern vor, als sich dies als notwendig erweist") risultino necessarie per conciliare tutela della vita privata e libertà d'espressione.

Inoltre queste deroghe possono riguardare soltanto le disposizioni generali sulla legalità del trattamento dei dati a carattere personale, quelle sul trasferimento dei dati a paesi terzi e quelle sull'Autorità di vigilanza. Conformemente al "considerando" 37 non sarà possibile accordare nessuna deroga alle disposizioni in materia di sicurezza e le Autorità di vigilanza competenti in tale materia dovrebbero essere dotate almeno di alcuni poteri ex-post facto, quali il potere di pubblicare regolari relazioni o di adire le Autorità giudiziarie.

2.3 Sintesi dell'attuale situazione in diritto nazionale

Le varie normative nazionali attualmente affrontano il problema in uno dei modi seguenti:

a) In alcuni casi le norme sulla tutela dei dati non prevedono espressamente esenzioni dall'applicazione ai media di tali disposizioni. È il caso di Belgio, Spagna, Portogallo, Svezia e Regno Unito.

b) In altri casi i media sono esentati dall'applicazione di varie disposizioni sulla protezione dei dati. Si tratta attualmente di Germania¹¹⁾ Francia, Paesi Bassi, Austria e Finlandia. Deroghe analoghe sono previste anche dai disegni di legge italiani.

c) In altri ancora i media sono esentati dalla normativa generale sulla protezione dei dati e disciplinati da specifiche disposizioni in materia. È il caso della Danimarca per tutti i media e della Germania per le emittenti pubbliche, che non sono soggette alle leggi federali o dei Länder sulla tutela dei dati, ma sottostanno a specifiche disposizioni in materia contenute negli accordi inter-Länder che le regolamentano.

Le differenze tra questi tre tipi di approccio non andrebbero, tuttavia, sopravvalutate. In molti casi, indipendentemente dall'esistenza o meno di una deroga espressa, la normativa sulla tutela dei dati non si applica integralmente ai media a motivo dello status costituzionale particolare delle norme sulla libertà di espressione e di stampa. Tali norme limitano de facto l'applicazione di disposizioni fondamentali per la tutela dei dati o quanto meno il loro effettivo rispetto.

D'altro canto il regime ordinario di tutela dei dati generalmente si applica alle attività non editoriali svolte dai media.

Le autorità garanti della tutela dei dati riconoscono, nell'applicare le norme in materia, la particolarità dei media a prescindere dall'eventuale esistenza di un regime giuridico speciale.

La portata effettiva delle deroghe, inoltre, non può essere valutata in astratto ma dipende dalla struttura generale della normativa sulla tutela dei dati in ogni singolo paese. Chiaramente la portata delle deroghe necessarie dipende da quanto effettivamente le norme sostanziali incidono sulle attività dei media.

Le differenze per quanto riguarda l'applicazione ai media delle norme sulla tutela dei dati possono altresì spiegarsi col mutare delle prospettive sia quanto al ruolo di tali norme, sia quanto all'utilizzazione delle tecnologie dell'informazione da parte dei media. Ai primordi dell'applicazione

11) Con un'importante eccezione, per la quale vedere lettera c).

della tutela dei dati l'attenzione, si è concentrata essenzialmente sulle banche dati dotate di una grande unità centrale. Allora tali norme sembravano avere scarsi effetti sui media e non sembrava quindi necessaria nessuna deroga. Il maggior rilievo assunto dalla nozione di trattamento dei dati rispetto alla normativa sulla tutela dei medesimi e l'uso diffuso delle tecnologie dell'informazione da parte dei media hanno sostanzialmente mutato la situazione.

Un importante elemento che emerge dallo stato attuale delle normative negli Stati membri è che i media, o quanto meno la stampa, sono obbligati a rispettare determinate norme che pur non appartenendo alla legislazione sulla tutela dei dati *stricto sensu*, contribuiscono al rispetto della vita privata delle persone. Tale legislazione e la giurisprudenza spesso abbondante in materia accordano forme specifiche di riparazione che sono talvolta considerate un surrogato alla mancanza di mezzi correttivi preventivi in base alla legge sulla tutela dei dati.

Il diritto di replica e la possibilità di ottenere la rettifica delle false informazioni, gli obblighi professionali dei giornalisti e le relative procedure specifiche di autoregolamentazione, insieme alle norme per la tutela dell'onore (disposizioni di diritto civile e penale concernenti la diffamazione), devono esser presi in considerazione nel valutare come sia tutelata la vita privata in relazione ai media.¹²⁾

L'evoluzione dei media tradizionali verso la pubblicazione elettronica e la prestazione di servizi on-line sembra aggiungere ulteriori elementi di riflessione. La distinzione tra attività editoriali e non editoriali assume nuove dimensioni per i servizi on-line che, diversamente da tutti i media tradizionali, consentono di identificare le persone che li ricevono.

3. Conclusioni

Quanto precede sembra confermare che in ogni Stato membro è necessario riconsiderare il quadro legislativo per l'applicazione ai media delle norme sulla tutela dei dati. In proposito è necessario valutare fino a che punto l'applicazione di ciascuna delle disposizioni dei capitoli II, IV e VI della direttiva debba essere limitata per tutelare la libertà di espressione.

A tal fine occorre tener presenti vari elementi:

- Le norme sulla tutela dei dati si applicano normalmente ai media. Deroche ed esenzioni possono essere accordate unicamente in relazione al capo II (condizioni generali di liceità dei trattamenti di dati personali), al capo IV (trasferimento di dati personali verso paesi terzi) e al capo VI (poteri delle Autorità di controllo). Non è possibile accordare deroghe o esenzioni con riferimento alle disposizioni di sicurezza. Le Autorità garanti responsabili per questo settore devono in tutti i casi conservare alcuni poteri *ex-post facto*.

12) Una delle principali conclusioni del lavoro del Consiglio d'Europa in materia è che l'esistenza di correttivi speciali in base alla legge sui media può giustificare deroghe alla normativa sulla tutela dei dati e proprio per questo all'articolo 8 della CEDU, soltanto in determinate circostanze. Il rapporto del Consiglio d'Europa (*supra*) suggerisce che, per compensare la non applicazione di alcuni principi di tutela dei dati, la legislazione sui media si conformi alla risoluzione 428 dell'assemblea parlamentare del Consiglio d'Europa (1970) sui mezzi di comunicazione di massa e sui diritti dell'uomo e alla risoluzione del Comitato dei ministri sul diritto di replica. Il diritto di replica è stato inserito nell'articolo 8 della Convenzione europea sulla televisione transfrontaliera (European Treaty Series, n. 132/89).

- Derghe ed esenzioni ai sensi dell'articolo 9 devono rispettare il principio di proporzionalità e devono essere accordate soltanto in relazione alle disposizioni che possono ledere la libertà d'espressione e unicamente nella misura necessaria all'effettivo esercizio di tale libertà conciliandola con il diritto al rispetto della vita privata della persona cui si riferiscono i dati.

- Derghe ed esenzioni ai sensi dell'articolo 9 potrebbero non essere necessarie se la flessibilità delle varie disposizioni della direttiva o le deroghe accordate in base ad altre disposizioni specifiche (che naturalmente vanno interpretate restrittivamente) permettono già di conciliare in modo soddisfacente il rispetto della vita privata con la libertà d'espressione.¹³⁾

- L'articolo 9 della direttiva rispetta il diritto delle persone alla libertà di espressione. Le deroghe e le esenzioni ai sensi dell'articolo 9 non possono essere accordate ai media o ai giornalisti in quanto tali, ma soltanto a chi effettui il trattamento dei dati personali esclusivamente a scopi giornalistici.

- Derghe ed esenzioni possono riguardare soltanto il trattamento dati per scopi giornalistici (editoriali) compresa la pubblicazione elettronica. Qualsiasi altra forma di trattamento dati da parte dei giornalisti o dei media è soggetta alle disposizioni ordinarie della direttiva. Tale distinzione è particolarmente importante per la pubblicazione elettronica. Il trattamento di dati degli abbonati a fini di fatturazione o il trattamento a fini di marketing diretto (compreso il trattamento dei dati sull'uso dei media per tracciare il profilo degli utenti) ricade nel regime ordinario di tutela dei dati.

- La direttiva esige che si concilino due libertà fondamentali. Per valutare se le limitazioni dei diritti ed obblighi derivanti dalla direttiva siano proporzionate alla finalità perseguita, consistente nel tutelare la libertà d'espressione, occorrerebbe prestare particolare attenzione alle garanzie specifiche di cui godono le persone in relazione ai media. I limiti al diritto d'accesso e di rettifica preventiva potrebbero essere proporzionati soltanto se le persone godono del diritto di replica o ottengono la rettifica delle informazioni false dopo la pubblicazione.

- Le persone hanno in ogni caso diritto a forme adeguate di riparazione in caso di violazione dei loro diritti.¹⁴⁾

Nel valutare se le esenzioni o le deroghe sono proporzionate, occorre prestare attenzione ai vigenti obblighi etici e professionali dei giornalisti e alle forme di autoregolamentazione previste dalla categoria.

Fatto a Bruxelles, addì 25 febbraio 1997

Per il gruppo
Il Presidente
P.J. Hustinx

13) Ad esempio, nel valutare se si debbano accordare esenzioni dall'articolo 11 occorre considerare che l'obbligo di informare le persone cui si riferiscono i dati non si applica quando ciò comporta un onere sproporzionato.

14) Non è possibile nessuna esenzione o deroga al capo III della direttiva.

**COMMISSIONE EUROPEA
DIREZIONE GENERALE XV****Mercato interno e servizi finanziari****Libera circolazione delle informazioni - Diritto delle società e informazione finanziaria****Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali****XV/5060/97- Final Corr IT
WP2****Gruppo sulla tutela delle persone
in relazione al trattamento dei dati personali****RACCOMANDAZIONE 2/97****Relazione e orientamento del Gruppo di lavoro internazionale sulla tutela dei dati nelle telecomunicazioni ("Memorandum di Budapest - Berlino sulla tutela dei dati e della vita privata su Internet")****adottato dal Gruppo il 3 dicembre 1997.**

IL GRUPPO PER LA TUTELA DELLE PERSONE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI**Istituito con direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995¹⁾****Visti gli articoli 29 e 30, paragrafo 3 di detta direttiva,****Visto il regolamento interno e in particolare gli articoli 12 e 14, ha adottato la seguente raccomandazione:****In occasione della sua 8ª riunione, tenutasi a Bruxelles il 3 dicembre 1997, il Gruppo prende atto della relazione e della guida del Gruppo internazionale sulla tutela dei dati nelle telecomunicazioni ("Memorandum di Budapest - Berlino sulla tutela dei dati e della vita privata su Internet");****Ritiene che tale iniziativa possa contribuire ad una migliore tutela dei diritti fondamentali della persona, in particolare la vita privata, su scala mondiale.**

**COMMISSIONE EUROPEA
DIREZIONE GENERALE XV****Mercato interno e servizi finanziari****Libera circolazione dell'informazione, diritto delle società e informazione finanziaria****Libera circolazione dell'informazione e protezione dei dati, inclusi gli aspetti internazionali****XV D /5022/97 def.
WP6**

1) GU n. L 281 del 23 novembre 1995, p. 31.

Gruppo per la tutela delle persone fisiche
con riguardo al trattamento dei dati personali

RACCOMANDAZIONE 3/97

Anonimato su Internet

Adottata dal gruppo di lavoro in data 3 dicembre 1997

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

Istituito con la direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995¹⁾

Visti gli articoli 29 e 30, paragrafo 3 della suddetta direttiva,

Visto il suo regolamento interno, in particolare gli articoli 12 e 14,

ha adottato la seguente raccomandazione:

Il gruppo di lavoro nel corso dell'ottava riunione svoltasi a Bruxelles il 3 dicembre 1997 ha adottato il documento di lavoro XV/5022 ("Anonimato su Internet") e ha preso atto della relazione e degli orientamenti espressi dal lavoro internazionale sulla tutela dei dati nelle telecomunicazioni ("Protocollo di Budapest-Berlino relativo alla tutela dei dati e sulla riservatezza su Internet");

Raccomanda che la Commissione europea sviluppi delle proposte sulla base del documento di lavoro allegato ("Anonimato su Internet"; Allegato 1) nonché delle raccomandazioni contenute nel protocollo Budapest-Berlino (Allegato 2) per favorirne l'applicazione in tutte le sedi internazionali appropriate.

DOCUMENTO DI LAVORO - ANONIMATO SU INTERNET

Adottato nel corso dell'ottava riunione

Introduzione

Il rapido sviluppo di Internet e la prolifica crescita dei tipi e del numero di servizi disponibili attraverso questo nuovo strumento sono già stati ben documentati. È chiaro che il fenomeno Internet sta già trasformando le nostre abitudini di vita e di lavoro, apportando enormi cambiamenti alle modalità di acquisto e vendita di beni e servizi e rimodellando il comportamento delle organizzazioni del settore sia pubblico che privato.

Trasformazioni così importanti e complesse comportano inevitabilmente nuovi problemi e nuove sfide per coloro cui spetta il compito di definire, sviluppare e applicare una nuova politica. Inizialmente l'attenzione degli operatori politici si è concentrata sul potenziale di Internet sia come sede per comportamenti penalmente rilevanti o "riprovevoli sulla rete" (come la distribuzione di pornografia infantile) e come "strumento sicuro" di comunicazione per facilitare le attività criminali "fuori della rete".

1) GU L281 del 23 novembre 1995, pag. 31.

A livello europeo queste preoccupazioni hanno costituito la motivazione principale di una serie di iniziative: il Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e d'informazione (COM (36) 483 def.), la Comunicazione della Commissione sul contenuto illegale e nocivo su Internet (COM (96) 487), la risoluzione del Consiglio del 28 novembre 1996 sul contenuto illegale e nocivo e la relazione del gruppo di lavoro sul contenuto illegale e nocivo preparata dal Consiglio informale riunito a Bologna.

Gradualmente, tuttavia, è emerso con chiarezza che vi sono connessi anche altri problemi. La comunicazione della Commissione "Una iniziativa europea in materia di commercio elettronico" (COM (97) 157) cerca di ampliare il dibattito includendo un'ampia serie di altri settori importanti come l'imposizione fiscale (in particolare l'IVA) dell'attività commerciale on-line e la tutela dei diritti di proprietà intellettuale rispetto al contenuto distribuito sulla rete²⁾

In tutti questi settori vengono discusse nuove idee e vengono presentate nuove potenziali soluzioni al fine di assicurare che i valori tradizionali e gli interessi societari sviluppati nel corso di molti decenni possano continuare a essere conservati anche in questa nuova età tecnologica. Un problema che tocca molti di questi ambiti risiede nella difficoltà di individuare il verificarsi di un atto illegale e successivamente identificare il responsabile. Chi è responsabile per l'inserimento di un particolare documento di pornografia infantile su Internet? Chi ha trasmesso un particolare documento protetto da copyright? Chi non ha dichiarato l'IVA rispetto a servizi offerti sulla rete?

Di fronte a questi problemi una reazione comprensibile ha consistito nel suggerire che quanti desiderano accedere a Internet e ai suoi vari servizi in linea debbono essere debitamente identificati e che tutta l'attività in linea possa essere individuabile.

La prospettiva della riservatezza

Lo sviluppo di una politica nei confronti di Internet non avviene in uno spazio vuoto, ma piuttosto sulla base di principi e valori ben stabiliti. I critici dei tentativi di limitare o disciplinare l'attività nel ciberspazio citano frequentemente il diritto alla libera espressione, un diritto fondamentale garantito in Europa dall'articolo 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo (ECHR) e incluso come principio generale del diritto comunitario nell'articolo K.2. del trattato sull'Unione europea. Tuttavia, il diritto alla riservatezza (articolo 8 della Convenzione europea dei diritti dell'uomo, analogamente inserito nel diritto comunitario) è altrettanto importante quando si tratta di valutare la politica da adottare nei confronti di Internet.

Nel corso degli ultimi 25 anni è emerso chiaramente che una delle maggiori minacce al diritto fondamentale alla riservatezza è la capacità delle organizzazioni di accumulare un gran numero di informazioni sulle persone, in forma digitale, la quale si presta alla manipolazione, alterazione e comunicazione a terzi ad alta velocità (ed ora a basso costo). Le preoccupazioni in merito a tali sviluppi e al potenziale abuso di questi dati personali ha indotto tutti gli Stati europei (ed ora anche la Comu-

2) Quest'ultimo problema è già stato affrontato nel Libro verde e nella comunicazione della Commissione "Iniziativa da prendere a seguito del Libro verde sul diritto d'autore e i diritti connessi nella società dell'informazione".

nità con la direttiva 95/46/CE) ad adottare una legislazione specifica in materia di protezione dei dati, introducendo così un quadro normativo che disciplina il trattamento delle informazioni personali.

Un principio fondamentale in materia di protezione dei dati (vedi articoli 6(1)(c) e 7 della direttiva 95/46/CE) è che i dati personali raccolti in qualsiasi situazione debbano limitarsi a quanto è strettamente necessario e attinente alla finalità in questione. Ogni tipo d'informazione personale costituisce una minaccia potenziale alla riservatezza di una persona ed è quindi necessario fare in modo che, quando tali informazioni vengono raccolte, ciò avvenga per una finalità legittima e che la quantità d'informazioni raccolte sia limitata al minimo indispensabile.

Una caratteristica delle reti di telecomunicazioni e di Internet in particolare è il loro potenziale atto a generare una grande quantità di dati transazionali (i dati generati per assicurare le connessioni corrette). Le possibilità di uso interattivo delle reti (una caratteristica che distingue molti servizi Internet) aumentano ulteriormente il numero di dati transazionali. Quando consulta un giornale sulla rete, l'utilizzatore "interagisce" scegliendo le pagine che desidera leggere. Queste scelte creano un "clickstream" di dati transazionali. Le notizie e i servizi d'informazione più tradizionali, invece vengono consumati in modo molto più passivo (come la televisione, ad esempio), dove la interattività è limitata al mondo off-line delle edicole e delle librerie. Sebbene i dati transazionali in taluni ordinamenti ricevano un certo grado di protezione nel quadro della legislazione che tutela la riservatezza della corrispondenza, la crescita massiccia della quantità di questi dati costituisce tuttavia una fonte di legittime preoccupazioni.

Dato che i servizi sulla rete si sviluppano sia dal punto di vista della loro sofisticazione che della loro popolarità, il problema dei dati transazionali non potrà che aggravarsi. Per ogni dove ci spostiamo su Internet, lasciamo una traccia digitale. Nella misura in cui un sempre maggior numero delle nostre attività quotidiane viene condotto sulla rete, sempre più quello che facciamo, le nostre scelte, le nostre preferenze, diventerà oggetto di registrazione.

Ma i rischi alla nostra riservatezza personale risiedono non solo nell'esistenza di grandi quantitativi di dati personali su Internet, ma anche nello sviluppo del software capace di esplorare la rete e mettere assieme tutti i dati disponibili relativi a una determinata persona. Un articolo apparso recentemente sul Minneapolis Star Tribune ha spiegato come si poteva compilare una biografia dettagliata di una persona scelta a caso, utilizzando tale software e sfruttando le informazioni provenienti da tutti i gruppi di discussione a cui la persona ha partecipato. In tal modo il giornale è stato in grado di scoprire l'indirizzo e il numero di telefono di una persona, il suo luogo di nascita, dove essa ha studiato, la sua professione, il suo attuale posto di lavoro, la sua passione per le recite di attori dilettanti, il tipo di birra che preferisce, i ristoranti e luoghi di vacanza abituali e la sua opinione su argomenti diversi come Bill Gates o lo Stato dell'Indiana considerato "socialmente repressivo". Vi è già una serie di siti negli Stati Uniti che offrono a titolo commerciale questi "servizi di ricerca".

I dati anonimi - un modo per affrontare le preoccupazioni relative alla riservatezza

I dati transazionali costituiscono una minaccia per la riservatezza dell'individuo solo se essi fanno riferimento a una determinata persona. Evidentemente, un modo per venire incontro alle preoccupazioni relative