125 RACCOMANDAZIONE RELATIVA AI REQUISITI MINIMI PER LA RACCOLTA DI DATI ON-LINE NELL'UNIONE EUROPEA (ADOTTATA IL 17 MAGGIO 200)1

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 1, lettera a), e paragrafo 3 di detta direttiva,

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

ha adottato la presente raccomandazione:

1. Introduzione

1. Nel documento di lavoro intitolato "Tutela della vita privata su Internet–Un approccio integrato dell'EU alla protezione dei dati *on-line*", del 21 novembre 2001 (2), il Gruppo di lavoro ha evidenziato come sia importante garantire la messa in atto di strumenti adeguati per assicurare che l'utente Internet riceva tutte le informazioni necessarie affinché possa riporre la propria fiducia, con cognizione di causa, sui siti visitati e, se necessario, esercitare determinate scelte conformemente ai propri diritti come previsto dalla normativa europea. Tale fattore risulta particolarmente importante in considerazione del fatto che l'uso di Internet moltiplica le possibilità di raccolta di dati personali e, conseguentemente, i pericoli per i diritti fondamentali e le libertà degli individui, soprattutto per quel che riguarda la loro vita privata. Nel suo Parere n. 4/2000 del 16 maggio 2000 sul livello di tutela dei dati offerto dai principi dell'"approdo sicuro" (*Safe Harbor*), il Gruppo di lavoro ha invitato la Commissione a valutare con urgenza l'opportunità di creare un marchio di qualità per i siti Internet, che si basi su criteri comuni che potrebbero essere stabiliti a livello comunitario.

Questa raccomandazione fa seguito ai due documenti sopracitati. Essa intende contribuire all'effettiva ed omogenea applicazione delle disposizioni nazionali adottate in conformità alle direttive (3) sulla tutela dei dati personali fornendo indicazioni concrete sull'attuazione delle norme contenute in tali direttive relativamente alle pratiche più comuni esercitate attraverso Internet. Tali pratiche si verificano soprattutto al momento del "contatto iniziale" tra l'utente Internet ed un sito *web* sia nel caso di esclusiva ricerca di informazioni, sia nel caso di esecuzione di operazioni commerciali su base graduale.

Le indicazioni fornite di seguito riguardano in particolar modo la raccolta di dati personali su Internet e si prefiggono di identificare le misure che dovranno essere attuate nei confronti delle persone interessate per garantire la lealtà e la liceità di tali pratiche (applicazione degli articoli 6, 7, 10 e 11 della direttiva 95/46/CE). Tali indicazioni focalizzano in particolare sul come, quando e quali informazioni occorre fornire all'utente individuale, con l'aggiunta di dettagli pratici relativi a diritti ed obblighi risultanti da dette direttive.

Il principale obiettivo di questa raccomandazione consiste dunque nel fornire un concreto valore aggiunto all'attuazione dei principi generali della direttiva. Il Gruppo di lavoro considera la presente raccomandazione come la prima iniziativa per la presentazione a livello europeo dell'insieme "minimo" di obblighi ai quali i responsabili del trattamento (le persone fisiche o giuridiche responsabili del trattamento dati nell'ambito di un sito *web*) (4) che si occupano di siti Internet in cui vengono richieste infor-

---

1 Gazzetta ufficiale L 281 del 23/11/1995, pag. 31, disponibile su:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

2 WP 37 (5063/00): documento di lavoro - Tutela della vita privata su Internet – Un approccio integrato dell'EU alla protezione dei dati on-line. Adottato il 21 novembre 2000. Disponibile su:
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp37en.htm

3 Direttiva 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e direttiva 97/66/CE del 15 dicembre 1997 sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. Disponibili su:
http://europa.eu.int/comm/inernal_market/en/media/dataprot/law.htm

4 A titolo di riferimento, l'articolo 2 della direttiva 95/46/CE definisce il responsabile del trattamento come "la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali. Quando le finalità e i mezzi del trattamento sono determinati da disposizioni legislative o regolamentari nazionali o comunitarie, il responsabile del trattamento o i criteri specifici per la sua designazione possono essere fissati dal diritto nazionale o comunitario".

mazioni particolareggiate o la specificazione del campo d'azione (5) possano facilmente conformarsi. Certamente questa raccomandazione non esonera i responsabili del trattamento dall'obbligo attualmente vigente di verificare la conformità di tali trattamenti all'intera serie di requisiti e condizioni precisati nel diritto nazionale applicabile per renderlo legittimo, verifica senza la quale tale trattamento non risulta idoneo.

Tale raccomandazione si applica nel caso in cui il responsabile del trattamento abbia sede in uno degli Stati membri dell'Unione europea. In questa circostanza sarà applicato il diritto nazionale dello Stato membro in oggetto al trattamento dei dati personali che avvenga nel contesto delle attività di tale stabilimento. Tale raccomandazione si applica altresì quando il responsabile del trattamento non ha sede nel territorio della Comunità ma ricorre, ai fini del trattamento di dati personali, a strumenti automatizzati o non automatizzati situati nel territorio di uno degli Stati membri dell'UE. Tale trattamento è contemplato dalla legislazione nazionale dello Stato membro in cui si trovano i supporti tecnici o le risorse (6).

2. La raccomandazione, per poter conseguire tale obiettivo, è rivolta particolarmente:

– ai responsabili del trattamento che raccolgono dati *on-line*, dotandoli di una guida pratica che elenchi l'insieme minimo delle misure concrete da attuare;

– ai singoli utenti Internet affinché siano informati a riguardo e affinché possano esercitare i propri diritti;

– alle istituzioni desiderose di assegnare un'etichetta certificante la conformità delle procedure di trattamento impiegate alle direttive europee sulla protezione dei dati, dotandole di criteri di riferimento per l'assegnazione di tale etichetta riguardo alle informazioni da apporre e alla raccolta di dati personali. È ovvio che, al momento dell'assegnazione dell'etichetta, occorrerà tener conto di separati criteri concernenti altri obblighi e diritti oltre ai suddetti criteri di riferimento. Il Gruppo di lavoro pubblicherà successivamente un esauriente documento relativo a detta problematica;

alle autorità europee responsabili della protezione dei dati per poterle dotare di un quadro di riferimento comune per il loro compito di verifica della conformità alle disposizioni nazionali adottate dagli Stati membri, conformemente alle direttive sopracitate;

3. Il Gruppo di lavoro è inoltre del parere che tale raccomandazione dovrebbe servire da riferimento per la definizione dei criteri per *software* e *hardware* preposti alla raccolta e al trattamento di dati personali su Internet.

II. Raccomandazioni sulle informazioni da fornire in caso di raccolta di dati nel territorio degli Stati membri dell'Unione europea.

2.1. Informazioni da fornire alla persona interessata e tempi da rispettare

4. Qualsiasi raccolta di dati personali individuali ottenuta attraverso un sito *web* richiede l'anticipata fornitura di determinate informazioni. In termini di contenuto la conformità a tale obbligo rende necessario:

5. menzionare l'identità, l'indirizzo fisico e quello elettronico del responsabile del trattamento e, ove possibile, quello dell'eventuale rappresentante in forza all'articolo 4.2 della direttiva;

---

5 Le raccomandazioni concrete della presente raccomandazione costituiscono i requisiti minimi nel senso che non sono le uniche. In futuro tali raccomandazioni dovrebbero essere integrate da altre relative al trattamento di dati personali ancor più sensibili, come il trattamento riguardante siti sanitari e siti rivolti a bambini o i servizi offerti dai portali. In quanto ad altre specifiche modalità di trattamento, come la divulgazione di dati personali in un sito o la conservazione dei dati sul traffico da parte dei fornitori di servizi Internet e dei fornitori di contenuti e servizi Internet, si rimanda alle raccomandazioni del Gruppo di lavoro contenute nel documento citato nella nota n. 1 e alle altre posizioni del caso assunte dal Gruppo di lavoro, come il WP 25 (5085/99): Raccomandazione 3/99 relativa alla conservazione dei dati sulle comunicazioni da parte dei fornitori di servizi Internet a fini giudiziari. Approvata il 7 settembre 1999. WP 18 (5005/99): Raccomandazione 2/99 relativa al rispetto della vita privata nel contesto dell'intercettazione delle telecomunicazioni. Approvata il 3 maggio 1999. WP 17 (5093/98): Raccomandazione 1/99 sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software ed hardware. Approvata il 23 febbraio 1999. Tutto disponibile su: cfr. nota n. 1.

6 Cfr. articolo 4, paragrafo 1, punti a) e c) della direttiva 95/46/CE. È necessario mantenere nettamente distinto tale aspetto dalla questione del trasferimento legale di dati personali dall'UE ad un paese terzo. Tale problematica è trattata dagli articoli 25 e 26 della direttiva 95/46/CE e dalle connesse decisioni della Commissione europea relative all'adeguatezza della tutela nei paesi terzi. Ad esempio, se un sito web americano fa uso di strumenti situati all'interno dell'UE per la raccolta ed il trattamento di dati personali sarà applicata alle operazioni di raccolta e di trattamento la legislazione dello stato europeo in questione, a prescindere dall'adeguatezza del livello di protezione fornito da tale compagnia e conformemente alla decisione della Commissione europea relativa all'approdo sicuro. Tale problematica relativa all'adesione o meno dello Stato destinatario di dati all'approdo sicuro sarà pertinente esclusivamente in merito alla liceità delle successive cessioni di dati personali dalla compagnia con sede all'interno dell'UE a quell'altra

6. menzionare chiaramente la/le finalità del trattamento con il quale il responsabile raccoglie dati attraverso un sito *web*. Ad esempio, nel caso in cui tali dati vengano raccolti per stipulare un contratto (abbonamento ad Internet, ordine di prodotti, ecc.) ed anche per la commercializzazione diretta, occorre che il responsabile specifichi chiaramente le due finalità in questione;

7. menzionare chiaramente il carattere obbligatorio o facoltativo delle informazioni richieste. Le informazioni obbligatorie sono quelle indispensabili all'espletamento del servizio richiesto. Ad esempio, è possibile evidenziare il carattere obbligatorio o facoltativo apponendo un asterisco all'informazione di carattere obbligatorio oppure, in alternativa, è possibile scrivere "facoltativo" accanto all'informazione non obbligatoria. Il fatto che la persona interessata non fornisca informazioni facoltative non deve tornarle a svantaggio in nessun modo;

8. menzionare l'esistenza di diritti, e delle condizioni per il loro esercizio, in base ai quali l'interessato possa esprimere il proprio consenso o, eventualmente, opporsi al trattamento di dati personali (7). È necessario parimenti fornire indicazioni sulle modalità di accesso, di rettifica o di cancellazione di tali dati o informazioni, sia riguardo la persona o il servizio al quale occorre rivolgersi per l'esercizio di tali diritti, che relativamente alla possibilità di esercitarli on-line e all'indirizzo fisico del responsabile;

9. elencare i destinatari o le categorie di destinatari delle informazioni raccolte. Al momento della raccolta di dati i siti Internet dovrebbero specificare se i dati raccolti saranno comunicati o resi disponibili a terzi – tra cui, in particolare, partner commerciali, imprese figlie, ecc. – e le relative motivazioni (con finalità diverse dalla fornitura del servizio richiesto e per la commercializzazione diretta (8). In questi casi è fondamentale che gli utenti Internet dispongano di un'effettiva possibilità di opporsi *on-line* a detta comunicazione cliccando su di una casella di spunta ed esprimendo così il proprio favore alla comunicazione dei dati con finalità diverse dalla fornitura del servizio richiesto. Dal momento che il diritto di opporsi può essere esercitato in qualunque momento, occorre menzionare anche nelle informazioni fornite alla persona interessata la possibilità di esercitare tale diritto *on-line*. Il Gruppo di lavoro, consapevole degli svantaggi recati dal sovraccarico di informazioni negli schermi, è del parere che, se non appaiono nomi di destinatari, il responsabile del trattamento si impegna a non comunicare le informazioni raccolte a terzi i cui nomi ed indirizzi non siano stati forniti (a meno che la loro identità sia ovvia), garantisce che la comunicazione dei dati sia necessaria all'espletamento del servizio richiesto dall'utente Internet e che tale comunicazione sia effettuata esclusivamente con quella finalità.

10. Nel caso in cui sia previsto che il responsabile del trattamento trasmetta i dati a paesi esterni all'Unione europea, specificare se tali paesi garantiscono una protezione adeguata degli individui riguardo al trattamento dei loro dati personali, in forza dell'articolo 25 della direttiva 95/46/CE. In questo caso è necessario fornire informazioni specifiche a proposito dell'identità e dell'indirizzo dei destinatari (indirizzo fisico e/o elettronico) (9) ;

11. fornire nome ed indirizzo (indirizzo fisico e/o elettronico) del servizio o della persona incaricata di rispondere ad eventuali quesiti riguardanti la protezione di dati personali;

12. menzionare chiaramente l'esistenza di procedure di raccolta automatica di dati prima di utilizzare simili metodi per detta raccolta (10) . Nel caso di un ricorso a tali procedure è necessario che la persona interessata riceva le informazioni contenute in questo documento. Detta persona dovrà inoltre essere

---

7 Il trattamento a finalità specifiche è consentito solo se motivato da una delle considerazioni elencate nell'articolo 7 della direttiva 95/46/CE (tra l'altro nei casi in cui la persona interessata abbia fornito esplicitamente il proprio consenso, in cui il trattamento risulti indispensabile per l'esecuzione del contratto con la persona interessata, in cui il trattamento risulti indispensabile per adempiere ad un obbligo legale del responsabile del trattamento e in cui tale trattamento risulti indispensabile per il perseguimento dell'interesse legittimo del responsabile oppure di quello di terzi che hanno fatto uso di tali dati, a meno che l'interesse della persona in oggetto non risulti prevalente).

Il diritto ad opporsi (cfr. articolo 14) è fissato dagli Stati membri in almeno due situazioni di cui all'articolo 7, inclusa l'ultima menzionata sopracitata. L'individuo ha il diritto, salvo disposizione contraria prevista dalla normativa nazionale, di opporsi in qualsiasi momento per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che lo riguardano. Il diritto di opporsi su richiesta e gratuitamente sussiste in ogni caso quando il trattamento in oggetto è finalizzato alla commercializzazione diretta. La persona interessata può inoltre opporsi gratuitamente (una volta informata ed a partire dalla prima comunicazione) alla comunicazione di dati personali a terzi o al loro utilizzo per conto di terzi per la commercializzazione diretta.

8 La comunicazione a terzi è consentita solo nel caso in cui la finalità prevista non sia incompatibile con quella per la quale i dati sono stati raccolti e se motivata da una delle considerazioni elencate nell'articolo 7, condizioni che rendono legittimo il trattamento.

9 Informazioni riguardo l'adeguatezza delle decisioni sono disponibili sul sito Web della Commissione al seguente indirizzo:
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

10 Il trattamento "invisibile" ed automatico dei dati personali è soggetto alle medesime modalità, condizioni e garanzie delle altre tipologie di trattamento di dati personali. Cfr. Raccomandazione 1/99 del Gruppo di lavoro sul trattamento invisibile ed automatico dei dati personali su Internet effettuato da software e hardware (23 febbraio 1999), disponibile sul sito web citato nella nota n. 1.

informata circa il nome del dominio dal quale il server del sito trasmette le procedure di raccolta automatica, le finalità di dette procedure, il loro periodo di validità, l'eventualità in cui l'accettazione di tali procedure sia necessaria per visitare il sito e le possibili conseguenze di una loro disattivazione. Se vi sono altri responsabili del trattamento coinvolti nella raccolta dei dati personali occorre che la persona interessata riceva tutte le informazioni riguardanti l'identità del responsabile e le finalità del trattamento relativamente a ciascun responsabile di detto trattamento. È necessario comunicare la possibilità di opporsi alla raccolta prima di ricorrere a qualsiasi procedura automatica che provochi la connessione di un utente PC ad un altro sito *web*. Es. allo scopo di evitare che un secondo sito possa raccogliere dati ad insaputa di in utente Internet nel caso in cui questo venga automaticamente connesso da un sito *web* ad un altro per visualizzare pubblicità sotto forma di *banner*. Ad esempio, se un cookie viene collocato dal server del responsabile del trattamento è necessario comunicare detta informazione prima che venga spedito all'*hard disk* dell'utente Internet, in aggiunta alle informazioni fornite grazie alla tecnologia esistente che si limita a specificare il nome del sito di trasmissione ed il periodo di validità di detto cookie (11).

13. Indicare le misure di sicurezza a garanzia dell'autenticità del sito, del grado di completezza e riservatezza delle informazioni trasmesse nella detta rete in applicazione della legislazione nazionale applicabile. (12)

14. Fornire le informazioni in tutte le lingue usate nel sito *web* e, specialmente, in quei passaggi ove avviene la raccolta dei dati personali.

15. Che i responsabili del trattamento verifichino la coerenza delle informazioni contenute nei vari documenti destinati al sito (le sezioni "dati personali e protezione della vita privata", i moduli elettronici, testi relativi alle condizioni generali di vendita e ad altre comunicazioni commerciali).

2.2. *Modalità di presentazione delle informazioni*

16. Il Gruppo di lavoro ritiene che le seguenti informazioni debbano apparire direttamente sullo schermo prima che avvenga la raccolta, così da assicurare un giusto trattamento dei dati.

Dette informazioni riguardano:
l'identità del responsabile del trattamento;
la/le finalità;
la natura obbligatoria o facoltativa delle informazioni richieste;
i destinatari o le categorie di destinatari dei dati raccolti;
l'esistenza del diritto di accesso e di rettifica;
l'esistenza del diritto di opporsi a qualsiasi comunicazione dei dati a terzi con finalità diverse dalla fornitura del servizio richiesto e le modalità per esercitare tale diritto (ad esempio fornendo la possibilità di cliccare su una casella di spunta);
le informazioni da fornire in caso di utilizzo di procedure di raccolta automatica;
il livello di sicurezza nel corso di tutte le fasi del trattamento compresa la trasmissione, ad esempio sulle reti.

In tali situazioni le informazioni devono essere fornite interattivamente e devono apparire sullo schermo. Così, nel caso di metodi automatici di raccolta dati, dette informazioni possono essere fornite, se necessarie, tramite la tecnica delle finestre *pop-up*.

A proposito del livello di sicurezza nel corso della trasmissione dei dati dall'apparecchiatura occorre visualizzare un'intestazione del tipo "Stai accedendo ad una connessione protetta" oppure le procedure di informazione automatica presenti nei *browser*, come la comparsa di icone specifiche sotto forma di chiave o di lucchetto.

17. Il Gruppo di lavoro ritiene inoltre che sia necessario poter accedere ad informazioni esaustive riguardo alla politica di tutela della sfera privata (comprese le modalità per l'esercizio del diritto d'accesso) direttamente dalla pagina d'entrata del sito e ovunque vengano raccolti dati personali on-line. Il

11 Se il cookie è collocato da un'organizzazione attraverso il proprio sito web e soltanto questa è in grado di accedere al contenuto di detto cookie non occorre fornire informazioni aggiuntive riguardo l'organizzazione responsabile del collocamento del cookie, purché l'organizzazione che ospita tale sito web sia già stata adeguatamente identificata.

12 Cfr. le norme specifiche dell'articolo 17, paragrafi 1 e 3 secondo trattino della direttiva 95/46/CE.

titolo dell'intestazione su cui cliccare deve essere sufficientemente messo in risalto, chiaro e preciso in modo da consentire all'utente Internet di crearsi un'idea chiara del contenuto al quale sta per accedere. Ad esempio, l'intestazione potrebbe asserire "Stiamo raccogliendo e trattando dati personali che La riguardano. Per ulteriori informazioni clicchi qui" oppure "Dati personali o tutela della sfera privata". Il contenuto delle informazioni alle quali l'utente Internet è indirizzato deve altresì essere sufficientemente preciso.

III. Raccomandazioni per il perfezionamento degli altri diritti e doveri

Il Gruppo di lavoro desidera inoltre attirare l'attenzione dei destinatari della presente Raccomandazione su altri diritti dell'individuo ed obblighi dei responsabili del trattamento basati su direttive di particolare attinenza nell'ambito della raccolta di dati personali su siti *web*. Il Gruppo di lavoro ritiene che le raccomandazioni seguenti, così come le indicazioni sulle informazioni, abbiano un'utilità pratica immediata sia per i responsabili del trattamento che per gli utenti Internet.

18. Raccogliere esclusivamente i dati necessari per il conseguimento dello scopo prefisso;

19. garantire che i dati siano trattati esclusivamente nelle suddette legittime modalità, conformemente ad uno dei criteri elencati nell'articolo 7 della direttiva 95/46/CE;

20. garantire l'effettivo esercizio del diritto di accesso e di rettifica; l'esercizio di tali diritti dovrebbe essere possibile sia all'indirizzo fisico del responsabile del trattamento che *on-line*. È necessario predisporre particolari misure di sicurezza affinché esclusivamente la persona interessata abbia accesso *on-line* alle informazioni che la riguardano;

21. conformarsi al principio della "finalità" o "scopo" in base al quale occorre far uso di dati personali solo se necessario e per finalità determinate. In altri termini, in assenza di un motivo legittimo, non è possibile fare uso di dati personali ed è necessario mantenere l'anonimato degli individui (articolo 6, paragrafo 1, punto b) della direttiva 95/46/CE). Detto principio è altresì denominato "principio di minimizzazione".

22. Fornire ed incoraggiare la consultazione in modalità anonima di siti commerciali, nello stesso ambito descritto nel punto 21, senza richieste di identificazione degli utenti per cognome, nome, indirizzo di posta elettronica o altri dati identificativi. Qualora sia necessario un collegamento ad una persona senza completa identificazione della stessa è bene suggerire ed accogliere l'uso di pseudonimi di qualsivoglia natura. Ove non sussistano necessità di identificazione legale occorre incoraggiare ed accogliere l'uso di pseudonimi, anche nel caso di determinate operazioni. Un esempio è dato dall'uso di certificati pseudonimi per le firme elettroniche (cfr. articolo 8 della direttiva 1999/93/CE relativa ad un quadro comunitario per le firme elettroniche).

23. Stabilire un periodo di conservazione per i dati raccolti. È possibile conservare detti dati esclusivamente per il tempo necessario allo scopo del trattamento indicato e perseguito (articolo 6 della direttiva 95/46/CE e articolo 6 della direttiva 97/66/CE).

24. Adottare gli accorgimenti necessari per garantire la sicurezza dei dati nel corso del loro trattamento e della loro trasmissione (ad esempio limitare e determinare il numero delle persone che hanno accesso ai dati, far uso di trasmissioni cifrate, ecc.; articolo 17 della direttiva 95/46/CE).

25. Se è coinvolto un responsabile per l'elaborazione, ad esempio per ospitare un sito web, stipulare un contratto che gli imponga di attuare appropriate misure di sicurezza in conformità anche della normativa dello Stato membro in cui si trova il responsabile per l'elaborazione, nonché effettuare il trattamento dei dati personali attenendosi esclusivamente alle indicazioni del responsabile di detto trattamento.

26. A seconda dei casi e in forza della legge nazionale, procedere alla notificazione dell'autorità di controllo (se il responsabile dell'elaborazione del sito si trova nell'Unione europea o se lo stesso dispone di un rappresentante nell'Unione europea). Il numero di registrazione di detta notifica può essere indicato all'interno del sito, in modo vantaggioso, al di sotto dell'intestazione destinata alla protezione dei dati.

27. Se vengono trasferite informazioni ad un paese terzo in cui non è garantito un adeguato livello di protezione è necessario assicurare che il trasferimento dei dati avvenga esclusivamente se lo stesso è in linea con le deroghe all'articolo 26 della direttiva 95/46/CE. In questi casi occorre informare le persone delle adeguate garanzie fornite affinché il trasferimento risulti lecito.

IV. Raccolta di indirizzi per la commercializzazione diretta tramite posta elettronica e per la spedizione di newsletter

28. Per ciò che concerne la commercializzazione diretta per posta elettronica:

il Gruppo di lavoro ripropone il proprio parere secondo il quale gli indirizzi di posta elettronica reperiti nelle aree pubbliche di Internet all'insaputa delle persone interessate, ad esempio nei gruppi di discussione, non sono stati raccolti lecitamente. Tali indirizzi non possono perciò essere utilizzati con finalità diverse da quelle per le quali sono stati originariamente resi pubblici; in particolar modo non possono essere utilizzati per la commercializzazione diretta (13);

fare uso di indirizzi di posta elettronica per la commercializzazione diretta a condizione che questi siano stati raccolti lealmente e legalmente. Affinché la raccolta sia leale e legale è necessario che le persone interessate siano state informate della possibilità dell'uso di tali dati per la commercializzazione diretta e che dette persone abbiano potuto acconsentire a tale uso direttamente al momento della raccolta (cliccando su una casella di spunta) (14) . L'invio di posta elettronica a scopo promozionale deve altresì prevedere la possibilità di esercitare il recesso *on-line* dall'elenco di indirizzi impiegato (15).

29. Per ciò che concerne la spedizione di *newsletter*:

Procurarsi il previo consenso delle persone interessate e garantire la possibilità di un loro recesso da tali spedizioni in qualsiasi momento; occorrerà pertanto informare dette persone riguardo a questa possibilità ogniqualvolta viene spedita una *newsletter*.

Il gruppo di lavoro invita il Consiglio d'Europa, la Commissione europea, il Parlamento europeo e gli Stati membri a tener conto della presente raccomandazione.

Il gruppo si riserva la facoltà di formulare ulteriori osservazioni.

Fatto a Bruxelles, 21 maggio 2001

Per il gruppo

Il Presidente

Stefano RODOTÀ

13 Cfr. WP 28 (5007/00): "Parere 1/2000 su alcuni aspetti del commercio elettronico relativi alla protezione dei dati personali", approvato il 3.2.2000, WP 29 (5009/00);"Parere 2/2000 concernente la revisione generale del quadro giuridico delle telecomunicazioni", approvato il 3.2.2000, e, specialmente, riguardo l'applicazione degli articoli 6 e 7 della direttiva 95/46/CE. WP 36 (5042/00): "Parere 7/2000 sulla proposta della Commissione europea di direttiva del Parlamento europeo e del Consiglio relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche del 12 luglio 2000 (COM(2000)385)", approvato il 2.11.2000 e WP 37 (5063/00); "Documento di lavoro: Tutela della vita privata su Internet. un approccio integrato dell'UE alla protezione dei dati on-line", approvato il 21.11.2000.

14 All'interno dell'Unione europea cinque Stati membri (Germania, Austria, Italia, Finlandia e Danimarca) hanno adottato misure intese a vietare le comunicazioni commerciali non sollecitate. In altri Stati membri esiste un sistema di possibilità di recesso oppure permane una situazione poco chiara. È bene notare che la proposta di direttiva della Commissione relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (COM(2000) 385) del 12 luglio 2000 è in favore di una soluzione armonizzata basata sulla possibilità di adesione; tale approccio è stato unanimemente sostenuto dal Gruppo di lavoro nel Parere 7/2000 (WP 36 sopracitato). Si veda inoltre lo studio di S. Gauthronet e di E. Drouard (ARETE) per la Commissione. "Messaggi pubblicitari indesiderati e protezione dei dati personali", gennaio 2001. http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamsumit.pdf

15 La direttiva sul commercio elettronico stabilisce ulteriori requisiti relativi alle comunicazioni commerciali non sollecitate in quei casi in cui è consentita la possibilità di recesso conformemente alla direttiva 97/66/EC.

126 RACCOMANDAZIONE N. 1/2001 SULLE VALUTAZIONI RELATIVE A LAVORATORI

5008/01/EN final WP 42
Adopted on 22.3.2001

Draft Recommendation on Employee Evaluation Data

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT RECOMMENDATION:

Directive 95/46/EC on the protection of individuals with regard to the processing of their personal data and the free movement of such data calls upon Member States to protect the fundamental rights and freedoms of individuals, and in particular their right to privacy with respect to the processing of personal data.

The Directive is part of the Community measures necessary to remove obstacles to flows of personal data in the various spheres of economic, administrative and social activity within the internal market, and that to this end it aims at harmonising the rules on processing of personal data by affording a high level of protection in the Community.

Based on the definition included in Article 2(a) of Directive 95/46/EC, personal data means any information relating to an identifiable or identified person, such as for instance data relating to his/her physical, physiological, mental, economic, cultural or social identity.

The scope of this definition implies that personal data includes not only population registry data or information resulting from objective factors which can be verified or rectified, but also any other element, information or circumstance having an information content such as to add to the knowledge of an identified or identifiable person.

Personal data can be therefore found in subjective judgments and evaluations which can actually include elements specific to the physical, physiological, psychical, economic, cultural or social identity of data subjects. This is equally true if a judgment or a evaluation is summarised by a score or rank or is expressed by means of other evaluation criteria.

The fact that under national law a few of these subjective data cannot be always accessed and rectified directly, or that they can be rectified by the inclusion of statements or notes made by data subjects, does not prevent them from being personal data, with a view to transparency of processing and the exercise of right of access.

Similar considerations apply in respect of the fact that direct access to the data included in subjective judgments or evaluations can be deferred or limited under national law.

PAGINA BIANCA

AUTORITÀ DI CONTROLLO COMUNE SCHENGEN

127 QUARTA RELAZIONE DI ATTIVITÀ DELL'AUTORITÀ DI CONTROLLO COMUNE: MARZO 1999 - FEBBRAIO 2000

SOMMARIO:

NOTA DI SINTESI

Il presente documento riporta la quarta relazione annuale di attività dell'Autorità di controllo comune Schengen (ACC). In uno spirito di trasparenza e di apertura democratica, ACC ritiene opportuno rendere conto ad un pubblico quanto più vasto possibile dei suoi sforzi costanti intesi a difendere gli interessi dell'individuo nella tutela della vita privata. Le attività svolte dall'ACC nel periodo compreso tra marzo 1999 e febbraio 2000 dimostrano una volta di più che l'autorità di controllo è parte integrante della struttura di Schengen.

L'ACC, basandosi su relazioni, ha formulato anche questa volta raccomandazioni o pareri, proposte e suggerimenti riguardanti sia il controllo della sicurezza del SIS che la tutela degli interessi dei singoli individui segnalati, o ancora l'adempimento dell'obbligo d'informazione nei confronti del cittadino.

Questa volontà di contribuire in modo costruttivo al corretto funzionamento del meccanismo Schengen che anima tutti i colleghi delegati delle autorità di controllo nazionali e gli osservatori dei paesi candidati all'adesione, contrasta talvolta fortemente con il trattamento ingeneroso riservato all'ACC, soprattutto per quanto concerne il debito rispetto della sua autonomia e rigorosa indipendenza e l'assegnazione delle risorse finanziarie necessarie per garantirle.

La chiara volontà manifestata dall'attuale Presidenza dell'UE di pervenire a un segretariato comune di tutte le autorità di controllo nel settore di polizia europeo (Schengen, Europol, Sistema d'informazione doganale, ecc.) può rappresentare un passo nella buona direzione e l'ACC non può che compiacersene. Soltanto con risorse proprie - e la correlata responsabilizzazione - l'autonomia potrà essere reale ed efficace.

Il 1° gennaio 2000 vi è stato un cambiamento della Presidenza dell'ACC. A nome di tutti i colleghi mi pregio di trasmettere al sig. Joào Labescat i nostri vivi ringraziamenti e tutta la nostra riconoscenza per lo straordinario impegno e la perseveranza con cui ha curato gli interessi dell'ACC - e dunque di tutti i cittadini - nel difficile periodo della sua integrazione nell'ambito dell'Unione europea.

Bruxelles, 9 maggio 2000

Il Presidente
Bart De Schutter

PRIMA PARTE: INTRODUZIONE

Sono trascorsi 15 anni da quel giorno del 1985 in cui, in un villaggio della Mosella lussemburghese da cui avrebbe tratto il nome, fu firmato l'accordo di Schengen.

Precursore dello spazio di libertà, sicurezza e giustizia che avrebbe poi creato il trattato di Amsterdam, l'accordo ha indubbiamente avuto successo, come dimostra il numero crescente di paesi che hanno aderito all'accordo stesso e alla relativa convenzione di applicazione firmata nel 1990. Ai cinque paesi firmatari del 1985 se ne sono infatti nel frattempo aggiunti altri dieci e, se nel 1995 erano sette i paesi che soddisfavano le condizioni necessarie all'attuazione della convenzione, saranno presto 15 i paesi che applicheranno l'acquis di Schengen[1] all'inizio del 2001[2].

Si ricorda che lo scopo dell'accordo di Schengen e della relativa convenzione di applicazione è l'abolizione dei controlli alle frontiere interne degli Stati membri e, quindi, la creazione di un grande spazio di libera circolazione delle persone. Per conseguire questo obiettivo garantendo nel contempo, all'interno di tale spazio, un livello di sicurezza almeno pari a quello esistente in precedenza, la convenzione di applicazione dell'accordo di Schengen prevede misure compensative, principalmente: armonizzazione della politica dei visti, definizione di una politica comune in materia di determinazione dello Stato responsabile dell'esame di una domanda di asilo, miglioramento della cooperazione di polizia e giudiziaria, intensificazione della lotta al traffico illecito di stupefacenti, armonizzazione del livello dei controlli alle frontiere esterne dello spazio Schengen e creazione di un sistema d'informazione Schengen (SIS).
Il SIS è un sistema comune che collega tutti i paesi che applicano la convenzione di Schengen e consente ai suoi utenti (uffici con compiti di polizia, ambasciate e consolati, uffici stranieri, ecc.) di disporre in tempo reale delle informazioni necessarie all'esercizio dei loro compiti rispettivi inserite da uno degli Stati membri che applicano la convenzione.

Tali informazioni riguardano le persone (ricercate per arresto estradizionale, non ammissibili nel territorio, scomparse o oggetto di una sorveglianza discreta) e gli oggetti (veicoli, armi, documenti, banconote rubate, sottratte o smarrite).

Alla creazione del SIS si è affiancata quella di un'Autorità di controllo comune per la protezione dei dati personali, incaricata segnatamente di vigilare sul rispetto delle disposizioni della convenzione relative all'unità di supporto tecnico del SIS (articolo 115). A quest'organo, composto di due rappresentanti di ogni autorità di controllo nazionale della Parti contraenti, è inoltre attribuito un compito di consulenza e di armonizzazione delle prassi e delle dottrine nazionali.

Sin dal giugno 1992, una decisione ministeriale ha istituito un'autorità di controllo comune provvisoria, organo che ha compiuto i primi passi nella preparazione dell'applicazione dei principi della protezione dei dati.

Il 26 marzo 1995, contestualmente alla messa in applicazione della convenzione nei sette paesi membri che soddisfacevano le condizioni preliminari, l'autorità di controllo provvisoria si è trasformata in definitiva, ossia nell'Autorità di controllo comune Schengen (ACC) prevista all'articolo 115 della convenzione.

Fin dalla messa in applicazione della convenzione, il 26 marzo 1995, l'ACC ha dovuto faticare molto perché ne fossero riconosciute le competenze e l'indipendenza rispetto agli organi esecutivi di Schengen. Prova ne è la prima relazione di attività, che sottolinea in particolare le difficoltà incontrate per ottenere un bilancio autonomo o quelle sperimentate dal gruppo di esperti cui l'ACC aveva affidato il controllo dell'unità centrale del SIS (C.SIS) installata a Strasburgo. A oltre un anno di distanza l'ACC non aveva ancora ottenuto dagli organi esecutivi di Schengen una risposta alle raccomandazioni formulate in base al controllo del C.SIS, cui aveva replicato soltanto il ministero dell'interno francese. Soltanto dal febbraio 1998 l'ACC può disporre delle informazioni inerenti al SIS che le sono necessarie per svolgere i propri compiti, perché le autorità responsabili del sistema esaminavano le richieste d'informazioni caso per caso.

---

[1] *A seguito dell'integrazione di Schengen nell'ambito dell'Unione europea gli Stati membri non applicano più la convenzione di applicazione dell'accordo di Schengen, bensì "l'acquis di Schengen integrato nell'Unione europea".*

[2] *Danimarca, Finlandia, Islanda, Norvegia e Svezia dovrebbero applicare pienamente l'acquis di Schengen dall'inizio del 2001.*

Nonostante i progressi compiuti il cammino è ancora lungo. Nelle visite di controllo che l'ACC ha effettuato nel 1996 e 1999 presso il sistema centrale di Strasburgo si è sì constatato il buon funzionamento complessivo del sistema, ma si sono anche rilevati diversi problemi, tra cui alcuni che pongono reali difficoltà in termini d'integrità.
I problemi rilevati dall'ACC hanno acquisito un'importanza vieppiù significativa quando, alla fine del 1997, il numero di Stati Schengen che applicano la convenzione è passato da 7 a 10 e, in prospettiva, con il passaggio a 15 all'inizio del 2001. Il numero dei dati inseriti nel SIS aumenta infatti di conseguenza.

Al pari di tutti i sistemi d'informazione nel settore della polizia, anche quello di Schengen registra un'evoluzione, cui deve affiancarsi un potenziamento del ruolo delle pertinenti autorità di controllo indipendenti. L'integrazione di Schengen nell'Unione europea risultante dal trattato di Amsterdam[1] deve migliorare la trasparenza e offrire maggiori garanzie per i diritti fondamentali del cittadino. I parlamenti nazionali e gli organi europei possono ora intervenire più attivamente per la realizzazione di questi obiettivi.

SECONDA PARTE: UN ANNO DI ATTIVITA' DELL'ACC

CAPITOLO I: PARERI E RACCOMANDAZIONI

I.1. Sicurezza degli uffici SIRENE

Nel dicembre 1997, a seguito di una fuga di documenti e di informazioni prodottasi presso un ufficio SIRENE qualche settimana prima, l'ACC ha incaricato le autorità nazionali di controllo di verificare la sicurezza dei rispettivi uffici SIRENE.

Avvalendosi delle relazioni nazionali l'ACC ha elaborato un documento di sintesi relativo alla sicurezza degli uffici SIRENE, nel quale ricordava i requisiti di sicurezza, previsti all'articolo 118 della convenzione di Schengen, cui devono conformarsi tutti gli uffici SIRENE e formulava dieci raccomandazioni. L'8 gennaio 1999 il documento di sintesi è stato trasmesso ai competenti organi di Schengen (Comitato esecutivo, Gruppo centrale, Gruppo di lavoro "SIRENE").

Una risposta è giunta il 19 novembre 1999, vale a dire dopo l'integrazione di Schengen nell'ambito dell'Unione europea (SCHAC 2512/99). In essa il Presidente del Comitato dell'articolo 36 –che può essere considerato il consesso cui fanno ora capo, segnatamente, le competenze del Gruppo centrale di Schengen- afferma: *"In generale gli Stati membri ritengono che buona parte delle raccomandazioni dell'Autorità di controllo comune siano già attuate negli uffici SIRENE.*
Gli Stati membri desiderano altresì richiamare l'attenzione sul fatto che alcune raccomandazioni sono piuttosto onerose sotto il profilo tecnico ed organizzativo rispetto all'obiettivo perseguito. Essi ritengono che, poiché il SIS, per contenuto e qualità dei dati, costituisce una base di dati di polizia utilizzata quotidianamente, le misure intese a garantire la sicurezza dei dati non possano avere l'effetto di limitare eccessivamente l'utilizzazione degli stessi."
Nella risposta specifica acclusa alla lettera del Presidente del Comitato dell'articolo 36, il Gruppo SIRENE sostiene inoltre, riguardo alla tracciatura e alla verifica dei motivi delle interrogazioni: *"Considerato che gli agenti di polizia di tutti gli Stati devono consultare quanto più possibile il SIS, l'utilizzazione del SIS costituisce parte della regolare attività di servizio. In alcuni Stati non è fattibile, sotto il profilo tecnico ed organizzativo, fornire una motivazione per ogni singola interrogazione del SIS, per via del numero elevato delle interrogazioni (in Germania, ad esempio, 5,4 milioni al mese)".*
"La verifica regolare dei motivi di una interrogazione del SIS è effettuata soltanto in alcuni paesi (...). Si considera che, in principio, gli agenti di polizia agiscano in modo legittimo nell'assolvimento dei loro compiti. Al posto di una verifica regolare del motivo di una interrogazione SIS, sono pertanto ipotizzabili soltanto controlli per sondaggio".

L'ACC, nel prendere atto della risposta, ha deciso di perseverare affinché la sicurezza degli uffici SIRENE fosse migliorata e uniformata. Ha in particolare convenuto di stendere un questionario uniforme che permetta alle autorità nazionali di controllo per la protezione dei dati di effettuare le verifiche in modo armonizzato.

[1] *V. articolo 7 del protocollo sull'integrazione dell'acquis di Schengen nell'ambito dell'Unione europea, allegato al trattato di Amsterdam.*

I.2 Parere relativo all'archiviazione dei dossier ad avvenuta cancellazione di una segnalazione

Fin dal 1997 uno dei membri dell'ACC aveva chiesto all'Autorità come andasse interpretato l'articolo 102, paragrafo 1 della convenzione, relativo alla conservazione dei documenti ad avvenuta cancellazione di una segnalazione. Gli Stati membri davano infatti interpretazioni diverse alla disposizione: alcuni di essi conservano i documenti relativi alle segnalazioni dopo che queste sono state cancellate e li utilizzano per completare gli schedari di polizia.

L'articolo 102, paragrafo 1 vieta però alle Parti contraenti di utilizzare i dati di cui agli articoli da 95 a 100 per fini diversi da quelli enunciati per ciascuna delle segnalazioni di cui ai detti articoli.
Nel parere 98/1 del 3 febbraio 1998 l'ACC ha ricordato i principi della convenzione e i diritti fondamentali in materia di protezione dei dati, chiedendo poi che ciascuna Parte contraente distrugga immediatamente tutta la documentazione relativa a una segnalazione cancellata, conformemente all'articolo 112 della convenzione e che il manuale SIRENE sia riveduto per eliminare le disposizioni che violano la convenzione di Schengen.

Nel gennaio 1999 il Gruppo centrale ha replicato al parere dell'ACC senza tener conto né dell'esigenza di rispettare il principio di finalità né della necessità di armonizzare le prassi. L'ACC ha allora redatto una nota complementare in cui insisteva sull'obbligo di rispettare il principio di finalità, in base al quale il dossier può essere utilizzato soltanto per i fini che hanno motivato l'inserimento della segnalazione, e sottolineava che i requisiti di finalità e di conservazione limitata alla finalità per la quale la segnalazione è stata effettuata sono altresì enunciati nell'articolo 5 della convenzione n. 108 del Consiglio d'Europa, del 28 gennaio 1981, che tutti gli Stati sono tenuti a osservare (articolo 126, paragrafo 1 della convenzione di Schengen).

Questa raccomandazione complementare al parere n. 98/1 dell'ACC è stata approvata dall'ACC il 22 ottobre 1999 (SCHAC 2505/99) ed esaminata dal Comitato dell'articolo 36 il 15 dicembre 1999.

Al riguardo, i risultati dei lavori di tale riunione del Comitato dell'articolo 36 affermano:
Al Comitato è stato sottoposto il parere dell'Autorità di controllo circa l'uso dei documenti relativi a una segnalazione dopo che i dati sono stati distrutti nel SIS. Il Servizio giuridico ritiene che il parere dell'ACC si riferisca alla prassi seguita in alcuni Stati membri e non alle regole del Consiglio.

Il Comitato decide di consultare il Gruppo SIS per verificare se occorra modificare il manuale SIRENE alla luce delle osservazioni dell'ACC.

Da allora l'ACC non ha più ricevuto notizie.

I. 3 Parere sull'introduzione nel sistema d'informazione Schengen di segnalazioni sulle persone la cui identità è stata usurpata

In caso di usurpazione d'identità alcuni Stati membri introducono nel SIS il nome del titolare legittimo dell'identità usurpata, mentre il bersaglio è piuttosto l'usurpatore.

In altre parole, l'identità segnalata nel sistema non corrisponde, né di fatto né di diritto, all'identità del ricercato, bensì a quella della vittima dell'usurpazione. Tuttavia, il titolare legittimo non è assolutamente informato del fatto che la sua identità sia stata introdotta nel SIS.

Alcuni Stati sono favorevoli ad una procedura secondo la quale i dati di carattere personale relativi alle persone la cui identità è stata usurpata dovrebbero essere immediatamente cancellati, mentre altri sostengono che la segnalazione contenente l'identità usurpata dovrebbe essere mantenuta anche se il titolare legittimo dell'identità inserita nel SIS ne richiedesse la cancellazione: l'argomento da essi addotto a sostegno della loro tesi è la necessità di trovare il responsabile.

Nel parere 98/2 del febbraio 1998 l'ACC ha ricordato i diritti fondamentali e i principi della convenzione in materia di protezione dei dati, sottolineando soprattutto il principio di proporzionalità, che impone di raggiungere un equilibrio fra i diritti della persona la cui identità è stata usurpata e la necessità di individuare gli usurpatori.

L'Autorità proposto che, fino all'avvio del SIS II, si cerchi di definire una soluzione comune e, se possibile, si indichi che la segnalazione riguarda un'identità usurpata.

In risposta a tale parere il Comitato dell'articolo 36 ha comunicato all'ACC le soluzioni ipotizzate (nel prossimo futuro, misure temporanee per il SIS I +, a fine 2000, e soluzione definitiva a più lungo termine per il SIS II).
L'ACC ha esaminato queste proposte nel dicembre 1999 e nel febbraio 2000. Un altro parere, complementare al primo reso dall'ACC al riguardo, è stato approvato con procedura scritta nel marzo 2000. In esso l'ACC ribadisce il principio di proporzionalità, in virtù del quale non tutti i casi di usurpazione d'identità giustificano la segnalazione del nome del titolare legittimo e sottolinea che l'elaborazione dei dati relativi alle persone la cui identità è stata usurpata potrà essere consentita solo previo libero ed esplicito accordo delle stesse o dietro loro richiesta. Devono inoltre essere previste altre misure, quali la possibilità di rilasciare al titolare legittimo dell'identità usurpata un documento supplementare, ad esempio integrativo al passaporto, che attesti che il titolare non è la persona che usurpa l'identità.

CAPITOLO II: ATTIVITÀ DI CONTROLLO

II.1. Controllo del C.SIS

Nel corso del 1998 l'ACC ha messo a punto, in collaborazione con il Ministero dell'interno francese, un documento contenente i principi applicabili alle visite e ai controlli del C.SIS. Il tempo trascorso dall'ultimo controllo effettuato e l'adesione al sistema di tre nuovi paesi (Austria, Grecia e Italia) giustificavano l'organizzazione di un nuovo controllo. L'ACC ha creato un gruppo tecnico costituito di esperti delle autorità di controllo nazionali, coordinato dal rappresentante lussemburghese. Tale gruppo di esperti si è riunito tre riprese, principalmente alla vigilia delle riunioni plenarie dell'ACC, per preparare la missione d'ispezione. Al termine del controllo effettuato nell'aprile 1999, gli esperti hanno completato per iscritto il loro progetto di relazione redatto Strasburgo. Si sono quindi riuniti a Bruxelles il 9 settembre 1999 per metterlo a punto. Il 17 settembre 1999 tale progetto è stato trasmesso al Ministero dell'interno francese, invitato a presentare le sue osservazioni entro un termine di un mese. Il gruppo di esperti ha esaminato queste ultime il 1° dicembre 1999 e ha apportato su tale base varie correzioni alla sua relazione. Le osservazioni del Ministero dell'interno francese sono quindi state allegate alla relazione dell'ACC, quali parte integrante della medesima.
La visita di controllo è stata effettuata nell'aprile 1999. Ne è emersa la possibilità di migliorare la sicurezza del sistema, giudicata globalmente soddisfacente. Una sintesi delle raccomandazioni figura in appresso.

Potrebbero essere apportati miglioramenti relativamente alla sicurezza fisica, in particolare per quanto concerne la separazione fisica tra le zone riservate rispettivamente al personale del C.SIS e al Ministero dell'interno francese o un controllo più severo dell'accesso alla sala operativa del C.SIS, grazie ad un elenco delle persone autorizzate o ad un lettore di tessere magnetiche. Le stesse osservazioni valgono per la cassaforte che custodisce i nastri contenenti i dati, per i quali dovrebbe essere messa a punto una procedura formale di distruzione.

Le funzioni fondamentali che consentono l'audit trail non sono attivate, in quanto ostacolano il corretto funzionamento del sistema. Benché il C.SIS abbia compiuto sensibili progressi per compensare tale mancanza di traccia, è possibile utilizzare le potenziali risorse non sfruttate del sistema SINIX in modo da aggiungere meccanismi di controllo nelle aree più sensibili.

Le procedure di autorizzazione e di verifica periodica dei diritti degli utenti dovrebbero essere formalizzate, l'elenco degli utenti dovrebbe essere aggiornato periodicamente e il loro accesso dovrebbe essere controllato.

Dovrebbero essere studiate varie misure tecniche in grado di migliorare la protezione contro i tentativi di intrusione.

In materia di telecomunicazioni, alcuni elementi delle apparecchiature di cifratura sono stati giudicati problematici e potrebbero provocare lacune gravi nella sicurezza delle trasmissioni.

La procedura di raffronto delle basi di dati è ancora troppo lunga e occorre pertanto prendere opportune disposizioni in modo da assicurare che le discrepanze vengano tempestivamente individuate e corrette. D'altra parte, tutte le divergenze o discrepanze, per quanto minime, devono essere debitamente rilevate e corrette in modo da rendere tutti gli archivi nazionali identici l'uno all'altro.

I dati relativi a segnalazioni che sono stati cancellati sono conservati per più di un anno presso il C.SIS, contravvenendo in tal modo alle disposizioni dell'articolo 113, paragrafo 2.
Alcune Parti contraenti hanno inserito per errore segnalazioni su persone ai sensi dell'articolo 96 della convenzione per cittadini dell'Unione europea. Il C.SIS dovrebbe inserire delle procedure di monitoraggio che rilevino l'inserimento nel SIS di segnalazioni ai sensi dell'articolo 96 (persone non ammissibili) per cittadini dell'Unione europea.

L'articolo 112, paragrafi 1 e 2, stabilisce che i dati personali inseriti nel C.SIS ai fini della ricerca di persone sono conservati soltanto per il periodo necessario ai fini per i quali sono stati forniti. Al massimo tre anni dopo il loro inserimento, la Parte contraente che ha fornito l'informazione deve esaminare la necessità di conservarli. Dalla verifica degli esperti è emerso che la procedura attualmente seguita permette di garantire la soppressione dei dati al termine in cui spira ciascuna segnalazione inserita nella base di dati del C.SIS. Ciononostante, numerose date di inserimento nelle tabelle relative alle persone segnalate sono inesatte, il che significa che le procedure di verifica delle date registrate nel C.SIS sono inadeguate. Risulta quindi necessario introdurre misure che consentano di controllare l'esattezza delle date di inserimento delle segnalazioni.

La relazione riservata sulla visita di controllo è stata approvata nel febbraio 2000 ed è stata trasmessa, corredata di una sintesi, al Comitato dell'articolo 36. Il passo che segue è tratto dai risultati dei lavori della riunione del Comitato dell'articolo 36 del 28/29 febbraio 2000, durante la quale la relazione dell'ACC è stata esaminata:

"I gruppi "SIS" hanno ricevuto il mandato per preparare entro la fine del mese di maggio un progetto di risposta sulla relazione dell'ACC in merito alla visita di controllo al C.SIS; il Coreper sarà informato dei lavori effettuati dall'ACC e delle raccomandazioni formulate".

II.2. Gruppi tecnici ed esperti

In seguito alla riunione informativa tenutasi il 20 novembre 1998, nella quale esperti dell'ACC hanno ricevuto informazioni sulla futura rete SIS II dai rappresentanti dell'IBM e dagli esperti dei gruppi di lavoro Schengen interessati, l'ACC aveva deplorato che l'IBM non avesse ancora potuto esaminare in modo approfondito, in particolare, gli aspetti legati alla sicurezza. Essa aveva allora ottenuto informazioni tecniche supplementari e l'assicurazione di poter prendere conoscenza del capitolato d'oneri per conoscere i criteri che avevano portato alla scelta delle architetture prese in considerazione e i criteri di sicurezza. Gli Stati membri non hanno ancora stabilito i requisiti funzionali della futura rete.

II.3. Criptazione dei collegamenti SIS

Durante un controllo dell'ufficio nazionale SIRENE, uno dei membri dell'ACC non ha potuto ottenere informazioni relative all'algoritmo di cifratura utilizzato nei collegamenti SIS, in quanto esso era stato messo a punto dall'Ufficio federale tedesco per la sicurezza in materia di tecnologie dell'informazione[1] e dalla società Bosch Telecom. L'ACC ha quindi chiesto al Comitato dell'articolo 36 di fornirle tali informazioni per accertarsi che i collegamenti SIS siano sufficientemente sicuri. Il Comitato dell'articolo 36 ha annunciato, nella riunione del 28/29 febbraio 2000, che la Germania avrebbe comunicato all'ACC tali informazioni entro la fine del mese di maggio del 2000.

II.4. Elenco delle autorità autorizzate a consultare direttamente il SIS

Per verificare se i requisiti ai quali la convenzione subordina l'accesso al SIS siano rispettati da tutti gli Stati membri e applicati in modo uniforme, l'ACC ha chiesto al Comitato dell'articolo 36 di trasmet-

[1] *Il BSI, ossia il "Bundesamt für die Sicherheit in der Informationstechnik".*