

COMMISSIONE DELLE COMUNITA' EUROPEE

COM(90) 314 def. SYN 287 e 288

Bruxelles, 24 settembre 1990

COMUNICAZIONE DELLA COMMISSIONE

concernente la protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e la sicurezza dei sistemi d'informazione

Proposta di

DIRETTIVA DEL CONSIGLIO

SYN 277

concernente la protezione delle persone
relativamente al trattamento dei dati personali

Progetto di

RISOLUZIONE DEI RAPPRESENTANTI DEI GOVERNI DEGLI STATI MEMBRI
DELLE COMUNITA' EUROPEE RIUNITI IN SEDE DI CONSIGLIO

DICHIARAZIONE DELLA COMMISSIONE

relativa all'applicazione alle istituzioni e agli organismi delle Comunità europee dei principi della direttiva del Consiglio
concernente la protezione delle persone
relativamente al trattamento dei dati personali

Proposta di

DIRETTIVA DEL CONSIGLIO

SYN 288

sulla protezione dei dati personali e della vita privata
nell'ambito delle reti digitali pubbliche di telecomunicazione,
con particolare riferimento all'ISDN (rete digitale integrata nei servizi)
e alle reti digitali per servizi pubblici di radiotelefonía mobile

Raccomandazione di

DECISIONE DEL CONSIGLIO

relativa all'apertura di negoziati in vista dell'adesione delle
Comunità europee alla Convenzione del Consiglio d'Europa sulla protezione
delle persone nel trattamento automatizzato dei dati di carattere personale

Proposta di

DECISIONE DEL CONSIGLIO

nel settore della sicurezza dei sistemi d'informazione

COMUNICAZIONE DELLA COMMISSIONE

concernente la protezione delle persone per quanto riguarda
il trattamento dei dati personali nella Comunità
e la sicurezza dei sistemi d'informazione

I. INTRODUZIONE

1. Il crescente ricorso al trattamento di dati personali in tutti gli aspetti delle attività economiche e sociali, come anche le nuove esigenze in materia di scambio di dati connesse al rafforzamento della costruzione comunitaria, rendono indispensabile nella Comunità l'adozione di misure volte a garantire la protezione delle persone relativamente al trattamento di dati personali e a rafforzare la sicurezza del trattamento di dati nel contesto, in particolare, dello sviluppo delle reti aperte di telecomunicazioni.
2. In effetti, mentre i progressi compiuti nel campo delle tecnologie dell'informazione facilitano notevolmente il trattamento e lo scambio di dati di qualsiasi natura, l'attuale stato della protezione delle persone relativamente a tali attività nella Comunità registra notevoli difformità negli Stati membri. Negli anni '70, le preoccupazioni relative alla protezione delle persone relativamente al trattamento dei dati personali hanno alimentato in numerosi Stati membri un complesso di iniziative legislative volte a limitare e a disciplinare l'utilizzazione di questo tipo di dati. Tuttavia, allo stato attuale, soltanto sette Stati membri si sono dotati di una legislazione specifica in materia. Inoltre, sebbene i loro obiettivi siano gli stessi, le legislazioni sui dati personali adottano talvolta soluzioni divergenti, come, ad esempio, sulla questione del campo d'applicazione (inclusione o meno degli archivi manuali, protezione o meno delle persone giuridiche) o su quella delle condizioni da rispettare per poter effettuare il trattamento dei dati (portata dell'obbligo di notifica, informazione all'atto della raccolta, trattamento dei dati sensibili).

3. Al di là del contesto nazionale, e oltre alla raccomandazione del Consiglio dell'OCSE concernente le linee direttrici che disciplinano la protezione della vita privata e i flussi transfrontalieri di dati personali, del 23 settembre 1980, il solo strumento di diritto internazionale in materia è la convenzione del Consiglio d'Europa del 28 gennaio 1981 per la protezione delle persone relativamente al trattamento automatizzato dei dati personali. La convenzione prevede peraltro numerose opzioni per l'applicazione dei principi basilari da essa definiti ed è stata ratificata soltanto da sette Stati membri, uno dei quali rimane ancora sprovvisto di una legislazione interna.
4. Questa situazione ha già dato adito a preoccupazioni nella Comunità. Il Parlamento europeo le ha fatte proprie e ha adottato fin dal 1976 varie risoluzioni ⁽¹⁾ con le quali manifesta la sua inquietudine in materia e invita la Commissione a predisporre una proposta di direttiva volta ad armonizzare le legislazioni in materia di protezione dei dati personali.
5. In una raccomandazione del 29 luglio 1981, la Commissione sottolinea che tale protezione riveste il carattere di un diritto fondamentale e auspica che tutti gli Stati membri intraprendano iniziative al fine di un ravvicinamento delle legislazioni in materia. Essa raccomanda inoltre agli Stati membri di ratificare entro il 1982 la convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone relativamente al trattamento automatizzato dei dati personali. Tuttavia, la raccomandazione precisa che "se entro un lasso di tempo ragionevole tutti gli Stati membri non avranno firmato e ratificato la convenzione, la Commissione si riserva di proporre al Consiglio l'adozione di un atto giuridico basato sul trattato CEE".

(1) GU C 100 del 3.5.1976, pag. 27; GU C 140 del 5.6.1979, pag. 34; GU C 87 del 5.4.1982, pag. 39.

6. La diversità degli approcci nazionali e la mancanza di un sistema di protezione a livello della Comunità costituiscono un ostacolo al completamento del mercato interno. In effetti, se i diritti fondamentali delle persone interessate, in particolare il diritto alla vita privata, non sono garantiti a livello comunitario, si potrebbe assistere ad una limitazione del flusso transfrontaliero di dati, nel momento stesso in cui tale flusso è diventato indispensabile per le attività delle imprese e degli organismi di ricerca, come anche per la collaborazione fra le amministrazioni degli Stati membri nel quadro dello spazio senza frontiere previsto dall'articolo 8 A del trattato. In quest'ottica, recentemente, il Consiglio europeo di Strasburgo dell'8 e 9 dicembre 1989, nel contesto delle misure a favore della libera circolazione delle persone e dell'Europa dei cittadini, ha sottolineato la necessità "di vigilare a che le modalità della cooperazione tra amministrazioni garantiscano la protezione dei cittadini relativamente all'utilizzazione delle banche di dati personali".
7. Un approccio comunitario in materia di protezione delle persone relativamente al trattamento dei dati personali si rivela altresì un'esigenza essenziale per lo sviluppo dell'industria dell'informatica e dei servizi telematici a valore aggiunto. La rapida introduzione di disposizioni armonizzate concernenti la protezione dei dati e della vita privata nel contesto delle reti digitali di telecomunicazione è indispensabile per la realizzazione del mercato interno delle apparecchiature e dei servizi di telecomunicazione.

8. La penetrazione dell'informatica in tutte le sfere dell'attività economica e sociale e la costituzione di sistemi globali di comunicazione che facilitano l'integrazione di più attività rappresentano un'altra sfida che richiede una "protezione" adeguata ai rischi che potrebbero derivare da eventuali carenze tecniche o umane accidentali o volontarie. Un'efficace sicurezza dei sistemi d'informazione è un elemento essenziale per garantire una protezione effettiva della vita privata e per preservare l'integrità del patrimonio che costituiscono oggi i dati registrati e trasmessi sotto forma elettronica. Le politiche e i programmi comunitari per lo sviluppo delle industrie dell'informazione e delle telecomunicazioni e la realizzazione del mercato interno rischiano di essere fortemente ostacolati se non viene adottata una politica attiva di creazione, di sviluppo e di promozione di norme di sicurezza per i sistemi d'informazione. Dato che le telecomunicazioni permettono oggi gli scambi di dati su scala planetaria, la politica da adottare deve tenere conto di questa dimensione. Inoltre, è essenziale che le politiche nazionali in materia di sicurezza dell'informazione non diventino un ostacolo per la promozione dello sviluppo armonioso della Comunità e per le relazioni con i paesi terzi.

II. L'APPROCCIO PROPOSTO

9. L'approccio proposto mira a garantire un elevato livello di protezione mediante un sistema comunitario di protezione che si basa su una gamma di misure fra loro complementari.

A. Un elevato livello di protezione

10. Dato che le legislazioni nazionali hanno per oggetto di garantire i diritti fondamentali delle persone, in particolare il diritto alla vita privata, e dato che la stessa Comunità si è espressa per la protezione dei diritti fondamentali, in particolare nel terzo paragrafo del preambolo dell'Atto unico europeo, l'azione della Comunità non deve avere per effetto di ridurre la protezione, ma anzi di garantire un elevato livello di protezione nell'insieme della Comunità. Mediante un'azione comunitaria è possibile garantire un elevato livello di protezione equivalente in tutti gli Stati membri della Comunità e conseguentemente sopprimere alcuni ostacoli che si frappongono all'istituzione del mercato interno conformemente all'articolo 100 A.
11. Ad integrazione del ravvicinamento, ad un livello elevato, dei diritti riconosciuti alle persone, è indispensabile intraprendere una politica attiva in materia di sicurezza dei sistemi d'informazione. La sicurezza dei sistemi d'informazione è capitale per le persone come per il commercio, l'industria e le amministrazioni pubbliche. L'obiettivo essenziale è quello di garantire una sicurezza efficace e pratica dell'informazione detenuta sotto forma elettronica evitando la formazione di nuovi ostacoli tecnici fra Stati membri o nei riguardi dei paesi terzi. Questa esigenza richiede l'esame a livello comunitario dei bisogni e delle opzioni possibili in stretta collaborazione con gli operatori del settore e gli Stati membri.

B. Un approccio globale

12. Per istituire nella Comunità un sistema di protezione delle persone nei riguardi del trattamento dei dati personali, è necessario prevedere più misure che permettano di coprire i vari aspetti del problema.

13. Sul piano interno, oltre ad una direttiva-quadro volta al ravvicinamento di talune disposizioni legislative, regolamentari e amministrative degli Stati membri concernenti la protezione delle persone relativamente al trattamento dei dati personali (direttiva generale), che è l'elemento centrale del sistema di protezione, si propone un insieme di altre misure complementari volte a garantire una protezione per quanto possibile completa. Ciascuna delle misure proposte si adatta ad una situazione specifica, ma tutte si basano sugli stessi principi di protezione che figurano nella direttiva generale. In tale ottica, una risoluzione dei rappresentanti dei governi degli Stati membri riuniti in sede di Consiglio e una dichiarazione della Commissione hanno per oggetto di rendere applicabili i principi della direttiva agli archivi che non rientrano nel suo campo di applicazione. Inoltre, è necessario adottare una direttiva settoriale nel contesto delle reti digitali pubbliche di telecomunicazione. Infine, la sicurezza dei sistemi d'informazione richiede un piano d'azione comunitario.

14. Sul piano esterno, la Comunità europea deve promuovere presso i suoi partner l'adozione di disposizioni di protezione adeguate e sostenere gli sforzi intrapresi dal Consiglio d'Europa. In tale contesto, è tra l'altro auspicabile che la Comunità avvii trattative per la sua adesione alla convenzione 108 del Consiglio d'Europa.

Queste proposte non possono essere dissociate le une dalle altre senza pregiudicare l'omogeneità e la coerenza del sistema di protezione proposto.

C. Presentazione delle proposte

15. La proposta di direttiva generale ha per oggetto di predisporre una protezione equivalente di elevato livello in tutti gli Stati membri della Comunità al fine di eliminare gli ostacoli agli scambi dei dati necessari al funzionamento del mercato interno. A tal fine, gli Stati membri debbono garantire i principi enunciati nel progetto di proposta di direttiva. Tali principi riguardano in particolare le condizioni in cui un trattamento di dati personali è legittimo, i diritti della persona interessata (diritto all'informazione, diritto di accesso, diritto di rettifica, diritto di opposizione, ecc.), le qualità che debbono avere i dati (essi debbono essere esatti, raccolti in maniera leale, registrati per finalità determinate e legittime, ecc.), la creazione di un Gruppo per la protezione dei dati personali che consigli la Commissione sulle questioni di protezione dei dati. Il progetto di proposta di direttiva copre il settore privato e il settore pubblico le cui attività rientrano nel campo d'applicazione del diritto comunitario. Poiché tutte le persone beneficeranno in ogni Stato membro di una protezione equivalente di elevato livello relativamente al trattamento di dati personali, gli Stati membri non possono più opporre restrizioni alla circolazione di tali dati nella Comunità fondate sulla protezione della persona interessata.

16. Il progetto di risoluzione dei rappresentanti degli Stati membri delle Comunità europee riuniti in sede di Consiglio ha per oggetto di estendere l'applicazione dei principi della direttiva generale agli archivi del settore pubblico non contemplati dalla direttiva, ossia agli archivi delle amministrazioni le cui attività non rientrano nel campo d'applicazione del diritto comunitario. In effetti, a fini di coerenza, sarebbe auspicabile che tutti gli archivi delle amministrazioni, anche quelli che non rientrano nel campo d'applicazione della direttiva generale, siano soggetti agli stessi principi di protezione. A tal fine, gli Stati membri dovrebbero impegnarsi ad avviare le necessarie procedure legislative nazionali.

17. La dichiarazione della Commissione relativa all'applicazione delle disposizioni della direttiva generale alle istituzioni e agli organismi della Comunità auspica che i principi della direttiva si applichino alle istituzioni e agli organismi della Comunità. A tale proposito, essa prevede che la Commissione adotterà e proporrà le misure necessarie e indica che, nel frattempo, la Commissione applicherà le disposizioni della direttiva ai propri archivi.
18. Una proposta di direttiva del Consiglio sulla protezione dei dati a carattere personale e sulla tutela della riservatezza nell'ambito delle reti digitali pubbliche di telecomunicazioni, con particolare riferimento all'ISDN (Rete digitale integrata nei servizi) e alle reti digitali per servizi pubblici di radiotelefonía mobile, completa la direttiva generale applicando i principi generali della protezione dei dati ai bisogni specifici delle nuove reti di telecomunicazioni. La direttiva mira a garantire agli utilizzatori delle telecomunicazioni in tutti gli Stati membri un livello di base di protezione mediante misure che debbono essere integrate nei servizi offerti dalle nuove reti. Il Consiglio e il Parlamento europeo hanno sottolineato a più riprese l'importanza di misure appropriate per garantire la protezione dei dati e della vita privata relativamente ai futuri sviluppi delle telecomunicazioni, in particolare l'ISDN ⁽¹⁾. Questa preoccupazione è stata espressa con forza dalle autorità degli Stati membri responsabili per la protezione dei dati nel loro incontro annuale a Berlino dell'agosto 1989.

(1) GU C 257 del 4.10.1988, pag. 1; GU C 196 del 1°.8.1989, pag. 4; GU C 7 del 12.1.1987, pag. 334; GU C 12 del 16.1.1989, pag. 66; GU C 12 del 16.1.1989, pag. 69.

19. La raccomandazione di decisione del Consiglio concernente l'adesione della Comunità europea alla convenzione del Consiglio d'Europa per la protezione delle persone relativamente al trattamento automatizzato dei dati personali costituisce uno degli aspetti esterni dell'approccio della Comunità in materia di protezione dei dati personali. In effetti, l'adesione alla convenzione garantirà, nelle relazioni fra la Comunità e i paesi terzi aderenti, la protezione delle persone interessate e la circolazione transfrontaliera dei dati personali.

20. La proposta di decisione del Consiglio concernente l'adozione di un piano d'azione di due anni in materia di sicurezza dei sistemi d'informazione completerà il dispositivo volto a rafforzare i diritti delle persone relativamente al trattamento dei dati personali. La sicurezza dell'informazione, ossia la protezione dei dati conservati, trattati e trasmessi sotto forma elettronica contro le minacce di qualsiasi natura (accidentali o volontarie) è essenziale per l'esercizio effettivo dei diritti delle persone relativamente al trattamento dei dati personali. Si tratta più in generale di un'esigenza primordiale per la protezione dei beni e delle persone che, nel contesto dello sviluppo delle reti di telecomunicazioni aperte, richiede lo sviluppo di una strategia globale, azioni concertate sul piano comunitario nel campo delle tecnologie, norme e procedure di convalida e di prova, nonché sviluppi tecnologici che implicano una collaborazione nella fase precompetitiva di ricerca e sviluppo.

21. Il piano d'azione proposto prevede lo sviluppo di un contesto strategico per la sicurezza dei sistemi d'informazione, l'analisi dei bisogni in materia di sicurezza, l'elaborazione di soluzioni a taluni bisogni prioritari, l'elaborazione di specifiche, norme e prove di convalida, l'integrazione degli sviluppi tecnologici e operativi in materia di sicurezza dei sistemi d'informazione in un quadro strategico generale e l'integrazione di talune funzioni di sicurezza nei sistemi d'informazione.

SYN 287

Proposta di
DIRETTIVA DEL CONSIGLIO
concernente la protezione delle persone
relativamente al trattamento dei dati personali

S O M M A R I O

Riassunto

Relazione

I. Introduzione

II. Necessità di una protezione nella Comunità

- La disparità delle legislazioni nazionali
e l'assenza di una protezione equivalente nella Comunità
- Conseguenze di tale situazione per la Comunità

III. L'approccio adottato

- Un livello di protezione equivalente nella Comunità
- Un livello di protezione elevato

IV. Esame delle disposizioni

Proposta di direttiva

Riassunto

La proposta di direttiva generale ha per oggetto di predisporre una protezione equivalente di elevato livello in tutti gli Stati membri della Comunità al fine di eliminare gli ostacoli agli scambi dei dati necessari al funzionamento del mercato interno. A tal fine, gli Stati membri debbono garantire i principi enunciati nel progetto di proposta di direttiva. Tali principi riguardano in particolare le condizioni in cui un trattamento di dati personali è legittimo, i diritti della persona interessata (diritto all'informazione, diritto di accesso, diritto di rettifica, diritto di opposizione, ecc.), le qualità che debbono avere i dati (essi debbono essere esatti, raccolti in maniera leale, registrati per finalità determinate e legittime, ecc.), la creazione di un Gruppo per la protezione dei dati personali che consigli la Commissione sulle questioni di protezione dei dati. Il progetto di proposta di direttiva copre il settore privato e il settore pubblico le cui attività rientrano nel campo d'applicazione del diritto comunitario. Poiché tutte le persone beneficeranno in ogni Stato membro di una protezione equivalente di elevato livello relativamente al trattamento dei dati personali, gli Stati membri non potranno più opporre restrizioni alla circolazione di tali dati nella Comunità fondate sulla protezione della persona interessata.

Relazione

I. INTRODUZIONE

Le preoccupazioni che si sono andate esprimendo in questi ultimi quindici anni sulla protezione delle persone relativamente al trattamento di dati personali derivano sia dalle possibilità offerte dal progresso tecnico nel campo dell'elaborazione dell'informazione, sia dal ricorso sempre più frequente al trattamento di dati personali in molteplici settori. Esse si sono manifestate in contesti diversi e sono state all'origine di varie iniziative legislative in numerosi Stati membri. La Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone relativamente al trattamento automatizzato dei dati a carattere personale è attualmente l'unico strumento di diritto internazionale in materia. L'OCSE ha elaborato delle linee direttrici per la protezione della vita privata e i flussi transfrontalieri di dati personali in una raccomandazione del 23 settembre 1980 e altrettanto sono in procinto di fare le Nazioni Unite.

Preoccupazioni analoghe si sono manifestate anche nell'ambito comunitario. In effetti, a partire dal 1976 il Parlamento europeo ha adottato numerose risoluzioni ⁽¹⁾ in cui manifesta la sua inquietudine in proposito e invita la Commissione a preparare una proposta di direttiva volta ad armonizzare le legislazioni in materia di protezione dei dati personali.

(1) GU C 100 del 3.5.1976, pag. 27; GU C 140 del 5.6.1979, pag. 34; GU C 87 del 5.4.1982, pag. 39.

La Commissione, nella raccomandazione del 29 luglio 1981, sottolinea che tale protezione riveste il carattere di un diritto fondamentale, e auspica un ravvicinamento delle legislazioni in materia. Essa raccomanda agli Stati membri di ratificare entro la fine del 1982 la convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone per quanto riguarda il trattamento automatizzato dei dati a carattere personale, precisando che "se entro un lasso di tempo ragionevole tutti gli Stati membri non avranno firmato e ratificato la convenzione, la Commissione si riserva di proporre al Consiglio l'adozione di un atto giuridico basato sul trattato CEE".

Il Consiglio europeo di Strasburgo dell'8 e 9 dicembre 1989, nel quadro delle misure a favore della libera circolazione delle persone e dell'Europa dei cittadini, ha sottolineato la necessità "di adoperarsi affinché le modalità della cooperazione tra amministrazioni garantiscano prioritariamente la protezione dei cittadini nei riguardi dell'utilizzazione delle banche di dati personali".

Oltre a queste prese di posizione sulla necessità di una protezione generale, preoccupazioni in materia sono state altresì manifestate nel quadro di azioni specifiche o settoriali della Comunità, in particolare nel campo delle nuove tecnologie dell'informazione.

Vista la situazione nel settore dell'elaborazione dei dati personali, e considerate le esigenze della costruzione comunitaria, diventa indispensabile l'adozione di una direttiva volta a garantire la protezione delle persone nei riguardi di questo tipo di trattamenti.

II. LA NECESSITA' DI UNA PROTEZIONE NELLA COMUNITA'

La disparità delle legislazioni nazionali e l'assenza di protezione equivalente nella Comunità

La protezione delle persone in materia di dati personali è al centro di una diversità di approcci negli Stati membri. Tale diversità è dovuta sia al fatto che taluni Stati membri non hanno una legislazione specifica in materia, sia al fatto che, qualora l'abbiano, essa varia per il contenuto.

Attualmente, sette Stati membri (Danimarca, Germania, Francia, Irlanda, Lussemburgo, Paesi Bassi, Regno Unito) dispongono di legislazioni specifiche, mentre dei lavori sono in corso in alcuni altri Stati membri.

Pur perseguendo tutte lo stesso obiettivo, vale a dire la protezione della persona interessata, le legislazioni nazionali adottano soluzioni diverse a causa della molteplicità delle scelte possibili. Ad esempio, la disciplina applicabile agli archivi manuali, la protezione delle persone giuridiche, le procedure preventive alla creazione degli archivi, la portata dell'obbligo di notifica, l'informazione al momento della raccolta dei dati, il trattamento di dati sensibili, il trasferimento verso altri paesi, sono tutti temi suscettibili di essere trattati in maniera diversa. Inoltre, gli sviluppi della tecnologia possono portare gli Stati a reagire in modo diverso e, conseguentemente, ad accentuare tale disparità.

La convenzione del 28 gennaio 1981 del Consiglio d'Europa relativa alla protezione delle persone nei riguardi del trattamento automatizzato dei dati a carattere personale non ha permesso di contenere tale disparità in quanto, da un lato, lascia in sospeso varie opzioni per attuare i principi di base da essa definiti e, d'altro lato, è stata ratificata soltanto da sette Stati membri (Repubblica federale di Germania, Danimarca, Spagna, Francia, Irlanda, Lussemburgo, Regno Unito), di cui uno (Spagna) non dispone ancora di una legislazione nazionale. La raccomandazione della Commissione del 29 luglio 1981, che invita gli Stati membri della Comunità a ratificare la convenzione del Consiglio d'Europa, non ha modificato tale situazione.

Considerando la disparità degli approcci nazionali, la protezione delle persone nei riguardi del trattamento di dati personali non è equivalente in tutti gli Stati membri in quanto il suo livello può variare da uno Stato all'altro.

Conseguenze di tale situazione per la Comunità

Nella Comunità, questa situazione solleva tre tipi di difficoltà:

- L'assenza di legislazioni nazionali specifiche o le loro lacune non corrispondono all'importanza che la Comunità attribuisce al rispetto dei diritti fondamentali, quale sottolineata nella dichiarazione comune del Parlamento europeo, del Consiglio e della Commissione sui diritti fondamentali del 5 aprile 1987 e dal terzo paragrafo del preambolo dell'Atto unico europeo. Oltre a questi testi, in diritto comunitario, il rispetto dei diritti fondamentali costituisce parte integrante dei principi generali del diritto di cui la Corte di giustizia delle Comunità europee assicura il rispetto.
- La circolazione dei dati personali, quando avviene nel rispetto dei diritti della persona interessata, appare come una necessità nell'ambito dell'instaurazione e del funzionamento del mercato interno. Infatti, tenuto conto degli sviluppi tecnici nel settore del trattamento dell'informazione, in particolare dell'installazione di reti digitali di telecomunicazione nella Comunità, la dimensione transfrontaliera dei flussi di dati emerge a tre livelli:
 - . L'utilizzazione dei dati personali interviene in vari stadi dell'attività economica. L'esercizio della libera circolazione delle merci, delle persone, dei servizi e dei capitali richiede la trasmissione di dati personali tra gli operatori che svolgono attività transfrontaliere.
 - . Nel processo d'integrazione comunitaria, in particolare nel contesto dell'abolizione delle frontiere, si intensificheranno sempre più la cooperazione e la collaborazione tra le amministrazioni nazionali, che saranno quindi chiamate a svolgere compiti che spetterebbero all'amministrazione di un altro Stato membro. La circolazione dei dati diventa quindi una condizione indispensabile del processo di cooperazione. Il dovere di collaborare e di chiedere e comunicare informazioni, che sarà pertanto imposto alle amministrazioni dal diritto comunitario, esige, parallelamente, che sia pienamente assicurata la protezione delle persone interessate.

. Gli scambi di dati sono altresì necessari per la cooperazione scientifica.

Questo bisogno di consentire la circolazione di dati tra Stati membri attualmente si scontra con la disparità degli approcci nazionali in materia di protezione delle persone relativamente al trattamento di dati personali. Tale disparità può infatti indurre uno Stato membro a ostacolare la circolazione dei dati invocando l'assenza o l'insufficienza della protezione nello Stato di provenienza o di destinazione.

- L'attuale disparità potrebbe anche in alcuni casi falsare il gioco della concorrenza fra gli operatori privati a seconda degli obblighi cui sono soggetti nel loro paese.

III. L'APPROCCIO ADOTTATO

Un livello di protezione equivalente nella Comunità

Al fine di garantire a tutte le persone che risiedono nella Comunità una protezione nei riguardi dei trattamenti di dati personali e consentire la circolazione di questo tipo di dati tra gli Stati membri, è necessario stabilire un livello di protezione equivalente in tutta la Comunità. All'uopo risulta indispensabile un ravvicinamento delle legislazioni. Peraltro il programma di lavoro della Commissione per il 1990 indica tra le priorità la protezione dei dati nel quadro del completamento del mercato interno (1).

La base giuridica adeguata in materia è offerta dall'articolo 100A del trattato, dato che una protezione equivalente di livello elevato è indispensabile per il completamento del mercato interno. L'instaurazione e il funzionamento del mercato interno, definito nell'articolo 8A come "uno spazio senza frontiere interne, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali secondo le disposizioni del presente trattato", richiedono, per i motivi già posti in evidenza, un ravvicinamento delle legislazioni in materia.

(1) Boll. CE Suppl. 1/90, pagg. 18, 26 e 28.

Nel formulare la presente proposta, la Commissione ha tenuto conto delle esigenze dell'articolo 8C del trattato e ha concluso che nella fase attuale non risulta utile o giustificata l'adozione di disposizioni speciali o di deroghe. Essa ha inoltre esaminato il problema dell'elevato livello di protezione in materia di sanità, sicurezza, ambiente e consumatori previsto dall'articolo 100A, paragrafo 3 del Trattato CEE.

Un livello di protezione elevato

Dato che le legislazioni nazionali in questo campo hanno per oggetto la protezione dei diritti fondamentali, in particolare il diritto alla vita privata, il loro ravvicinamento deve mirare a garantire un livello di protezione elevato. Ad eccezione degli adattamenti impliciti in qualsiasi ravvicinamento delle legislazioni, tale processo non deve avere per effetto una diminuzione del livello di protezione già garantito negli Stati membri.

I principi generali enunciati nella Convenzione del Consiglio d'Europa sono un riferimento di cui tener conto in quanto costituiscono già una base comune per i paesi che l'hanno ratificata. Pertanto pur adottando soluzioni compatibili con quelle della Convenzione, la direttiva completa tali principi generali al fine di istituire una protezione equivalente di livello elevato.

Un livello elevato di protezione richiede che la protezione garantita dalla direttiva abbia una portata molto ampia e che siano contemplate tutte le situazioni in cui il trattamento di dati personali comporta un rischio per le persone interessate. La direttiva riguarda perciò sia gli archivi manuali che automatizzati, gli archivi del settore pubblico e quelli del settore privato.

I principi enunciati dalla direttiva, in particolare quelli relativi alla legittimità dei trattamenti, alla comunicazione dei dati a terzi, alle procedure di notifica, ai diritti della persona interessata, alla qualità dei dati, mirano a garantire un livello elevato di protezione prendendo come punto di riferimento le diverse soluzioni adottate nelle legislazioni nazionali. Inoltre, sono stati attentamente studiati i mezzi atti ad assicurare, oltre ai normali meccanismi di controllo dell'applicazione del diritto comunitario, l'effettiva applicazione delle disposizioni della direttiva. Questa preoccupazione spiega anche le disposizioni relative alla responsabilità e alla creazione di un Gruppo per la protezione dei dati personali.

I principi della direttiva potranno, se del caso, essere completati. A tal fine, la direttiva prevede in numerose disposizioni che gli Stati membri possono apportare precisazioni per gli archivi soggetti alla loro legislazione. Potranno altresì essere necessarie misure complementari per l'applicazione di taluni principi generali a settori che presentano peculiarità importanti.

IV. ESAME DELLE DISPOSIZIONI

CAPO I

Disposizioni generali

Articolo 1

Oggetto della direttiva

Questo articolo stabilisce che gli Stati membri sono tenuti ad assicurare la protezione delle persone relativamente al trattamento di dati personali applicando le disposizioni della direttiva. Dato che, in virtù della presente direttiva, la protezione è garantita secondo gli stessi principi in tutti gli Stati membri ed è quindi equivalente, questi ultimi non possono limitare, per i settori oggetto della direttiva, la circolazione dei dati per motivi relativi alla protezione della persona interessata. Tuttavia, la protezione delle persone e la circolazione dei dati sono garantiti a norma della presente direttiva unicamente per i settori da essa disciplinati. Pertanto, agli archivi detenuti per finalità private e a quelli appartenenti ad associazioni senza scopo di lucro, non sono applicabili le disposizioni del presente articolo in quanto l'articolo 3, paragrafo 2, li esclude dal campo di applicazione della direttiva.

Articolo 2

Definizioni

Questo articolo definisce i principali concetti utilizzati nella direttiva. Le definizioni riprendono quelle della convenzione 108 del Consiglio d'Europa apportandovi tuttavia gli adattamenti e le precisazioni necessari per garantire una protezione equivalente di elevato livello nella Comunità.

- a) "Dato personale". Come nella convenzione 108, si è scelta una definizione ampia onde applicarla a tutte le informazioni che possono essere collegate ad una persona. Infatti, a seconda della finalità per cui è impiegato, qualsiasi dato relativo ad una persona, anche apparentemente inoffensivo, può rivestire un certo carattere di sensibilità (ad esempio un semplice indirizzo postale). Onde evitare che mezzi di identificazione indiretta consentano di eludere tale definizione, si precisa che si considera identificabile la persona che può essere identificata mediante riferimento ad un numero o ad un'informazione analoga.
- b) "Rendere anonimi i dati". Tale concetto mira a permettere l'esclusione di dati che non sono identificabili dall'applicazione di talune disposizioni della direttiva. Un dato può essere considerato come reso anonimo anche se teoricamente potrebbe essere di nuovo personalizzato mediante mezzi tecnici e finanziari sproporzionati.
- c) "Archivio di dati personali". La definizione si basa sul criterio della possibilità di accesso ai dati personali sia mediante un trattamento manuale consistente in una raccolta di dati strutturati, sia mediante un trattamento automatizzato che consenta il raggruppamento di dati disseminati o di selezionare dati da un testo integrale secondo un metodo di consultazione corrispondente a quello di un archivio.

La definizione si applica pertanto anche agli archivi meccanografici e manuali strutturati. Sono invece esclusi i dossier individuali, in particolare quelli amministrativi, che non contengono una raccolta strutturata di dati personali, tenuto conto delle particolarità e diversità delle legislazioni nazionali in materia.

- d) "Trattamento". Nell'enumerare le principali azioni di trattamento, tale definizione adatta quella della convenzione al campo di applicazione più ampio del concetto di archivio. Per trattamento si intendono le operazioni di interconnessione di dati in quanto consentono di elaborare nuovi dati (ad es. profilo elettronico). Il riferimento al congelamento riguarda il caso di dati il cui accesso è bloccato al di là delle normali misure di sicurezza senza tuttavia che ciò equivalga alla loro cancellazione.
- e) "Responsabile dell'archivio". Il concetto di "capo dell'archivio" della convenzione subisce un duplice adattamento: da un lato, ci si richiama al diritto comunitario per contemplare i casi in cui direttive specifiche contengono disposizioni concrete relative alla protezione dei dati personali e, d'altro lato, si precisa che chi autorizza la consultazione, in particolare nel caso dell'interrogazione diretta, è il responsabile dell'archivio.
- f) "Autorità di controllo". Tale definizione sottolinea che l'autorità deve essere indipendente e rinvia all'articolo 26, il quale precisa le funzioni dell'autorità di controllo.
- g) e h) "Settore pubblico" e "Settore privato". Le definizioni del settore pubblico e del settore privato figurano nella direttiva in quanto talune sue disposizioni sono specifiche all'uno o all'altro di tali settori (capi II e III relativi alla legittimità dei trattamenti di dati personali nel settore pubblico e nel settore privato). Le definizioni si basano sulla natura del servizio fornito dall'organismo in questione, sia esso privato o pubblico. A seconda che eserciti attività commerciali o funzioni di servizio pubblico, l'organismo dovrà applicare le norme proprie del settore privato o del settore pubblico.

Articolo 3

Campo d'applicazione

La direttiva si applica a tutti gli archivi i cui responsabili rientrano nel settore privato o nel settore pubblico. Infatti, per quest'ultimo, lo svolgimento di numerose attività amministrative richiede, a norma del diritto comunitario, una cooperazione tra le amministrazioni degli Stati membri. Tuttavia, sono esclusi gli archivi del settore pubblico utilizzati esclusivamente per attività che non rientrano nel campo d'applicazione del diritto comunitario (come i servizi segreti).

Il paragrafo 2 prevede due eccezioni giustificate dal fatto che è poco probabile che sorga il rischio di violazioni della vita privata in quanto trattasi di un'utilizzazione di dati per fini assolutamente privati, come è il caso dell'agenda elettronica personale, oppure perché trattasi di registri di membri di un'associazione il cui consenso a figurarvi può essere presunto dalla loro semplice adesione e per il motivo che le informazioni contenute in tale registro non sono trasmesse a terzi.

Articolo 4

Diritto applicabile

Questo articolo fissa i criteri geografici d'applicazione in ciascuno Stato membro delle disposizioni della presente direttiva. La scelta dei criteri, al paragrafo 1, è dettata dalla preoccupazione di evitare che la persona interessata sia sottratta alla protezione, in particolare qualora si eluda la legge. Si è quindi adottato il criterio concreto del luogo di localizzazione dell'archivio. A questo proposito, ciascuna parte di un archivio multilocalizzato o suddiviso tra più Stati membri deve essere considerata come un archivio a tutti gli effetti.

La stessa preoccupazione di proteggere la persona interessata in caso di delocalizzazione è all'origine di una disposizione che impone all'utente che consulta un archivio situato in un paese terzo a partire da un terminale che si trova in uno Stato membro, di rispettare le disposizioni della direttiva relative alla legittimità dei trattamenti, all'informazione della persona interessata in caso di comunicazione di dati, ai dati sensibili, alla sicurezza dei dati ed alla responsabilità. Tale obbligo non sussiste in caso di utilizzazione sporadica.

Tenuto conto della facilità di spostamento degli archivi, lo spostamento temporaneo di un archivio non costituisce un cambiamento di localizzazione. Lo spostamento di supporti in cui sono registrati i dati non deve dare luogo a nuove formalità rispetto a quelle che sono già state soddisfatte nello Stato di localizzazione permanente.

Questo articolo si propone inoltre di evitare i casi di cumulo delle leggi applicabili.

*

CAPO II

Legittimità del trattamento nel settore pubblico

I dati personali possono essere sottoposti a trattamento soltanto se quest'ultimo è legittimo. Questo capo, come il capo III, precisa le condizioni in cui un trattamento è legittimo. La legittimità deriva, a seconda del caso, dal consenso della persona interessata, da una disposizione della direttiva o di diritto comunitario o da un atto giuridico nazionale.

Articolo 5

Principi

Questo articolo dispone che la creazione di un archivio del settore pubblico e il trattamento di dati sono legittimi soltanto se risultano necessari per l'esercizio delle funzioni dell'autorità pubblica responsabile dell'archivio.

Sono previsti quattro casi in cui il trattamento di dati può essere effettuato per una finalità diversa da quella per la quale è stato creato l'archivio: qualora vi sia il consenso della persona interessata, qualora il trattamento abbia una base giuridica, qualora, dopo aver proceduto ad una valutazione degli interessi in causa, risulti che un interesse legittimo della persona interessata non vi si oppone e, infine, in caso di minaccia imminente all'ordine pubblico oppure di rischio grave di violazione del diritto di terzi.

Questi principi non riguardano il caso specifico della comunicazione di dati a terzi previsto dall'articolo 6.

Articolo 6

Trattamento nel settore pubblico avente per oggetto la comunicazione di dati personali

Per la comunicazione di dati a terzi è necessaria una disposizione specifica giacché questo tipo di trattamento presenta il maggior rischio per la persona interessata. Il paragrafo 1 prevede due casi in cui i dati possono essere comunicati a terzi, a seconda che il destinatario appartenga al settore pubblico o al settore privato. Nel primo caso, la comunicazione deve essere necessaria all'esercizio delle funzioni dell'amministrazione che domanda o che comunica i dati; nel secondo, si impone una valutazione degli interessi in causa onde determinare la fondatezza dell'interesse legittimo del richiedente ed evitare che prevalga l'interesse della persona interessata.

Gli Stati membri hanno la possibilità di precisare nella loro legislazione le condizioni di legittimità della comunicazione nei limiti dei due principi sopra enunciati. Le precisazioni potranno consistere, ad esempio, nel definire in quali casi, in taluni settori, prevale l'interesse della persona interessata.

Per evitare che la comunicazione di dati al settore privato pregiudichi gli interessi della persona interessata, è prevista una procedura di informazione. Tuttavia è possibile derogare a tale obbligo previa autorizzazione dell'autorità di controllo, che può subordinare la deroga a determinate condizioni o decidere di informare essa stessa la persona interessata.

Articolo 7

Obbligo di notifica all'autorità di controllo

L'obbligo di notifica all'autorità di controllo, previsto da questo articolo, si limita agli archivi del settore pubblico i cui dati sono suscettibili di essere comunicati. Tale soluzione consente il minimo di trasparenza necessario all'esercizio dei diritti della persona interessata e semplifica nello stesso tempo le formalità preventive, che potrebbero costituire un onere notevole per l'autorità di controllo data l'ampiezza della nozione di archivio. Gli Stati membri possono tuttavia estendere l'obbligo di notifica ad altri archivi del settore pubblico.

CAPO III

Legittimità del trattamento nel settore privato

Articolo 8

Principi

La legittimità del trattamento di dati personali nel settore privato può essere basata sul consenso della persona interessata. Tale consenso deve essere espresso in conformità con le disposizioni dell'articolo 12, relativo al consenso della persona debitamente informata, e dell'articolo 13, relativo all'informazione al momento della raccolta dei dati.

Se manca il consenso della persona interessata, la legittimità del trattamento può basarsi sull'esistenza di una relazione di tipo contrattuale tra il responsabile dell'archivio e la persona interessata purché il trattamento sia necessario all'esecuzione del contratto (ad esempio, trattamento di ordini o fatture).

La legittimità del trattamento può anche derivare dal fatto che i dati provengono da fonti generalmente accessibili al pubblico (annuari accessibili al pubblico) qualora il trattamento sia destinato unicamente alla corrispondenza.

Infine, la legittimità del trattamento può basarsi su una valutazione degli interessi in causa da cui risulti che il responsabile dell'archivio ha un interesse legittimo e che l'interesse della persona interessata non è preminente.

La comunicazione di dati è legittima soltanto se è compatibile con la finalità dell'archivio, quale notificata all'autorità di controllo (art. 11, par. 2) e rispettata al momento della memorizzazione dei dati (art. 16, par. 1, lettera b). In caso di comunicazione di dati, il responsabile dell'archivio deve inoltre informare la persona interessata conformemente agli articoli 9 e 10. Gli Stati membri possono precisare nella loro legislazione le condizioni di legittimità nei limiti dei principi testé enunciati. Le precisazioni potranno ad esempio consistere nel definire, per taluni settori, i casi in cui prevale l'interesse della persona interessata.

Articolo 9

Obbligo di informare la persona interessata

Per consentire alla persona interessata di esercitare i suoi diritti, il primo paragrafo impone al responsabile dell'archivio l'obbligo di informare la persona interessata in merito alla comunicazione di dati che la riguardano. La persona interessata può in tal modo esercitare il suo diritto di accesso e opporsi alla continuazione del trattamento. L'obbligo di informare la persona interessata non si applica nel caso in cui i dati provengano da fonti generalmente accessibili al pubblico e il loro trattamento sia unicamente destinato alla corrispondenza.

Articolo 10

Deroghe particolari all'obbligo d'informare la persona interessata

Questo articolo riconosce agli Stati membri la possibilità di disporre nella loro legislazione che, qualora nel procedere all'informazione della persona interessata emergano gravi difficoltà di ordine pratico oppure interessi legittimi preminenti del responsabile dell'archivio o un interesse analogo di terzi, l'autorità di controllo può autorizzare, su domanda del responsabile dell'archivio, una deroga all'obbligo di informare la persona interessata. L'autorità di controllo può precisare - entro i limiti fissati dalla legislazione che le conferisce tale facoltà - le condizioni della deroga e decidere d'informare essa stessa la persona interessata.

Un'importante difficoltà di ordine pratico può essere, ad esempio, quella di non conoscere l'indirizzo della persona interessata.

Articolo 11

Obbligo di notifica all'autorità di controllo

Per gli stessi motivi che hanno dettato l'obbligo di notifica nel settore pubblico (art. 7), l'obbligo di notifica nel settore privato non si applica agli archivi i cui dati non sono destinati ad essere comunicati oppure provengono da fonti generalmente accessibili al pubblico. La notifica deve essere aggiornata in caso di cambiamento di finalità dell'archivio.

Le informazioni da notificare devono fornire gli elementi necessari al controllo del rispetto delle disposizioni della presente direttiva (perlomeno il nome e l'indirizzo del responsabile dell'archivio, la finalità dell'archivio, una descrizione dei tipi di dati ivi contenuti, i terzi cui i dati sono suscettibili di essere comunicati e una descrizione delle misure di sicurezza). Gli Stati membri possono estendere il campo di applicazione dell'obbligo di notifica.

CAPO IV

Diritti della persona interessata

Articolo 12

Il consenso della persona interessata

Questo articolo stabilisce i criteri applicabili ai fini della validità del consenso della persona interessata al trattamento dei dati che la riguardano, tanto nel settore pubblico che in quello privato.

Il consenso della persona interessata al trattamento dei dati che la riguardano costituisce una base importante per giustificare il trattamento di dati personali da parte del responsabile dell'archivio. La nozione di "consenso", quale figura all'articolo 12, significa "consenso previa informazione". Per consentire alla persona interessata di valutare i rischi e i vantaggi connessi al previsto trattamento dei dati che la riguardano e di esercitare i suoi diritti a norma dell'articolo 14 della direttiva (rettifica, cancellazione, congelamento), il responsabile dell'archivio deve fornire alla persona interessata tutte le informazioni necessarie ai fini della sua decisione, ad esempio il nome e l'indirizzo del responsabile dell'archivio, la finalità dell'archivio, i dati memorizzati nell'archivio ecc.

Quanto alla forma del consenso, la direttiva, per motivi pratici, non esige che la persona interessata manifesti il suo consenso per iscritto. Tuttavia, esso deve essere esplicito.

Inoltre, il consenso della persona interessata deve essere specifico, deve cioè riferirsi al trattamento dei dati che la riguardano effettuato dal responsabile di un determinato archivio e per una o più finalità specifiche. Infine, il consenso deve essere preciso, ossia deve specificare i tipi di dati sottoposti a trattamento, le forme di elaborazione e i potenziali destinatari in caso di trasferimento a terzi.

La lettera c) prevede il diritto della persona interessata di revocare in qualsiasi momento il suo consenso. La revoca non ha tuttavia effetto retroattivo, poiché, se così fosse, un trattamento di dati personali inizialmente legittimo potrebbe successivamente diventare illegittimo.

Articolo 13

Informazione della persona interessata al momento della raccolta dei dati

Un'efficace protezione dei dati esige che la persona interessata sia pienamente informata circa il trattamento dei dati personali non solo quando tali dati sono già stati memorizzati ed elaborati in un archivio, ma sin dalla fase precedente, e cioè nella fase della raccolta delle informazioni personali.

A norma dell'articolo 16, paragrafo 1, lettera a), i dati devono essere raccolti in maniera leale e legittima. L'articolo 13 precisa tali requisiti per il caso in cui i dati siano ottenuti direttamente dalla persona interessata.

La raccolta leale e legittima di dati personali presuppone che la persona interessata possa decidere se rivelarli o meno a chi ne effettua la raccolta sulla base di informazioni precise ed attendibili riguardanti la finalità del trattamento, l'identità del responsabile dell'archivio e l'obbligatorietà o discrezionalità delle risposte. Inoltre, per esercitare i diritti conferiti dall'articolo 14 della direttiva e per controllare effettivamente l'uso dei suoi dati, la persona interessata deve essere informata circa il suo diritto di accesso e di rettifica dei dati nonché in merito ai loro destinatari.

Il paragrafo 1 impone agli Stati membri di prevedere nelle loro legislazioni nazionali relative alla protezione dei dati che la persona interessata deve ottenere dette informazioni.

Alla raccolta materiale dei dati provvederanno spesso persone diverse dal responsabile dell'archivio nel quale i dati finiranno per essere memorizzati ed elaborati. Al fine di esercitare i suoi diritti nei confronti di tale responsabile, è importante che la persona interessata ne conosca il nome e l'indirizzo già al momento della raccolta dei dati.

Il paragrafo 2 autorizza gli Stati membri a limitare l'obbligo d'informare la persona interessata durante la raccolta dei dati qualora sia in causa un interesse generale preminente. In base a tale disposizione, l'informazione di cui al paragrafo 1 non è più obbligatoria quando ostacola l'esercizio delle funzioni di controllo e di verifica dell'autorità pubblica o il mantenimento dell'ordine pubblico.

Articolo 14

Diritti complementari della persona interessata

Questo articolo riguarda i diritti e reclami della persona interessata nei riguardi del responsabile dell'archivio. La protezione dei dati mira a salvaguardare il diritto alla vita privata della persona interessata. Pertanto, i diritti e reclami di quest'ultima nei confronti del responsabile dell'archivio costituiscono una parte fondamentale di tale protezione.

Il paragrafo 1 accorda alla persona interessata il diritto di opporsi, per motivi legittimi, al trattamento di dati che la riguardano. Per motivi legittimi si intende la mancanza di una base giuridica per una determinata elaborazione di dati personali, ad esempio il fatto che per un particolare trattamento di dati non siano stati soddisfatti i requisiti di cui ai capi II e III della direttiva.

Il paragrafo 2 protegge la persona interessata dal rischio di essere sottoposta a decisioni che la riguardano, adottate da istituzioni pubbliche o private, che implicano una valutazione del comportamento umano avente come unico fondamento un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato. Tale misura intende tutelare l'interesse della persona in questione a partecipare a processi decisionali che la riguardano direttamente. L'impiego da parte di importanti istituzioni pubbliche e private di profili personali ottenuti dal trattamento automatizzato di dati priva l'individuo della capacità di influire sui processi decisionali all'interno di dette istituzioni quando le decisioni sono adottate unicamente in base ad un profilo.

Per poter esercitare efficacemente i suoi diritti di rettifica, cancellazione o congelamento dei dati nei confronti del responsabile dell'archivio, è essenziale che la persona interessata abbia accesso ai dati contenuti nell'archivio, diritto concesso dai paragrafi 3 e 4. Il paragrafo 3 accorda infatti alla persona interessata il diritto di essere informata in merito a fatti importanti relativi al trattamento dei suoi dati personali da parte del responsabile dell'archivio in modo da poter esercitare i suoi diritti in materia di rettifica, cancellazione e congelamento ed esercitare un effettivo controllo sul trattamento dei dati che la riguardano. Il paragrafo 4 accorda alla persona interessata il diritto di ottenere a intervalli ragionevoli, senza ritardi e costi eccessivi, la conferma della memorizzazione dei suoi dati personali e, in caso affermativo, la comunicazione degli stessi in maniera intelligibile.

I paragrafi 3 e 4 lasciano agli Stati membri la libertà di decidere come trasmettere dette informazioni alla persona interessata.

Gli Stati membri sono inoltre liberi di decidere cosa si intenda per "intervalli ragionevoli". Tenuto conto degli interessi della persona interessata e del responsabile dell'archivio, le legislazioni degli Stati membri possono disporre che il responsabile dell'archivio addebita alla persona interessata che esercita il suo diritto di accesso i soli costi connessi a tale operazione, che non devono essere eccessivi.

Il paragrafo 4 autorizza inoltre gli Stati membri a disporre una norma speciale per l'esercizio da parte della persona interessata del diritto di accesso in caso di dati medici. Per tutelare la persona interessata da choc psicologici che potrebbero in casi estremi portare al suicidio, tale informazione potrebbe esserle fornita da un consulente medico.

Il paragrafo 5 accorda alla persona interessata il diritto di rettifica, cancellazione o congelamento dei suoi dati personali qualora il trattamento non sia conforme alle disposizioni della direttiva.

La persona interessata può esigere la rettifica dei suoi dati qualora essi siano inesatti, incompleti, imprecisi, ingannevoli e non aggiornati. L'esercizio del diritto di cancellazione o congelamento presuppone che i dati non siano stati trattati conformemente alle disposizioni del progetto di direttiva. In tale ottica, il paragrafo 5 si riferisce a tutte le disposizioni della direttiva in materia di raccolta, memorizzazione, trattamento ed impiego di dati personali.

Il concetto di congelamento deriva dalla legge della Repubblica federale tedesca sulla protezione dei dati (§§ 14, 27, 35 BDSG: sperrung). Se i dati sono congelati, perché sono stati raccolti, memorizzati, elaborati o utilizzati in violazione delle norme della direttiva, il responsabile dell'archivio può continuare a conservarli nel suo archivio ma deve astenersi dall'elaborarli o dall'utilizzarli, in particolare dal comunicarli a terzi. I dati congelati devono essere debitamente segnalati nell'archivio in modo da informare gli eventuali utenti dell'avvenuto congelamento.

L'espressione impiegata nel progetto di direttiva "se del caso" lascia alle legislazioni degli Stati membri relative alla protezione dei dati la definizione del diritto di cancellazione, congelamento o rettifica della persona interessata per quanto riguarda le varie situazioni in cui i dati personali sono elaborati e utilizzati in violazione delle disposizioni della direttiva.

Spesso i dati, oltre ad essere sottoposti a trattamento dal responsabile di un archivio, sono anche comunicati a terzi. Se il responsabile dell'archivio deve correggere, cancellare o congelare dati perché sono inesatti oppure sono stati illegittimamente elaborati o utilizzati, la persona interessata ha interesse a che la rettifica, la cancellazione o il congelamento siano notificati a tali terzi, in modo che essi possano a loro volta correggerli, cancellarli o congelarli. Tale interesse è tutelato dal paragrafo 7.

Il paragrafo 6 accorda alla persona interessata il diritto di far cancellare i suoi dati da archivi costituiti a fini commerciali o di pubblicità per corrispondenza. Pertanto, la persona interessata può tutelarsi dal rischio di un'indesiderata pubblicità per corrispondenza.

Infine, il paragrafo 8 obbliga gli Stati membri a riconoscere alla persona interessata il diritto di disporre di un mezzo di ricorso giurisdizionale in caso di violazione dei diritti garantiti da questo articolo.

Articolo 15

Deroghe al diritto di accesso della persona interessata agli archivi del settore pubblico

Questo articolo autorizza gli Stati membri a limitare il diritto di accesso della persona interessata agli archivi del settore pubblico per tutelare interessi pubblici preminenti o interessi di privati equivalenti al diritto alla vita privata della persona interessata. Spetta agli Stati membri decidere quali deroghe ai sensi dell'articolo 15 inserire nella loro legislazione sulla protezione dei dati. Le deroghe indicate nella presente disposizione sono quelle strettamente necessarie alla tutela dei valori fondamentali in una società democratica e devono essere autorizzate mediante un atto giuridico formale. L'elenco degli interessi che possono giustificare la limitazione del diritto di accesso a norma dell'articolo 15 è tassativo.

Per "sicurezza dello Stato" si deve intendere la protezione della sovranità nazionale da minacce interne ed esterne.

L'espressione "procedimenti penali" riguarda crimini già commessi, mentre il concetto di "pubblica sicurezza" comprende tutte le funzioni di polizia esercitate da organi statali, inclusa la prevenzione della criminalità.

L'espressione "importanti interessi economici e finanziari di uno Stato membro o della Comunità" si riferisce a tutti gli strumenti di politica economica e a tutti i mezzi di finanziamento di politiche di uno Stato membro o della Comunità, ad esempio, controllo dei cambi, controllo del commercio estero, riscossione delle imposte. La restrizione del diritto di accesso è giustificata unicamente da un interesse importante di questo tipo.

Infine, sono considerati motivi validi per restringere il diritto di accesso l'interesse di terzi equivalente al diritto di accesso della persona interessata oppure i diritti e le libertà altrui. Nella fattispecie, si tratta, ad esempio, di segreti commerciali di terzi oppure della libertà di stampa.

Qualora alla persona interessata sia negato l'accesso ai suoi dati personali memorizzati in un archivio a causa di uno degli interessi citati al paragrafo 1, l'autorità di controllo, a richiesta dell'interessato, è tenuta a compiere le indagini e verifiche necessarie relativamente all'archivio in questione.

Il paragrafo 3 autorizza gli Stati membri a limitare il diritto di accesso ai dati che siano stati raccolti soltanto temporaneamente al fine di ottenere informazioni statistiche in quanto tali operazioni non presentano soltanto rischi secondari per la persona interessata.

CAPO V

Qualità dei dati

I principi relativi alla protezione dei dati stabiliti al capo V hanno un campo d'applicazione ben più ampio di quanto indichi il titolo: infatti si applicano non solo alla qualità dei dati (art. 6), ma anche al trattamento di particolari categorie di dati ritenuti particolarmente sensibili per gli interessi della persona cui si riferiscono (art. 17) e alle opportune misure in materia di sicurezza dei dati (art. 18).

Articolo 16

Principi

Questo articolo obbliga gli Stati membri ad includere i principi fondamentali riguardanti la qualità dei dati personali nella loro legislazione nazionale relativa alla protezione dei dati. Tali principi mirano ad assicurare il diritto alla vita privata della persona interessata imponendo restrizioni alla raccolta e al trattamento di dati personali nonché al contenuto stesso degli archivi.

Il paragrafo 1, lettera a) stabilisce che la raccolta e il trattamento di dati personali devono essere effettuati in maniera leale e legittima.

Questa disposizione si applica al trattamento di dati personali quale definito dall'articolo 2, lettera b), e alla loro raccolta.

Essa esclude, ad esempio, l'impiego di dispositivi tecnici celati alla persona interessata destinati ad ottenere dati segretamente e ad insaputa di quest'ultima, come la registrazione o il controllo telefonico o altri metodi analoghi, e impedisce inoltre al responsabile dell'archivio di costituire e di impiegare archivi clandestini contenenti dati personali.

Il paragrafo 1, lettera b) stabilisce il principio della specificazione della finalità. In base a tale principio, i dati personali possono essere memorizzati soltanto per finalità determinate, esplicite e legittime.

La finalità della memorizzazione di dati personali deve essere determinata, vale a dire deve essere definito e specificato nella maniera più netta possibile lo scopo perseguito con la memorizzazione e l'impiego dei dati. Una definizione o descrizione generica oppure vaga della finalità di un archivio (ad esempio, una sua destinazione a "scopi commerciali") non soddisfa il principio della specificazione della finalità enunciato da questa disposizione.

La finalità deve essere specificata prima che sia effettuata la memorizzazione. Qualora i dati siano raccolti direttamente presso la persona interessata, l'articolo 13 esige che la finalità sia già determinata al momento in cui ha luogo la raccolta dei dati.

Successivi cambiamenti della finalità del trattamento sono ammissibili soltanto se non sono incompatibili con la finalità iniziale.

Il paragrafo 1, lettera b) stabilisce inoltre che il responsabile dell'archivio precisa in maniera esplicita la finalità della memorizzazione e dell'uso dei dati. Questa disposizione mira ad impedire la memorizzazione e l'impiego di dati personali a fini segreti.

Il fatto di imporre la legittimità sia alla finalità della memorizzazione che all'impiego di dati personali limita le potenziali finalità che un archivio di dati potrebbe perseguire: esso può essere creato ed impiegato unicamente per fini compatibili con le disposizioni della direttiva e con le legislazioni degli Stati membri. Inoltre, sono considerate legittime soltanto le finalità conformi alle funzioni amministrative dei responsabili di archivi del settore pubblico e alle attività commerciali dei responsabili di archivi del settore privato. Il paragrafo 1, lettera b) stabilisce chiaramente che il principio della specificazione delle finalità si applica non solo al trattamento di dati personali, ma anche al loro impiego, che deve essere compatibile con la finalità dell'archivio.

Il paragrafo 1, lettera c) stabilisce che i dati contenuti in un archivio devono essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono stati memorizzati. Tale principio è volto a garantire la conformità del contenuto di un archivio alla sua finalità.

La disposizione del paragrafo 1, lettera d) si riconnette strettamente ai principi enunciati dal paragrafo 1, lettere b) e c). I dati personali memorizzati in un archivio devono essere esatti, e, se necessario, aggiornati. Qualora siano inesatti o incompleti rispetto alla finalità dell'archivio, essi devono essere cancellati o rettificati.

Il paragrafo 1, lettera e) pone limiti temporali alla memorizzazione di dati personali. In effetti la conservazione di dati in una forma che consenta l'identificazione della persona interessata è permessa soltanto per il periodo di tempo necessario alla realizzazione delle finalità per cui sono stati memorizzati.

Tuttavia, potrebbe essere necessario, ad esempio per fini statistici, che i dati siano mantenuti oltre tale periodo. E' in tal caso essenziale, ai fini della protezione della persona interessata, che sia eliminato il nesso tra il suo nome e gli altri dati.

Il paragrafo 2 impone l'obbligo al responsabile dell'archivio di garantire il rispetto delle disposizioni riguardanti la qualità dei dati enunciate al paragrafo 1.

Articolo 17

Categorie particolari di dati

E' opinione generalmente riconosciuta che il diritto alla vita privata può essere compromesso non tanto dal contenuto di un archivio, quanto dal contesto in cui si opera un trattamento di dati personali. Tuttavia, negli Stati membri viene altrettanto generalmente ammesso che alcuni tipi di dati, per il loro solo contenuto - a prescindere dal contesto in cui sono elaborati - possono violare il diritto alla vita privata delle persone interessate. Pertanto, l'articolo 17 della direttiva limita rigorosamente il trattamento automatizzato e l'uso di informazioni sensibili a mezzo di archivi di dati personali.

Questo articolo enumera le seguenti categorie di dati sensibili: origine razziale (ivi comprese le informazioni sul colore della pelle); opinioni politiche, convinzioni religiose e filosofiche (ivi compresa l'informazione secondo la quale una persona non ha convinzioni religiose); (tali categorie comprendono le informazioni sull'attività della persona interessata connesse a convinzioni politiche, religiose o filosofiche); l'informazione sull'adesione a sindacati; informazioni riguardanti la salute della persona interessata (ivi comprese le informazioni sullo stato fisico e mentale passato, presente e futuro della persona interessata e le informazioni sull'abuso di droghe e alcol); le informazioni concernenti la vita sessuale.

Come regola generale, il paragrafo 1 vieta il trattamento automatizzato di dati sensibili, salvo accordo libero, esplicito e scritto della persona interessata.

Gli Stati membri possono però derogare a questa regola (paragrafo 2) per consentire il trattamento di dati sensibili qualora lo richieda un importante interesse generale. Ai fini della deroga è comunque necessaria l'adozione di un atto giuridico che specifichi i tipi di dati sensibili di cui si autorizza il trattamento, le persone aventi accesso ai dati e le opportune garanzie contro il rischio di utilizzazione abusiva e di accesso non autorizzato.

Il paragrafo 3 riguarda le informazioni relative ai procedimenti penali, la cui conservazione è consentita soltanto negli archivi del settore pubblico.

Il campo di applicazione dell'articolo 17 è limitato poiché riguarda soltanto il trattamento automatizzato.

Esso non si applica alla messa in memoria e all'elaborazione elettronica di dati relativi ad opinioni politiche, convinzioni religiose, filosofiche e sindacali quando essi sono elaborati da organizzazioni senza scopo di lucro ai sensi dell'articolo 3, paragrafo 2, lettera b).

Articolo 18

Sicurezza dei dati

Il diritto alla vita privata della persona interessata può essere compromesso non solo dal responsabile dell'archivio che raccoglie, memorizza, elabora e comunica per fini propri dati personali, ma anche dalla loro utilizzazione abusiva da parte di terzi non autorizzati ad accedere all'archivio.

Il primo comma del paragrafo 1 precisa che gli Stati membri impongono al responsabile dell'archivio l'obbligo di adottare le misure organizzative e tecniche necessarie per proteggere i dati memorizzati in archivio dall'intrusione non autorizzata di terzi o dalla loro perdita accidentale, dalla loro distruzione accidentale o non autorizzata, dalla loro alterazione, dall'accesso non autorizzato e da qualsiasi altro trattamento non consentito.

Le misure tecniche necessarie per la sicurezza dei dati includono: le misure di sicurezza concernenti l'accesso ai locali adibiti al trattamento e alla messa in memoria dei dati, l'adozione di codici di identificazione per le persone aventi accesso ai locali, le misure di controllo, tra cui l'impiego di parole d'ordine per accedere agli archivi, la cifratura dei dati, la sorveglianza in materia di manipolazioni non autorizzate o di altre attività non abituali in un archivio. Quanto alle misure organizzative, il responsabile dell'archivio adotta opportuni provvedimenti procedurali all'interno della gerarchia dell'autorità pubblica o dell'impresa commerciale cui appartiene, ad esempio istituendo livelli di autorità per quanto riguarda l'accesso ai dati.

Il secondo comma del paragrafo 1 precisa il livello delle misure di sicurezza per la protezione degli archivi. Esse devono garantire un adeguato livello di sicurezza che tenga conto, da un lato, delle attuali conoscenze in materia e del costo della loro applicazione e, d'altro lato, della natura dei dati memorizzati e della valutazione dei rischi potenziali. Per valutare l'adeguatezza delle misure relative alla sicurezza dei dati, il responsabile dell'archivio deve prendere in considerazione le raccomandazioni in materia di sicurezza informatica e di interoperatività delle reti adottate dalla Comunità a norma dell'articolo 29 della direttiva.

L'obbligo di adottare appropriate misure di sicurezza non si limita ai locali adibiti all'elaborazione dei dati o all'hardware e software impiegato per il trattamento. In caso di trasmissione di dati tra elaboratori o tra elaboratore e terminale mediante una rete di telecomunicazioni, il paragrafo 2 prevede infatti l'adozione di misure di sicurezza specifiche per la rete al fine di garantire un trasferimento sicuro e ininterrotto di dati.

Il paragrafo 3 riguarda l'accesso diretto di un utente ad un archivio tramite una consultazione in linea. La facoltà dell'utente di ottenere dati dall'archivio è specificata e limitata dal contratto sottoscritto con il responsabile dell'archivio. La direttiva stabilisce che il responsabile dell'archivio predispone l'hardware e il software impiegati per la consultazione in linea in modo che l'accesso dell'utente non oltrepassi i limiti dell'autorizzazione concessagli dal responsabile dell'archivio.

Il paragrafo 4 precisa ulteriormente le responsabilità per gli obblighi previsti dai paragrafi 1-3. Anche le persone che - di fatto o per contratto - controllano le operazioni relative ad un archivio devono soddisfare i requisiti richiesti per la sicurezza dei dati. I destinatari di questa disposizione possono essere, a seconda del caso, il responsabile di un archivio, l'utente in caso di consultazione in linea, le società prestatarie di servizi di selezione e di elaborazione di dati che operano per conto del responsabile dell'archivio.

Infine, il paragrafo 5 impone l'obbligo del segreto professionale ai dipendenti del responsabile dell'archivio e a chiunque, nell'esercizio della sua attività professionale, abbia accesso a informazioni personali contenute in un archivio. Tali persone non possono comunicare a terzi, senza l'autorizzazione del responsabile dell'archivio, le informazioni cui hanno accesso.

CAPO VI

Disposizioni specifiche per taluni settori

Articolo 19

Gli Stati membri possono stabilire deroghe alle disposizioni della presente direttiva a favore degli organismi di stampa e audiovisivi al fine di conciliare i diritti fondamentali delle persone, in particolare il diritto alla vita privata, con la libertà di informazione e la libertà di stampa. Vi è infatti il rischio di conflitti fra queste due categorie di diritti fondamentali. La soluzione prescelta insiste, in caso di deroga, sull'obbligo di valutare gli interessi in causa. Tale valutazione potrà prendere in considerazione, tra l'altro, la possibilità per la persona interessata di proporre ricorso o di usufruire di un diritto di risposta, l'esistenza di un codice di deontologia professionale, i limiti fissati dalla Convenzione europea dei diritti dell'uomo, i principi generali del diritto.

Articolo 20

Quest'articolo stabilisce che gli Stati membri incoraggiano gli ambienti professionali ad elaborare codici europei di deontologia o di buona condotta atti a facilitare l'applicazione dei principi della direttiva in determinati settori.

La Commissione appoggerà iniziative di questo tipo e ne terrà conto, se del caso, nell'esercizio del suo potere regolamentare o per formulare nuove proposte.

CAPO VII

Responsabilità e sanzioni

Articolo 21

Responsabilità

In caso di danno provocato dal mancato rispetto delle disposizioni della direttiva, questo articolo ne imputa la responsabilità al responsabile dell'archivio, al quale la persona interessata può chiedere un congruo risarcimento. Il concetto di danno si applica sia al danno materiale che morale. La responsabilità del responsabile dell'archivio è limitata in caso di perdita, distruzione oppure accesso non autorizzato, purché dimostri che sono state rispettate le misure di sicurezza.

Articolo 22

Trattamento per conto del responsabile dell'archivio

Quest'articolo si prefigge di evitare che il trattamento effettuato da terzi per conto del responsabile dell'archivio riduca la protezione della persona interessata. A tal fine, esso prevede una serie di obblighi sia per il responsabile dell'archivio che per i terzi che effettuano il trattamento.

Articolo 23

Sanzioni

Per garantire il rispetto delle disposizioni adottate in applicazione della direttiva, gli Stati membri hanno l'obbligo di disporre sanzioni effettivamente dissuasive, ad esempio penali, tenendo conto in particolare del fatto che il mancato rispetto dei principi della protezione della persona interessata costituisce una violazione di un diritto fondamentale.

CAPO VIII

Trasferimento di dati personali verso paesi terzi

Articolo 24

Principi

Questo articolo sancisce il principio secondo il quale il trasferimento di dati personali da uno Stato membro verso un paese terzo può aver luogo soltanto a condizione che quest'ultimo garantisca un livello di protezione adeguato. Spetta agli Stati membri, e se del caso alla Commissione, determinare se un paese garantisce un livello di protezione adeguato. Gli Stati membri devono comunicare alla Commissione i casi in cui un paese terzo importatore non garantisce tale livello di protezione. In tal caso la Commissione può avviare negoziati con il paese terzo interessato.

La Commissione, nell'esercizio del potere di esecuzione attribuitole dall'articolo 29, può decidere che un paese garantisce un livello di protezione adeguato basandosi sulla sua legislazione nazionale e/o sugli impegni internazionali da esso sottoscritti. La Convenzione del Consiglio d'Europa del 28 gennaio 1981, relativa alla protezione delle persone per quanto riguarda il trattamento di dati personali, rientra tra gli impegni di cui la Commissione tiene conto. Essa può inoltre avvalersi della competenza del Gruppo per la protezione dei dati personali in questo settore.

Articolo 25

Deroghe

Qualora un paese non garantisca un livello di protezione adeguato, gli Stati membri possono concedere una deroga per permettere il trasferimento di dati in occasione di un'esportazione specifica. Lo Stato membro in cui è situato l'archivio può autorizzare tale trasferimento qualora il responsabile dell'archivio garantisca un livello di protezione adeguato per detta esportazione e ammesso che non vi si oppongano gli altri Stati membri o la Commissione. A tal fine è prevista una procedura d'informazione con un termine di notifica di opposizione di dieci giorni. In caso di notifica di opposizione, la Commissione può adottare le misure appropriate, in particolare può decidere di vietare il trasferimento.

CAPO IX

Autorità di controllo e Gruppo per la protezione dei dati personali

Articolo 26

L'autorità di controllo

Quest'articolo prevede l'istituzione di un'autorità di controllo indipendente dotata di mezzi investigativi e poteri d'intervento adeguati alla funzione di sorveglianza conferitale. Le legislazioni nazionali devono garantire queste caratteristiche. L'espressione "autorità di controllo" non pregiudica l'adozione di una struttura interna articolata in funzione del sistema costituzionale degli Stati membri.

Articolo 27

Gruppo per la protezione dei dati personali

In considerazione della specificità del settore, questo articolo istituisce un comitato di tipo consultivo, il Gruppo per la protezione dei dati personali, caratterizzato dalla sua indipendenza; esso è composto dai rappresentanti delle autorità di controllo nazionali ed è presieduto da un rappresentante della Commissione.

Articolo 28

Compiti del Gruppo per la protezione dei dati personali

Questo articolo definisce i compiti del Gruppo per la protezione dei dati personali. Detto Gruppo apporta alla Commissione il contributo delle sue conoscenze e della sua esperienza nel settore della protezione delle persone per quanto riguarda il trattamento di dati personali. Esso contribuisce pertanto all'applicazione omogenea delle norme nazionali adottate in applicazione della direttiva; valuta il livello di protezione esistente nella Comunità e nei paesi terzi e ne informa la Commissione; può consigliare la Commissione in merito a progetti di misure aggiuntive da adottare.

Il Gruppo per la protezione dei dati personali può formulare raccomandazioni che, su sua richiesta, possono essere trasmesse al comitato consultivo, il quale interviene nell'ambito dei poteri di esecuzione conferiti alla Commissione.

Il Gruppo per la protezione dei dati personali redige una relazione annua sulla situazione in materia di protezione dei dati nella Comunità e nei paesi terzi. Tale relazione è trasmessa alla Commissione.

CAPO X

Potere regolamentare della Commissione

Articoli 29 e 30

Esercizio del potere regolamentare

Comitato consultivo

L'articolo 29 conferisce alla Commissione le competenze di esecuzione relative alle modalità tecniche di applicazione che sono necessarie tenuto conto dell'ampiezza e del carattere tecnico del settore del trattamento dei dati personali.

Poiché la direttiva ha per oggetto di contribuire alla realizzazione del mercato interno, l'articolo 30 prevede l'intervento di un comitato consultivo per assistere la Commissione nell'esercizio delle sue competenze di esecuzione ed applica le procedure stabilite dalla decisione del Consiglio del 13 luglio 1987 che fissa le modalità di esercizio delle competenze di esecuzione conferite alla Commissione.

**Proposta di
DIRETTIVA DEL CONSIGLIO**

concernente la protezione delle persone
relativamente al trattamento dei dati personali

IL CONSIGLIO DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità economica europea, in particolare l'articolo 100 A e l'articolo 113,

vista la proposta della Commissione (1),

in cooperazione con il Parlamento europeo (2),

visto il parere del Comitato economico e sociale (3),

(1) considerando che gli obiettivi della Comunità, enunciati nel trattato quale modificato dall'Atto unico europeo, mirano a realizzare un'unione sempre più stretta tra i popoli europei, a istituire relazioni più strette tra gli Stati che la Comunità riunisce, ad assicurare mediante un'azione comune il progresso economico e sociale eliminando le barriere che dividono l'Europa, a promuovere il miglioramento costante delle condizioni di vita, a rafforzare le difese della pace e della libertà e a promuovere la democrazia basandosi sui diritti fondamentali sanciti dalle costituzioni e dalle leggi degli Stati membri e dalla convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali;

(2) considerando che la realizzazione e il funzionamento del mercato interno, nel quale, conformemente all'articolo 8 A del trattato CEE, è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare, qualunque sia lo Stato membro in cui sono stati trattati o richiesti, ma anche che siano salvaguardati i diritti fondamentali, tenuto conto del ricorso sempre più frequente nella Comunità al trattamento di dati personali nei vari settori delle attività economiche e sociali;

(3) considerando che il mercato interno comporta uno spazio senza frontiere; che, pertanto, le amministrazioni nazionali dei vari Stati membri, in applicazione del diritto comunitario, debbono sempre più spesso ricorrere alla reciproca collaborazione e allo scambio di dati personali per poter svolgere la loro funzione o esercitare compiti per conto di un'amministrazione di un altro Stato membro;

(4) considerando che il rafforzamento della cooperazione scientifica e tecnica e l'istituzione coordinata di nuove reti di telecomunicazioni nella Comunità richiedono e facilitano la circolazione transfrontaliera di dati personali;

(5) considerando che il divario nei livelli di protezione della vita privata garantiti negli Stati membri relativamente al trattamento di dati personali può impedire la trasmissione dei dati stessi dal territorio di uno Stato membro a quello di un altro, e può pertanto costituire un ostacolo all'esercizio di una serie di attività economiche su scala comunitaria, falsare la concorrenza e ostacolare, nell'adempimento dei loro compiti, le amministrazioni che intervengono nell'applicazione del diritto comunitario; che detto divario nei livelli di protezione deriva dalla disparità delle disposizioni legislative, regolamentari ed amministrative nazionali;

(6) considerando che per eliminare gli ostacoli alla circolazione dei dati personali il livello di protezione della vita privata relativamente al trattamento di tali dati deve essere equivalente in tutti gli Stati membri; che, a tal fine, è necessario un ravvicinamento delle legislazioni applicabili in materia;

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

(8) considerando che i principi della protezione della vita privata relativamente al trattamento di dati personali oggetto della presente direttiva potranno essere completati o precisati, in particolare per taluni settori, da norme specifiche ad essi conformi;

(9) considerando che i principi relativi alla protezione si devono applicare a tutti gli archivi quando le attività del responsabile dell'archivio rientrano nel campo d'applicazione del diritto comunitario; che gli archivi del settore pubblico che non rientrano nel campo d'applicazione del diritto comunitario dovrebbero essere soggetti agli stessi principi della protezione figuranti nelle legislazioni nazionali, come prevede la risoluzione dei rappresentanti dei governi degli Stati membri delle Comunità europee riuniti in sede di Consiglio il; che, tuttavia, devono essere esclusi gli archivi riguardanti esclusivamente l'esercizio del diritto alla vita privata di una persona fisica, quali ad esempio gli archivi personali d'indirizzi;

(10) considerando che è necessario che il trattamento di dati personali nella Comunità rispetti la legislazione dello Stato membro nel quale si trova l'archivio, onde evitare che una persona venga privata della protezione che deve esserle garantita a norma della presente direttiva; che, a questo proposito, tutte le parti di un archivio suddiviso tra più Stati membri devono essere considerate come un archivio unico a tutti gli effetti; che lo spostamento in un paese terzo non deve impedire tale protezione;

(11) considerando che qualsivoglia trattamento di dati personali deve essere legittimo; che la sua legittimità deve basarsi sul consenso della persona interessata, sul diritto comunitario o sulle legislazioni nazionali;

(12) considerando che le legislazioni nazionali hanno la possibilità di precisare, nelle condizioni stabilite dalla direttiva, le norme relative alla legittimità del trattamento; che, tuttavia, tale possibilità non può servire a giustificare il controllo da parte di uno Stato membro diverso dallo Stato in cui si trova l'archivio, poiché l'obbligo incombente a quest'ultimo di garantire, conformemente alla presente direttiva, la protezione della vita privata relativamente al trattamento di dati personali è sufficiente, sotto il profilo del diritto comunitario, per consentire la libera circolazione dei dati;

(13) considerando che le procedure di notifica, per gli archivi del settore pubblico o privato, e d'informazione al momento della prima comunicazione, per gli archivi del settore privato, sono volte a garantire la trasparenza indispensabile all'esercizio del diritto di accesso di qualsiasi persona ai dati che la riguardano;

(14) considerando che, alla persona interessata, devono essere fornite, perchè il suo consenso sia valido a quando i dati che la riguardano sono raccolti direttamente presso di essa, informazioni accurate e complete;

(15) considerando che la persona interessata deve godere del diritto d'accesso per poter verificare la legittimità del trattamento dei dati che la riguardano e la loro qualità;

(16) considerando che ai fini di un eventuale trattamento i dati devono rispondere a determinati requisiti; che il trattamento di dati di per sé suscettibili di nuocere al diritto alla vita privata deve essere vietato salvo consenso esplicito della persona interessata; che tuttavia, per motivi importanti d'interesse pubblico, in particolare per le professioni mediche, possono essere previste deroghe in base ad una legge che fissi esattamente e rigorosamente le condizioni e i limiti del trattamento di tale tipo di dati;

(17) considerando che la protezione della vita privata relativamente al trattamento di dati personali richiede l'adozione di misure di sicurezza adeguate a livello sia della progettazione che della tecnologia del trattamento al fine di impedire eventuali trattamenti non autorizzati;

(18) considerando che nel settore dei media gli Stati membri possono derogare alle disposizioni della presente direttiva se ed in quanto esse siano intese a conciliare il diritto alla vita privata con la libertà d'informazione e il diritto di ricevere o di comunicare informazioni, quale garantito dall'articolo 10 della convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali;

(19) considerando che gli Stati membri devono incoraggiare l'elaborazione, da parte degli ambienti professionali, di codici di deontologia o di buona condotta europei concernenti taluni settori particolari; che la Commissione appoggerà le iniziative in materia e ne terrà conto al momento di valutare l'opportunità di nuove misure specifiche per taluni settori;

(20) considerando che in caso di inosservanza delle disposizioni della presente direttiva il responsabile dell'archivio deve essere considerato responsabile dei danni provocati; che, per assicurare una protezione effettiva, si devono applicare sanzioni dissuasive;

(21) considerando che è altresì necessario che il trasferimento di dati personali possa aver luogo con i paesi terzi aventi un livello di protezione adeguato; che, in assenza di tale protezione nei paesi terzi, la presente direttiva prevede, in particolare, l'avvio di negoziati con i medesimi;

(22) considerando che i principi fissati dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale;

(23) considerando che l'esistenza in ciascuno Stato membro di un'autorità di controllo indipendente è un elemento essenziale della protezione delle persone riguardo al trattamento di dati personali; che a livello comunitario è opportuno istituire un Gruppo per la protezione dei dati personali che eserciti le sue funzioni in piena indipendenza; che, tenuto conto di tale sua caratteristica specifica, esso deve consigliare la Commissione e contribuire all'applicazione omogenea delle norme nazionali adottate in applicazione della presente direttiva;

(24) considerando che l'adozione delle misure complementari per l'applicazione dei principi della presente direttiva impone di attribuire alla Commissione un potere regolamentare e di istituire un comitato consultivo secondo le modalità fissate nella decisione 87/373/CEE del Consiglio⁽¹⁾,

HA ADOTTATO LA PRESENTE DIRETTIVA:

CAPO I

DISPOSIZIONI GENERALI

Articolo 1

Oggetto della direttiva

1. Gli Stati membri garantiscono, conformemente alle disposizioni della presente direttiva, la protezione della vita privata delle persone relativamente al trattamento di dati personali contenuti in archivi.
2. Gli Stati membri non possono, per motivi relativi alla protezione garantita a norma del paragrafo 1, restringere o vietare la libera circolazione dei dati personali tra Stati membri.

Articolo 2

Definizioni

(1) GU L 197 del 18.7.1987, pag. 33.

Al fini della presente direttiva si intende per:

- a) "dati personali": qualsiasi informazione concernente una persona fisica identificata o identificabile ("persona interessata"); in particolare si considera identificabile la persona che può essere identificata mediante riferimento ad un numero d'identificazione o a un'informazione analoga;
- b) "rendere anonimi i dati": una modifica dei dati personali in modo che le informazioni ivi contenute non possano più essere associate ad una persona fisica determinata o determinabile, salvo mediante uno sforzo eccessivo in termini di personale, spese e tempo;
- c) "archivio di dati personali" (archivio): qualsiasi insieme di dati personali, centralizzati o ripartiti in vari siti, sottoposti a trattamento automatizzato oppure che, pur non essendovi sottoposti, sono strutturati ed accessibili in una raccolta organizzata secondo criteri tali da facilitarne l'utilizzo o l'interconnessione;
- d) "trattamento": le operazioni, effettuate con o senza l'aiuto di procedimenti automatizzati: memorizzazione, archiviazione, interconnessione di dati, loro modifica, utilizzo e comunicazione, in particolare la trasmissione, la divulgazione, la selezione, nonché il congelamento e la cancellazione;
- e) "responsabile dell'archivio": la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo cui compete, secondo il diritto comunitario o il diritto interno di uno Stato membro, la decisione in materia di finalità dell'archivio, scelta delle categorie di dati personali da memorizzare, operazioni da effettuare, accesso di terzi;
- f) "autorità di controllo": l'autorità pubblica indipendente, o qualsiasi altro organismo indipendente, designati da ciascuno Stato membro conformemente all'articolo 26 della presente direttiva;

- g) "settore pubblico": l'insieme delle amministrazioni, degli organismi o enti di diritto pubblico di uno Stato membro, ad eccezione di quelli che svolgono un'attività industriale o commerciale, nonché gli organismi ed enti di diritto privato qualora partecipino all'esercizio dell'autorità pubblica;
- h) "settore privato": qualsiasi persona fisica o giuridica o associazione, ivi compresi le amministrazioni, gli organismi o enti del settore pubblico che esercitano un'attività industriale o commerciale.

Articolo 3

Campo d'applicazione

1. Gli Stati membri applicano le disposizioni della presente direttiva agli archivi del settore privato e del settore pubblico, ad esclusione degli archivi del settore pubblico la cui attività non rientra nel campo d'applicazione del diritto comunitario.
2. Le disposizioni della presente direttiva non si applicano agli archivi:
 - a) detenuti da una persona fisica esclusivamente a fini privati e personali, o
 - b) detenuti da associazioni senza scopo di lucro, in particolare a carattere politico, filosofico, religioso, culturale, sindacale, sportivo o ricreativo, nel quadro del loro scopo legittimo, a condizione che riguardino unicamente i membri e i corrispondenti dell'associazione che hanno acconsentito a figurarvi e che non siano comunicati a terzi.

Articolo 4

Diritto applicabile

1. Ciascuno Stato membro applica le disposizioni della presente direttiva:

- a) a tutti gli archivi situati sul suo territorio;
 - b) al responsabile dell'archivio che risiede nel suo territorio e che, a partire da questo, utilizza un archivio situato in un paese terzo la cui legislazione non prevede un livello di protezione adeguato, salvo in caso di utilizzazione sporadica.
2. Ciascuno Stato membro applica le disposizioni degli articoli 5, 6, 8, 9, 10, 17, 18 e 21 all'utente che consulta un archivio situato in un paese terzo a partire da un terminale che si trova nel territorio di uno Stato membro, salvo in caso di utilizzazione sporadica.
3. Qualora un archivio sia temporaneamente trasferito da uno Stato membro ad un altro Stato membro, quest'ultimo non oppone ostacoli e non esige formalità addizionali rispetto alle norme applicabili nello Stato membro in cui si trova permanentemente l'archivio.

CAPO II

LEGITTIMITÀ DEL TRATTAMENTO NEL SETTORE PUBBLICO

Articolo 5

Principi

1. Fatte salve le disposizioni dell'articolo 6, gli Stati membri dispongono nella loro legislazione relativa agli archivi del settore pubblico che:
- a) la creazione di un archivio e qualsivoglia altro trattamento di dati personali sono legittimi se ed in quanto siano necessari per lo svolgimento dei compiti dell'autorità pubblica responsabile dell'archivio;
 - b) il trattamento di dati per una finalità diversa da quella per cui è stato costituito l'archivio è legittimo quando:
 - la persona interessata vi acconsente, o

- il trattamento viene effettuato in base al diritto comunitario o ad una legge o a un atto giuridico adottato in applicazione di una legge di uno Stato membro conforme alla presente direttiva che lo autorizzi e ne fissi i limiti, o
- a tale mutamento di finalità non si oppone un interesse legittimo della persona interessata, o
- il trattamento è necessario per prevenire una minaccia imminente all'ordine pubblico oppure una grave violazione del diritto di terzi.

Articolo 6

Trattamento nel settore pubblico avente per oggetto la comunicazione di dati personali

1. Gli Stati membri dispongono nella loro legislazione che la comunicazione di dati personali contenuti negli archivi di un organismo del settore pubblico è legittima soltanto:
 - a) quando sia necessaria per lo svolgimento dei compiti attribuiti all'organismo del settore pubblico che comunica o chiede la comunicazione di detti dati, o
 - b) su richiesta di una persona fisica o giuridica del settore privato che invochi un interesse legittimo, a condizione che non prevalga l'interesse della persona interessata.
2. Fatte salve le disposizioni di cui al paragrafo 1, gli Stati membri possono precisare le condizioni alle quali la comunicazione di dati personali è legittima.
3. Gli Stati membri dispongono nella loro legislazione che, nei casi contemplati dal paragrafo 1, lettera (b), il responsabile dell'archivio informa le persone interessate in merito alla comunicazione dei loro dati personali. Essi possono disporre che tale informazione sia sostituita da un'autorizzazione preventiva dell'autorità di controllo.

Articolo 7

Obbligo di notifica all'autorità di controllo

1. Gli Stati membri dispongono nella loro legislazione che la creazione di un archivio del settore pubblico contenente dati personali che potrebbero essere comunicati deve essere preventivamente notificata all'autorità di controllo, che l'annota in un apposito registro. Il registro può essere consultato da qualsiasi persona.
2. Gli Stati membri definiscono le informazioni che devono essere notificate all'autorità di controllo. Esse comprendono almeno il nome e l'indirizzo del responsabile dell'archivio, la finalità dell'archivio, una descrizione dei tipi di dati ivi memorizzati, i terzi cui i dati possono essere comunicati e una descrizione delle misure adottate in applicazione dell'articolo 18.
3. Gli Stati membri possono stabilire che le disposizioni dei paragrafi 1 e 2 si applicano ad altri archivi del settore pubblico e che la consultazione del registro può essere limitata per i motivi di cui all'articolo 15, paragrafo 1.

CAPO III

LEGITTIMITA' DEL TRATTAMENTO NEL SETTORE PRIVATO

Articolo 8

Principi

1. Gli Stati membri dispongono nella loro legislazione che, senza il consenso della persona interessata, la memorizzazione in un archivio e qualsiasi altro tipo di trattamento di dati personali sono legittimi soltanto nel rispetto delle disposizioni della presente direttiva e a condizione che:

- a) il trattamento abbia luogo nel quadro di un contratto, di un rapporto di fiducia quasi contrattuale, con la persona interessata e sia necessario all'esecuzione del medesimo, o
 - b) i dati provengano da fonti generalmente accessibili al pubblico e il loro trattamento sia destinato unicamente alla corrispondenza, o
 - c) il responsabile dell'archivio persegua un interesse legittimo, purché non prevalga l'interesse della persona interessata;
2. Gli Stati membri dispongono nella loro legislazione che il responsabile dell'archivio deve accertarsi, che nessuna comunicazione sia incompatibile con la finalità dell'archivio e contraria all'ordine pubblico. Gli stessi obblighi incombono all'utente in caso di consultazione in linea.
3. Fatte salve le disposizioni di cui al paragrafo 1, gli Stati membri possono precisare le condizioni nelle quali è legittimo il trattamento di dati personali.

Articolo 9

Obbligo d'informare la persona interessata

1. Per il settore privato, gli Stati membri stabiliscono nella loro legislazione che, in occasione della prima comunicazione o dell'apertura di una possibilità di consultazione in linea, il responsabile ne informa la persona interessata ed indica inoltre la finalità dell'archivio, i tipi di dati ivi contenuti, il suo nome e indirizzo.
2. L'informazione di cui al paragrafo 1 non è obbligatoria nel caso contemplato dall'articolo 8, paragrafo 1, lettera b). L'obbligo d'informare le persone interessate non sussiste quando la comunicazione è prevista per legge.
3. Qualora la persona interessata sia contraria alla comunicazione o a qualsiasi altro trattamento, il responsabile dell'archivio è tenuto a porre termine al trattamento contestato a meno che non vi sia esplicitamente autorizzato da una disposizione giuridica.

Articolo 10

Deroghe particolari all'obbligo d'informare la persona interessata

Qualora l'informazione della persona interessata, conformemente all'articolo 9, paragrafo 1, si riveli impossibile o comporti sforzi sproporzionati, oppure contrasti con interessi legittimi preminenti del responsabile dell'archivio o con un interesse analogo di un terzo, gli Stati membri possono stabilire nella loro legislazione che l'autorità di controllo può autorizzare una deroga.

Articolo 11

Obbligo di notifica all'autorità di controllo

1. Gli Stati membri stabiliscono nella loro legislazione che il responsabile dell'archivio notifica la creazione di un archivio di dati personali quando i dati sono destinati ad essere comunicati e non provengono da fonti generalmente accessibili al pubblico. La notifica deve essere fatta all'autorità di controllo dello Stato membro in cui si trova l'archivio oppure, se l'archivio non è situato in uno Stato membro, all'autorità di controllo dello Stato membro di residenza del responsabile. Il responsabile dell'archivio notifica alle autorità nazionali competenti qualsiasi mutamento di finalità dell'archivio o del suo indirizzo.
2. Gli Stati membri definiscono le informazioni che devono essere notificate all'autorità di controllo. Esse devono comprendere almeno il nome e l'indirizzo del responsabile dell'archivio, la finalità dell'archivio, una descrizione dei tipi di dati ivi contenuti, i terzi cui sono eventualmente comunicati i dati e una descrizione delle misure adottate in applicazione dell'articolo 18.
3. Gli Stati membri possono stabilire che le disposizioni di cui ai paragrafi 1 e 2 si applicano ad altri archivi del settore privato e che le informazioni contemplate dal paragrafo 2 sono accessibili al pubblico.

CAPO IV

DIRITTI DELLA PERSONA INTERESSATA

Articolo 12

Informazioni ai fini del consenso

Il consenso della persona interessata a un trattamento di dati personali ai sensi della presente direttiva è valido soltanto se:

- a) la persona dispone delle seguenti informazioni:
 - le finalità dell'archivio e i tipi di dati memorizzati;
 - il tipo di utilizzazione e, se del caso, i destinatari dei dati personali contenuti nell'archivio;
 - il nome e l'indirizzo del responsabile dell'archivio,
- b) è specifico ed esplicito e precisa i tipi di dati, le forme di trattamento e gli eventuali destinatari;
- c) può essere revocato dalla persona interessata in qualsiasi momento senza effetto retroattivo.

Articolo 13

L'informazione al momento della raccolta dei dati

1. Gli Stati membri garantiscono alle persone presso le quali viene effettuata una raccolta di dati personali il diritto di essere almeno informate in merito:

- a) alle finalità dell'archivio cui sono destinate le informazioni,
 - b) alla natura obbligatoria o volontaria della loro risposta alle domande oggetto della raccolta,
 - c) alle conseguenze nei loro confronti di un eventuale rifiuto di rispondere,
 - d) ai destinatari delle informazioni
 - e) all'esistenza del diritto di accesso e di rettifica dei loro dati personali,
 - f) al nome e indirizzo del responsabile dell'archivio.
2. Le disposizioni del paragrafo 1 non si applicano alla raccolta delle informazioni quando l'informazione della persona interessata impedirebbe l'esercizio delle funzioni di controllo e di verifica dell'autorità pubblica o il mantenimento dell'ordine pubblico.

Articolo 14

Diritti complementari della persona interessata

Gli Stati membri riconoscono alla persona interessata il diritto:

- 1. di opporsi, per motivi legittimi, al trattamento di dati personali che la riguardano;
- 2. di non essere sottoposta ad una decisione amministrativa o privata che implichi una valutazione del suo comportamento avente come unico fondamento un trattamento automatizzato di dati personali volto a definire il profilo o la personalità dell'interessato;
- 3. di conoscere l'esistenza di un'archivio, le sue finalità principali nonché l'identità e la residenza abituale, la sede o il domicilio del responsabile dell'archivio;

4. di ottenere a intervalli ragionevoli e senza ritardi o spese eccessive, la conferma dell'esistenza o meno in un archivio di dati personali che la riguardano e la loro comunicazione in forma intelligibile.

Gli Stati membri possono disporre che il diritto di accesso ai dati a carattere medico può essere esercitato soltanto per il tramite di un medico;

5. di ottenere, se del caso, la rettifica, la cancellazione o il congelamento di tali dati qualora il trattamento non sia conforme alle disposizioni della presente direttiva;
6. di ottenere, su richiesta, la cancellazione gratuita dei dati che la riguardano memorizzati in archivi contenenti informazioni in materia di ricerche di mercato o di pubblicità.
7. di ottenere, in caso di applicazione del paragrafo 5 del presente articolo e qualora i dati siano stati comunicati a terzi, la notifica a questi ultimi della loro rettifica, cancellazione o congelamento;
8. di disporre di un mezzo di ricorso giurisdizionale in caso di violazione dei diritti garantiti dal presente articolo.

Articolo 15

Deroghe al diritto di accesso della persona interessata agli archivi del settore pubblico

1. Gli Stati membri possono limitare per legge i diritti enunciati nei punti 3 e 4 dell'articolo 14 per motivi concernenti:
 - a) la sicurezza dello Stato,
 - b) la difesa,
 - c) procedimenti penali,
 - d) la pubblica sicurezza,
 - e) un interesse economico e finanziario imperativo, debitamente giustificato, di uno Stato membro o della Comunità,

- f) la necessità dell'autorità pubblica di esercitare funzioni di controllo o di ispezione,
 - g) un diritto equivalente di un'altra persona o diritti e libertà di terzi.
2. Nel casi di cui al paragrafo 1, l'autorità di controllo deve poter effettuare, su domanda della persona interessata, le necessarie verifiche dell'archivio.
 3. Gli Stati membri possono limitare il diritto di accesso della persona interessata ai dati temporaneamente compilati al fine di ricavare informazioni statistiche.

CAPO V

QUALITA' DEI DATI

Articolo 16

Principi

1. Gli Stati membri dispongono che:
 - a) la raccolta e il trattamento di dati personali devono essere effettuati in maniera leale e legittima;
 - b) i dati devono essere memorizzati per finalità ben determinate, esplicite e legittime ed utilizzati conformemente a tali finalità;
 - c) i dati devono essere adeguati, pertinenti e non eccessivi rispetto alle finalità per le quali sono stati memorizzati;
 - d) i dati devono essere esatti, e, se necessario, aggiornati; i dati inesatti o incompleti devono essere cancellati o rettificati;

e) I dati non devono essere conservati sotto una forma che consenta l'identificazione delle persone interessate per un periodo di tempo superiore a quello necessario alle finalità per cui sono stati memorizzati.

2. Il responsabile dell'archivio garantisce il rispetto delle disposizioni contemplate dal paragrafo 1.

Articolo 17

Categorie particolari di dati

1. Gli Stati membri vietano il trattamento automatizzato, salvo accordo libero, esplicito e scritto dalla persona interessata, di dati che ne rivelino l'origine razziale ed etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza a sindacati, nonché le informazioni relative allo stato di salute e alla vita sessuale.
2. Gli Stati membri possono, per importanti motivi d'interesse pubblico, stabilire deroghe alle disposizioni del paragrafo 1 in base ad una legge che precisi i tipi di dati memorizzabili, le persone aventi accesso all'archivio nonché le opportune garanzie contro il rischio d'utilizzazione abusiva e di accesso non autorizzato.
3. I dati relativi a condanne penali possono essere conservati soltanto in archivi del settore pubblico.

Articolo 18

Sicurezza dei dati

1. Gli Stati membri, nella loro legislazione, impongono al responsabile dell'archivio l'obbligo di adottare le misure tecniche ed organizzative necessarie per proteggere l'archivio dalla distruzione, accidentale o non autorizzata, dalla perdita accidentale dei dati o dalla loro alterazione, dall'accesso non autorizzato a dati personali o da qualsiasi altro trattamento non consentito.

Tali misure devono garantire agli archivi automatizzati un adeguato livello di sicurezza tenuto conto, da un lato, delle attuali conoscenze in materia e del costo della loro applicazione e, d'altro lato, della natura dei dati da proteggere e della valutazione dei rischi potenziali. A tal fine, il responsabile dell'archivio deve prendere in considerazione le raccomandazioni in materia di sicurezza informatica e d'interoperatività delle reti adottate dalla Commissione secondo le modalità previste dall'articolo 29.

2. Per la trasmissione di dati personali in una rete occorre scegliere metodi atti a fornire un adeguato livello di sicurezza.
3. In caso di consultazione in linea, le installazioni tecniche e il software devono essere predisposti in modo che la consultazione avvenga entro i limiti dell'autorizzazione concessa dal responsabile dell'archivio.
4. Gli obblighi di cui ai paragrafi 1-3 incombono anche alle persone che, di fatto o per contratto, esercitano il controllo sulle operazioni relative ad un archivio.

5. Chiunque acceda, nell'esercizio della sua attività professionale, a informazioni contenute in archivi, non può comunicarle a terzi senza l'accordo del responsabile dell'archivio.

CAPO VI

DISPOSIZIONI SPECIFICHE PER TALUNI SETTORI

Articolo 19

Al fine di conciliare il diritto alla vita privata con le norme che disciplinano la libertà d'informazione e di stampa, gli Stati membri possono accordare deroghe alla presente direttiva a favore degli organismi di stampa e audiovisivi.

Articolo 20

1. Gli Stati membri incoraggiano gli ambienti professionali a partecipare all'elaborazione di codici europei di deontologia o di buona condotta per determinati settori sulla base dei principi contenuti nella presente direttiva.

CAPO VII

RESPONSABILITA' E SANZIONI

Articolo 21

Responsabilità

1. Gli Stati membri stabiliscono nella loro legislazione che qualsiasi persona i cui dati personali siano memorizzati in un archivio e che subisca un danno per effetto del trattamento o di qualsiasi altra azione incompatibile con le disposizioni della presente direttiva, ha il diritto di chiedere al responsabile dell'archivio un adeguato risarcimento.

2. Gli Stati membri possono disporre che i danni risultanti dalla perdita o dalla distruzione di dati o da un accesso non autorizzato non sono imputabili al responsabile dell'archivio se quest'ultimo dimostra di aver adottato le opportune misure per conformarsi alle disposizioni degli articoli 18 e 22.

Articolo 22

Trattamento per conto del responsabile dell'archivio

1. Gli Stati membri dispongono nella loro legislazione che, in caso di trattamento effettuato per conto del responsabile dell'archivio, quest'ultimo deve accertarsi del rispetto delle necessarie misure di sicurezza e di organizzazione e scegliere una persona o un'impresa che fornisca garanzie sufficienti al riguardo.
2. Chiunque raccolga o tratti dati personali per conto del responsabile dell'archivio deve rispettare gli obblighi contemplati dagli articoli 16 e 18 della presente direttiva.
3. Il contratto deve essere stipulato per iscritto e specificare, in particolare, che i dati personali non possono essere divulgati dal prestatario o dai suoi dipendenti senza l'accordo del responsabile dell'archivio.

Articolo 23

Sanzioni

Gli Stati membri prevedono nelle loro legislazioni l'applicazione di sanzioni dissuasive al fine di garantire il rispetto delle disposizioni adottate in applicazione della presente direttiva.

CAPO VIII

TRASFERIMENTO DI DATI PERSONALI VERSO PAESI TERZI

Articolo 24

Principi

1. Gli Stati membri dispongono nella loro legislazione che il trasferimento temporaneo o definitivo, verso un paese terzo, di dati personali che formano oggetto di un trattamento, oppure raccolti a tal fine, può aver luogo soltanto a condizione che detto paese garantisca un livello di protezione adeguato.
2. Gli Stati membri comunicano alla Commissione i casi in cui un paese terzo importatore non garantisce un livello di protezione adeguato.
3. Qualora la Commissione constati, in base alle informazioni degli Stati membri o in base ad altre informazioni, che un paese terzo non dispone di un livello di protezione adeguato e che la situazione che ne deriva è pregiudizievole per gli interessi della Comunità e dello Stato membro, essa può avviare negoziati al fine di porvi rimedio.
4. La Commissione può decidere, in conformità della procedura definita dall'articolo 30, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato in considerazione dei suoi impegni internazionali o della sua legislazione nazionale.
5. Le misure adottate a norma del presente articolo sono conformi agli obblighi incombenti alla Comunità in virtù di accordi internazionali, sia bilaterali che multilaterali, relativi alla protezione delle persone relativamente al trattamento automatizzato dei dati personali.

Articolo 25

Deroghe

1. Uno Stato membro può derogare alle disposizioni dell'articolo 24, paragrafo 1, per un determinato trasferimento di dati verso un paese terzo, qualora il responsabile dimostri che nel caso di specie esistono sufficienti garanzie relativamente al rispetto di un livello di protezione adeguato. Lo Stato membro può accordare una deroga soltanto dopo averne informato la Commissione e gli Stati membri e se nessuno Stato membro o la Commissione notificano la loro opposizione entro un termine di 10 giorni.
2. In caso di opposizione, la Commissione adotta le misure appropriate, secondo la procedura di cui all'articolo 30, paragrafo 2.

CAPO IX

AUTORITA' DI CONTROLLO E GRUPPO PER LA PROTEZIONE DEI DATI PERSONALI

Articolo 26

L'Autorità di controllo

1. Gli Stati membri garantiscono che un'autorità indipendente competente controlli la protezione dei dati personali. Tale autorità ha il compito di sorvegliare l'applicazione delle disposizioni nazionali adottate in applicazione della presente direttiva e di esercitare tutte le funzioni attribuitele dalla presente direttiva.
2. L'autorità di controllo dispone di mezzi investigativi e di poteri effettivi d'intervento contro la creazione e lo sfruttamento di archivi non conformi alle disposizioni della presente direttiva. A tal fine, essa dispone in particolare del diritto di accesso agli archivi cui si applica la presente direttiva e deve poter raccogliere qualsiasi informazione necessaria all'esercizio della sua funzione di controllo.

3. All'autorità di controllo può rivolgersi qualsiasi persona che abbia interesse a presentarle una denuncia o un reclamo concernenti la protezione delle persone in materia di dati personali.

Articolo 27

Gruppo per la protezione dei dati personali

1. E' istituito un Gruppo per la protezione dei dati personali. Tale gruppo, a carattere consultivo e indipendente, è composto dai rappresentanti dell'autorità di controllo, prevista dall'articolo 26, di tutti gli Stati membri ed è presieduto da un rappresentante della Commissione.
2. Al segretariato del Gruppo per la protezione dei dati personali provvedono i servizi della Commissione.
3. Il Gruppo per la protezione dei dati personali adotta il proprio regolamento interno.
4. Il Gruppo per la protezione dei dati personali esamina le questioni iscritte all'ordine del giorno dal suo presidente, di sua iniziativa o su domanda motivata di un rappresentante delle autorità di controllo, concernenti l'applicazione delle disposizioni di diritto comunitario in materia di protezione dei dati personali.

Articolo 28

Compiti del Gruppo per la protezione dei dati personali

1. Il Gruppo per la protezione dei dati personali:
 - a) contribuisce all'interpretazione omogenea delle norme nazionali adottate in applicazione della presente direttiva;
 - b) formula un parere sul livello di protezione nella Comunità e nei paesi terzi;

- c) consiglia la Commissione in merito a progetti di misure addizionali o specifiche da adottare ai fini della protezione della vita privata.
2. Qualora il Gruppo per la protezione dei dati personali constati tra le legislazioni o prassi degli Stati membri in materia di protezione di dati personali divergenze tali da pregiudicare l'equivalenza della protezione nella Comunità, ne informa la Commissione.
 3. Il Gruppo per la protezione dei dati personali può formulare raccomandazioni su qualsiasi questione riguardante la protezione delle persone per quanto concerne i dati personali nella Comunità. Le raccomandazioni vengono messe a verbale e possono essere trasmesse al Comitato consultivo di cui all'articolo 30. La Commissione informa il Gruppo per la protezione dei dati personali del seguito da essa dato alle raccomandazioni.
 4. Il Gruppo per la protezione dei dati personali redige una relazione annuale sullo stato della protezione delle persone per quanto riguarda il trattamento dei dati personali nella Comunità e nei paesi terzi, e la trasmette alla Commissione.

CAPO X

POTERE REGOLAMENTARE DELLA COMMISSIONE

Articolo 29

Esercizio del potere regolamentare

1. La Commissione, secondo la procedura di cui all'articolo 30, paragrafo 2, stabilisce le modalità tecniche necessarie per applicare la presente direttiva alle specificità di taluni settori, tenuto conto delle conoscenze attuali in materia e dei codici di buona condotta.

Articolo 30

Comitato consultivo

1. La Commissione è assistita da un Comitato consultivo composto dai rappresentanti degli Stati membri e presieduto dal rappresentante della Commissione.
2. Il rappresentante della Commissione sottopone al Comitato un progetto delle misure da adottare. Il Comitato, entro un termine che il presidente può fissare in funzione dell'urgenza della questione in esame, formula il suo parere sul progetto eventualmente procedendo a votazione. Il parere è iscritto a verbale; inoltre, ciascuno Stato membro ha il diritto di chiedere che la sua posizione figuri a verbale. La Commissione tiene in massima considerazione il parere formulato dal Comitato. Essa lo informa del modo in cui ha tenuto conto del suo parere.

DISPOSIZIONI FINALI

Articolo 31

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari ed amministrative necessarie per conformarsi alla presente direttiva entro e non oltre il 1° gennaio 1993.

Le disposizioni adottate in virtù del primo comma fanno espresso riferimento alla presente direttiva.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni di diritto interno che adottano nel settore disciplinato dalla

La Commissione presenta periodicamente al Consiglio e al Parlamento europeo una relazione sull'applicazione della presente direttiva, accompagnata, se del caso, dalle opportune proposte di modifica.

Articolo 33

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, addì

Per il Consiglio

Fiche Financière

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL
VISANT AU RAPPROCHEMENT DE CERTAINES DISPOSITIONS
LEGISLATIVES, REGLEMENTAIRES ET ADMINISTRATIVES
DES ETATS MEMBRES
RELATIVES A LA PROTECTION DES PERSONNES
A L'EGARD DU TRAITEMENT DES DONNEES
A CARACTERE PERSONNEL

1. Ligne budgétaire concernée (éventuellement à créer) :

A 2511 : Frais de réunions de comités dont la consultation n'est pas un élément obligatoire de la procédure de formation d'actes communautaires.

2. Base légale (ou autre) :

Article 100 A

3. Proposition de classification en dépense obligatoire/non obligatoire

(avec justification succincte en vertu de la déclaration commune du 30 juin 1982) :
non-obligatoire

4. Description et justification de l'action :

- 4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,
- permettre la circulation transfrontière de données à caractère personnel dans la Communauté,
- permettre le bon fonctionnement du marché intérieur.

4.2. Création de 2 comités compétents en matière de protection des personnes à l'égard des données à caractère personnel (Art. 27,30)

personnes concernées : 1. Pour le Comité de protection des données à caractère personnel (Art. 27) :
représentants de l'autorité de contrôle de tous les Etats membres (groupe 4)

2. Pour le Comité consultatif (Art.30) :
représentants des Etats membres (groupe 3)

4.3. Un représentant de la Commission préside le Comité de protection des données à caractère personnel et le Comité consultatif.
Le secrétariat du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions

(frais de participation des membres des 2 Comités)

5.2. Calcul : - Comité de protection des données :

24 membres (non-gouvernementaux) x 3 réunions

a 2 jours x 1180 ECU (590 ECU/jour) = 84.960 ECU*

- Comité consultatif :

24 membres (gouvernemental) x 1 réunion a 2 jours x

780 ECU (390 ECU/jour) = 18.720 ECU*

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echancier des crédits d'engagement et de paiement

CE-CP

1993 : 103.680 ECU

1994 : " "

1995 : " "

1996 : " "

1997 : " "

6.2. Part du financement communautaire dans le coût total : 100%

7. Observations :

1. Le Comité de protection des données à caractère personnel (Art. 27) :

Il est institué ce Comité à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tout les Etats membres, présidé par un représentant de la Commission.

Ce Comité établit son règlement intérieur. Le secrétariat du Comité est assuré par les services de la Commission.

Missions de ce Comité : voir Art.28.

2. Le Comité consultatif (Art.30) :

Il est institué un Comité consultatif composé des représentants des Etats membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.

* estimation

FICHE D'IMPACT SUR LA COMPETITIVITE ET L'EMPLOI

I. Quelle est la justification principale de la mesure ?

- Assurer la protection des personnes à l'égard des données à caractère personnel.
- Permettre la circulation transfrontière de données à caractère personnel dans la Communauté.
- Permettre le bon fonctionnement du marché intérieur.

II. Caractéristiques des entreprises concernées.

La proposition concerne toutes les entreprises qui utilisent des fichiers de données à caractère personnel quel que soit leur taille ou leur secteur d'activité.

III. Quelles sont les obligations imposées directement aux entreprises ?

Se conformer aux dispositions applicables aux traitements de données à caractère personnel, notamment celles relatives à la légitimité de ces traitements dans le secteur privé.

IV. Quelles sont les obligations susceptibles d'être imposées indirectement aux entreprises via les autorités locales ?

Aucune.

V. Y a-t-il des mesures spéciales pour les PME ?

Non.

VI. Quel est l'effet prévisible ?

a) sur la compétitivité des entreprises ?

Les règles de protection s'appliquent à toutes les entreprises et élimineront les distorsions de concurrence dues à l'actuelle disparité des législations nationales. En ce qui concerne leur compétitivité internationale, la directive prévoit des négociations avec les pays tiers qui n'assurent pas encore un niveau de protection adéquat.

b) sur l'emploi ?

La directive prévoit la création d'instances de contrôle nationales.

VII. Les partenaires sociaux ont-ils été consultés sur cette proposition ?

Non.

PROGETTO DI
RISOLUZIONE DEI RAPPRESENTANTI DEI GOVERNI DEGLI STATI MEMBRI
DELLE COMUNITA' EUROPEE RIUNITI IN SEDE DI CONSIGLIO

I rappresentanti dei governi degli Stati membri delle Comunità europee riuniti in sede di Consiglio

considerando che la direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali garantisce la protezione della vita privata delle persone relativamente al trattamento dei dati personali contenuti in archivi del settore privato e del settore pubblico, ad eccezione degli archivi del settore pubblico le cui attività non rientrano nel campo d'applicazione del diritto comunitario;

desiderosi di facilitare la cooperazione fra le amministrazioni degli Stati membri nei settori che non rientrano nel campo d'applicazione del diritto comunitario e di garantire nel contempo un elevato livello di protezione della vita privata delle persone interessate;

considerando che i principi contenuti nella direttiva precisano e ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa per la protezione delle persone riguardo al trattamento automatizzato dei dati a carattere personale;

hanno convenuto la seguente risoluzione :

I governi degli Stati membri s'impegnano ad applicare al settore pubblico che non rientra nel campo d'applicazione del diritto comunitario i principi contenuti nella direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali e ad avviare le procedure legislative all'uopo necessarie.

**Dichiarazione della Commissione relativa all'applicazione
alle istituzioni e agli organismi delle Comunità europee
dei principi della direttiva del Consiglio
- concernente la protezione delle persone
relativamente al trattamento dei dati personali**

1. La Commissione considera che i principi della direttiva concernente la protezione delle persone relativamente al trattamento dei dati personali ("la direttiva") debbono essere applicati alle istituzioni e agli organismi delle Comunità europee.
2. A tal fine, la Commissione adotterà e proporrà nei più brevi termini le misure necessarie.
3. In attesa che tali misure siano adottate, la Commissione s'impegna ad applicare i principi contenuti nella direttiva ai trattamenti dei dati personali che rientrano nella sua competenza.
4. La Commissione considera che le altre istituzioni della Comunità debbono parimenti impegnarsi ad applicare i principi contenuti nella direttiva ai trattamenti di dati personali che rientrano nella loro competenza.

SYN 288

Proposta di

DIRETTIVA DEL CONSIGLIO

SULLA PROTEZIONE DEI

DATI A CARATTERE PERSONALE E SULLA TUTELA DELLA RISERVATEZZA
NELL'AMBITO DELLE RETI DIGITALI PUBBLICHE DI TELECOMUNICAZIONE

CON PARTICOLARE RIFERIMENTO

ALL'ISDN (RETE DIGITALE INTEGRATA NEI SERVIZI)

E ALLE RETI DIGITALI PER SERVIZI PUBBLICI DI RADIOTELEFONIA MOBILE

INDICE

A SOMMARIO

B RELAZIONE

I. Introduzione

II. Nuove esigenze specifiche per quanto riguarda la protezione di dati a carattere personale e la tutela della riservatezza nel settore delle telecomunicazioni

III. Orientamento proposto: le disposizioni del progetto di direttiva

IV. Conclusioni

PROPOSTA DI DIRETTIVA DEL CONSIGLIO SULLA PROTEZIONE DEI DATI A CARATTERE PERSONALE E SULLA TUTELA DELLA RISERVATEZZA NELL'AMBITO DELLE RETI DIGITALI PUBBLICHE DI TELECOMUNICAZIONE, CON PARTICOLARE RIFERIMENTO ALL'ISDN (RETE DIGITALE INTEGRATA NEI SERVIZI) E ALLE RETI DIGITALI PER SERVIZI PUBBLICI DI RADIOTELEFONIA MOBILE.

A. SOMMARIO

L'introduzione delle reti digitali pubbliche di telecomunicazione è attualmente in corso in tutta la Comunità. Nei primi anni di questo decennio oltre il 70% delle trasmissioni interurbane, oltre il 50% delle commutazioni interurbane e oltre il 30% delle commutazioni urbane saranno digitalizzate.

L'introduzione su vasta scala delle reti digitali pubbliche di telecomunicazione nella Comunità permette, soprattutto grazie alla realizzazione dell'ISDN (Rete digitale integrata nei servizi), di aumentare sensibilmente il numero delle funzioni di telecomunicazione ma richiede anche che si adotti in tutta la Comunità un approccio comune per la tutela della riservatezza, la protezione dei dati a carattere personale e la loro sicurezza.

Il Consiglio ed il Parlamento europeo hanno più volte riconosciuto l'importanza fondamentale di adeguate misure relative alla protezione dei dati e alla tutela della riservatezza per il futuro sviluppo delle telecomunicazioni nella Comunità Europea. In particolare, nella sua risoluzione del 14 dicembre 1988 sulle telecomunicazioni, il Parlamento europeo ha richiesto misure specifiche "a garanzia della segretezza dei dati e della tutela della riservatezza" ed ha ricordato alla Commissione "che, contemporaneamente alla presentazione di proposte legislative concernenti l'apertura dei mercati delle telecomunicazioni in forme giuridiche idonee, essa è politicamente responsabile dell'avvio d'iniziative a livello comunitario per la tutela dei dati relativi alle persone ...".

All'interno della Comunità si considera con maggiore attenzione l'impatto delle reti digitali sulla protezione dei dati a carattere personale e sulla tutela della riservatezza. In una risoluzione adottata a Berlino nell'agosto del 1989, i delegati degli Stati membri hanno richiesto che la protezione dei dati a carattere personale e la tutela della riservatezza siano tenute in particolare considerazione per quanto riguarda l'ISDN.

La proposta qui acclusa ha lo scopo di soddisfare tali esigenze specifiche per la protezione dei dati a carattere personale e per la tutela della riservatezza nel settore delle nuove reti digitali pubbliche di telecomunicazione. Essa è presentata nel contesto delle proposte della Commissione per la realizzazione di un quadro generale per la protezione dei dati all'interno della Comunità e ne rappresenta un complemento.

Un efficace sistema di protezione dei dati a carattere personale e della riservatezza sta diventando un presupposto essenziale per l'accettazione delle nuove reti digitali e dei nuovi servizi da parte della società. E' necessario che esso sia una delle componenti fondamentali della politica comunitaria delle telecomunicazioni al fine di garantire ai cittadini europei il pieno beneficio dei servizi di telecomunicazione avanzati, dato che l'ambiente comunitario sarà molto più ricco d'informazioni rispetto al passato.

La proposta di direttiva del Consiglio, qui acclusa, è stata redatta tenendo presente questo obiettivo globale.

B. RELAZIONE

I. INTRODUZIONE

L'attuale introduzione su vasta scala dei sistemi digitali di telecomunicazione pubblica all'interno della Comunità, ed in particolare la realizzazione dell'ISDN (rete digitale integrata nei servizi) (1) e dei nuovi servizi digitali di radiofonia mobile (2), consente di potenziare grandemente le funzioni di telecomunicazione per la popolazione in generale, ma richiede altresì un approccio comune a livello europeo per la tutela della riservatezza, dei dati a carattere personale e della sicurezza dei dati, tenuto conto delle esigenze specifiche del nuovo ambiente delle telecomunicazioni digitali.

Nella risoluzione del 12 dicembre 1986 sull'introduzione coordinata dell'ISDN nella Comunità europea (3), il Parlamento europeo pur affermando che "l'ISDN (Rete digitale integrata nei servizi), prodotto dell'evoluzione della rete telefonica, offrirà un gran numero di servizi supplementari agli abbonati, siano essi società o privati cittadini..." ha chiesto alla Commissione "di presentare proposte su un approccio concreto tendente ad assicurare all'interno dell'ISDN che si sta realizzando in tutt'Europa un grado di protezione della riservatezza dei dati che sia adeguato alle maggiori capacità tecniche di tale nuova rete". Il Parlamento europeo ha nuovamente sottolineato questa necessità, in un contesto più generale, nella risoluzione del 14 dicembre 1988 (4), in cui ha richiesto misure specifiche relative all'impiego delle reti di telecomunicazione "a garanzia della segretezza dei dati e della tutela della riservatezza" ed ha ricordato alla Commissione "che, contemporaneamente alla presentazione di proposte legislative concernenti l'apertura dei mercati delle telecomunicazioni in forme giuridiche idonee, essa è politicamente responsabile dell'avvio d'iniziative a livello comunitario per la tutela dei dati relativi alle persone ...".

(1) Raccomandazione del Consiglio del 22 dicembre 1986 sull'introduzione coordinata dell'ISDN (Rete integrata nei servizi) nella Comunità europea (86/659/CEE).

L'ISDN può essere considerata come l'evoluzione naturale della rete telefonica. Essa permette, tramite un unico accesso utilizzando l'attuale linea dell'abbonato, la trasmissione di voce (telefonia), testi, dati e immagini sotto forma di innumerevoli servizi più efficienti o del tutto nuovi (per maggiori informazioni vedi la raccomandazione del Consiglio 86/659/CEE e il capitolo II.).

Conformemente alla raccomandazione del Consiglio, sono stati finora presentati dalla Commissione due rapporti sullo stato di avanzamento della realizzazione dell'ISDN (COM(88)589; COM(90)123)

(2) Raccomandazione del Consiglio del 25 giugno 1987 relativa all'introduzione coordinata del servizio pubblico digitale cellulare paneuropeo di radiotelefonía mobile terrestre nella Comunità (87/371/CEE, G.U. L 196 del 17 luglio 1987, p. 81) e direttiva del Consiglio del 25 giugno 1987 sulle bande di frequenza da assegnare per l'introduzione coordinata del servizio pubblico digitale cellulare paneuropeo di radiotelefonía mobile terrestre nella Comunità (87/372/CEE, G.U. L 196 del 17 luglio 1987, p. 85) nonché successive proposte della Commissione nel campo del servizio pubblico digitale di radiotelefonía mobile.

(3) Risoluzione sulla raccomandazione del Consiglio 86/659/CEE, G.U. C7 del 12 gennaio 1987, p.334.

(4) Risoluzione sulle Poste e telecomunicazioni, G.U. C12 del 16 gennaio 1989, p.69; risoluzione sulla necessità di superare la frammentazione nel settore delle telecomunicazioni, G.U. C12 del 16 gennaio 1989, p.66.

Nella risoluzione del 30 giugno 1988, in cui sono stati adottati i principi del libro verde sullo sviluppo del mercato comune dei servizi e delle apparecchiature di telecomunicazione e in cui sono stati approvati in linea generale gli obiettivi del programma di azione stabilito nella comunicazione del 9 febbraio 1988 (7), il Consiglio ha definito come uno dei principali obiettivi politici quello "di tutelare i dati a carattere personale e di provvedere all'accesso delle singole persone, tramite i media della comunicazione, ad un ambiente notevolmente più ricco d'informazioni rispetto al passato".

Nella risoluzione relativa al rafforzamento del coordinamento per l'introduzione della rete digitale integrata nei servizi (ISDN) nella Comunità europea entro il 1992 (8), il Consiglio si è nuovamente espresso su questo punto nei riguardi dell'ISDN sottolineando la necessità di "continuare la discussione a livello europeo riguardo ai requisiti di tutela della vita privata degli utenti e ai requisiti in materia di sicurezza delle comunicazioni nel contesto della fornitura di nuovi servizi, sulla base della risoluzione del Parlamento europeo del 12 dicembre 1986 relativa alla raccomandazione 86/659/CEE".

I rappresentanti degli organismi nazionali competenti in materia di protezione dei dati, riuniti nella loro undicesima conferenza internazionale svoltasi a Berlino dal 28 al 31 agosto 1989, hanno adottato una risoluzione in cui si richiede che si prenda in maggiore considerazione la protezione dei dati e la tutela della riservatezza nell'ambito dell'ISDN.

Con la proposta qui acclusa la Commissione intende soddisfare tale richiesta di misure specifiche a livello comunitario relative alla protezione dei dati a carattere personale e alla tutela della riservatezza nel contesto della realizzazione delle nuove reti digitali per i servizi pubblici di telecomunicazione ed in particolare dell'ISDN (rete digitale integrata nei servizi) e delle reti digitali per servizi pubblici di radiotelefonía mobile. In essa viene tenuto conto delle profonde e giustificate preoccupazioni circa le implicazioni dirette delle reti digitali per quanto riguarda la protezione dei dati a carattere personale e la tutela della riservatezza. La Commissione ha inoltre riconosciuto che la protezione dei dati a carattere personale e la tutela della riservatezza sono requisiti fondamentali nel contesto del futuro sviluppo di un sistema aperto di reti all'interno della Comunità (9).

(5) Risoluzione del Consiglio del 30 giugno 1988 sullo sviluppo del mercato comune dei servizi e delle apparecchiature di telecomunicazione entro il 1992 (G.U. C257, p.1).

(6) COM(87) 290.

(7) Verso un mercato comunitario competitivo delle telecomunicazioni entro il 1992: attuazione del libro verde sullo sviluppo di un mercato comune dei servizi e delle apparecchiature di telecomunicazione. Comunicazione della Commissione (COM(88)48).

(8) G.U. C196 del 1° agosto 1989, p.4.

(9) Posizione comune adottata dal Consiglio il 5 febbraio 1990 in vista dell'adozione di una direttiva sull'istituzione del mercato interno per i servizi delle telecomunicazioni mediante la realizzazione della fornitura di una rete aperta (ONP) (G.U....).

La presente proposta di direttiva deve essere considerata nel contesto delle discussioni e dei principi di carattere generale stabiliti in Europa circa la protezione dei dati relativi alle persone nella convenzione del Consiglio d'Europa del 1981 per la tutela delle persone nei confronti dell'elaborazione automatica dei dati a carattere personale, convenzione che finora è stata ratificata da sette Stati membri della Comunità. La proposta è presentata nel contesto - e come complemento - delle proposte presentate parallelamente dalla Commissione in merito alla realizzazione di un quadro generale per la protezione dei dati all'interno della Comunità ed in particolare del progetto di direttiva del Consiglio riguardante il ravvicinamento di talune disposizioni legislative, regolamentari ed amministrative nei vari Stati membri circa la tutela delle persone fisiche nei confronti dell'elaborazione dei dati a carattere personale, del progetto di decisione del Consiglio riguardante l'apertura delle trattative in vista dell'adesione della Comunità europea, nei settori di sua competenza, alla convenzione del Consiglio d'Europa per la tutela delle persone nei confronti dell'elaborazione automatica dei dati a carattere personale nonché del progetto di decisione del Consiglio riguardante la sicurezza dei sistemi d'informazione; inoltre la Commissione svilupperà una serie di regolamenti interni allo scopo di garantire alle persone un grado di protezione conforme ai principi della direttiva del Consiglio di cui sopra.

In tale contesto generale, la proposta di direttiva qui acclusa prevede le disposizioni specifiche necessarie per il ravvicinamento dei provvedimenti legislativi, regolamentari ed amministrativi nella Comunità relativi alla protezione di dati a carattere personale e alla tutela della riservatezza nei confronti delle reti digitali fisse e di quelle mobili per servizi pubblici di telecomunicazione e delle nuove funzioni "intelligenti" che esse offrono.

II. NUOVE ESIGENZE SPECIFICHE PER QUANTO RIGUARDA LA PROTEZIONE DEI DATI A CARATTERE PERSONALE E LA TUTELA DELLA RISERVATEZZA NEL SETTORE DELLE TELECOMUNICAZIONI

La "digitalizzazione" delle reti pubbliche di telecomunicazione è attualmente in corso in tutta la Comunità. Nei primi anni di questo decennio oltre il 70% delle comunicazioni a lunga distanza, oltre il 50% delle commutazioni interurbane e oltre il 30% delle commutazioni urbane saranno digitalizzate.

Per digitalizzazione s'intende l'introduzione di centrali completamente computerizzate nonché l'elaborazione e la trasmissione di ogni tipo d'informazione trasmessa con reti di telecomunicazione - voce, dati e immagini - mediante un sistema numerico binario (10). Tale "flusso di bit" può quindi essere elaborato direttamente dai vari computer, sia all'interno della rete che nella stazione terminale dell'abbonato. La digitalizzazione consente una migliore qualità dei servizi rispetto alle tradizionali tecniche "analogiche" nonché un gran numero di nuove funzioni "intelligenti" che consentono una vasta gamma di nuove attività tramite reti di telecomunicazione. L'ISDN (rete digitale integrata nei servizi) in rapida evoluzione ed i nuovi servizi pubblici digitali di radiofonia mobile offrono la possibilità di effettuare comunicazioni digitali "da estremo a estremo" (da abbonato ad abbonato) (11).

Per quanto riguarda la protezione dei dati l'introduzione delle reti digitali pubbliche presenta due conseguenze fondamentali.

Da un lato, la possibilità di tecniche completamente computerizzate permette di aumentare notevolmente il grado di sicurezza dei dati soddisfacendo specifiche esigenze individuali, per es. tramite sofisticate tecniche di codifica.

Dall'altro, grazie all'elaborazione digitale dei dati operativi e di chiamata e al trattamento delle centrali computerizzate, si potrebbe - in assenza di adeguate misure per la protezione dei dati - registrare e controllare sistematicamente dati specifici relativi alla chiamata, come per esempio la provenienza della chiamata. Nelle tradizionali reti analogiche "non intelligenti" tale possibilità richiedeva l'impiego di notevoli mezzi tecnici e veniva perciò realizzata soltanto in casi veramente eccezionali.

Inoltre, le nuove funzioni intelligenti di telecomunicazione ("servizi supplementari" dell'ISDN (12)), offrono all'abbonato nuove ed importanti possibilità che migliorano la qualità del servizio stesso e, contemporaneamente, garantiscono una maggiore tutela del consumatore, come nel caso della fatturazione dettagliata. Tali nuove funzioni tuttavia richiedono nuove misure e disposizioni specifiche affinché la protezione della riservatezza sia garantita.

(10) I computer elaborano l'informazione sotto forma di "cifre binarie", cioè ogni informazione viene scomposta e ricostituita tramite due elementi fondamentali (bit): 0 e 1.

(11) Vedi Raccomandazioni del Consiglio 86/659/CEE e 87/371/CEE, note 1 e 2 qui sopra.

(12) Vedi Raccomandazione del Consiglio 86/659/CEE, nota 1.

Quindi, per quanto riguarda la protezione dei dati a carattere personale, l'introduzione delle reti digitali di telecomunicazione nella Comunità solleva importanti problemi specifici da prendere in considerazione e riguardanti:

- le informazioni relative all'abbonato, sempre più immagazzinate in archivi di abbonato;
- i dati di traffico e altri dati operativi;
- i dati contenuti nelle distinte di fatturazione;
- l'identificazione della linea chiamante (identificazione della provenienza della chiamata);
- l'invio automatico della chiamata a terzi;
- i messaggi non voluti;
- le caratteristiche tecniche specifiche per terminali o altre attrezzature che possono essere necessarie per un'adeguata protezione.

Le disposizioni generali in materia di protezione dei dati a carattere personale avviate dalla convenzione del Consiglio d'Europa e che devono essere stabilite per la Comunità con le iniziative della Commissione di cui più sopra costituiscono un quadro legislativo generale ma non forniscono i dettagli specifici necessari al trattamento di tali problemi.

Le disposizioni generali riguardanti la protezione dei dati a carattere personale non possono impedire che nei vari Stati membri vengano adottati provvedimenti legislativi, regolamentari ed amministrativi divergenti per quanto riguarda il funzionamento delle future reti digitali, il che rischia di compromettere il mercato comune dei servizi di telecomunicazione e quello delle attrezzature terminali.

Per esempio, per quanto riguarda l'identificazione della linea chiamante, alcuni Stati membri hanno in progetto d'instaurare un sistema empirico (caso per caso) per l'eliminazione di tale possibilità, a discrezione dell'abbonato chiamante. Questo potrebbe creare problemi per la libera circolazione di attrezzature terminali nella Comunità poiché tale eliminazione potrebbe avvenire per mezzo di un tasto sull'apparecchio telefonico mentre altri gestori potrebbero decidere di introdurre tale funzione tramite un codice da comporre prima del numero.

Da un confronto fra gli attuali provvedimenti nazionali emergono notevoli discordanze per quanto riguarda sia il contenuto che il tipo degli strumenti giuridici utilizzati. Tale situazione favorisce lo sviluppo di un clima d'incertezza dal punto di vista legislativo all'interno della Comunità nel campo delle reti e dei servizi di telecomunicazione, il che rappresenta una seria minaccia per lo sviluppo dell'offerta transfrontaliera di servizi.

In assenza di una direttiva riguardante i provvedimenti specifici necessari all'applicazione dei criteri generali per la protezione dei dati e la tutela della riservatezza nelle reti digitali fisse e in quelle mobili per servizi pubblici sarebbe impossibile impedire che gli sviluppi all'interno della Comunità avvengano in modo discordante.

Inoltre, le disposizioni a livello comunitario ai fini di creare un efficace sistema di protezione dei dati a carattere personale e della riservatezza stanno diventando un presupposto essenziale per l'accettazione delle nuove reti digitali e dei nuovi servizi da parte della società, il che è stato confermato dal Consiglio nella riunione del 7 novembre 1989 in cui si è affermato, per quanto riguarda gli aspetti sociali delle telecomunicazioni, che in una prospettiva europea è necessario tutelare la riservatezza e proteggere i dati a carattere personale.

La proposta di direttiva del Consiglio qui acclusa ha lo scopo di soddisfare tali esigenze specifiche.

III. ORIENTAMENTO PROPOSTO: LE DISPOSIZIONI DEL PROGETTO DI DIRETTIVA

L'obiettivo globale della direttiva proposta è quello di fornire, per l'intera Comunità, un livello di base di protezione dei dati a carattere personale e di tutela della riservatezza per i cittadini europei, livello che dovranno possedere i nuovi sistemi di telecomunicazione digitale offerti sul mercato, mentre le esigenze particolari in materia di sicurezza dei dati in singoli casi specifici vanno regolate con misure da sviluppare nel quadro del programma di lavoro stabilito nella proposta di decisione del Consiglio presentata dalla Commissione e riguardante la sicurezza nei sistemi d'informazione sopracitati.

La direttiva proposta ha lo scopo di garantire un livello di base di protezione dell'abbonato nel nuovo ambiente digitale mettendo l'accento su due principi essenziali:

- minimizzare il rischio di abuso limitando l'elaborazione e l'immagazzinamento dei dati, nell'ambito delle operazioni dei servizi pubblici di telecomunicazione, al minimo indispensabile per assicurare una funzionalità adeguata ed la qualità dei servizi;
- garantire il pieno diritto dell'abbonato a fissare le limitazioni dell'informazione, sia nei confronti dell'ente di telecomunicazione che fornisce il servizio sia nei confronti dell'altra parte in causa nella comunicazione come pure nei confronti di terzi che vogliano accedere ai dati trasmessi o forniti nell'ambito di qualunque transazione tramite una rete di telecomunicazione pubblica.

Dato che, in generale, l'impatto più importante del nuovo sistema di telecomunicazione sugli abbonati avverrà nel campo della telefonia in banda fonica, la direttiva proposta riguarda soprattutto questo settore. Essa prevede, tuttavia, una procedura per l'eventuale applicazione delle disposizioni relative al servizio di telefonia in banda fonica ad altri servizi pubblici di telecomunicazione digitale, quali i servizi pubblici di trasmissione di dati nell'ambito dell'ISDN e delle reti dati pubbliche a commutazione di pacchetto e a commutazione di circuito, come pure altri servizi pubblici di telecomunicazione ad essi collegati.

Inoltre, dato che le reti pubbliche di telecomunicazione nella Comunità si trovano attualmente in una fase di transizione ed in particolare dato che alcune centrali SPC ("Stored Programme-Controlled" ("con comando a programma registrato")), anche se non sono ancora completamente digitalizzate, forniscono una buona parte delle funzioni intelligenti in questione, la direttiva proposta prevede che, nel caso in cui uno Stato membro non abbia ancora introdotto l'ISDN o le reti digitali per servizi pubblici di radiotelefonía mobile, le disposizioni siano applicabili anche ai servizi basati su reti analogiche.

Tenendo presente tali criteri generali, il contenuto della direttiva proposta riguarda in particolare: la raccolta, l'immagazzinamento e l'elaborazione di dati a carattere personale nell'archivio dell'abbonato; l'immagazzinamento e l'elaborazione di dati di traffico e di fatturazione (soprattutto per il foglio-

distinta delle chiamate); il problema dell'identificazione della linea chiamante; l'accesso da parte di terzi; chiamate non richieste; le procedure da scegliere per stabilire specifiche norme tecniche che potrebbero essere necessarie.

Breve spiegazione degli articoli della direttiva.

Gli articoli 1 e 2 descrivono gli obiettivi globali della direttiva e la sua applicazione alla protezione dei dati e alla tutela della riservatezza in relazione ai servizi pubblici di telecomunicazione nelle reti digitali all'interno della Comunità.

L'articolo 3 contiene la definizione di alcuni termini importanti in armonia con la proposta di direttiva del Consiglio sulla realizzazione della fornitura di una rete aperta (ONP) di cui si è parlato sopra (13).

Nell'articolo 4 è enunciato il principio generale secondo cui la raccolta, l'immagazzinamento e l'elaborazione di dati a carattere personale da parte di qualunque ente di telecomunicazione sono giustificati unicamente ai fini della fornitura del servizio in questione e non possono essere impiegati per alcun altro scopo senza specifica autorizzazione legale o senza il consenso precedentemente registrato dell'abbonato. Nell'articolo 5 tale principio viene applicato alla costituzione di archivi di abbonato. Come stabilito in un "considerando" della direttiva, la raccolta, l'immagazzinamento e l'elaborazione di dati a carattere personale non possono, in particolare, essere utilizzati in modo tale che certi enti di telecomunicazione possano trarne un vantaggio concorrenziale sleale nei confronti di altri fornitori degli stessi servizi.

L'articolo 6 elenca i diritti dell'abbonato relativi ai suoi dati personali in possesso dell'ente di telecomunicazione e l'articolo 7 enuncia il principio secondo cui tali dati non possono essere comunicati a terzi senza il consenso dell'abbonato o l'autorizzazione legale.

L'articolo 8 dovrebbe garantire un adeguato grado di protezione dei dati contro l'accesso non autorizzato.

Gli articoli 9 e 10 applicano il principio della raccolta, dell'immagazzinamento e dell'elaborazione di dati a carattere personale, limitatamente alle esigenze dei servizi di telecomunicazione, ai dati di fatturazione e di traffico.

L'articolo 11 ha lo scopo di tutelare la riservatezza degli abbonati in relazione alle distinte particolareggiate delle chiamate proteggendo l'anonimato dell'abbonato chiamato.

Gli articoli 12 e 13 contengono disposizioni dettagliate riguardo all'identificazione della linea chiamante. L'eliminazione di tale identificazione deve essere resa possibile perchè, tra le varie ragioni, è necessario che sia mantenuto l'anonimato per le chiamate in provenienza o in direzione di centri di riabilitazione per tossicodipendenti e alcolisti, di centri per la protezione contro i maltrattamenti da parte di familiari o per le chiamate con servizi psichiatrici e servizi "hot line" per l'AIDS e per la prevenzione dei suicidi.

(13) Vedi nota (9).

L'abbonato chiamato, tuttavia, può avere un legittimo interesse a ricevere soltanto chiamate identificate. Quindi, affinché il diritto dell'autodeterminazione dell'informazione sia garantito tanto per la parte chiamante quanto per la parte chiamata, quest'ultima deve avere la possibilità di accettare soltanto le chiamate entranti con identificazione del numero dell'abbonato chiamante.

Inoltre, l'ente di telecomunicazione deve disporre di una funzione di annullamento (blocco) dell'eliminazione della funzione d'identificazione in caso di chiamate malintenzionate; tale funzione deve poter essere usata anche per il perseguimento di reati e per servizi d'emergenza, quali quello dei vigili del fuoco, al fine d'impedirne l'abuso.

L'articolo 14 garantisce la tutela della riservatezza dell'abbonato chiamante e dell'abbonato chiamato anche nel caso in cui vengano usate le funzioni d'invio della chiamata a terzi.

L'articolo 15 ha lo scopo d'impedire che, tramite mezzi tecnici, il contenuto di chiamate telefoniche venga immagazzinato e/o divulgato a terzi senza informare in anticipo l'abbonato chiamante.

Gli articoli 16 e 17 intendono impedire l'impiego non autorizzato dei dati riguardanti la persona dell'abbonato da parte di fornitori di servizi di teleacquisto e videotex al fine d'impedire la costituzione del profilo del consumatore nonché di tutelare la riservatezza dell'abbonato nei confronti di messaggi non voluti, quali annunci pubblicitari tramite mezzi di telecomunicazione.

L'articolo 18 ha lo scopo di ovviare alle restrizioni alla libera circolazione dei servizi e delle apparecchiature di telecomunicazione all'interno della Comunità che potrebbero derivare dall'introduzione delle caratteristiche tecniche rispondenti ai requisiti di protezione dei dati; tale articolo garantisce che vengano sviluppate, laddove richiesto, norme europee comuni per la realizzazione di specifiche caratteristiche tecniche. I lavori tecnici devono essere affidati ad organismi europei specializzati in normalizzazione, quali l'Istituto europeo delle norme per le telecomunicazioni (ETSI) e il CEN/CENELEC, conformemente alla direttiva del Consiglio sul ravvicinamento delle legislazioni degli Stati membri relative alle apparecchiature terminali di telecomunicazione, compreso il mutuo riconoscimento della loro conformità (14), e alla decisione del Consiglio n° 87/95/CEE del 22 dicembre 1986 sulla normalizzazione nel settore della tecnologia dell'informazione e delle telecomunicazioni (15).

Le disposizioni finali contenute negli articoli 19-25 riguardano il campo di applicazione, le procedure per le modifiche necessarie per adeguare la presente direttiva al progresso tecnico e le procedure di consultazione. Si prevede che per l'attuazione della direttiva la Commissione sia assistita da un comitato composto da rappresentanti degli organi nazionali competenti per la tutela dei dati e da un comitato composto da rappresentanti degli Stati membri. Si propone che tali comitati siano quelli definiti allo stesso scopo nel progetto di direttiva del Consiglio sul ravvicinamento di taluni provvedimenti legislativi, regolamentari e amministrativi negli Stati membri riguardo alla tutela delle persone fisiche nei confronti dell'elaborazione dei dati a carattere personale, che, come si è detto, è stato presentato parallelamente, ma che siano costituiti appositamente ai fini della presente direttiva.

(14) COM(89)289 -SYN 204, 27.7.1989.

(15) G.U. L 36, 7 febbraio 1987, p.31.

IV. CONCLUSIONI

Un efficace sistema di protezione dei dati a carattere personale e della riservatezza sta diventando, in tutta la Comunità, un presupposto essenziale per l'accettazione delle nuove reti digitali e dei nuovi servizi da parte della società.

In assenza di una direttiva riguardante i provvedimenti specifici necessari all'applicazione dei criteri generali per la protezione dei dati e la tutela della riservatezza per quanto riguarda i requisiti delle reti digitali fisse e di quelle mobili per servizi pubblici sarebbe impossibile impedire evoluzioni divergenti all'interno della Comunità, che potrebbero in breve tempo mettere in pericolo il mercato comune dei servizi di telecomunicazione e quello delle attrezzature terminali.

La direttiva qui acclusa ha lo scopo di prevedere tali disposizioni specifiche.

Il Consiglio è quindi invitato ad adottare la proposta di direttiva allegata.

SYN 288

Proposta di
DIRETTIVA DEL CONSIGLIO

sulla protezione dei dati personali
e della vita privata
nell'ambito delle reti digitali pubbliche di telecomunicazione
con particolare riferimento all'ISDN (rete digitale integrata nei servizi)
e alle reti digitali per servizi pubblici di radiotelefonía mobile

IL CONSIGLIO DELLE COMUNITA' EUROPEE

visto il Trattato che istituisce la Comunità economica europea, in particolare l'articolo 100,

vista la proposta della Commissione (1) ,

in cooperazione con il Parlamento europeo (2) ,

visto il parere del Comitato economico e sociale (3) ,

1. considerando che la direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali prevede che gli Stati membri assicurino la tutela della vita privata;

2. considerando che attualmente nella Comunità Europea si stanno introducendo nuove reti telefoniche pubbliche digitali di tecnologia avanzate che fanno emergere esigenze specifiche in relazione alla protezione nei dati personali e della vita privata dell'utente;

3. considerando che ciò riguarda in particolare l'introduzione dell'ISDN (Rete digitale integrata nei servizi) e delle reti digitali per servizi pubblici di radiotelefonía mobile;

-
- (1) ...
(2) ...
(3) ...

4. considerando che, nella risoluzione del 30 giugno 1988 sullo sviluppo del mercato comune dei servizi e delle apparecchiature di telecomunicazione entro il 1992 (4), il Consiglio ha chiesto che siano prese misure a garanzia della segretezza dei dati al fine di favorire la creazione di un ambiente propizio al futuro sviluppo delle telecomunicazioni nella Comunità; che, nella risoluzione del 18 giugno 1989 relativa al rafforzamento del coordinamento per l'introduzione dell'ISDN nella Comunità europea entro il 1992 (5), il Consiglio ha ribadito l'importanza della protezione dei dati personali della vita privata;

5. considerando che il Parlamento europeo ha sottolineato l'importanza della protezione dei dati personali e della vita privata nelle reti di telecomunicazione, con particolare riferimento all'introduzione dell'ISDN (Rete digitale integrata nei servizi) (6)(7)(8);

6. considerando che nella raccomandazione della Commissione n° 81/679/CEE si richiede l'adozione e la ratifica, da parte degli Stati membri, della convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale che definisce i principi generali per la protezione dei dati personali;

7. considerando che taluni Stati membri hanno adottato e ratificato tale convenzione;

(4) G.U. C 257, 04.10.1988, p.1.

(5) G.U. C 196, 11.8.1989, p.4.

(6) GU C 7 del 12.1.1987, pag. 334

(7) GU C 12, 16.1.1989, p. 69

(8) GU C 12 del 16.1.1989, pag. 66

8. considerando che la decisione del Consiglio (9) prevede l'apertura di negoziati in vista dell'adesione della Comunità Economica Europea, nei campi di sua competenza, alla convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale

9. considerando che la direttiva del Consiglio..... /CEE concernente la protezione delle persone relativamente al trattamento dei dati personali attua l'adozione di tali principi generali nella Comunità;

10. considerando che nel settore delle reti digitali pubbliche occorre prevedere disposizioni legislative, regolamentari e tecniche specifiche al fine di proteggere i dati

personali e la vita privata degli utenti dai rischi sempre maggiori di abuso legati all'immagazzinamento e ai trattamenti informatizzati di tali dati nelle suddette reti;

11. considerando che gli Stati membri stanno approntando disposizioni divergenti in tale settore;

12. considerando che, tenuto conto degli ostacoli derivanti da tali divergenze sul piano delle disposizioni legislative, regolamentari e tecniche relative alla protezione dei dati personali e della vita privata nell'ambito della realizzazione delle reti digitali pubbliche di telecomunicazione nella Comunità, in particolare dell'ISDN e delle reti digitali per servizi pubblici di radiotelefonía mobile, per

la completa instaurazione di un mercato dei servizi di telecomunicazione a livello comunitario è necessario adottare al più presto disposizioni armonizzate;

13. considerando che la presente direttiva deve prevedere i limiti entro cui possono essere raccolti, immagazzinati ed elaborati dati personali nel quadro della fornitura di servizi di telecomunicazione;

(9) G.U.

14. considerando che la raccolta, l'immagazzinamento e il trattamento di dati personali da parte di qualsivoglia ente di telecomunicazione sono giustificati esclusivamente ai fini della fornitura del servizio richiesto e che tali dati non possono essere impiegati per altri fini senza specifica autorizzazione per legge o senza previo consenso dell'abbonato; che la raccolta, l'immagazzinamento e il trattamento di dati personali non devono, in particolare, essere utilizzati dall'ente di telecomunicazione per trarne un vantaggio concorrenziale nei confronti degli altri fornitori di servizi;

15. considerando che la presente direttiva attua, nel settore delle telecomunicazioni, i principi generali del diritto dell'abbonato a verificare i dati riguardanti la sua persona e, se del caso, a correggerli o a cancellarli nonchè ad impedirne la divulgazione non autorizzata;

16. considerando che la presente direttiva deve prevedere l'armonizzazione delle normative degli Stati membri relative alla protezione della vita privata per quanto riguarda le distinte delle chiamate;

17. considerando che, per quanto riguarda l'identificazione della linea chiamante, è necessario sia garantire il diritto all'anonimato dell'abbonato chiamante sia proteggere la vita privata dell'abbonato chiamato nel caso di chiamate non identificate;

18. considerando che occorre prevedere misure a salvaguardia degli utenti di servizi di teleacquisto e videotex che impediscano l'impiego non autorizzato dei loro dati personali come

pure misure per tutelare gli abbonati in generale da interferenze nella loro vita privata mediante chiamate non richieste;

19. considerando che è necessario garantire che l'introduzione di caratteristiche tecniche delle apparecchiature per telecomunicazioni intese a proteggere i dati sia armonizzata in modo da essere compatibile con la realizzazione del mercato interno del 1992;

20. considerando che l'attuazione della presente direttiva per quanto riguarda paesi terzi deve tener conto del grado di protezione dei dati personali e della vita privata in quei paesi in conformità della direttiva .../CEE concernente la protezione delle persone relativamente al trattamento dei dati personali;

21. considerando - per tutti gli aspetti relativi alla protezione dei dati e della vita privata nell'ambito di reti digitali per servizi pubblici di telecomunicazione, che non rientrano nel campo di applicazione della presente direttiva specifica, si applica la direttiva ... /CEE;

22. considerando che la presente direttiva non riguarda i problemi della protezione dei dati personali o della vita privata relativi alla sicurezza nazionale;

23. considerando che, per elaborare misure intese ad attuare ovvero a modificare la presente direttiva, è opportuno ricorrere all'esperienza del gruppo composto dei rappresentanti degli organi nazionali competenti per la protezione dei dati istituito in conformità dell'articolo 27 della direttiva ... /CEE concernente la protezione delle persone relativamente al trattamento di dati personali;

24. considerando che tali misure devono essere elaborate con l'assistenza del comitato composto da rappresentanti degli Stati membri istituito in conformità dell'articolo 30 della direttiva .../CEE ... concernente la protezione delle persone relativamente al trattamento di dati personali;

HA ADOTTATO LA PRESENTE DIRETTIVA :

Articolo 1

1. La presente direttiva prevede l'armonizzazione delle disposizioni atte a garantire un livello uniforme di protezione della vita privata all'interno della Comunità nonché la libera circolazione delle attrezzature e dei servizi di telecomunicazione sia tra Stati membri che all'interno di essi.

2. Gli Stati membri adottano in conformità della presente direttiva le disposizioni specifiche necessarie ad assicurare la protezione dei dati personali e la vita privata nel settore delle telecomunicazioni.

Articolo 2

1. Fatte salve le disposizioni generali della direttiva .../CEE concernente la protezione delle persone relativamente al trattamento dei dati personali la presente direttiva riguarda specificamente la raccolta, l'immagazzinamento e il trattamento dei dati personali da parte di enti di telecomunicazione in relazione alla fornitura di servizi pubblici di telecomunicazione in reti digitali pubbliche di telecomunicazione all'interno della Comunità ed in particolare tramite l'ISDN (rete digitale integrata nei servizi) e le reti digitali per servizi pubblici di radiotelefonía mobile.

2. Per gli Stati membri che non dispongano ancora dell'ISDN (rete digitale integrata nei servizi) né di reti digitali per servizi pubblici di radiotelefonía mobile, le disposizioni della presente direttiva ricevono attuazione se ed in quanto si applichino anche ai servizi basati su reti analogiche.

Articolo 3

Ai sensi della presente direttiva si intende per :

1. "dati personali" : qualsiasi

informazione concernente una persona fisica identificata o identificabile;

2. "ente di telecomunicazione" : ogni organismo

pubblico o privato a cui uno Stato membro abbia concesso diritti speciali ovvero esclusivi per la gestione di una rete di telecomunicazione pubblica ed eventualmente di un servizio pubblico di telecomunicazione;

3. "rete di telecomunicazione pubblica" :

l'infrastruttura di telecomunicazione pubblica che permette la trasmissione di segnali tra determinati punti terminali di una rete tramite fili, microonde, mezzi ottici o altri mezzi elettromagnetici;

4. "servizio pubblico di telecomunicazione" :

qualsiasi servizio di telecomunicazione la cui fornitura è stata affidata da uno Stato membro, inter alia, a uno o più enti di telecomunicazione.

Articolo 4

1. La raccolta, l'immagazzinamento e il trattamento di dati personali da parte di un ente di telecomunicazione sono giustificati unicamente per scopi di telecomunicazione e, in particolare, al fine di stabilire collegamenti per trasmettere voce, dati o immagini, per compilare fatture o indirizzari e per svolgere ogni altra attività purchè legittima, per esempio, riparare guasti, impedire l'uso scorretto delle apparecchiature dell'ente di telecomunicazione o ancora registrare le chiamate in arrivo conformemente all'articolo 13 (1).

2. L'ente di telecomunicazione non deve servirsi di tali dati per costituire, con mezzi elettronici, profili degli abbonati ovvero classificazioni di singoli abbonati per categoria.

Articolo 5

1. La raccolta e l'immagazzinamento di dati relativi alla persona dell'abbonato sono consentiti nella misura in cui essi siano necessari per stipulare, modificare ovvero porre termine al contratto con l'ente di telecomunicazione. Alla scadenza del contratto, tali dati devono essere cancellati salvo qualora siano necessari, e limitatamente al tempo richiesto, per trattare reclami, per ottenere rimborsi o per assolvere ad ogni altro obbligo di legge dello Stato membro, in conformità del diritto comunitario.

2. Il contenuto dell'informazione trasmessa non può essere conservato dall'ente di telecomunicazione dopo la fine della comunicazione, salvo diversamente previsto dalle leggi dello Stato membro, in conformità del diritto comunitario.

Articolo 6

1. L'abbonato ha il diritto di:

- ottenere, ad intervalli ragionevoli e senza ritardi o spese eccessivi, la conferma del fatto se siano stati immagazzinati o meno dati relativi alla sua persona nonché comunicazione di tali dati in forma intelligibile,
- ottenere, se del caso, la rettifica o la cancellazione di tali dati qualora essi siano stati trattati in violazione delle disposizioni legislative in vigore nello Stato membro, in conformità del diritto comunitario.

Articolo 7

1. In linea di principio, tutti i dati personali elaborati nell'ambito di reti e servizi di telecomunicazione devono essere considerati dati riservati.

2. I dati personali non possono essere divulgati al di fuori dei servizi o della rete dell'ente di telecomunicazione senza l'apposita autorizzazione: per legge ovvero senza il preventivo consenso dell'abbonato. L'abbonato è considerato aver dato il proprio consenso soltanto qualora lo abbia dato su richiesta specifica dell'ente di telecomunicazione. Senza il preventivo consenso dell'abbonato, tali dati personali non possono essere comunicati ad alcuna persona, all'interno dell'ente di telecomunicazione, escludendo alla fornitura dei servizi cui si riferiscono i dati in questione.

3. L'ente di telecomunicazione non può subordinare la fornitura del servizio al suddetto consenso.

Articolo 8

L'ente di telecomunicazione deve assicurare una protezione dei dati personali, adeguata e tecnologicamente aggiornata, contro l'accesso e l'impiego non autorizzati.

2. Nei casi in cui il rischio di violazione della sicurezza della rete sia particolarmente elevato, come per esempio nel campo della radiotelefonía mobile, l'ente di telecomunicazione ha l'obbligo di informarne gli abbonati e di offrire loro un servizio di codifica da estremo ad estremo.

Articolo 9

1. Possono essere immagazzinati e trattati tutti i dati relativi alla fatturazione quali il numero telefonico o l'identificazione della stazione dell'abbonato, l'indirizzo dell'abbonato ed il tipo di stazione, il numero totale di scatti da fatturare, il numero di telefono chiamato, il tipo e la durata delle chiamate effettuate nonché la quantità di dati trasmessi come pure qualunque altra informazione necessaria ai fini della fatturazione, per esempio pagamenti anticipati, pagamenti per installazione, disattivazioni e solleciti.

2. La conservazione dei dati per fatturazione è consentita sino alla scadenza del termine previsto dalla legge entro cui la fattura può essere contestata.

Articolo 10

1. La raccolta, l'immagazzinamento e il trattamento delle informazioni di traffico contenenti i dati personali necessari per determinare le chiamate, per fini di fatturazione o per qualsiasi altro scopo operativo, ad esempio, numero telefonico dell'abbonato chiamante e di quello chiamato, momento dell'inizio e della fine di ogni chiamata, tipo di servizio di telecomunicazione usato dall'abbonato, sono consentiti nella misura in cui ciò sia necessario per la fornitura del servizio richiesto.

2. I dati di traffico immagazzinati nei centri di commutazione dell'ente di telecomunicazione devono essere cancellati al termine della chiamata a meno che tali dati siano resi anonimi o siano necessari per scopi di fatturazione o per qualunque altro fine consentito ai sensi dell'articolo 4.

Articolo 11

Su richiesta dell'abbonato può essere fornita la distinta delle chiamate, contenente, tra l'altro, il numero di telefono degli abbonati chiamati senza le ultime quattro cifre.

Articolo 12

1. Per quanto riguarda le comunicazioni tra abbonati collegati a centrali digitali, l'abbonato chiamante deve avere la possibilità di eliminare, caso per caso e con semplici mezzi tecnici, l'indicazione del suo numero telefonico sul dispositivo di visualizzazione del terminale dell'abbonato chiamato.

La funzione di trasmissione del numero telefonico può inoltre essere eliminata in modo permanente dall'ente di telecomunicazione su richiesta dell'abbonato chiamante.

2. L'abbonato chiamato può richiedere che sia eliminata in modo permanente l'identificazione delle chiamate in arrivo; egli deve inoltre avere la possibilità di escludere la funzione di visualizzazione del suo terminale ovvero di sopprimere la funzione di memoria del medesimo, al fine di impedire, caso per caso, l'identificazione delle chiamate in arrivo.

L'abbonato chiamato deve avere la possibilità di accettare soltanto le chiamate in arrivo con identificazione del numero dell'abbonato chiamante.

3. Nel caso in cui la comunicazione avvenga tra un abbonato collegato ad una centrale analogica ed abbonati collegati a centrali digitali, il primo deve essere informato del fatto che l'indicazione del suo numero telefonico compare ad ogni chiamata; deve essergli inoltre offerta la possibilità di sopprimere tale indicazione in modo permanente, su richiesta, o di eliminarla, caso per caso.

Articolo 13

1. L'ente di telecomunicazione può, per un periodo di tempo limitato, **derogare alla** soppressione dell'identificazione della linea chiamante

a) su richiesta di un abbonato che chiede l'identificazione di chiamate malintenzionate. In tal caso, i

dati relativi all'identificazione dell'abbonato chiamante sono immagazzinati dall'ente di telecomunicazione e messi a disposizione, su richiesta, dell'autorità giudiziaria o di pubblica sicurezza dello Stato membro interessato;

b) su apposito provvedimento del giudice allo scopo di prevenire o sanzionare reati gravi.

2. Una funzione permanente di **deroga deve essere messa alla**
disposizione , su richiesta,

a) di organizzazioni, riconosciute da uno Stato membro, che rispondono alle chiamate d'emergenza e **che trattano tali chiamate e**

b) al corpo dei vigili del fuoco dipendenti da uno Stato membro o da esso riconosciuti.

3. Gli enti di telecomunicazione prendono le misure necessarie per assicurare che tale funzione sia operativa tanto a livello nazionale quanto a livello comunitario.

Articolo 14

1. Il ricevente può rinviare una chiamata ad un terzo soltanto previo consenso di quest'ultimo; il terzo può limitare il rinvio automatico alle chiamate che riportano il numero dell'abbonato chiamante; il terzo deve essere informato, tramite un apposito segnale del messaggio, che si tratta di una chiamata rinviata.
2. L'abbonato chiamante deve essere informato automaticamente, mentre viene operato il collegamento, del fatto che la chiamata è rinviata ad un terzo.

Articolo 15

1. Qualora il contenuto di una telefonata sia reso accessibile a terzi per mezzo di strumenti tecnici quali altoparlanti o altri apparecchi collegati o sia registrato su nastro ad uso proprio o di terzi, si devono prendere le disposizioni necessarie affinché le parti interessate ne siano informate, mediante procedure adeguate, prima che si sia dato inizio alla diffusione o alla registrazione e per l'intera durata.
2. Il paragrafo 1 non si applica ai casi contemplati dall'articolo 13, paragrafo 1.

Articolo 16

1. L'ente di telecomunicazione deve assicurare che il numero telefonico e gli altri dati personali dell'abbonato ed in particolare quelli riguardanti la quantità e il tipo delle sue ordinazioni tramite servizio di teleacquisto ovvero le informazioni richieste tramite servizio videotex, siano immagazzinati soltanto se ed in quanto strettamente necessari alla fornitura del servizio e che siano utilizzati dal prestatore del servizio unicamente a fini autorizzati dall'abbonato.

2. Fatte salve le disposizioni dell'articolo 20, il prestatore del servizio non può costituire, con mezzi elettronici, profili degli abbonati né classificazioni di singoli abbonati per categoria, senza il loro preventivo consenso.

Articolo 17

1. Gli abbonati che ricevono chiamate non richieste a scopo di pubblicità o di offerta di forniture di merci e servizi possono notificare all'ente di telecomunicazione che trasmette tali messaggi che essi non desiderano ricevere questo tipo di chiamate.

2. L'ente di telecomunicazione deve prendere le misure necessarie per porre fine all'invio di tali messaggi all'abbonato in questione. Inoltre l'ente di telecomunicazione deve costituire un elenco specifico di tali notifiche e metterlo a disposizione dell'autorità di controllo per eventuali ispezioni, allo scopo di porre termine a tali chiamate.

Articolo 18

1. Nell'attuazione delle disposizioni della presente direttiva, gli Stati membri assicurano che, fatto salvo il disposto nei paragrafi 2 e 3 non siano imposti, per i terminali o altre apparecchiature di telecomunicazione - obblighi inderogabili - caratteristiche relativi alla tecniche specifiche che potrebbero ostacolare l'immissione sul mercato e la libera circolazione di tali apparecchiature tra i vari Stati membri e nel loro interno.

2. Qualora talune disposizioni possano essere attuate soltanto attraverso l'imposizione di caratteristiche tecniche specifiche, gli Stati membri informano la Commissione in conformità delle procedure di cui alla direttiva del Consiglio 83/189/CEE (10) che prevede una procedura d'informazione nel settore delle norme e delle regolamentazioni tecniche.

3. Se del caso, la Commissione assicura l'elaborazione di norme europee comuni per l'attuazione di caratteristiche tecniche specifiche, in conformità della direttiva .../CEE del Consiglio sul ravvicinamento delle legislazioni degli Stati membri relative alle apparecchiature terminali di telecomunicazione, compreso il mutuo riconoscimento della loro conformità (11), e alla decisione 7/95/CEE del Consiglio del 22 dicembre 1986, relativa alla normalizzazione nel settore delle tecnologie dell'informazione e delle telecomunicazioni (12).

Articolo 19

1. Le disposizioni della presente direttiva relative al servizio telefonico si applicano ad altri servizi pubblici di telecomunicazione digitale nella misura in cui tali servizi presentino rischi analoghi per la vita privata dell'utente.

(10) G.U. L 109, 26.4.1983, p. 8.

(11) G.U. C

(12) G.U. L 36, 07.02.1987, p. 31.

2. La Commissione adotta le misure necessarie per l'attuazione del disposto del paragrafo 1 previa consultazione del comitato di cui all'articolo 22 e in conformità della procedura di cui all'articolo 23.

Articolo 20

Se ed in quanto la piena realizzazione degli obiettivi della presente direttiva esiga l'applicazione delle disposizioni da essa previste a prestatori di servizi diversi dagli enti di telecomunicazione, la Commissione può adottare le misure necessarie per l'applicazione della presente direttiva ai suddetti prestatori previa consultazione del gruppo di cui all'articolo 22, in conformità della procedura di cui all'articolo 23.

Articolo 21

La Commissione stabilisce in conformità della procedura di cui all'articolo 23 le modalità tecniche necessarie per l'applicazione della presente direttiva e le modifiche necessarie per adeguarla al progresso tecnico.

Articolo 22

1. Il Gruppo per la protezione dei dati personali istituito a norma dell'articolo 27 della direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento di dati personali svolge i compiti previsti dall'articolo 28 della direttiva medesima anche per quanto riguarda le misure di protezione dei dati personali che

sono oggetto della presente direttiva.

2. Il gruppo è costituito appositamente ai fini della presente direttiva.

Articolo 23

1. Si applica la procedura definita all'articolo 30 della direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento di dati personali.

2. Il comitato istituito nel quadro della procedura di cui al paragrafo 1 è costituito appositamente ai fini della presente direttiva.

Articolo 24

1. Gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi alla presente direttiva entro il 1° gennaio 1993.

Le disposizioni adottate a norma del primo comma fanno espresso riferimento alla presente direttiva.

2. Gli Stati membri comunicano alla Commissione il testo delle disposizioni di diritto interno che essi adottano nel settore disciplinato dalla presente direttiva.

Articolo 25

Gli Stati membri sono destinatari della presente direttiva.

Fatto a Bruxelles, addì

Per il Consiglio

FICHE FINANCIERE

PROJET DE PROPOSITION DE DIRECTIVE DU CONSEIL CONCERNANT LA PROTECTION DES DONNEES A CARACTERE PERSONNEL ET DE LA VIE PRIVEE DANS LE CONTEXTE DES RESEAUX DE TELECOMMUNICATIONS NUMERIQUES PUBLICS, ET EN PARTICULIER DU RESEAU NUMERIQUE A INTEGRATION DE SERVICES (RNIS) ET DES RESEAUX NUMERIQUES MOBILES PUBLICS.

1. Ligne budgétaire concernée

En 1990 : B 7700

En 1991 et exercices ultérieurs : B5-4010

2. Base légale

Article 100 A

3. Proposition de classification en dépense obligatoire /non obligatoire

non -obligatoire

4. Description et justification de l'action :

4.1. Objectifs : - assurer la protection des personnes à l'égard des données à caractère personnel,

- permettre la circulation transfrontalière de données à caractère personnel dans la Communauté,

- permettre le bon fonctionnement du marché intérieur.

4.2. Réunions spécifiques du groupe de protection des données à caractère personnel (Art 22) et du Comité consultatif (Art 23), créés par la directive, représentant les Etats membres .

4.3. Un représentant de la Commission préside le groupe de protection des données à caractère personnel et le Comité consultatif. Le secrétariat du groupe et du Comité de protection des données à caractère personnel est assuré par les services de la Commission.

5. Nature de la dépense et mode de calcul :

5.1. Nature : réunions

(frais de participation des membres des 2 Comités)

5.2. Calcul : - Groupe de protection des données : (cf. fiche financière de la directive générale)

- Comité consultatif :

24 membres (gouvernementaux) x 3 réunions x 2 jours x 390 ECU/jour =
56.160 ECU *

6. Incidence financière de l'action sur les crédits d'intervention :

6.1. Echancier des crédits d'engagement et de paiement

CE-CP

1993 : 56.160 ECU

1994 : 56.160 "

1995 : 56.160 "

1996 : 56.160 "

1997 : 56.160 - "

6.2. Part du financement communautaire dans le coût total : 100 %

* estimation

7. Observations :

1. Le groupe de protection des données à caractère personnel (Art. 22) :

Il est institué ce groupe à caractère consultatif et indépendant et est composé de représentants de l'autorité de contrôle de tous les Etats membres, présidé par un représentant de la Commission.

Ce groupe établit son règlement intérieur. Le secrétariat du groupe est assuré par les services de la Commission.

Missions de ce groupe : voir Art. 22

2. Le Comité consultatif (Art . 23)

Il est institué un Comité consultatif composé des représentants des Etats Membres, présidé par le représentant de la Commission.

La Commission est assistée par ce Comité afin de prendre les éventuelles mesures complémentaires nécessaires pour adapter les dispositions de la directive aux spécificités de certains secteurs.

Raccomandazione di decisione del Consiglio relativa all'apertura di negoziati in vista dell'adesione delle Comunità europee alla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale

RELAZIONE

1. La protezione delle persone relativamente al trattamento di dati personali costituisce un diritto della persona e una condizione necessaria per lo sviluppo del commercio internazionale.

2. Il trattamento di dati aventi carattere personale è indispensabile all'attuazione degli scambi internazionali di beni e servizi e ad una collaborazione più stretta tra i paesi.

3. La Commissione ha presentato al Consiglio una proposta di direttiva volta ad assicurare nell'insieme della Comunità un elevato livello di protezione delle persone relativamente al trattamento dei dati personali. E' auspicabile che tale azione sia integrata da iniziative intese a garantire alle persone un livello di protezione equivalente negli scambi di dati tra la Comunità ed i paesi terzi.

4. Una Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale è stata conclusa in seno al Consiglio d'Europa nel 1981. L'obiettivo di tale Convenzione è di garantire sul territorio di ciascuna parte contraente ad ogni persona fisica, qualsiasi sia la sua nazionalità o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata nel confronti del trattamento automatizzato dei dati di carattere personale che la riguardano. Tale Convenzione prevede altresì che una parte non possa, ai soli fini della protezione della vita privata, vietare o condizionare ad un'autorizzazione speciale i flussi oltre frontiera di dati di carattere personale destinati al territorio di un'altra parte.

5. Nella sua raccomandazione del 29 luglio 1981, la Commissione ha invitato gli Stati membri a ratificare la Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale, precisando che qualora entro un lasso di tempo ragionevole tutti gli Stati membri non avessero firmato e ratificato tale Convenzione, essa si sarebbe riservata il diritto di proporre al Consiglio di emanare un atto basato sul Trattato CEE.

6. Attualmente, la Convenzione non è ancora stata ratificata da tutti gli Stati membri (1). È auspicabile e necessario che la Comunità aderisca alla Convenzione per assicurare la protezione e la circolazione oltre frontiera di dati di carattere personale con i paesi terzi e per rafforzare l'attrattiva della Convenzione per i paesi terzi che desiderano avere uno scambio di dati possibilmente libero con la Comunità.

7. La Commissione raccomanda pertanto al Consiglio di autorizzare la Commissione a negoziare, con il Consiglio d'Europa e gli Stati che sono

(1) Per quel che concerne gli Stati membri della Comunità, la Convenzione (STE 106 del 26 gennaio 1981) è stata firmata dal Belgio, dalla Grecia, dall'Irlanda, dall'Italia, dal Paesi Bassi e dal Portogallo; tale Convenzione è stata ratificata dalla Danimarca, dalla Francia, dalla RFT, dal Lussemburgo, dalla Spagna e dal Regno Unito.

parte della Convenzione sulla protezione delle persone rispetto al del trattamento automatizzato dei dati di carattere personale, un protocollo addizionale che consenta alle Comunità europee, per i campi di loro competenza, di divenire parte di tale Convenzione.

8. La Commissione condurrà tali negoziati, in consultazione con i rappresentanti degli Stati membri, nel quadro delle Direttive allegate alla presente comunicazione o di quelle che le dovessero eventualmente essere indirizzate dal Consiglio.

9. Gli Stati membri della Comunità, membri del Consiglio d'Europa, appoggeranno in pieno l'azione della Comunità durante tutti i negoziati che devono condurre all'adesione della Comunità europea, ogniqualvolta tale questione sia menzionata negli organi del Consiglio d'Europa.

Allegato: Direttive di negoziato

DIRETTIVE PER I NEGOZIATI

1. I negoziati perseguono l'obiettivo di assicurare la conclusione di un protocollo addizionale che consenta alla Comunità di divenire parte contraente della Convenzione, nei campi che sono di sua competenza, nel rispetto dei principi enumerati in appresso:

2. In seno al Comitato Consultivo, istituito dall'articolo 18 della Convenzione, la Comunità europea sarà rappresentata, in quanto membro, dalla Commissione delle Comunità europee.

In seguito a coordinazione comunitaria, su iniziativa della Commissione, il rappresentante della Comunità europea disporrà di un numero di voti corrispondente alla somma dei voti delle delegazioni nazionali degli Stati membri della Comunità aderenti alla Convenzione, per tutte le questioni riguardanti il trattamento di dati aventi carattere personale nei campi di competenza comunitaria.

Per gli altri argomenti, ogni delegazione nazionale esprime un voto.

3. Al fine di consentire l'entrata in vigore, entro termini ragionevoli del protocollo addizionale che consente alla Comunità di divenire parte contraente della Convenzione, la Commissione proporrà, con l'appoggio degli Stati membri, che sia inserita nel testo del protocollo una disposizione di "notifica negativa" (opting out procedure) per l'adozione del protocollo addizionale.

**PROPOSTA DI DECISIONE DEL CONSIGLIO
NEL SETTORE DELLA
SICUREZZA DEI SISTEMI D' INFORMAZIONE**

Sommario

L'informazione, nei suoi vari aspetti, contribuisce sempre più alla ricchezza delle persone, delle imprese e delle nazioni. Lo sviluppo economico e la formazione di circa due terzi del prodotto nazionale lordo si basano su una produzione industriale o di servizi altamente dipendente dalle tecnologie dell'informazione, dalle telecomunicazioni e dall'audiovisivo e dipendono quindi in modo critico dall'esattezza, dalla sicurezza e dall'attendibilità dell'informazione. Ciò è molto importante ed interessante tanto per gli individui quanto per il commercio, l'industria e le amministrazioni pubbliche. Per questo motivo, la protezione dell'informazione in tutte le sue forme, qui denominata Sicurezza dell'Informazione¹, è diventata una questione politica fondamentale ed di portata mondiale.

Durante gli ultimi decenni sono avvenuti notevoli cambiamenti, ma le future trasformazioni potrebbero essere ancora più importanti. I super calcolatori da tavolo di piccole dimensioni, la radiodiffusione diretta via satellite, le radio mobili digitali, le comunicazioni integrate a banda larga ed altre nuove applicazioni delle tecnologie sono in fase di sviluppo e forniscono mezzi di comunicazione a basso costo, mobili, ad alto livello di prestazione, universali, su scala senza precedenti. L'introduzione di comunicazioni globali efficaci ha ulteriormente accentuato la necessità di fornire una "protezione" adeguata a livello di disponibilità dei servizi, di integrità dei messaggi e di tutela della riservatezza, proporzionata al grado previsto di pericolo di tipo amministrativo o tecnico.

L'argomento è di notevole importanza per lo sviluppo socio-economico della Comunità Europea e per la realizzazione del Mercato Interno del 1992. Affrontare tale questione in maniera consistente a livello europeo dovrebbe creare contemporaneamente un più forte sentimento di fiducia riguardo alle nuove Tecnologie dell'Informazione e delle Telecomunicazioni (TIT), e permettere di evitare la formazione di nuove barriere tecniche fra gli Stati membri o nei confronti dei paesi terzi. E' urgente, perciò, esaminare le esigenze e le scelte possibili in vista di un'azione a livello comunitario in stretta collaborazione con gli attori del settore e con gli Stati membri. Qualsiasi provvedimento deve tenere conto degli sviluppi commerciali, giuridici e tecnici a livello tanto nazionale quanto internazionale. Dato che la sicurezza dell'informazione non comprende solo la protezione delle persone e dei beni, ma anche quella della società stessa, gli Stati membri la considerano questione di competenza della sovranità nazionale.

Allo stesso tempo, è vitale per la Comunità e per i suoi Stati membri che la sicurezza dell'informazione non diventi una limitazione all'incentivazione dello sviluppo armonioso nella Comunità e delle relazioni con i paesi terzi. Lo sviluppo di un approccio armonizzato della sicurezza dell'informazione deve, di per sé, costituire parte integrante delle politiche comunitarie relative al rafforzamento delle prestazioni socio-economiche della Comunità Europea, della competitività internazionale e relative alla realizzazione del Mercato interno.

La questione fondamentale è fornire agli utenti privati, alle amministrazioni e agli ambienti finanziari una sicurezza efficace e pratica dell'informazione, senza compromettere gli interessi del pubblico.

¹ La Sicurezza dei Sistemi d'Informazione (SSI) si occupa della protezione dell'informazione, quando è immagazzinata, trattata o trasmessa elettronicamente, contro gli abusi fortuiti o volontari. I servizi d'informazione elettronica necessitano un'infrastruttura di telecomunicazioni protetta, terminali protetti (inclusi i processori e le basi di dati) e procedure protette.

Un' azione a livello comunitario dovrà implicare alcuni sforzi concertati per stabilire le tecnologie, le norme, le procedure di verifica e di certificazione e le eventuali regolamentazioni necessarie nell' ambito del processo di decisione comunitaria.

L' intento della Commissione è di incoraggiare una discussione con gli attori del settore all'interno della Comunità sui problemi di sicurezza dell' informazione, e di pervenire a un accordo sulle opportune tappe da considerare. Questa discussione potrebbe iniziare in base ad una dichiarazione di principi e alle linee d'azione identificate nell'allegato a questa nota. In questa discussione, a causa delle responsabilità degli Stati membri in questo settore, è assolutamente opportuno che l'iniziativa comunitaria possa avvalersi di una stretta collaborazione con gli alti funzionari degli Stati membri.

Per questi motivi si propone che la Commissione sia assistita da un comitato consultivo, composto da rappresentanti degli Stati membri e presieduto da un rappresentante della Commissione. Il funzionamento di questo comitato dovrebbe rispecchiare le specificità del settore. Questo comitato potrebbe essere denominato "Gruppo di alti funzionari sulla sicurezza dell'informazione" (SOG-IS, Seniors Officials Group on Information Security). Il suo mandato e la sua composizione sono descritti nei paragrafi 37, 38 e 39 del presente comunicato.

La questione importantissima della protezione dei dati a carattere personale è trattata in una proposta di direttiva presentata parallelamente alla presente comunicazione.

A. LE NUOVE PROSPETTIVE E L'IMPORTANZA SOCIALE, ECONOMICA, STRATEGICA E POLITICA DELLA SICUREZZA DEI SISTEMI D'INFORMAZIONE

1. La gestione e l'utilizzazione dell'informazione mediante le tecnologie dell'informazione e dei servizi informatici si sta diffondendo in tutte le sfere della vita economica, sociale e politica. Ciò ha permesso l'integrazione delle attività grazie ad un sistema globale di comunicazione, che collega sia le unità di fabbricazione, gli stabilimenti di ricerca, le basi di dati, i centri di calcolo, gli esercenti di servizi che i centri di decisione politici ed economici.
2. Questa accresciuta integrazione di attività distinte genera un valore aggiunto considerevole in termini di risparmio o di maggiore efficienza ed è ormai un fattore chiave della competitività internazionale. Aumenta però così anche la necessità di proteggere i giusti interessi degli individui, delle masse, dei commercianti, degli industriali, degli operatori, degli esercenti di servizi e delle amministrazioni pubbliche.
3. Al fine di permettere al settore dei servizi di espandersi, e di investire nelle telecomunicazioni, nella radiodiffusione, negli equipaggiamenti di terminali e in una grande varietà di applicazioni telematiche, bisognerebbe offrire uno spazio europeo sicuro per l'informazione gestita elettronicamente. Una vasta accoglienza e l'approvazione di tutte le parti sono importanti per salvaguardare gli interessi legittimi e per impedire il cattivo uso e l'abuso dell'informazione. Ciò deve essere realizzato in modo allo stesso tempo efficace e adeguato per utenti soggetti a sistemi giuridici diversi. Per di più, i sistemi di sicurezza dell'informazione devono tutelare, oltre ad altri interessi, la riservatezza, la proprietà intellettuale, la lealtà della concorrenza e la sicurezza nazionale.
4. Con l'introduzione dei microelaboratori, l'utilizzazione delle tecnologie dell'informazione, delle telecomunicazioni e dell'audiovisivo è andata aldilà del settore professionale ed è diventata una "attività da consumatori" con i corrispondenti "servizi di consumo". Contemporaneamente a questo cambiamento quantitativo, è avvenuto un cambiamento qualitativo molto significativo: le telecomunicazioni permettono ora gli scambi di lavoro e la comunicazione su scala globale.
5. Durante gli ultimi decenni sono avvenuti notevoli cambiamenti, ma le future trasformazioni potrebbero essere ancora più importanti. I super calcolatori da tavolo di piccole dimensioni, la radiodiffusione diretta via satellite, le radio mobili digitali, le comunicazioni integrate a banda larga ed altre nuove applicazioni delle tecnologie sono in fase di sviluppo e forniranno mezzi di comunicazione a basso costo, mobili, ad alto livello di prestazione, universali, su scala senza precedenti.
6. L'introduzione di comunicazioni globali efficaci rappresenta una nuova sfida dai punti di vista qualitativo e quantitativo, con la necessità di fornire una "protezione" adeguata a livello di disponibilità dei servizi, di integrità dei messaggi e di tutela della riservatezza, proporzionata al grado previsto di pericolo di tipo amministrativo o tecnico.
7. Il desiderio crescente dell'industria, dell'amministrazione e della società nel suo insieme di utilizzare i servizi d'informazione ha reso questi ultimi parte integrante della trama della vita quotidiana. Le funzioni di comando, di comunicazione e di controllo in generale, i controlli di processo nell'industria, i trasporti, i servizi finanziari, i sistemi d'automazione d'ufficio, ecc., richiedono livelli di disponibilità e di robustezza operativa non completamente considerati al momento della concezione iniziale del servizio o del componente.
8. Saranno definite e realizzate nuove applicazioni che potranno non essere messe in opera nel quadro architettonico attuale. Potrebbe essere necessaria una ridefinizione fondamentale delle norme di architettura e di prestazione (compresa la necessità di assicurare la conformità) relative ai servizi e ai componenti sottostanti.

9. Dovranno essere create nuove discipline ed organizzazioni / occupazioni di sostegno per soddisfare questi più alti livelli di aspettative operative. Le esigenze più importanti saranno tuttavia determinate da cambiamenti culturali e non tecnologici. Lo sfruttamento globale dei servizi dell'informazione, sostenuti da reti globali di telecomunicazioni, cambierà la percezione dei rapporti organizzativi e umani nella società.
10. La comunicazione si farà sempre più attraverso intermediari, come accade a vari livelli di servizi a valore aggiunto mediante le tecnologie dell'informazione, oppure direttamente dopo che gli intermediari abbiano approvato il contatto. In tali situazioni, la fiducia dovrà essere definita esplicitamente nel contesto delle relazioni d'organizzazione, nelle autorità e nei privilegi e in numerosi "controlli di qualità" sui servizi e sui prodotti. In una tale società, è bene badare a che i diritti degli individui e delle organizzazioni siano dovutamente considerati nella legislazione e nei controlli regolamentari. Parallelamente, le tecnologie dell'informazione e delle telecomunicazioni devono essere concepite e realizzate in modo da soddisfare le esigenze di sicurezza.

B. NECESSITÀ DI UN' AZIONE A LIVELLO COMUNITARIO IN COLLABORAZIONE CON GLI STATI MEMBRI

11. Nella misura in cui sono in gioco la tutela della proprietà, della persona e persino della società nel suo insieme, è chiaro che la sicurezza dell'informazione è di competenza della più alta responsabilità degli Stati membri. La difesa e il funzionamento normale delle istituzioni richiedono agli Stati membri il controllo della loro sicurezza. Queste necessità hanno condotto le amministrazioni nazionali ad acquisire nel corso della storia una competenza solida e duratura nei settori della sicurezza dell'informazione, della sua tecnologia e delle sue tecniche, al fine di impedire la diffusione di informazioni riservate. Benché ogni utente sia responsabile della scelta della propria sicurezza, le sue scelte si basano essenzialmente su garanzie richieste, in fin dei conti, alle autorità pubbliche, per esempio tramite i limiti legali stabiliti.
12. Le politiche ed i programmi della Comunità per lo sviluppo delle industrie dell'informazione e delle telecomunicazioni e per la realizzazione del Mercato interno rischiano di essere gravemente ostacolati se non sarà adottata una politica attiva di creazione, di sviluppo e di promozione di una strategia globale di sicurezza per i servizi di informazione. Per la Comunità, è essenziale che la sicurezza dell'informazione non diventi un ostacolo alla promozione di uno sviluppo armonioso nella Comunità e ai rapporti con i paesi terzi. In quanto tale, lo sviluppo di un approccio armonizzato della sicurezza dell'informazione deve costituire parte integrante delle politiche comunitarie relative al rafforzamento delle prestazioni socio-economiche e della competitività internazionale dell'industria europea e alla realizzazione del Mercato interno.
13. Più precisamente, esso deve implicare sforzi concertati per lo stabilimento delle norme, delle procedure di verifica e di certificazione, degli sviluppi tecnologici e degli eventuali regolamenti necessari nell'ambito del processo di decisione comunitaria. A causa della natura molto tecnica delle questioni in gioco, la concertazione degli sforzi implica una collaborazione degli attori allo stadio della ricerca e sviluppo tecnologico precompetitivi.
14. L'adozione delle Norme per i Sistemi Aperti da parte dei governi (GOSIP negli Stati Uniti e nel Regno Unito), della difesa occidentale (NATO/NOSI), dell'industria dell'informatica e delle telecomunicazioni, oltre a quella da parte dagli esercenti di rete (norme OSI dell'ISO) ha condotto a mettere ancor più l'accento sui problemi di sicurezza nei sistemi d'informazione, nelle architetture, nelle norme, nei protocolli di comunicazione e nelle componenti tecniche relative al settore dell'informazione.

15. Solo un 2% dei servizi che saranno disponibili nell'anno 2000 nella Comunità lo è già attualmente. I servizi saranno allora generalmente in grado di rispondere alle esigenze degli utenti offrendo loro una varietà di caratteristiche integrate che combineranno in modo flessibile la voce, i dati e l'immagine. Correlativamente sarà più difficile soddisfare le esigenze degli utenti in materia di sicurezza dell'informazione, siano essi per la protezione dei dati, la tutela della riservatezza, l'autenticazione, l'autorizzazione, la fatturazione, ecc. E' per questa ragione che la sicurezza dell'informazione e le caratteristiche tecniche che le sono legate, quale l'integrità, devono essere oggetto di sviluppi e di ricerche sistematici. Le autorità statunitensi finanziano programmi sui sistemi informatici affidabili, sulle architetture di sistemi aperti, sui protocolli e le tecniche che accelereranno l'utilizzazione di soluzioni di tutela della proprietà nella comunità internazionale degli utenti. La preoccupazione principale degli Stati membri dovrà avere di porsi come interlocutori in situazione di parità nelle discussioni sulla normalizzazione in questo settore. Seguire una normalizzazione esistente, rischierebbe di creare nuove dipendenze tecnologiche che potrebbero ostacolare seriamente la competitività internazionale delle economie europee. Ciò implica che siano compiuti sforzi corrispondenti nella Comunità come presupposto ad una interazione costruttiva con i paesi terzi, principalmente con gli Stati Uniti.
16. Riassumendo, a causa delle loro responsabilità rispettive, la Comunità e gli Stati membri hanno un grande interesse per le seguenti questioni:
- Come definire e promulgare specifiche e norme efficaci in materia di sicurezza dei sistemi d'informazione?
 - Come realizzare le valutazioni e le certificazioni formali di conformità alle norme di sicurezza dei prodotti e dei sistemi (a livello delle funzionalità e di garanzia)?
 - Come realizzare, fornire ed utilizzare i prodotti e i sistemi di sicurezza dei sistemi d'informazione?
17. La sicurezza dei sistemi d'informazione è un esempio tipico d'applicazione del principio di "sussidiarietà" di fronte all'intrinseca complessità del soggetto, alla presenza di numerosi attori in gioco ed alla necessità di impiegare un ventaglio di strumenti politici diversi. E' essenziale un piano d'azione che definisca cosa deve essere fatto, da chi e come. Da una parte, infatti, gli Stati membri devono trattare queste questioni; dall'altra, per la Comunità è importante trovare una soluzione che permetta la compatibilità fra, da una parte la realizzazione del Mercato interno, quella dell'Europa dei cittadini, la messa in opera di una politica di telecomunicazioni e la competitività delle industrie comunitarie dell'elettronica e, dall'altra, la risposta alle esigenze fondamentali degli individui e dell'economia in materia di sicurezza dei sistemi d'informazione. Di conseguenza, al fine di concentrare gli sforzi, sono presentati qui di seguito vari tipi d'azione ed una struttura procedurale che potranno servire da punto di partenza per futuri studi approfonditi, e per misure da prendere agli opportuni livelli.

PROPOSTA DI DECISIONE DEL CONSIGLIO
NEL SETTORE DELLA
SICUREZZA DEI SISTEMI D'INFORMAZIONE

IL CONSIGLIO DELLE COMUNITA' EUROPEE

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 235,

vista la proposta della Commissione,⁽¹⁾

visto il parere del Parlamento europeo,⁽²⁾

visto il parere del Comitato economico e sociale,⁽³⁾

considerando che la Comunità ha il compito, di promuovere, mediante l'instaurazione di un mercato comune e il graduale ravvicinamento delle politiche economiche degli Stati membri, uno

sviluppo armonioso delle attività economiche nell'insieme della Comunità, un'espansione continua ed equilibrata, una stabilità accresciuta, un miglioramento sempre più rapido di vita e più strette relazioni fra gli Stati membri;

considerando che l'informazione immagazzinata, trattata e trasmessa con l'aiuto di mezzi elettronici acquista un ruolo sempre più importante nell'attività economica e sociale;

considerando che l'introduzione di comunicazioni globali efficaci e dell'impiego generalizzato del trattamento elettronico dell'informazione ha accentuato la necessità di fornire agli utenti un'adeguata tutela;

considerando che il Parlamento europeo ha più volte messo l'accento nei suoi dibattiti e nelle sue decisioni sull'importanza della sicurezza dei sistemi d'informazione;

considerando che il Comitato economico e sociale ha sottolineato l'esigenza di trattare le questioni relative alla sicurezza dei sistemi d'informazione nelle azioni della Comunità, soprattutto in vista degli effetti del completamento Mercato interno;

(1) GU n. C...

(2) GU n. C...

(3) GU n. C...

considerando che è necessario sviluppare una strategia globale di sicurezza dei sistemi d'informazione per garantire la sicurezza degli utenti sul piano comunitario ed evitare la creazione di nuovi ostacoli tecnici agli scambi;

considerando che la complessità inerente alle questioni di sicurezza dell'informazione impone l'applicazione del principio di sussidiarietà, l'adesione di numerosi soggetti settoriali ed il ricorso concertato a varie politiche;

considerando che azioni a livello nazionale, internazionale e comunitario costituiscono una buona base;

considerando che vi è una stretta relazione fra le telecomunicazioni, la normalizzazione, il mercato dell'informazione e le politiche di ricerca e sviluppo tecnologico e delle telecomunicazioni, così come i lavori già intrapresi dalla Comunità in questi settori;

considerando che è opportuno garantire la concertazione degli sforzi basandosi sui lavori già esistenti ai livelli nazionale ed internazionale e promuovendo la cooperazione fra i principali interessati, e che è quindi opportuno procedere nell'ambito di un piano d'azione coerente;

considerando che la responsabilità degli Stati membri in questo settore comporta un'impostazione di concerto su una stretta collaborazione con alti funzionari degli Stati membri.

DECIDE:

Articolo 1

1. E' adottato un piano d'azione nel settore della sicurezza dei sistemi d'informazione della durata di 24 mesi a decorrere dal ...
2. Il piano d'azione ha lo scopo di sviluppare una strategia globale intesa a fornire agli utenti d'informazioni immagazzinate, trattate o trasmesse elettronicamente una protezione dei sistemi d'informazione contro le minacce fortuite o volontarie.
3. Tale azione tiene conto e sostiene le attività di normalizzazione in corso per questo settore su scala europea e mondiale.

Articolo 2

Il piano d'azione di cui all'articolo 1 è descritto in modo particolareggiato in allegato comprende le seguenti linee d'azione:

- I. sviluppo di un quadro strategico per la sicurezza dei sistemi d'informazione;
- II. analisi delle esigenze in materia di sicurezza dei sistemi d'informazione;
- III. elaborazione di soluzioni a certe esigenze prioritarie;
- IV. elaborazione di specifiche, norme e test di convalida in materia di sicurezza dei sistemi d'informazione;
- V. integrazione degli sviluppi tecnologici ed operativi in materia di sicurezza dei sistemi d'informazione in un quadro strategico generale;
- VI. integrazione di alcune funzioni di sicurezza nei sistemi d'informazione.

Articolo 3

La Commissione attua il piano d'azione in collaborazione con gli organismi e le imprese interessate e in stretta associazione con gli Stati membri.

Articolo 4

Gli stanziamenti previsti per questa azione sono determinati annualmente nel quadro della procedura di bilancio.

Articolo 5

La Commissione trasmette al Parlamento europeo ed al Consiglio una relazione sui risultati del piano d'azione nei tre mesi successivi al suo completamento.

Articolo 6

Per l'attuazione del piano d'azione, la Commissione consulta, ove necessario, un gruppo di alti funzionari sulla sicurezza dei sistemi d'informazione (SOGIS). Questo gruppo è costituito da due rappresentanti di ciascuno Stato membro e della Commissione ed è presieduto da un rappresentante della Commissione.

I membri del gruppo possono essere assistiti da esperti o consiglieri in base alla natura dei problemi in esame.

Le deliberazioni del gruppo sono riservate. Il gruppo adotta il proprio regolamento interno. Il segretariato del gruppo provvede i servizi della Commissione.

Fatto a Bruxelles, addì

Per il Consiglio

ALLEGATO 1

SOMMARIO DELLE LINEE D'AZIONE

1. PRIMA LINEA D'AZIONE: SVILUPPO DI UN QUADRO STRATEGICO PER LA SICUREZZA DEI SISTEMI D'INFORMAZIONE

1.1 Problematica

1. Si ritiene che una buona sicurezza dei sistemi d'informazione sia un requisito generalmente necessario in una società moderna. I servizi d'informazione elettronica richiedono infrastrutture di telecomunicazioni sicure, terminali affidabili (compresi i processori e le basi di dati) e condizioni d'utilizzazione sicure. Deve essere stabilita una strategia globale, che tenga conto di tutti gli aspetti della sicurezza dei sistemi d'informazione, evitando di affrontare tale questione in modo frammentario. Ogni strategia per la sicurezza dell'informazione trattata elettronicamente deve tener conto del bisogno di ogni società di potere agire efficacemente, pur proteggendosi, in un mondo in rapida trasformazione.

1.2 Obiettivo

2. E' necessario creare un quadro strategico per trovare un accordo fra gli obiettivi sociali, economici e politici e le scelte tecniche, operative e giuridiche. Il delicato equilibrio fra le varie preoccupazioni, gli obiettivi e le limitazioni deve essere trovato dai responsabili del settore che collaborano per sviluppare un'impostazione comune ed una strategia convenuta. Tali sono i presupposti per conciliare gli interessi e le esigenze dell'azione politica e dello sviluppo industriale.

1.3 Situazione e tendenze

3. La situazione è caratterizzata da una crescente presa di coscienza della necessità di agire. Tuttavia, in assenza di un'iniziativa per coordinare gli sforzi, le energie disperse in molti settori potrebbero creare una situazione "de facto" contraddittoria, ponendo progressivamente problemi giuridici, sociali ed economici sempre più seri.

1.4 Esigenze, scelte e priorità

4. In questo quadro si dovrà prendere in esame l'analisi e la gestione del rischio per quanto concerne la vulnerabilità dei sistemi d'informazione e dei servizi corrispondenti, l'armonizzazione delle leggi e dei regolamenti relativi al cattivo uso e all'abuso dell'informatica e delle telecomunicazioni, le infrastrutture amministrative, comprese le politiche di sicurezza e le modalità di attuazione di tali politiche da parte delle varie industrie e discipline e, infine, le preoccupazioni sociali e di tutela della riservatezza (per esempio l'applicazione dell'identificazione, dell'autenticazione e degli eventuali schemi d'autorizzazione in un ambiente democratico).
5. Dovrà essere fornito un chiaro orientamento affinché vengano sviluppate architetture fisiche e logiche per quanto concerne i servizi d'informazione distribuiti sicuri, norme, linee direttrici e definizioni in merito a prodotti, servizi, progetti pilota e prototipi garantiti sicuri, onde stabilire il grado di efficienza delle varie strutture amministrative, delle architetture e delle norme relative alle esigenze di settori specifici.

6. Dovrà essere incoraggiata una presa di coscienza dei problemi di sicurezza in modo da sensibilizzare gli utenti a questa problematica.

2. SECONDA LINEA D'AZIONE: ANALISI DELLE ESIGENZE IN MATERIA DI SICUREZZA DEI SISTEMI D'INFORMAZIONE

2.1 Problematica

7. La sicurezza dell'informazione è una condizione indispensabile alla tutela della riservatezza, della proprietà intellettuale, del segreto commerciale e della sicurezza nazionale. Questo pone il problema dell'equilibrio delicato - e talvolta delle scelte da fare - fra il sostegno alla libertà di commercio e la tutela della riservatezza e della proprietà intellettuale. Scelte e compromessi devono farsi in base a una valutazione globale delle esigenze e delle conseguenze delle possibili opzioni adottate in materia di sicurezza dell'informazione.
8. Le esigenze degli utenti implicano funzionalità di sicurezza dell'informazione legate ad aspetti tecnologici, operazionali e regolamentari. Un lavoro di ricerca sistematica sulle esigenze di sicurezza dei sistemi d'informazione costituisce, pertanto, una condizione indispensabile per lo sviluppo di misure adeguate ed efficaci.

2.2 Obiettivo

9. Occorre stabilire la natura e le caratteristiche delle esigenze degli utenti e i loro rapporti con le misure in materia di sicurezza dei sistemi d'informazione.

2.3 Situazione e tendenze

10. Fino ad ora, nessuno sforzo concertato è stato intrapreso per stabilire le esigenze in rapida evoluzione e trasformazione dei più importanti interessati in materia di sicurezza dei sistemi d'informazione. Alcuni Stati membri della Comunità hanno individuato le esigenze d'armonizzazione delle attività nazionali (specialmente i "criteri di sicurezza delle tecnologie d'informazione"). Criteri di valutazione uniformi e Regole per il riconoscimento reciproco dei risultati e delle certificazioni di valutazione sono della massima importanza.

2.4 Esigenze, scelte e priorità

11. Come base per un'analisi approfondita e trasparente delle giuste esigenze degli attori del settore, sembra necessario sviluppare una classificazione comunemente accettata delle esigenze degli utenti e del loro rapporto con le misure in materia di sicurezza dei sistemi d'informazione.
12. E' importante anche stabilire le esigenze in materia di legislazione, di regolamentazione e di codici di comportamento alla luce di una valutazione delle tendenze, delle caratteristiche e della tecnologia dei servizi. Ciò al fine di sviluppare delle strategie alternative che permettano di raggiungere gli obiettivi attraverso disposizioni amministrative, di servizio, operative e tecniche, ed anche per valutare l'efficacia, la "user-friendliness" e i costi delle varie opzioni in materia di sicurezza dei sistemi d'informazione e delle strategie, per gli utenti, per gli esercenti di servizi e per gli operatori.

3. TERZA LINEA D'AZIONE: RICERCA DI SOLUZIONI AD ALCUNE ESIGENZE PRIORITARIE.

3.1 Problematica

13. E' attualmente possibile impedire efficacemente l'accesso non autorizzato agli elaboratori con misure d'isolamento prestabilite da un punto di vista organizzativo e fisico. Lo stesso vale per le comunicazioni all'interno di un gruppo chiuso di utenti operanti su una rete privata. La situazione è molto diversa quando l'informazione è ripartita fra vari gruppi di utenti o scambiata attraverso una rete pubblica o di accesso generale. In questi casi né la tecnologia, i terminali e i servizi da un lato, né le norme e le procedure associate dall'altro, sono generalmente in grado di garantire un livello analogo di sicurezza dell'informazione.

3.2 Obiettivo

14. A breve scadenza, l'obiettivo è di fornire soluzioni che possano rispondere alle esigenze più immediate degli utenti e aperte alle necessità e alle soluzioni future.

3.3 Situazione e tendenze

15. Alcuni gruppi di utenti hanno sviluppato tecniche e procedure per il loro uso specifico, rispondenti in particolare alle esigenze di autenticazione, di integrità e di non rifiuto (non-repudiation). Di solito vengono utilizzate carte magnetiche, carte con memoria o con processore o, talvolta, tecniche più o meno sofisticate di crittografia. Spesso ciò ha portato alla definizione di "autorità" specifiche nei gruppi di utenti. E' comunque difficile generalizzare queste tecniche e metodi in ambiente aperto.
16. L'ISO sta svolgendo lavori sulla sicurezza OSI dell'informazione (ISO DIS 7468-2), così come il CCITT nel contesto dell'X400. E' anche possibile inserire segmenti di sicurezza dell'informazione nei messaggi. L'autenticazione, l'integrità e il non rifiuto (non-repudiation) sono trattati come parti dei messaggi EDIFACT e di X 400 MHS.
17. Attualmente, il quadro giuridico degli scambi di dati (EDI) è ancora in fase di elaborazione. La Camera di commercio internazionale ha pubblicato alcune regole di condotta uniformi per lo scambio dei dati commerciali attraverso le reti di telecomunicazioni. In questo codice di comportamento noto sotto il nome di UNCID si precisano le procedure di base da seguire per gli utenti di EDI. Esso può essere considerato una buona base di riferimento.
18. Vari paesi (per esempio RF di Germania, Francia, Regno Unito e USA) hanno sviluppato o sviluppano criteri per valutare l'affidabilità dei prodotti e dei sistemi di TIT e le corrispondenti procedure per svolgere delle valutazioni. Questi criteri sono stati coordinati con i fabbricanti nazionali e condurranno ad una vasta gamma di prodotti e di sistemi affidabili. La creazione di organizzazioni nazionali incaricate di condurre le valutazioni e di concedere le certificazioni sosterrà questa iniziativa.
19. Le disposizioni in materia di riservatezza sono considerate meno importanti dalla maggior parte degli utenti. In avvenire, tuttavia, è probabile che la loro posizione cambi in seguito alla diffusione dei servizi di comunicazione avanzati e, soprattutto, mobili.

3.4 Esigenze, scelte e priorità

20. E' essenziale mettere a punto al più presto le procedure, le norme, i prodotti e gli strumenti atti a garantire la sicurezza degli elaboratori, dei terminali e delle reti pubbliche di comunicazione. La precedenza dovrebbe essere data a progetti pilota di autenticazione, di integrità e di non rifiuto (non-repudiation) realizzati per stabilire la validità delle soluzioni proposte. Le soluzioni concernenti alcune esigenze prioritarie quali quelli concernenti l'EDI saranno raggiunte nell'ambito del programma TEDIS e nell'ambito più vasto del presente programma d'azione.

4. QUARTA LINEA D'AZIONE: ELABORAZIONE DELLE SPECIFICHE, DELLE NORME E DEI TEST DI CONVALIDA IN MATERIA DI SICUREZZA DEI SISTEMI D'INFORMAZIONE.

4.1 Problematica

21. Le esigenze di sicurezza nel settore dell'informazione sono generali e per questo motivo l'esistenza di specifiche e di norme comuni è di fondamentale importanza. La loro assenza potrebbe costituire un handicap importante per il progresso delle procedure e dei servizi basati sull'informazione nell'economia e nella società. Alcune azioni dovrebbero accelerare lo sviluppo e l'utilizzazione di tecnologie e di norme in numerosi settori della comunicazione oltre a quello delle reti informatizzate di importanza cruciale per gli utenti, l'industria e le amministrazioni.

4.2 Obiettivo

22. E' necessario un impegno considerevole per fornire i mezzi di sostenere e realizzare funzioni specifiche nei settori generali dell'OSI, l'ONP, l'ISDN/IBC, gestione e sicurezza di reti per l'informazione riservata ma non segreta. Le tecniche e le concezioni in materia di controllo sono legati alla normalizzazione ed alla determinazione di specifiche.

4.3 Situazione e tendenze

23. Gli Stati Uniti, in particolare, hanno lanciato importanti iniziative per trattare la questione della sicurezza dell'informazione in campo civile. In Europa, questo argomento rientra nel contesto della normalizzazione delle TTT nel quadro dell'ETSI e del CEN/CENELEC, in preparazione al lavoro del CCITT e dell'ISO.
24. Viste le crescenti preoccupazioni, l'attività negli USA è stata rapidamente intensificata e tanto i venditori quanto gli esercenti di servizi hanno accresciuto i loro sforzi in questo settore. In Europa, in Francia, nella RF di Germania e nel Regno Unito hanno cominciato, indipendentemente, attività simili, ma uno sforzo comune corrispondente a quello americano si sta sviluppando solo lentamente.

4.4 Esigenze, scelte e priorità

25. Nel settore della sicurezza dei sistemi d'informazione, esiste una relazione molto stretta fra gli aspetti regolamentari, operativi, amministrativi e tecnici. Le regolamentazioni devono riflettersi nelle norme e i provvedimenti in materia di sicurezza dei sistemi d'informazione devono conformarsi alle norme e alle regolamentazioni. Sotto numerosi aspetti le regolamentazioni richiedono specifiche che vadano al di là dell'obiettivo convenzionale della normalizzazione, cioè che includano codici di pratica. Esigenze in materia di norme e di codici di pratica si trovano in tutti i settori della sicurezza dei sistemi d'informazione ed una distinzione deve essere fatta fra le esigenze di protezione corrispondenti agli obiettivi di sicurezza e le esigenze tecniche che possono essere affidate agli organismi europei competenti nel settore della normalizzazione (CEN/CENELEC/ETSI).
26. Le specifiche e le norme devono coprire i campi dei servizi di sicurezza dei sistemi d'informazione (autenticazione delle persone e delle società, protocolli di non rifiuto (non-repudiation) prova elettronica giuridicamente valida, controllo d'autorizzazione), i servizi di comunicazione (riservatezza riguardo alla comunicazione dell'immagine, della voce e dei dati, protezione dei dati e delle banche di immagini, sicurezza dei servizi integrati), la gestione della comunicazione e della sicurezza (sistemi di chiavi pubbliche/private per l'esercizio delle reti aperte, protezione della gestione delle reti, protezione degli esercenti di servizi) e la certificazione (criteri e livelli di garanzia della sicurezza dei sistemi d'informazione, procedure di garanzia della sicurezza).

5. QUINTA LINEA D'AZIONE: INTEGRAZIONE DEGLI SVILUPPI TECNOLOGICI ED OPERATIVI IN MATERIA DI SICUREZZA DEI SISTEMI D'INFORMAZIONE IN UN QUADRO STRATEGICO GENERALE.

5.1 Problematica

27. Un lavoro di ricerca sistematica ed uno sviluppo tecnologico che permetta di trovare delle risposte economicamente redditizie ed operativamente soddisfacenti per una serie di esigenze presenti e future in materia di sicurezza dell'informazione, sono le condizioni necessarie allo sviluppo del mercato dei servizi e alla competitività dell'insieme dell'economia europea.
28. Ogni sviluppo tecnologico in materia di sicurezza dei sistemi d'informazione dovrà comprendere allo stesso tempo gli aspetti della sicurezza informatica e della sicurezza delle comunicazioni dato che la maggior parte dei sistemi attuali sono sistemi distribuiti il cui accesso è realizzato attraverso servizi di comunicazione.

5.2 Obiettivo

29. Un lavoro di ricerca sistematica ed uno sviluppo tecnologico che consenta di trovare risposte economicamente accettabili e soddisfacenti da un punto di vista operativo ad una serie di esigenze presenti e future in materia di sicurezza dei sistemi d'informazione.

5.3 Esigenze, scelte e priorità

30. Il lavoro in materia di sicurezza dei sistemi d'informazione dovrebbe concernere le strategie di sviluppo e di realizzazione, le tecnologie e la loro integrazione e verifica.
31. Il lavoro strategico di ricerca e sviluppo tecnologico dovrebbe coprire modelli concettuali di sistemi per quanto possibile sicuri, modelli di esigenze funzionali, modelli di rischio e architetture per la sicurezza.
32. Il lavoro di ricerca e sviluppo tecnologico dovrebbe includere l'autenticazione dell'utente e del messaggio (per esempio grazie all'analisi della voce o alle firme elettroniche), le interfacce tecniche e i protocolli per il cifraggio, i meccanismi di controllo d'accesso ed i metodi di messa in opera per sistemi garantiti sicuri.
33. La ricerca dovrebbe anche vertere sulla verifica e la convalida della sicurezza tecnica dei sistemi e della sua applicabilità attraverso progetti d'integrazione e verifica.
34. Oltre al consolidamento e allo sviluppo della tecnologia della sicurezza, sono necessarie numerose misure d'accompagnamento in materia di creazione, mantenimento ed applicazione coerente delle norme, di convalida e di certificazione dei prodotti TIT relativamente alle loro proprietà in materia di sicurezza, comprese la convalida e la certificazione dei metodi di progettazione e di realizzazione dei sistemi.
35. Il terzo programma quadro comunitario per la ricerca e lo sviluppo tecnologico potrà essere utilizzato per promuovere progetti di cooperazione a livello pre-concorrenziale e prenormativo.

6. SESTA LINEA D'AZIONE: L'INTEGRAZIONE DI ALCUNE FUNZIONI DI SICUREZZA NEI SISTEMI D'INFORMAZIONE.

6.1 Problematica

36. Vista la natura esatta degli aspetti della sicurezza dei sistemi d'informazione, adeguate funzionalità dovranno essere installate in vari settori dei sistemi di comunicazione (terminali / elaboratori, servizi, gestione della comunicazione fino ai dispositivi crittografici, alle carte con memoria o con processore, alla gestione delle chiavi pubbliche e private, eccetera. Ci si può aspettare che alcune di queste funzionalità siano incorporate negli elaboratori o nei software forniti dai venditori, mentre altre potranno sia far parte di sistemi distribuiti (per esempio, gestione della comunicazione), sia appartenere a utenti individuali (per esempio carte con memoria o con processore) sia, infine essere fornite da un organismo specializzato (per esempio chiavi pubbliche e private).
37. La maggior parte dei prodotti e dei servizi in materia di sicurezza dei sistemi d'informazione saranno probabilmente forniti da venditori, esercenti di servizi o operatori. Per alcune funzioni specifiche, come per esempio la fornitura di chiavi pubbliche e private, l'audit o il controllo d'accesso, potrà essere necessario far ricorso ad organismi appropriati fornendo loro un mandato.
38. Lo stesso dicasi per la certificazione dei prodotti rispetto alle norme, la valutazione e la verifica della qualità del servizio, che sono funzioni da affidare ad organismi indipendenti dagli interessi dei venditori, degli esercenti di servizi o degli operatori. Tali organismi potrebbero essere privati, pubblici, o incaricati dallo stato per svolgere queste funzioni attraverso una delega.

6.2 Obiettivo

39. Per facilitare uno sviluppo armonioso della messa in opera della sicurezza dell'informazione nella Comunità tutelando sia i privati cittadini sia gli interessi commerciali, sarà necessario affrontare in modo approfondito tale problema. Qualora vengano incaricati organismi indipendenti, le loro funzioni e le condizioni di funzionamento dovranno essere definite e, se necessario, incluse nel quadro regolamentare. L'obiettivo sarebbe di arrivare ad una ripartizione definita e convenuta delle responsabilità fra vari interessati a livello comunitario, come presupposto al reciproco riconoscimento.

6.3 Situazione e tendenze

40. Attualmente, le disposizioni in materia di sicurezza dei sistemi d'informazione sono bene organizzate solo per campi specifici, e rispondono solo a precise esigenze. L'organizzazione a livello europeo è spesso informale e il reciproco riconoscimento della verifica e della certificazione non avviene al di fuori di alcuni gruppi ristretti. L'importanza sempre maggiore della sicurezza dei sistemi d'informazione rende urgente la definizione di un'esatta concezione delle disposizioni in questo settore in Europa e a livello internazionale.

6.4 Esigenze, scelte e priorità

41. Visto il numero degli interessati e in considerazione delle strette relazioni esistenti fra questioni regolamentari e legislative, è particolarmente importante trovare un accordo preliminare sui principi che governano le disposizioni in materia di sicurezza dei sistemi d'informazione.

Per affrontare questa tematica in modo realistico, si dovranno trattare gli aspetti di identificazione e specifica delle funzioni che, per la loro stessa natura, implicano che sia dato un ruolo ad un organismo indipendente (o ad organismi che lavorano congiuntamente). Ciò potrebbe concernere funzioni quali l'amministrazione dei sistemi di chiavi pubbliche e private.

E' inoltre opportuno identificare e specificare abbastanza rapidamente le funzioni che devono essere affidate ad un organismo indipendente (o a organismi che collaborino tra di loro) per motivi di interesse pubblico. Ciò potrebbe comprendere l'audit, la garanzia della qualità, la verifica, la certificazione ed altre funzioni analoghe.

FINANCIAL STATEMENT

Information Security (INFOSEC) Preparatory Action

BUDGET HEADING

Subsection B6, Item 8104

2. LEGAL BASE AND PROPOSED CLASSIFICATION

Article [235]

Non compulsory expenditure.

3. DESCRIPTION

Collaboration in the development of proposals and actions relating to information security as far as they require or significantly benefit from a concerted approach at Community level. The focus of the work is to relate to the needs of the general public, commerce, service providers and administrations and addresses the requirements for a collaborating approach to technological research, standardisation and related issues as relevant for the development of a consistent European approach to information security with particular reference to the completion of the internal market in 1992.

The goal of the INFOSEC action is to make a major contribution to the objective of the

"development of actions to providing effective and practical security for information held in an electronic form to the general users, administrations and business community without compromising the interest of the public at large."

The present proposal is the result of the preliminary investigations by experts, consultations and on-going related work.

The scope of the preparatory action is to focus on

- I. development of an information security strategy framework
- II. information security requirements
- III. solutions for immediate and interim needs
- IV. specifications, standardisation and verification of information security
- V. technological and operational developments for information security
- VI. information security provision.

4. JUSTIFICATION

Development of a harmonised approach to information security must form an integral part of the Community policies related to the completion of the Internal Market, strengthening of socio-economic performance and international competitiveness. It is vital that Information Security does not become a constraint to the promotion of harmonious development in the Community and to relations with other countries. In addition, information security systems must protect privacy, intellectual property, fair competition, national security and other interests.

The proposed action responds to an urgent need to facilitate and accelerate the emergence of generally accepted, effective and practicable measures in information security. The action will benefit from synergies with on-going programmes in the field of information technologies (ESPRIT) and telecommunications (RACE) as well as the on-going work on telecommunications, standardisation and information market policies.

5. INDICATIVE FINANCIAL PLANNING

5.0 Implications for expenditure.

5.0.0 Total cost over the whole of the expected duration of 2 years (in MioECU)

From the Budget of the Communities:	12.0
From the other sectors at the national level:	0.0
TOTAL	12.0

5.0.1 Multi-annual schedule (in MioECU):

	Commitment Appropriations	Payment Appropriations
1991	6	4
1992	6	6
1993	-	2
	12	12

5.0.2 Method of calculation

a) Expenditure by contract

This expenditure covers the Community's financial contribution to analytical work as required to support the development of specific actions proposed, the consultation and establishment of consensus.

b) Operational expenditure

Given the fact that the action is financed in Subsection 6 of the budget devoted to Research and investment expenditure, administrative costs (Committee and working party meetings, consultation of experts, missions, document distribution or dissemination of techniques, use of data processing, telecommunication and broadcasting equipment) are covered directly by the budget item.

The following table gives the indicative breakdown over the various categories of expenditure (in MioECU):

		1991	1992
5.0.2	a)	4,823	4,100
5.0.2	b)	in total 1,177	1,900
of which	Experts	0,400	0,600
	Other operational expenditure	0,500	0,725
	Infrastructure	0,050	0,100
	Information and publication	0,050	0,100
	Statutory staff	0,177	0,375

6. FINANCIAL IMPLICATIONS FOR STAFF AND CURRENT ADMINISTRATIVE APPROPRIATIONS

The statutory research staff involved, i.e. 3 A, 1 B, 1 C, will be entered in the research staff table and is paid out of the appropriations entered onto Item B6-8104.

The administrative expenditure will be governed by the internal rules on mini-budgets decided by the Commission on 22 May 1990.

FINANCING OF EXPENDITURE

The appropriations to cover the Community's contribution to this project will be determined in the context of the annual budgetary procedure.

IMPLICATIONS FOR REVENUE

Contribution of the statutory research staff to the retirement scheme and the sickness insurance.

9. TYPE OF CONTROL

- Administrative control by the Director General for Financial Control as regards budget implementation;
- Control of achievement:
 - . SOG-IS
 - . control by officials of the Commission
 - . audit by the Court of Auditors in accordance with provisions of the Treaty;
- In accordance with Article 2 of the Financial Regulations, the use of appropriations will be subject to analyses of cost-effectiveness and the realisation of quantified objectives will be monitored.