gnia aerea (articolo 26, paragrafo 1, lettera *b)*. Tuttavia, la conservazione dei dati (compresi i dati riservati sulla salute dell'individuo) nella base di dati della compagnia aerea non può essere giustificata in base a questi motivi. Il trasferimento dei dati alla compagnia aerea deve quindi essere giustificato da una diversa deroga.

Come nel caso (1), la soluzione migliore è il consenso dell'interessato, che potrebbe essere ottenuto dall'agenzia di viaggi di Lisbona per conto della compagnia aerea. L'interessato va informato dei rischi derivanti dal fatto che i dati saranno conservati nel paese B, nonché del fatto che il trasferimento e la conservazione dei dati nella base di dati della compagnia aerea non sono necessari per ragioni riguardanti il volo prenotato.

CASO (3): IL TRASFERIMENTO DI DATI DI ELENCHI COMMERCIALI

Una società dei Paesi Bassi è specializzata nella creazione di «mailing lists». Utilizzando varie fonti di informazione pubblica disponibili nei Paesi Bassi e liste di clienti noleggiate da altre società olandesi, compila elenchi di persone che corrispondono a un particolare profilo socioeconomico. Questi elenchi sono poi venduti dalla società olandese a clienti nei Paesi Bassi e nell'Ue, nonché in numerosi altri paesi terzi. Le società acquirenti utilizzano gli elenchi (che comprendono indirizzi postali, numeri di telefono e spesso indirizzi di posta elettronica) per contattare le persone e proporre loro l'acquisto di una vastissima gamma di prodotti e servizi. Numerose persone che figurano su questi elenchi hanno sporto reclamo presso le autorità olandesi di tutela dei dati a causa delle proposte commerciali che hanno ricevuto.

Le norme applicabili pertinenti

Alcune delle società che hanno acquistato le «mailing lists» offerte dalla società olandese hanno sede in paesi con leggi generali sulla tutela dei dati che prevedono il diritto di rifiutare queste proposte commerciali. Altre sono situate in paesi privi di tali leggi, ma sono membri di associazioni autoregolamentate che hanno introdotto codici di protezione dei dati. Altre ancora non sono soggette ad alcuna norma sulla tutela dei dati.

Valutazione del contenuto delle norme applicabili

Questo caso specifico richiede la valutazione di una serie di leggi e di codici diversi. Se la società con sede nei Paesi Bassi continua questo tipo di vendita e di noleggio di liste a società in vari paesi del mondo, si verificheranno inevitabilmente situazioni in cui il livello di tutela non è adeguato.

FASE 2: RICERCA DI UNA SOLUZIONE

In questo caso, poiché i dati sono raccolti da fonti pubbliche e senza un contatto diretto con gli interessati, sarebbe molto problematico per la società situata nei Paesi Bassi chiedere il consenso di ogni persona alla sua inclusione nelle «mailing lists». È quindi improbabile che possa essere applicata una delle deroghe previste dall'articolo 26, paragrafo 1.

La società olandese ha due possibilità, che può utilizzare alternativamente oppure insieme. La prima è quella di limitare il suo commercio di mailing list a società soggette a giurisdizioni che garantiscono una tutela adeguata mediante

leggi o strumenti efficaci di autodisciplina. In questa sua decisione la società potrebbe essere guidata da una qualsiasi «lista bianca». La seconda possibilità sarebbe quella di chiedere un impegno contrattuale a tutte le società acquirenti (o almeno a quelle soggette a giurisdizioni «non adeguate») circa la tutela dei dati trasferiti. Questi accordi contrattuali dovrebbero seguire le indicazioni contenute nel capitolo 4 del presente documento. In virtù di tali accordi, in particolare, la società olandese dovrebbe rimanere responsabile, secondo la legislazione nazionale, di ogni violazione dei principi di tutela dei dati risultante da azioni della società cliente a cui sono state trasferite le «mailing lists».

Una tale soluzione contrattuale, se applicata in modo appropriato, contribuirebbe a superare gli ostacoli al commercio creati dalla mancanza in vari paesi terzi di una tutela adeguata dei dati.

Fatto a Bruxelles, il 24 luglio 1998

Per il gruppo di lavoro
Il presidente P.J. HUSTINX

5.7.6 Documento di lavoro sulla procedura relativa alla valutazione dei codici di condotta comunitari

COMMISSIONE EUROPEA
DIREZIONE GENERALE XV
Mercato interno e servizi finanziari
Libera circolazione delle informazioni, diritto delle società ed informazioni finanziarie
Libera circolazione delle informazioni, protezione dei dati e relativi aspetti internazionali

DG XV D/5004/98
WP 13

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

Attività futura riguardante i codici di condotta: Documento di lavoro sulla procedura relativa alla valutazione dei codici di condotta comunitari

Adottato il 10 settembre 1998

INTRODUZIONE

Il gruppo intende definire la procedura per la presentazione dei codici di condotta da parte degli interessati e per la loro valutazione ai sensi degli articoli 27 e 29 della direttiva 95/46/CE.

Nel presente documento vengono riepilogate le principali fasi della procedura e vengono definite norme specifiche per ciascuna di esse. Tali norme potranno essere riviste alla luce dell'esperienza acquisita nella loro futura applicazione.

PRINCIPALI FASI DELLA PROCEDURA

La procedura per la valutazione dell'ammissibilità e del merito dei codici di condotta si articola nelle seguenti fasi:

I) Presentazione e ammissione;
II) Elaborazione del parere del gruppo;
III) Adozione del parere del gruppo e comunicazione agli interessati.

Art. 1 - *Norme generali*

Ai fini delle presenti norme si intende per:

1.1 «direttive»: la direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, e la direttiva 97/66/CE del Parlamento Europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni;

1.2 «gruppo di tutela»: il gruppo per la tutela della persone con riguardo al trattamento dei dati personali, di cui all'articolo 29 della direttiva 95/46/CE;

1.3 «Codice di condotta»: qualsiasi codice di condotta ai sensi dell'articolo 27, § 3, della direttiva 95/46/CE nonché qualsiasi modifica e proroga di codici comunitari previgenti.

Art. 2 - *Norme riguardanti la presentazione e l'ammissione dei codici per l'esame svolto dal gruppo tutelare*

2.1 I progetti di codice di condotta possono essere sottoposti all'esame del gruppo tutelare da qualsiasi organizzazione rappresentativa di un determinato settore, che abbia sede od operi in un numero significativo di Stati membri.

2.2 I progetti devono essere preparati in modo accurato, preferibilmente in consultazione con le persone interessate o con i loro rappresentanti, e devono indicare chiaramente l'organizzazione o il settore cui sono destinati.

2.3 I progetti di codice devono essere inviati al presidente del gruppo di tutela - tramite il segretariato (Commissione europea, DG XV-D1) - in una lingua comunitaria e con la traduzione in lingua francese o inglese; essi devono inoltre essere corredati da una relazione illustrativa.

2.4 I progetti prematuri o comunque non conformi ai criteri sopra indicati (ai punti 1 e 2) non sono ammessi all'esame del gruppo tutelare.

2.5 Il segretariato rilascia un avviso di ricevimento all'organizzazione che ha presentato il progetto.

2.6 Previa consultazione del presidente, il segretariato redige una relazione sulla rispondenza del progetto ai criteri di ammissibilità indicati nei punti 2.1- 2.3.

2.7 Il presidente determina se il progetto risponde ai criteri di ammissibilità. Qualora constati che il progetto non risponde a tali criteri, egli informa i membri del gruppo di tutela assegnando loro un termine per la comunicazione di eventuali osservazioni. Salvo che due o più membri chiedano che la questione sia dibattuta nella successiva riunione del gruppo di tutela, la decisione del presidente viene notificata, insieme alla motivazione della valutazione negativa, all'organizzazione che ha presentato il progetto.

Art. 3 - *Norme sull'elaborazione del parere del gruppo di tutela*

3.1 I progetti di codice rispondenti ai criteri di ammissibilità sono trasmessi a tutti i membri del gruppo di tutela.

3.2 Sentito il presidente, il segretariato redige proposte per l'elaborazione del parere che saranno successivamente discusse dal gruppo di tutela. Tali proposte:

– possono prevedere l'istituzione di gruppi di lavoro o unità operative *ad hoc*, composti da uno o più membri del gruppo di tutela e coadiuvati dal segretariato,

– possono prevedere una procedura semplificata per l'esame di un determinato codice, segnatamente nell'ipotesi di modifica o proroga di un codice previgente, e

– consigliano il gruppo di tutela sul se e sul come raccogliere le osservazioni delle persone interessate, dei loro rappresentanti o di altri soggetti.

3.3 Nel dibattito preliminare relativo al codice sottopostogli, il gruppo di tutela definisce, in base alle proposte di cui all'articolo 3, punto 3.2, la procedura da seguire per l'adozione e l'elaborazione del parere.

3.4 Nell'ambito dell'elaborazione del parere possono tenersi consultazioni con l'organizzazione che ha presentato il progetto nonché con gli altri interessati, onde ottenere informazioni o chiarimenti ulteriori e discutere sui necessari miglioramenti da apportare al codice in vista della presentazione di un progetto modificato.

3.5 Il gruppo di tutela può stabilire ulteriori orientamenti o istruzioni per l'elaborazione del parere relativo al codice sottopostogli.

Art. 4 - *Norme riguardanti l'adozione del parere del gruppo di tutela e la sua comunicazione agli interessati*

4.1 Il gruppo di tutela determina se il codice di condotta sottopostogli:

– è conforme alle direttive sulla tutela dei dati e, se del caso, alle disposizioni nazionali emanate per la loro attuazione;

– possiede un livello qualitativo ed una coerenza interna sufficienti e fornisce un apporto sufficiente alla disciplina stabilita dalle direttive e dagli altri provvedimenti legislativi sulla tutela dei dati, verificando in particolare se esso sia sufficientemente incentrato sulle questioni e sui problemi specifici dell'organizzazione e del settore cui è destinato e se offra soluzioni sufficientemente chiare per tali questioni o problemi.

4.2 Il gruppo di tutela comunica il parere sia all'organizzazione che ha presentato il progetto sia agli altri interessati. I pareri sfavorevoli devono contenere la motivazione della valutazione negativa.

4.3 La Commissione può dare adeguata pubblicità al parere emesso dal gruppo di tutela.

Fatto a Bruxelles, il 10 settembre 1998

Per il gruppo di tutela
Il Presidente P.J. HUSTINX

5.7.7 Parere 1/99 - Il livello di protezione dei dati negli Stati Uniti e il dibattito in corso

5092/98/EN/final
WP15

Gruppo di lavoro sulla protezione delle persone
rispetto al trattamento di dati personali

Parere 1/99: Il livello di protezione dei dati negli Stati Uniti e il dibattito in corso fra la Commissione europea e il Governo degli Stati Uniti

Adottato dal Gruppo di lavoro il 26 gennaio 1999

Il Gruppo di lavoro è a conoscenza del dibattito in corso fra la Commissione europea e il Governo degli Stati Uniti che mira a garantire sia livelli elevati di tutela per i dati personali sia la libera circolazione di dati personali fra le due sponde dell'Atlantico. Il Gruppo di lavoro attribuisce grande importanza a tale dibattito e spera che sia possibile giungere quanto prima a risultati positivi. Alla luce del dibattito in oggetto, è stata trasmessa una lettera con il relativo allegato a firma del sottosegretario Aaron, del 4 novembre 1998, contenente una serie di proposte destinate ad essere discusse negli USA fra rappresentanti di imprese statunitensi e il Federal Department of Commerce. In questo contesto, il Gruppo di lavoro invita i soggetti partecipanti a tale discussione ed i governi degli Stati membri dell'UE riuniti nel comitato istituito ai sensi dell'articolo 31 della Direttiva 95/46/CE [78] a tenere presenti i punti di seguito indicati.

Le norme in materia di protezione dei dati non mirano esclusivamente a tutelare gli utilizzatori di nuove tecnologie (in particolare informatica e Internet) al fine di garantire fiducia e sicurezza e quindi contribuire allo sviluppo di tali tecnologie ed allo scambio di dati a livello internazionale. Queste norme esprimono anche l'adesione a una serie di principi e diritti fondamentali basati su una cultura comune di rispetto per la *privacy* ed altri valori propri degli esseri umani, che è condivisa allo stesso modo dagli Stati membri dell'Unione europea e dagli Stati Uniti.

1. Negli Stati Uniti, *privacy* e protezione dei dati sono rinvenibili in un complesso intreccio di regolamentazione settoriale, a livello sia federale sia statale, unita all'autoregolamentazione da parte delle imprese. Negli ultimi mesi sono stati compiuti sforzi notevoli per migliorare credibilità ed applicabilità dell'autoregolamentazione da parte delle imprese, particolarmente nell'ambito di Internet e del commercio elettronico. Tuttavia, il Gruppo di lavoro è del parere che al momento non si possa fare affidamento sull'attuale collage di legislazione settoriale ad alta specificità e autoregolamentazione su base volontaria quale garanzia di una protezione adeguata in tutti i casi di trasferimento di dati personali dall'Unione europea.

---

[78] Direttiva 95/46/EC del Parlamento europeo e del Consiglio del 24 ottobre 1995 sulla protezione delle persone rispetto al trattamento di dati personali e sulla libera circolazione di tali dati. GU L 281, 23 novembre 1995.

2. Data la complessità dell'attuale sistema statunitense di tutela della *privacy* e dei dati, la definizione negli USA di uno standard concordato «di riferimento» per tale tutela, sotto forma di una serie di principi che rappresentino un «porto sicuro» e siano offerti a tutti i soggetti economici ed agli operatori statunitensi, costituisce un utile approccio che, in determinati casi, potrebbe necessitare di integrazioni attraverso soluzioni contrattuali. Tuttavia, occorrono miglioramenti ulteriori per garantire la libera circolazione di dati verso gli Stati Uniti sulla base di questi principi in materia di *privacy*. Inoltre, potrebbe risultare necessario prevedere una metodologia che chiarisca quali sono le imprese per le quali valgono i principi del «porto sicuro».

3. Si deve osservare che la decisione di aderire a questo insieme di principi spetta esclusivamente alla singola impresa, per cui resta il problema costituito dalle imprese che non desiderano applicare i principi in oggetto, in assenza di una legislazione generale in materia.

4. In via generale, occorre chiarire la natura di questi principi. L'adesione ai principi può essere volontaria in prima istanza, ma una volta che un'impresa abbia deciso di aderire e quindi di usufruire dei vantaggi del «porto sicuro», il rispetto dei principi deve essere obbligatorio.

5. La credibilità dell'intero sistema risulta gravemente compromessa dall'assenza del requisito di un monitoraggio indipendente del rispetto dei principi, e dalla circostanza per cui si fa esclusivo affidamento sull'autocertificazione delle imprese. Il controllo indipendente sarebbe necessariamente serio, ma al contempo potrebbe essere fattibile, anche per le piccole imprese. I modelli in via di definizione negli USA ad opera di Better Business Bureau OnLine e di TrustE vanno nella direzione giusta.

6. Deve essere possibile che i reclami presentati da soggetti i cui dati sono stati trasferiti dall'Unione europea vengano gestiti in modo fattivo ed efficiente, e che la decisione in merito sia presa, in ultima istanza, da un organismo indipendente. A tale riguardo, un punto fondamentale è l'individuazione di uno o più enti pubblici indipendenti ovvero organismi terzi, negli USA, che siano disposti a ed in grado di fungere da punti di contatto per le autorità preposte alla protezione dei dati nell'Ue, collaborando negli accertamenti relativi a tali reclami. Si deve fare in modo di garantire l'esistenza di disposizioni pratiche per tutti i settori pertinenti negli USA. Gli organismi di regolamentazione già esistenti, quali la Federal Trade Commission e l'Office of the Comptroller of the Currency, possono svolgere questa funzione nei settori di competenza.

7. Alla luce del contenuto sostanziale, qualsiasi insieme accettabile di principi costituenti un «porto sicuro» deve comprendere, quale requisito minimo, tutti i principi fissati nelle Linee-guida in materia di *privacy* elaborate dall'OCSE nel 1980, adottate, fra gli altri, dagli USA e recentemente ribadite nel corso della Conferenza OCSE di Ottawa sul commercio elettronico. Questi principi trovano applicazione anche nella Direttiva 95/46/CE e nella normativa nazionale degli Stati membri dell'Unione europea. A tale riguardo, il documento di consultazione sopra ricordato, relativo ai principi, pubblicato dal Department of Commerce degli USA il 4 novembre 1998, suscita alcune perplessità, e in particolare:

a) Il diritto di accesso dei singoli è limitato a quanto è «ragionevole». Le Linee-guida dell'OCSE in materia di *privacy* non prevedono limitazioni a questo diritto in quanto tale, affermando più semplicemente che esso deve essere esercitato «in modo ragionevole».

b) Manca ogni riferimento al principio per cui le finalità del trattamento devono essere conformi, contenuto nelle Linee-guida dell'OCSE in materia di *privacy*, che è sostituito solo in parte da un principio di «scelta» per cui, di fatto, dati raccolti per un determinato scopo possono essere utilizzati per un altro scopo, purché i singoli abbiano la possibilità di «chiamarsi fuori» (*opt-out*).

c) I dati protetti dal diritto d'autore ed i dati sottoposti a trattamento non automatizzato sono del tutto esclusi dall'ambito di applicazione dei principi USA, mentre il principio di «scelta» non offre alcuna tutela per i dati raccolti presso terzi, e il principio di «accesso» esclude i dati ricavabili da atti pubblici.

d) In base al terzo paragrafo dell'introduzione, «l'adesione ai principi è subordinata» a una serie di eccezioni e limitazioni quali la «gestione dei rischi», e la «sicurezza delle informazioni». Il Gruppo di lavoro è del parere che si tratti di concetti eccessivamente vaghi e indefiniti, e ne raccomanda un chiarimento o l'eliminazione.

Fatto a Bruxelles il 26 gennaio 1999

Per il Gruppo di lavoro
Il Presidente: Prof. Stefano RODOTÀ

5.8 Commissione europea

5.8.1 Progetto di direttiva per le firme elettroniche [79)]

UNIONE EUROPEA
IL CONSIGLIO

Bruxelles, 19 novembre 1998 (24.11)
(Or. en)

13189/98
LIMITE
ECO 418
CODEC 635

Risultati dei lavori
del : COREPER
in data : 18 novembre 1998
al : CONSIGLIO «TELECOMUNICAZIONI»

n. doc. prec. : 12935/98 ECO 406 CODEC 603
n. prop. Comm. : 9708/98 ECO 233 CODEC 355

Presentato al Consiglio «Telecomunicazioni» del 27 novembre 1998 [80)].

OGGETTO: Progetto di direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comune per le firme elettroniche

Progetto di direttiva del Parlamento europeo e del Consiglio relativa ad un quadro comune per le firme elettroniche

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA

Visto il trattato che istituisce la Comunità europea, in particolare l'articolo 57, paragrafo 2, l'articolo 66 e l'articolo 100 A,

Vista la proposta della Commissione,

Visto il parere del Comitato economico e sociale,

Visto il parere del Comitato delle regioni,

Deliberando in conformità della procedura di cui all'articolo 189 B del trattato,

1) considerando che il 16 aprile 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni una comunicazione intitolata «Un'iniziativa europea in materia di commercio elettronico»;

[79)] Ultimo testo disponibile in lingua italiana.
[80)] Ultimo testo disponibile in lingua italiana.

2) considerando che l'8 ottobre 1997 la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale e al Comitato delle Regioni la comunicazione intitolata «Garantire la sicurezza e l'affidabilità nelle comunicazioni elettroniche - Verso la definizione di un quadro europeo in materia di firme digitali e di cifratura»;

3) considerando che il 1° dicembre 1997 il Consiglio ha invitato la Commissione a presentare quanto prima una proposta di direttiva del Parlamento europeo e del Consiglio relativa alle firme digitali;

4) considerando che le comunicazioni elettroniche e il commercio elettronico necessitano di firme elettroniche e dei servizi ad esse relativi, atti a consentire l'autenticazione dei dati; che la divergenza delle regole in materia di riconoscimento giuridico delle firme elettroniche e di accreditamento dei prestatori di servizi di certificazione negli Stati membri può costituire un grave ostacolo all'uso delle comunicazioni elettroniche e del commercio elettronico e, di conseguenza, impedire lo sviluppo del mercato intemo; che la divergenza degli interventi negli Stati membri sottolinea l'esigenza di un'armonizzazione a livello comunitario;

5) considerando che occorre promuovere l'interoperabilità dei prodotti di firma elettronica; che ai sensi dell'articolo 7 A del trattato, il mercato interno comporta uno spazio senza frontiere interne, nel quale deve essere assicurata la libera circolazione delle merci; che per garantire la libera circolazione nell'ambito del mercato interno e per infondere fiducia nelle firme elettroniche è necessaria la conformità ai requisiti essenziali specifici relativi ai prodotti di firma elettronica utilizzati dai fornitori di servizi di certificazione;

6) considerando che la rapida evoluzione tecnologica e il carattere globale di Internet rendono necessario un approccio aperto alle varie tecnologie e servizi che consentono di autenticare i dati in modo elettronico; che tuttavia, le firme digitali basate sulla crittografia a chiave pubblica costituiscono attualmente la forma piu riconosciuta di firma elettronica;

7) considerando che il mercato interno consente ai prestatori di servizi di certificazione di sviluppare le proprie attività transfrontaliere ai fini di accrescere la competitività, e pertanto di offrire ai consumatori e alle imprese nuove opportunità di scambiare informazioni e di effettuare negozi per via elettronica in modo sicuro, indipendentemente dalle frontiere; che al fne di stimolare la prestazione su scala comunitaria di servizi di certificazione sulle reti aperte, i prestatori di servizi di certificazione debbono essere generalmente liberi di offrire i rispettivi servizi senza preventiva autorizzazione; che non vi è immediata necessità di garantire la libera circolazione dei servizi di certificazione armonizzando le disposizioni nazionali che impongono restrizioni giustificate e proporzionate alla prestazione di tali servizi;

8) considerando che i sistemi di accreditamento facoltativo intesi a migliorare il livello di servizio fornito possono offrire ai prestatori di servizi di certificazione il contesto appropriato per l'ulteriore sviluppo dei loro servizi verso i livelli di fiducia, sicurezza e qualità richiesti dall'evoluzione del mercato; che tali sistemi debbono incoraggiare lo sviluppo di prassi ottimali tra i prestatori di servizi di certificazione; che questi ultimi debbono essere liberi di aderire a tali sistemi di accreditamento e di trarne vantaggio; che gli Stati membri non debbono vietare ai prestatori di servizi di certificazione di operare al di fuori di tali sistemi di accreditamento; che si deve garantire che i sistemi di accredita-

mento non riducano la concorrenza nel settore dei servizi di certificazione; che è importante raggiungere l'equilibrio tra esigenze dei consumatori ed esigenze delle imprese;

9) considerando che la presente direttiva contribuisce pertanto all'uso e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità; che le firme elettroniche usate esclusivamente all'interno di sistemi chiusi non esigono una disciplina comune; che, nella misura consentita dal diritto nazionale, va rispettata la libertà delle parti di accordarsi sulle condizioni di accettazione dei dati firmati in modo elettronico; che la presente direttiva non è intesa ad armonizzare le normative nazionali sui contratti, in particolare in materia di formazione ed esecuzione dei contratti, od altre formalità non contrattuali che richiedano l'apposizione di firme; che per tale motivo, le disposizioni sugli effetti giuridici delle firme elettroniche non devono riguardare i requisiti legali di forma previsti dal diritto nazionale sulla conclusione dei contratti o le regole di determinazione del luogo della conclusione del contratto;

10) considerando che, al fine di contribuire all'accettazione generale delle firme elettroniche, la validità giuridica di una firma elettronica non deve essere disconosciuta unicamente per il fatto che si presenta sotto forma di dati elettronici, oppure che essa non è basata su un certificato qualificato o su un certificato rilasciato da un prestatore di servizi di certificazione accreditato, oppure per il fatto che il prestatore di servizi che ha rilasciato il relativo certificato appartiene ad un altro Stato membro; che le firme elettroniche connesse ad un prestatore di servizi di certificazione affidabile che si conformi ai requisiti essenziali debbono avere la stessa efficacia giuridica delle firme autografe; che è necessario garantire che le firme elettroniche possano essere utilizzate come prove nei procedimenti giudiziari in tutti gli Stati membri; che il riconoscimento giuridico delle firme elettroniche deve basarsi su criteri oggettivi e non essere connesso ad un'autorizzazione rilasciata al prestatore di servizi interessato; che regole armonizzate relative all'efficacia giuridica delle firme elettroniche devono garantire una disciplina giuridica coerente in tutta la Comunità;

11) considerando che la responsabilità dei prestatori di servizi di certificazione che offrono tali servizi al pubblico è disciplinata dal diritto nazionale; che l'eterogeneità della portata e del contenuto di tali regole può compromettere la certezza del diritto, soprattutto per quanto riguarda i terzi che si affidano ai servizi dei citati prestatori; che tale incertezza può danneggiare lo sviluppo del commercio transfrontaliero e ostacolare il corretto funzionamento del mercato interno; che l'armonizzazione delle regole in materia di responsabilità garantisce la sicurezza e la prevedibilità sul piano giuridico sia per i prestatori di servizi di certificazione, sia per i consumatori; che tali regole contribuiranno all'accettazione generale e al riconoscimento giuridico delle firme elettroniche nell'ambito della Comunità, e di conseguenza influiranno positivamente sul funzionamento del mercato interno;

12) considerando che lo sviluppo del commercio elettronico internazionale rende necessari dispositivi transfrontalieri che coinvolgono i paesi terzi; che tali dispositivi dovrebbero essere elaborati a livello commerciale; che al fine di garantire l'interoperabilità a livello globale, potrebbe essere utile stiputare accordi con i paesi terzi relativi a regole multilaterali per il reciproco riconoscimento dei servizi di certificazione;

13) considerando che al fine di stimolare le comunicazioni elettroniche e il commercio elettronico garantendo la fiducia da parte degli utenti, gli Stati membri debbono obbligare i prestatori di servizi di certificazione a rispettare la-

legislazione in materia di protezione dei dati e la vita privata degli individui, e debbono richiedere a questi ultimi di fornire, qualora il firmatario lo richieda, anche servizi di certificazione relativi a pseudonimi; che il diritto nazionale deve stabilire in quali casi e a quali condizioni i dati che rivelano l'identità della persona cui i dati medesimi si riferiscono debbano essere trasferiti ai fini di inchieste penali; che i prestatori di servizi di certificazione debbono informare preventivamente gli utenti, per iscritto e in termini facilmente comprensibili e utilizzando mezzi di comunicazione durevoli, in merito alle condizioni praticate, in particolare alle precise modalità d'uso dei certificati rilasciati ed ai limiti della loro responsabilità;

14) considerando che ai fini dell'applicazione della presente direttiva la Commissione deve essere assistita da un comitato a carattere consultivo;

15) considerando che, conformemente ai principi di sussidiarietà e proporzionalità di cui all'articolo 3 B del trattato, l'obiettivo di un quadro giuridico armonizzato per la prestazione di firme elettroniche e dei servizi ad esse relativi non può essere sufficientemente realizzato dagli Stati membri e può pertanto essere meglio realizzato a livello comunitario; che la presente direttiva si limita ai requisiti minimi essenziali per la realizzazione di tale obiettivo e non esula da ciò che è necessario a questo scopo,

HANNO ADOTTATO LA PRESENTE DIRETTIVA

Art. 1
Campo di applicazione [81)]

La presente direttiva è intesa ad agevolare l'uso delle firme elettroniche e a contribuire al loro riconoscimento giuridico. Essa istituisce un quadro giuridico per le firme elettroniche e taluni servizi di certificazione al fine di garantire il corretto funzionamento del mercato interno.

Essa non disciplina aspetti relativi alla conclusione e alla validità dei contratti o altri obblighi giuridici quando esistono requisiti di forma prescritti dal diritto nazionale o comunitario, né pregiudica le norme e i limiti che disciplinano l'uso dei documenti contenuti nel diritto nazionale o comunitario.

Art. 2
Definizioni

Ai fini della presente direttiva, valgono le seguenti definizioni:

1. «firma elettronica», dati in forma elettronica allegati, oppure connessi tramite associazione logica, ad altri dati elettronici, utilizzata come metodo di autenticazione [82)].

[81)] Considerando supplementare che dovrà essere confermato dopo il Consiglio: «considerando che la presente direttiva fa salve le disposizioni nazionali inerenti all'ordine e alla sicurezza pubblici o relative alla fornitura di servizi intesi a garantire la riservatezza».

[82)] Riserva di *F.*

1-*bis* «firma elettronica avanzata», una firma elettronica che soddisfi i seguenti requisiti:

a) essere connessa esclusivamente al firmatario;

b) essere idonea ad identificare il firmatario;

c) essere creata con mezzi sui quali il firmatario può conservare il proprio esclusivo controllo;

d) essere collegata ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva alterazione [83] di detti dati.

2. «firmatario», colui che detiene un dispositivo per la creazione di una firma e agisce o per se stesso o per conto dell'entità da esso rappresentata.

3. «dispositivo per la creazione di una firma», dati peculiari, come codici o chiavi crittografiche private, oppure un dispositivo materiale di configurazione esclusiva utilizzato dal firmatario per creare una firma elettronica.

4. «dispositivo di verifica della firma», dati, come codici o chiavi crittografiche pubbliche, oppure un dispositivo materiale di configurazione utilizzato per verificare la firma elettronica;

4-*bis* «certificato», un attestato digitale che collega un dispositivo di verifica della firma ad una data persona e conferma l'identità di tale persona;

5. «certificato qualificato», un certificato conforme ai requisiti di cui all'allegato I e fornito da un prestatore di servizi di certificazione che soddisfa i requisiti di cui all'allegato II;

6. «prestatore di servizi di certificazione» [84], una persona o un'entità che rilascia certificati o fornisce altri servizi connessi alle firme elettroniche [85].

7. «prodotto di firma elettronica», macchinari o programmi per elaboratori elettronici, oppure i componenti pertinenti dei medesimi destinati ad essere utilizzati da un prestatore di servizi di certificazione per la prestazione di servizi di firma elettronica.

---

[83] Riserva di *UK*.

[84] Considerando supplementare che dovrà essere esaminato dopo il Consiglio: «Considerando che i servizi di certificazione possono essere offerti o da un'entità pubblica ovvero da una persona giuridica o fisica, stabilita a norma della legislazione nazionale.»

[85] È stato concordato il seguente considerando supplementare (all'inizio del considerando n.7):

«considerando che le firme elettroniche verranno usate in una grande varietà di circostanze ed applicazioni, che comporteranno un'ampia gamma di nuovi servizi e prodotti facenti uso di firme elettroniche o ad esse collegati;

che la definizione di tali prodotti e servizi non dovrebbe essere limitata al rilascio e alla gestione di certificati, ma comprendere anche ogni altro servizio e prodotto facente uso di firme elettroniche o ad esse ausiliario, quali servizi di immatricolazione, servizi di apposizione del giorno e dell'ora, servizi di repertorizzazione, servizi informatici o consulenza relativi alle firme elettroniche;

che la libera circolazione di tutti i suddetti prodotti e servizi deve essere assicurata conformemente alle disposizioni del trattato;».

Art. 3

Accesso al mercato

1. Gli Stati membri non subordinano ad autorizzazione preventiva la prestazione di servizi di certificazione [86].

2. Salvo il disposto del paragrafo 1, gli Stati membri possono introdurre o conservare sistemi di accreditamento facoltativi [87] intesi a fornire servizi di certificazione di livello più elevato. Tutte le condizioni relative a tali sistemi devono essere obiettive, trasparenti, proporzionate e non discriminatorie. Gli Stati membri non possono limitare il numero di prestatori di servizi di certificazione accreditati per motivi che rientrano nel campo d'applicazione della presente direttiva.

2-*bis* Gli Stati membri provvedono affinché venga istituito un sistema appropriato che consenta il controllo dei prestatori di servizi di certificazione stabiliti nel loro territorio che rilasciano certificati qualificati al pubblico [88].

3. Secondo la procedura di cui all'articolo 9, la Commissione può determinare e pubblicare sulla Gazzetta ufficiale delle Comunità europee i numeri di riferimento di norme generalmente riconosciute relative a prodotti di firma elettronica. Un prodotto di firma elettronica conforme a tali norme viene considerato dagli Stati membri conforme ai requisiti di cui all'allegato II, punto e) [e allegato III].

4. Gli Stati membri possono assoggettare ad eventuali requisiti supplementari l'uso delle firme elettroniche [89], nel settore pubblico. Tali requisiti debbono essere obiettivi, trasparenti, proporzionati e non discriminatori, e riguardare unicamente le caratteristiche specifiche dell'uso di cui trattasi.

---

[86] Considerando supplementare che dovrà essere esaminato dopo il Consiglio: «considerando che per autorizzazione preventiva non s'intende solo qualsiasi permesso che imponga al prestatore di servizi di certificazione interessato di ottenere dalle autorità nazionali una decisione prima di essere autorizzato a prestare i propri servizi di certificazione, ma anche ogni altro requisito il cui effetto sia di rendere tale disposizione dipendente da una decisione, una misura o un atto specifico da parte di un'autorità nazionale;»

[87] È stato concordato il seguente considerando: «considerando che per accreditamento facoltativo si intende qualsiasi permesso, che stabilisca diritti ed obblighi specifici della fornitura di servizi di certificazione, il quale sia concesso, su richiesta del prestatore di servizi di certificazione, dall'autorità incaricata dell'elaborazione e della sorveglianza del rispetto di tali diritti ed obblighi, fermo restando che il prestatore di servizi di certificazione non è autorizzato ad esercitare i diritti derivanti dal permesso fino a che non abbia ricevuto la decisione da parte dell'autorità».

[88] È stato concordato il seguente considerando: «considerando che gli Stati membri possono decidere come garantire il controllo del rispetto delle disposizioni contenute nella presente direttiva; che la direttiva non esclude l'istituzione di sistemi di controllo basati nel settore privato;». Tuttavia dovrebbe essere presa in considerazione dopo il Consiglio la seguente aggiunta: «Considerando che la presente direttiva non obbliga i prestatori di servizi di certificazione a chiedere il controllo in base a un qualsiasi accordo d'accreditamento o licenza.».

[89] Considerando supplementare che dovrà essere confermato dopo il Consiglio: «considerando che le firme elettroniche saranno utilizzate nel settore pubblico nell'ambito delle amministrazioni nazionali e comunitarie e nelle comunicazioni tra tali amministrazioni nonché con i cittadini e gli operatori economici, ad esempio nei settori degli appalti pubblici, della fiscalità, della sicurezza sociale, della sanità e dell'amministrazione della giustizia;».

Art. 4

Principi del mercato interno

1. Ciascuno Stato membro applica le norme di attuazione della presente direttiva ai prestatori di servizi di certificazione stabiliti sul suo territorio e ai servizi da essi forniti. Gli Stati membri non possono limitare la prestazione di servizi di certificazione originati in un altro Stato membro nella materia disciplinata dalla presente direttiva.

2. Gli Stati membri provvedono a che i prodotti di firma elettronica conformi alla presente direttiva circolino liberamente nel mercato interno [90].

Art. 5

Effetti giuridici [91]

1. Gli Stati membri provvedono a che le firme elettroniche avanzate basate su un certificato qualificato [e che sono create da dispositivi che soddisfano ai requisiti di cui all'allegato III] [92]:

a) soddisfino i requisiti giuridici di una firma in relazione ai dati in forma elettronica così come una firma autografa soddisfa tali requisiti in relazione a dati cartacei;

b) siano ammesse come prova nei procedimenti giudiziari.

2. Gli Stati membri provvedono affinché una firma elettronica non sia considerata inefficace e inammissibile come prova nei procedimenti giudiziari unicamente a causa della sua forma elettronica, o per il fatto che non è basata su un certificato qualificato o su un certificato rilasciato da un prestatore di servizi di certificazione accreditato [93] [ovvero non è creata da un dispositivo per la creazione di una firma che soddisfa ai requisiti di cui all'allegato III].

---

[90] È stato concordato di riformulare questo considerando:

«considerando che dovrebbe essere promossa l'interoperabilità dei prodotti di firma elettronica; che, a norma dell'articolo 7A del trattato, il mercato interno dovrà comprendere una zona in cui sarà assicurata la libera circolazione delle merci; che i requisiti fondamentali propri dei prodotti di firma elettronica usati dai prestatori di servizi di certificazione devono essere soddisfatti per garantire la libera circolazione nel mercato interno e creare la fiducia nelle firme elettroniche, fatto salvo il regolamento (CE) n. 3381/94 che istituisce un regime comunitario di controllo delle esportazioni di beni a duplice uso e la decisione 94/942/CFSP relativa all'azione comune, adottata dal Consiglio in base all'articolo J.3 del trattato sull'Unione europea, riguardante il controllo dell'esportazione dei beni a duplice uso;».

[91] È stato concordato il seguente considerando:

«considerando che il diritto nazionale disciplina l'uso dei documenti elettronici e delle firme elettroniche;».

[92] È stato concordato il seguente considerando:

«considerando che il diritto nazionale disciplina l'uso dei documenti elettronici e delle firme elettroniche;».

[93] Considerando supplementare che dovrà essere confermato dopo il Consiglio:

«considerando che la presente direttiva non ha lo scopo di interferire con le norme nazionali in materia di libero uso delle prove in sede giudiziaria».

Art. 6

Responsabilità [94)]

Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato o che garantisce al pubblico un certificato, sia responsabile per danni provocati a chiunque faccia ragionevole affidamento sul certificato in questione, per quanto riguarda:

a) l'esattezza di tutte le informazioni contenute nel certificato qualificato a partire dalla data di rilascio,

b) [...]

c) la garanzia che, ai momento del rilascio del certificato, il titolare identificato nei certificato qualificato detenesse il dispositivo di creazione della firma corrispondente al dispositivo di verifica della firma riportato o identificato nel certificato;

d) la garanzia che il dispositivo di creazione della firma e il dispositivo di verifica della firma, garanzia che i due dispositivi funzionino insieme in modo complementare, nei casi in cui il fornitore di servizi di certificazione generi i due dispositivi.

a meno che il prestatore di servizi di certificazione non provi di non aver agito con negligenza.

1-*bis*. Gli Stati membri provvedono almeno a che il prestatore di servizi di certificazione che rilascia al pubblico un certificato come certificato qualificato sia responsabile, nei confronti di chiunque faccia ragionevole affidamento sul certificato, dei danni provocatigli, tra cui la mancata registrazione della revoca del certificato, a meno che non provi di non aver agito con negligenza.

2. Gli Stati membri provvedono a che un prestatore di servizi di certificazione sia esentato dalla responsabilità derivante da eventuali errori contenuti nelle informazioni riportate nel certificato qualificato e a suo tempo fornite dalla persona cui è stato rilasciato il certificato, qualora detto prestatore possa dimostrare di aver usato tutta la necessaria diligenza per verificare tali informazioni.

3. Gli Stati membri provvedono a che un prestatore di servizi di certificazione possa indicare, nel certificato qualificato, i limiti d'uso di un determinato certificato. Il prestatore di servizi di certificazione deve essere esentato dalla responsabilità per i danni derivanti dall'uso indebito di un certificato qualificato ove siano precisati i limiti d'uso dello stesso.

4. Gli Stati membri provvedono affinché un prestatore di servizi di certificazione abbia la facoltà di indicare nel certificato qualificato un valore limite per i negozi per i quali può essere usato il certificato.

5. I paragrafi da 1 a 4 si applicano salvo il dispositivo della direttiva 93/13/CE del Consiglio.

[94)] Considerando supplementare che dovrà essere confermato dopo il Consiglio: «considerando che la presente direttiva non pregiudica alcun diritto di cui una persona che faccia affidamento su un certificato possa godere conformemente alle disposizioni della legislazione sulla responsabilità contrattuale o extracontrattuale o a un regime di responsabilità particolare esistente al momento dell'entrata in vigore della direttiva».