DECISIONE DEL CONSIGLIO

del 31 marzo 1992

nel settore della sicurezza dei sistemi di informazione

(92/242/CEE)

IL CONSIGLIO DELLE COMUNITÀ EUROPEE,

visto il trattato che istituisce la Comunità economica 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 del tenore 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 di informazione nelle azioni della Comunità, segnatamente in vista delle ripercussioni del completamento del mercato interno;

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

considerando che vi è una stretta relazione tra telecomunicazioni, tecnologia dell'informazione, normalizzazione, mercato dell'informazione e politiche di ricerca e sviluppo tecnologico, nonché con i lavori già intrapresi dalla Comunità in questi settori;

considerando che è opportuno concertare gli sforzi basandosi sui lavori già esistenti ai livelli nazionale e internazionale e promuovere la cooperazione tra le principali parti interessate; che è quindi opportuno procedere nel contesto di un piano d'azione coerente;

considerando che la complessità della sicurezza dei sistemi di informazione richiede lo sviluppo di strategie atte a rendere libera la circolazione delle informazioni nel mercato unico, garantendo nel contempo la sicurezza d'impiego dei sistemi di informazione in tutta la Comunità;

considerando che rientra nelle responsabilità di ciascuno Stato membro tener conto dei vincoli imposti dalla sicurezza e dall'ordine pubblico;

considerando che le responsabilità degli Stati membri in questo campo comportano un'impostazione concertata basata su una stretta collaborazione con gli alti funzionari degli Stati membri;

considerando che è necessario varare un'azione comprendente un piano d'azione per un periodo iniziale di ventiquattro mesi e l'istituzione di un comitato di alti funzionari, con un mandato a lungo termine, in veste di consulente della Commissione per le iniziative nel settore della sicurezza dei sistemi d'informazione;

considerando che l'esecuzione dell'azione per un periodo iniziale di ventiquattro mesi richiede un importo stimato a 12 milioni di ecu; che per il 1992, nel quadro delle attuali prospettive finanziarie, l'importo stimato necessario ammonta a 2 milioni di ecu;

considerando che le risorse da impegnare per il finanziamento del programma dopo l'esercizio 1992 dovranno rientrare nei limiti del vigente quadro finanziario comunitario,

DECIDE:

Articolo 1

Con la presente decisione è adottata un'azione nel settore della sicurezza dei sistemi d'informazione. Essa comporta:

— lo sviluppo di strategie globali di sicurezza dei sistemi di informazione (piano d'azione) per un periodo iniziale di ventiquattro mesi e

— l'istituzione di un gruppo di alti funzionari con mandato a lungo termine per consigliare la Commissione sulle azioni rientranti nel settore della sicurezza dei sistemi di informazione, in appresso denominato « comitato ».

(1) GU n. C 277 del 5. 11. 1990, pag. 18.
(2) GU n. C 94 del 13. 3. 1992.
(3) GU n. C 159 del 17. 6. 1991, pag. 38.

Articolo 2

1. La Commissione consulta sistematicamente il comitato sui problemi relativi alla sicurezza dei sistemi di informazione dei vari programmi della Comunità, in particolare sulla definizione di strategie e programmi di lavoro.

2. Il piano d'azione, come indicato nell'allegato, include un lavoro preparatorio sui seguenti temi:

I. sviluppo di un quadro strategico per la sicurezza dei sistemi d'informazione;

II. individuazione delle esigenze degli utenti e dei fornitori di servizi in fatto di sicurezza dei sistemi d'informazione;

III. elaborazione di soluzioni a certe esigenze prioritarie di utenti, fornitori e esercenti di servizi;

IV. elaborazione di specifiche, normalizzazione, valutazione e certificazione in materia di sicurezza dei sistemi di informazione;

V. sviluppi tecnologici ed operativi in materia di sicurezza dei sistemi d'informazione;

VI. attuazione della sicurezza dei sistemi di informazione.

Articolo 3

1. L'importo stimato necessario dei mezzi finanziari comunitari per l'esecuzione dell'azione per un periodo iniziale di 24 mesi è di 12 milioni di ecu, di cui 2 milioni di ecu per il 1992 nel quadro delle prospettive finanziarie 1988-1992.

Per l'ulteriore periodo di applicazione dell'azione, l'importo dovrà essere conforme al quadro finanziario comunitario in vigore.

2. L'autorità di bilancio stabilisce gli stanziamenti disponibili per ogni esercizio tenendo presenti i principi di una sana gestione previsti all'articolo 2 del regolamento finanziario applicabile al bilancio generale delle Comunità europee.

Articolo 4

Un gruppo di esperti indipendenti procede, per la Commissione, ad una valutazione dei progressi compiuti durante il periodo iniziale. La relazione di questo gruppo, con le eventuali osservazioni della Commissione, è trasmessa al Parlamento europeo e al Consiglio.

Articolo 5

1. La Commissione è responsabile dell'esecuzione dell'azione. Essa è assistita da un comitato consultivo composto da rappresentanti degli Stati membri e presieduto da un suo rappresentante.

2. Il piano d'azione viene attuato secondo le finalità di cui all'articolo 2 e, se necessario, aggiornato. Esso precisa gli obiettivi e i tipi d'azione da intraprendere, nonché le relative disposizioni finanziarie. La Commissione fa appello a proposte sulla base del piano d'azione.

3. Il piano d'azione è attuato in stretta collaborazione con gli operatori del settore. Esso prende in considerazione, promuove e integra le attività di normalizzazione svolte a livello europeo e internazionale in questo campo.

Articolo 6

1. La procedura prevista all'articolo 7 si applica alle misure relative alla politica della Comunità nel settore della sicurezza dei sistemi di informazione.

2. La procedura di cui all'articolo 8 si applica:

— alla preparazione e all'aggiornamento del piano d'azione previsto all'articolo 5;

— al contenuto dell'invito a presentare proposte, all'esame delle medesime e alla stima dell'importo del contributo comunitario alle misure qualora tale importo superi 200 000 ecu;

— alla cooperazione di organizzazioni non comunitarie ad azioni svolte a titolo della presente decisione;

— ai sistemi di divulgazione, protezione e sfruttamento dei risultati delle misure;

— alle disposizioni da prendere per valutare l'azione.

3. Se l'importo del contributo comunitario alle misure è inferiore o pari a 200 000 ecu, la Commissione consulta il comitato sulle misure da adottare e lo informa dei risultati dell'esame.

Articolo 7

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.

Articolo 8

Il rappresentante della Commissione sottopone al comitato un progetto delle misure da adottare. Il comitato formula il suo parere sul progetto entro un termine che il presidente può fissare in funzione dell'urgenza della questione in esame. Il parere è formulato alla maggio-

ranza prevista dall'articolo 148, paragrafo 2 del trattato per l'adozione delle decisioni che il Consiglio deve prendere su proposta della Commissione. Nelle votazioni al comitato, viene attribuita ai voti dei rappresentanti degli Stati membri la ponderazione definita all'articolo precitato. Il presidente non partecipa al voto.

La Commissione adotta le misure previste qualora siano conformi al parere del comitato.

Se le misure previste non sono conformi al parere del comitato, o in mancanza di parere, la Commissione sottopone senza indugio al Consiglio una proposta in merito alle misure da prendere. Il Consiglio delibera a maggioranza qualificata.

Se il Consiglio non ha deliberato entro un termine di tre mesi a decorrere dalla data in cui gli è stata sottoposta la proposta, la Commissione adotta le misure proposte, tranne nel caso in cui il Consiglio si sia pronunciato a maggioranza semplice contro tali misure.

Fatto a Bruxelles, addì 31 marzo 1992.

Per il Consiglio

Il Presidente

Vitor MARTINS

ALLEGATO

Prospetto delle linee d'azione

ORIENTAMENTI PER UN PIANO D'AZIONE NEL SETTORE DELLA SICUREZZA DEI SISTEMI DI INFORMAZIONE

INTRODUZIONE

Il piano d'azione ha lo scopo di sviluppare strategie globali intese a fornire agli utenti e ai produttori di informazioni immagazzinate, trattate o trasmesse elettronicamente un'adeguata protezione dei sistemi di informazione contro le minacce fortuite o volontarie.

Il piano d'azione tiene conto e sostiene le attività di normalizzazione in corso per questo settore su scala mondiale.

Esso comprende le seguenti linee di azione :

— sviluppo di un quadro strategico per la sicurezza dei sistemi di infomazione ;

— individuazione delle esigenze degli utenti e dei fornitori di servizi in fatto di sicurezza dei sistemi di informazione ;

— elaborazione di soluzioni a certe esigenze immediate e temporanee di utenti, fornitori e fornitori di servizi ;

— elaborazioni di specifiche, normalizzazione, valutazione e certificazione in materia di sicurezza dei sistemi d'informazione ;

— sviluppi tecnologici ed operativi in materia di sicurezza dei sistemi d'informazione ;

— attuazione della sicurezza dei sistemi d'informazione.

Il piano d'azione è attuato dalla Commissione in stretta connessione con le azioni correlate svolte negli Stati membri e in congiunzione con le pertinenti azioni comunitarie di ricerca e sviluppo.

1. Prima linea di azione — Sviluppo di un quadro strategico per la sicurezza dei sistemi d'informazione

1.1. *Problematica*

Si ritiene che la sicurezza dei sistemi d'informazione sia un requisito generalmente necessario nella società moderna. I servizi d'informazione elettronica richiedono infrastrutture di telecomunicazioni sicure, hardware e software affidabili, nonché condizioni sicure di utilizzazione e di gestione. 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 poter agire efficacemente, pur proteggendosi, in un mondo in rapida trasformazione.

1.2. *Obiettivo*

È necessario creare un quadro strategico per trovare un accordo fra gli obiettivi sociali, economici e politici e le scelte tecniche, operative e giuridiche della Comunità in un contesto internazionale. 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 un contesto strategico convenuto. Tali sono i presupposti per conciliare gli interessi e le esigenze dell'azione politica e dello sviluppo industriale.

1.3. *Situazione e tendenze*

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*

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, del non rifiuto e degli eventuali schemi d'autorizzazione in un ambiente democratico).

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.

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 — Individuazione delle esigenze degli utenti e dei fornitori di servizi in fatto di sicurezza dei sistemi d'informazione

2.1. *Problematica*

La sicurezza dell'informazione è una condizione indispensabile per l'integrità e affidabilità delle applicazioni commerciali, la proprietà intellettuale e la riservatezza. 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.

Le esigenze degli utenti implicano sicurezza di funzionamento dei sistemi di informazione connessa con gli 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*

Occorre stabilire la natura e le caratteristiche delle esigenze degli utenti e dei fornitori di servizi e il loro rapporto con le misure di sicurezza dei sistemi d'informazione.

2.3. *Situazione e tendenze*

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 delle certificazioni di valutazione sono della massima importanza.

2.4. *Esigenze, scelte e priorità*

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.

È 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 vari opzioni e strategie in materia di sicurezza dei sistemi d'informazione per gli utenti, i fornitori di servizi e gli operatori.

3. Terza linea d'azione — Elaborazione di soluzioni ad alcune esigenze prioritarie di utenti, fornitori ed esercenti di servizi

3.1. *Problematica*

È attualmente possibile impedire efficacemente l'accesso non autorizzato agli elaboratori con misure 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 dei sistemi d'informazione.

3.2. *Obiettivo*

A breve scadenza, l'obiettivo è di fornire soluzioni che possano rispondere alle esigenze più immediate degli utenti esercenti di servizi e produttori. Ciò comporta l'utilizzazione di comuni criteri di sicurezza delle tecnologie dell'informazione. Tali soluzioni devono essere aperte alle necessità e alle soluzioni future.

3.3. *Situazione e tendenze*

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. È comunque difficile generalizzare queste tecniche e metodi in ambiente aperto.

L'ISO sta svolgendo lavori sulla sicurezza OSI dell'informazione (ISO DIS 7498-2), così come il CCITT nel contesto dell'X400. È anche possibile inserire segmenti di sicurezza nei messaggi. L'autenticazione, l'integrità e il non rifiuto (non-repudiation) sono trattati come parti dei messaggi EDIFACT e di X400 MHS.

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.

Vari paesi (per esempio 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 sistemi affidabili. La creazione di organizzazioni nazionali incaricate di condurre le valutazioni e di concedere le certificazioni sosterrà questa iniziativa.

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*

È essenziale mettere a punto al più presto le procedure, le norme, i prodotti e gli strumenti atti a garantire la sicurezza sia dei sistemi di informazione in quanto tali (elaboratori, terminali) sia 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 quelle 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 di specifiche, normalizzazione, valutazione e certificazione in materia di sicurezza dei sistemi d'informazione

4.1. *Problematica*

Le esigenze di sicurezza dei sistemi d'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, inoltre, 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*

È necessario un impegno considerevole per fornire i mezzi per sostenere e realizzare funzioni di sicurezza specifiche nei settori generali dell'OSI, l'ONP, l'ISDN/IBC, e della gestione di reti. Le tecniche e le concezioni in materia di controllo sono legate alla normalizzazione ed alla determinazione di specifiche, compresa la certificazione intesa al reciproco riconoscimento. Se possibile, si devono appoggiare soluzioni accettate a livello internazionale. Andrebbero inoltre incoraggiati lo sviluppo e l'uso di sistemi informatici dotati di funzioni di sicurezza.

4.3. *Situazione e tendenze*

Gli Stati Uniti, in particolare, hanno lanciato importanti iniziative per trattare la questione della sicurezza dei sistemi di informazione in campo civile. In Europa, questo argomento rientra nel contesto della normalizzazione delle TIT nel quadro dell'ETSI e del CEN/CENELEC, in preparazione al lavoro del CCITT e dell'ISO.

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, in Germania e nel Regno Unito hanno cominciato, indipendentemente, attività similari, ma uno sforzo comune corrispondente a quello americano si sta sviluppando solo lentamente.

4.4. *Esigenze, scelte, priorità*

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).

Le specifiche e le norme devono contemplare i settori 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 — Sviluppi tecnologici ed operativi in materia di sicurezza dei sistemi d'informazione

5.1. *Problematica*

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 dei sistemi d'informazione sono le condizioni necessarie allo sviluppo del mercato dei servizi e alla competitività dell'insieme dell'economia europea.

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*

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*

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.

Il lavoro strategico di ricerca e sviluppo dovrebbe riguardare modelli concettuali per sistemi sicuri (al sicuro da compromissioni, modifiche non autorizzate, e rifiuto di funzionamento), modelli di esigenze funzionali, modelli di rischio e architetture per la sicurezza.

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.

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.

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.

Il terzo programma quadro comunitario per la ricerca e lo sviluppo tecnologico potrà essere utilizzato per promuovere progetti di cooperazione a livello preconcorrenziale e prenormativo.

6. Sesta linea d'azione — Attuazione della sicurezza dei sistemi d'informazione

6.1. *Problematica*

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 dell'informazione fino ai dispositivi crittografici, alle carte con memoria e con processore, alla gestione delle chiavi pubbliche e private, eccetera). Ci si può aspettare che alune 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).

La maggior parte dei prodotti e dei servizi in materia di sicurezza 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.

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*

Per facilitare una realizzazione armoniosa della sicurezza dei sistemi di informazione nella Comunità tutelando sia i privati cittadini sia gli interessi commerciali, sarà necessario definire una impostazione coerente atta a garantire l'attuazione di sistemi sicuri. 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*

Attualmente, le disposizioni in materia di sicurezza dei sistemi d'informazione sono bene organizzate solo per campi spefici, 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 una concenzione coerente delle disposizioni in questo settore in Europa e a livello internazionale.

6.4. *Esigenze, scelte e priorità*

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.

È 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.