D - DOCUMENTAZIONE ALLEGATA

NORMATIVA ITALIANA

NORMATIVA COMUNITARIA E COMUNICAZIONI ISTITUZIONALI

PREMESSA

Premessa

La società dell'informazione: definizione e dibattito internazionale

La trasformazione del quadro industriale del mondo sviluppato è stata accompagnata, negli anni recenti, dalla liberalizzazione delle telecomunicazioni e dalla diffusione massiccia di Internet. La caratteristica reticolare che hanno assunto attualmente l'economia e la società ha determinato la nascita della cosiddetta «società dell'informazione». Tale espressione, che trova la sua origine in quella di "società post-industriale" ed è stata usata per la prima volta nel 1973 da Daniel Bell, ordinario di sociologia a Harvard, sta ad indicare una società moderna che, giunta al culmine del processo di industrializzazione, deve - per continuare a crescere - concentrare i propri sforzi verso la produzione non più di beni materiali bensì di servizi immateriali. Il Segretario Generale dell'ONU, Kofi Annan, ha recentemente ricordato che per società dell'informazione si intende una società in cui tutte le potenzialità dell'essere umano vengono valorizzate grazie all'accesso alle tecnologie e all'educazione che permette di imparare ad utilizzarle in modo efficace. La società dell'informazione impone dunque lo sviluppo di conoscenze incrementali e l'espansione della formazione continua. Senza quest'ultima e senza l'universalità dei servizi di comunicazione le nuove tecnologie rischiano di generare atomizzazione anziché integrazione. La costruzione di una società dell'informazione aperta ed inclusiva - che è anche uno degli obiettivi che l'Unione europea ha fissato a Lisbona per condurre l'Europa, entro il 2010, verso un'economia più dinamica e competitiva - è dunque questione rilevante sia per uno sviluppo equo del mondo economicamente forte, sia per il ridimensionamento del *gap* esistente tra paesi ricchi e paesi poveri. Perché questo sia possibile è necessario in primo luogo intraprendere globalmente politiche volte a ridurre i costi di utilizzazione delle tecnologie innovative come, ad esempio, la connessione ad Internet o l'acquisto dei computer e dei telefoni mobili.

Durante gli ultimi anni il dibattito sugli aspetti generali e sui problemi specifici della società dell'informazione è stato ospitato anche in ambito ONU. Con la risoluzione n. 56/183 del 21 dicembre 2001, l'ONU ha decretato infatti la nascita di una sede di confronto internazionale denominata WSIS (*World Summit on the Information Society*). Il *summit* - supportato da un *Executive*

Secretariat (WSIS-ES) istituito presso l'*International Telecommunications Union* (ITU)[1] - rappresenta un'opportunità di riflessione su quello che è stato presentato, nella pubblicazione di promozione del primo appuntamento internazionale, come «un processo dinamico che promette una trasformazione profonda in ogni aspetto della nostra vita: la diffusione dei saperi, le interazioni sociali, i sistemi economici e commerciali, l'impegno politico, i *media*, la formazione, la salute, il divertimento e l'intrattenimento. Siamo infatti nel pieno di una rivoluzione, forse la maggiore che l'umanità abbia mai sperimentato ....». Il *summit*, articolato nelle due riunioni, di Ginevra (10-12 dicembre 2003) e di Tunisi (16-18 novembre 2005), si è delineato come processo tripartito al quale hanno partecipato i governi facenti parte delle Nazioni Unite[2], esponenti della società civile e agenzie internazionali. I due appuntamenti internazionali sono stati a loro volta preceduti da una fase preparatoria, costituita dalle conferenze preliminari (le cosiddette *PrepCom*, anche a carattere regionale) intervallate da altre occasioni di dialogo sul WSIS, quali i *meeting* della società civile[3]. Inoltre, per l'approfondimento di temi specifici sono stati formati appositi gruppi di lavoro, incaricati di predisporre documenti da esporre e discutere durante i *summit*.

Dei tre gruppi di lavoro costituiti - GFC (*Group of friends of the Chair*), WGIG (*Working Group on Internet Governance*) e TFFM (*Task Force on Financial Mechanisms*) in questa sede verrà illustrato brevemente quello incaricato dello studio della *governance* di Internet poiché attiene direttamente al tema trattato in questo volume. Il WGIG è stato istituito nel 2003 dal Segretariato generale dell'ONU in occasione del primo appuntamento internazionale del *summit,* a Ginevra. Proprio in quella circostanza, infatti, i capi di Stato e di governo - prendendo atto che Internet "occupa un posto centrale nell'infrastruttura della nascente società dell'informazione" - rilevarono che, poiché esistevano "opinioni divergenti sull'adeguamento delle istituzioni e sui meccanismi con i quali regolare la gestione del processo e l'elaborazione delle azioni politiche che riguardano la rete", sarebbe stato opportuno preparare il terreno per successive negoziazioni attraverso l'istituzione di un apposito gruppo di lavoro. In appendice a questa Premessa è

[1] La carica di Segretario Generale è attualmente ricoperta da Yoshio Utsumi, che è al contempo Segretario Generale dell'ITU.

[2] Hanno finora partecipato al *summit* 175 Stati.

[3] In preparazione dell'ultimo vertice di Tunisi, ad esempio, si sono svolte tre conferenze preliminari, la prima tenuta ad Hammamet (Tunisia), dal 24 al 26 giugno 2004, la seconda a Ginevra dal 17 al 25 febbraio 2005 e l'ultima ancora a Ginevra, dal 19 al 30 settembre 2005.

riportato un intervento di V. Bertola, membro del WGIG, illustrativo delle attività del gruppo di lavoro e delle indicazioni contenute nell'ultimo rapporto preparatorio del *summit* di Tunisi.

A conclusione dei due ricordati appuntamenti internazionali di Ginevra 2003 e Tunisi 2005 sono stati approvati quattro documenti conclusivi. A Ginevra furono elaborati una **Dichiarazione di principi** ed un **Piano d'azione,** dai quali è emerso soprattutto l'intento di promuovere la diffusione delle tecnologie innovative nei paesi in via di sviluppo anche al fine di migliorare le condizione di vita delle popolazioni più povere ed emarginate.

E' stato inoltre delineato il percorso per creare e sviluppare la connettività anche nelle aree sviluppate facendo riferimento a diversi punti di destinazione quali:

a) i villaggi ed i punti d'accesso comunitari;
b) le scuole secondarie o superiori e le scuole primarie;
c) i centri scientifici e i centri di ricerca;
d) le biblioteche pubbliche, i centri culturali, i musei, gli uffici postali e gli archivi;
e) i centri sanitari e gli ospedali;
f) le pubbliche amministrazioni, locali e centrali.

Durante il *summit* di Tunisi sono stati approvati un **Accordo** (*Tunis Commitment*) ed un'**Agenda** (*Tunis Agenda for the Information Society*) con i quali si è riconfermata l'adesione ai princìpi illustrati a Ginevra e la volontà di onorare gli impegni assunti.

I testi dei documenti, per la prima volta tradotti in italiano, sono pubblicati alla fine del presente volume[4].

Nel testo dell'**Accordo** viene rivolto ai Governi e al settore privato un invito a sostenere la modernizzazione tecnologica delle piccole e medie imprese, soprattutto attraverso un'opera di adeguamento giuridico e regolamentare. E' dato poi risalto alla necessità di realizzare le infrastrutture tecnologiche con applicazioni in lingua locale. La protezione e la promozione delle "diversità" e delle "identità" culturali - si sottolinea infatti nel documento

[4] La traduzione è stata effettuata a cura del Servizio Studi e rivista a cura dell'Unità operativa traduzione e interpretariato del Servizio Affari internazionali.

- sono una condizione essenziale per garantire l'inclusione. E' inoltre necessario monitorare costantemente i progressi realizzati per ridurre il *gap* tecnologico esistente fra i diversi Paesi. Il raggiungimento di questo obiettivo - si legge ancora nelle conclusioni - passa in primo luogo per la moltiplicazione dei punti di accesso pubblico alle tecnologie dell'informazione che, oltre a risultare pratica più equa, è anche finanziariamente più sostenibile. La garanzia di accesso egualitario ed universale si produce accordando un'attenzione speciale ai bisogni dei gruppi sociali emarginati e più deboli, come gli immigrati, i rifugiati, i disoccupati, i minorenni, i nomadi, gli anziani e gli handicappati.

Ciò comporta la focalizzazione dell'interesse mondiale verso i Paesi meno sviluppati, verso quelli con economia di transizione o bloccata o isolati geograficamente ovvero in guerra o colpiti da catastrofi naturali. Il documento evidenzia poi l'esistenza di un *gap* di conoscenza tecnologica tra i sessi e la necessità che le donne non siano più discriminate, ma anzi partecipino attivamente alla crescita della società della conoscenza attraverso l'inclusione nei processi decisionali. La rimozione degli ostacoli esistenti, così come l'attenzione rivolta alla protezione dell'infanzia ed il coinvolgimento diretto dei giovani nei programmi di sviluppo innovativo, sono inviti indirizzati a tutti i soggetti coinvolti. Per i programmi di inclusione informatica e di educazione scientifica, in particolare, viene auspicato l'impiego sempre più massiccio di programmi *open source* in un clima di collaborazione fattivo sia a livello nazionale che regionale e mondiale. A tal fine tutti i delegati intervenuti nel dibattito si sono impegnati all'attuazione rapida, completa e durevole del cosiddetto "Patto di solidarietà informatica" previsto dal paragrafo 27 del Piano d'azione di Ginevra, azione quest'ultima che non può prescindere dalla soluzione del problema del debito dei Paesi in via di sviluppo.

Nel testo dell'**Agenda** si fa richiamo al Rapporto del Gruppo di lavoro sui meccanismi di finanziamento (TFFM), incaricato di analizzare e di giudicare l'adeguatezza dei meccanismi di finanziamento esistenti per lo sviluppo delle tecnologie dell'informazione. Le conclusioni del Rapporto sono state usate per formulare una serie di raccomandazioni - recepite nell'Agenda - così riassumibili:

- **migliorare i meccanismi di finanziamento** per rendere le risorse adeguate, durevoli e libere dai condizionamenti, anche riducendo i

rischi di investimento ed i costi delle transazioni per gli operatori che si interessano ai mercati meno attrattivi attraverso programmi di collaborazione tra i Governi ed il mondo della finanza. Altra misura utile è individuata nell'appoggio della microfinanza locale per favorire in modo particolare la cooperazione tra Nord e Sud del mondo. Le misure che generano fondi per le tecnologie dell'informazione nei paesi in via di sviluppo dovranno produrre nuovi strumenti finanziari sotto forma di fondi di destinazione speciali e di capitali di partenza adatti alle diverse realtà economiche. Sulla base delle indicazioni del TFFM è stato creato un apposito "Fondo di solidarietà informatica";

- **utilizzare i meccanismi di alleggerimento del debito** come stabilito dal Piano d'azione di Ginevra;

- **intensificare la cooperazione regionale** con la realizzazione di partenariati anche in vista della creazione di strutture dorsali regionali;

- **incoraggiare la diffusione della tecnologia** di navigazione Internet **a banda larga;**

- **assicurare un facile accesso** alle tecnologie dell'informazione attuando anzitutto una riduzione dei costi per la navigazione in rete tramite lo sviluppo dei punti regionali di scambio e la diminuzione dei costi di interconnessione e, in secondo luogo, incoraggiando l'ITU a proseguire, in vista dell'elaborazione di raccomandazioni appropriate, lo studio del tema della connettività Internet internazionale;

- **sostenere la diffusione** delle tecnologie dell'informazione **nelle piccole imprese** attraverso gli strumenti di credito pubblico;

- **creare un *forum* virtuale di comunicazione tra le varie organizzazioni multilaterali, regionali e bilaterali** di sviluppo, sul tema dei progetti potenziali, sulle fonti e sui meccanismi istituzionali di finanziamento, intensificando, parallelamente, la collaborazione tra le organizzazioni stesse al fine di accrescerne la capacità di fornire assistenza ai Paesi in via di sviluppo riguardo alle politiche che stimolano la crescita delle TIC;

- **incoraggiare i Paesi a realizzare sforzi concreti** per far fronte ai propri impegni di pagamento in adesione alla Convenzione di Monterrey;

- **sostenere** la crescita dei **contributi volontari**.

Sul punto della *governance* - questione rimasta aperta a Ginevra circa la possibilità di individuare nell'ONU l'organismo guida - sono stati riconfermati i princìpi ispiratori espressi nel 2003 circa la multilateralità, la trasparenza e la democraticità come condizioni di base per ripartire equamente le risorse, garantire l'accesso globale, la stabilità e la sicurezza della Rete. A ciò si deve arrivare internazionalizzando la gestione tecnica della Rete. Per questo si è pensato di istituire - raccogliendo l'indicazione emersa a giugno 2005 nell'ultimo Rapporto del WGIG[5], preparatorio al *summit* - un apposito ***Forum* per il governo di Internet,** che costituirà un'occasione di dialogo tra i diversi attori dei governi, del settore privato e della società civile. Il *Forum* si riunirà - almeno inizialmente - a margine di conferenze internazionali realizzate in ambito ONU e farà riferimento alle strutture attualmente coinvolte nel governo di Internet (come l'ICANN), non potendo istituirne di nuove. Non eserciterà inoltre funzione di controllo. Il *Forum* dovrà anche dedicarsi all'esame degli aspetti riguardanti le politiche pubbliche, lo sviluppo, gli usi illegali di Internet e facilitare lo scambio di migliori pratiche e la partecipazione degli attori dei Paesi in via di sviluppo. La prima riunione istitutiva si svolgerà ad Atene nel 2006 e verrà formalmente convocata dal Segretario Generale delle Nazioni Unite.

Riassumendo, sul tema della *governance* di Internet Tunisi ha fissato tre obiettivi principali:

a) la realizzazione di interventi a favore della riduzione del divario digitale, attraverso l'abbassamento dei costi di connessione, e del multilinguismo;
b) la convergenza sulla lotta anti *spam* ed agli usi criminosi della Rete;
c) la legittimazione dei singoli Paesi sulla giurisdizione dei propri nomi a dominio.

[5] Si tratta del già richiamato Gruppo di lavoro sulla *governance* di Internet, istituito in seno al WSIS.

Sul fronte dei diritti umani è stato riconfermato il convincimento del ruolo benefico che il rispetto delle libertà fondamentali svolge per lo sviluppo dei popoli e l'aiuto che in questo senso può venire dall'esistenza di *media* liberi e indipendenti.

L'attuazione e lo sviluppo delle misure individuate dalle due fasi del *summit* continueranno ad essere seguiti e guidati, a livello internazionale, dal Segretariato Generale delle Nazioni Unite che ha il compito di presentare, tramite l'ECOSOC (*Economic and Social Council*), un Rapporto sul lavoro svolto, entro giugno 2006.

V. Bertola[6]

La *governance* di Internet: situazione e prospettive[7]

L'esperienza del WGIG

Le discussioni del WSIS, nell'ambito del processo più generale di riforma delle Nazioni Unite, assumono un ruolo speciale proprio in quanto le tecnologie dell'informazione rappresentano la punta del gigantesco quanto poco visibile *iceberg* sopra descritto, e legato a cambiamenti epocali nella struttura socio-politica del pianeta. In questo ambito, le discussioni del WGIG, essendo focalizzate specificamente su problemi di *governance*, rappresentano la punta della punta.

Il WGIG è stato creato nel novembre 2004 in risposta a una richiesta venuta dal s*ummit* di Ginevra: per la complessità dell'argomento e per la difficoltà di giungere ad una risoluzione comune da parte dei governi partecipanti alle negoziazioni del s*ummit*, si era ritenuto che un gruppo di esperti, formato da rappresentanti dei governi, del settore privato e della società civile partecipanti a titolo personale e nel contempo latori delle diverse posizioni e delle diverse culture della rete, potesse lavorare ad un approfondimento e ad un successivo rapporto che presentasse le diverse opzioni per l'evoluzione della *governance* globale di Internet, con particolare riferimento al problema del controllo sulle poche sue risorse centralizzate, come la *root zone* del *Domain Name System* e le politiche di allocazione degli indirizzi IP.

Il gruppo di lavoro si è riunito fisicamente quattro volte, utilizzando intensamente le comunicazioni elettroniche per l'avanzamento dei lavori tra incontri successivi, e producendo nel contempo una notevole mole di documenti che coprono i vari aspetti di Internet. In questi giorni è stato rilasciato il rapporto finale, che costituirà la base delle negoziazioni intergovernative al terzo comitato preparatorio nel mese di settembre, che dovrebbe poi preludere ai risultati del *summit* di Tunisi. Tutti gli *stakeholder* interessati possono inviare commenti scritti al rapporto entro il 15 agosto. Il processo del WGIG rappresenta in un certo senso uno dei suoi maggiori risultati. All'interno del gruppo di lavoro, tutti i membri erano uguali e tutte le opinioni avevano lo stesso peso, indipendentemente dal fatto che provenissero da un governo o meno. Questo ha permesso, forse per la prima volta su questi argomenti, di avere uno scambio di punti di vista franco e aperto, e quindi di iniziare a costruire una intesa comune tra tutti gli *stakeholder*, anziché perpetuare le forti e sterili contrapposizioni che avevano caratterizzato la discussione nella prima fase del *summit*.

Allo stesso tempo, la dimensione relativamente limitata - 40 membri - ha permesso di raggiungere un consenso e di produrre risultati tangibili, per quanto limitati ad un rapporto con valore consultivo, a differenza di altri ambiti (ad esempio la *Task*

---

[6] L'autore è membro del *Working Group on Internet Governance* delle Nazioni Unite; chairman, *At-Large Advisory Committee*, ICANN e membro del Consiglio di Società Internet. Si ricorda che Società Internet è il Chapter italiano della *Internet Society* che è l'editor mondiale dei protocolli della Rete. Ha inoltre fatto parte del Tavolo di consultazione con la società civile del Ministro per l'innovazione e le tecnologie.

[7] Estratto dell'intervento svolto in occasione del convegno dal titolo indicato, svolto a Roma il 18 luglio 2005 (<http://www.cris-italia.info/cris/articles/art_12031.html>)

Force ICT delle Nazioni Unite) dove a discussioni aperte e di elevato livello non è però stata associata la possibilità di produrre alcun risultato concreto.
In altre parole, il WGIG ha dimostrato che, quando tutti gli *stakeholder* accettano di riconoscere la reciproca legittimità ed il reciproco valore e di collaborare insieme, si possono ottenere risultati concreti anche su temi complessi e che coinvolgono una grande quantità di soggetti estremamente diversi, e si può governare la globalizzazione. Al contrario, quando questa collaborazione non avviene e quando i risultati non sono condivisi, l'unico risultato che si ottiene nel momento in cui si passa all'implementazione è quello di creare nuova conflittualità, impedendo qualsiasi avanzamento concreto, e trasformando le opportunità in problemi.

Il rapporto del WGIG

Il rapporto del WGIG è in realtà doppio: vi è un rapporto vero e proprio, di una ventina di pagine, che contiene il linguaggio e le raccomandazioni formalmente adottati, e vi è poi un rapporto complementare (*Background Report*), di un centinaio di pagine, che contiene una analisi più dettagliata dei vari problemi. Il Rapporto è destinato ai decisori, mentre il rapporto complementare permette di approfondire le questioni legate alle specifiche materie e di contestualizzare le conclusioni del rapporto.

La prima richiesta che era stata fatta al WGIG era quella di definire l'ambito della *governance* di Internet. Il WGIG ha inteso il problema della *governance* della rete in senso ampio, non limitato alla semplice prospettiva (pur importante) di una negoziazione intergovernativa sul controllo di specifiche risorse, ma esteso a problemi fondamentali per il futuro di Internet come lo *spam*, la proprietà intellettuale, l'estensione dell'accesso alla rete, il multilinguismo, solo per nominarne alcuni.

In altre parole, tutto ciò che si fa con Internet ricade almeno in una certa misura nell'ambito della sua *governance* e richiede quindi l'adozione dei principi base del WSIS, ben descritti nell'articolo 48 della Dichiarazione di Principi, ossia la trasparenza, la democrazia, e il multilateralismo inteso in senso lato, ovvero non solo con il coinvolgimento di tutti i governi, ma anche con quello di tutti gli altri *stakeholder*, generalmente raggruppati nelle due categorie del settore privato (commerciale) e della società civile (non commerciale, inclusi gli individui).

Questa considerazione ha fornito il punto di partenza per superare per quanto possibile lo scontro fondamentale tra due concezioni opposte a proposito della *governance* della rete: quella del governo e del settore privato americani, che attualmente controllano Internet e le ICT per la quasi totalità, secondo cui l'autoregolamentazione dell'industria e la liberalizzazione totale dell'iniziativa privata sono le soluzioni da seguire; e quella di numerosi paesi in via di sviluppo, secondo cui Internet deve ritornare nell'alveo della tradizionale regolamentazione internazionale delle telecomunicazioni, con processi decisionali puramente governativi e con politiche economiche di tipo dirigista.

Le considerazioni fatte finora mostrano come nessuno dei due modelli sopra citati possa funzionare nel ventunesimo secolo. La natura sia dei problemi che delle soluzioni riguardanti Internet è complessa e basata su una pluralità di azioni di tipo diverso e in ambienti diversi. La rete è intrinsecamente decentrata; allo stesso tempo, la sua evoluzione è determinata non soltanto dalla *hard law* dei governi, ma anche dalle scelte tecniche e politiche del settore privato e degli stessi utenti, che su Internet hanno

un ruolo attivo, di creatori di contenuti, di applicazioni e di tecnologia, sconosciuto nei sistemi di telecomunicazione precedenti.

E' provato dai fatti che Internet non si può governare per decreto, e che vecchi modelli iperregolamentati, ancora legati all'antico mondo delle telecomunicazioni nazionalizzate, sono inapplicabili e dannosi; allo stesso tempo, la totale libertà finora garantita al settore privato in molti aspetti dell'informatica e della telematica ha quasi sempre portato alla concentrazione del potere di indirizzo dell'ICT nelle mani di pochi grandi soggetti in poche grandi nazioni, e a politiche che antepongono l'interesse economico di pochi ai diritti dei cittadini, allo sviluppo sociale, alla creazione di impresa e di ricchezza diffusa, e, in ultima analisi, al bene della collettività.

Per queste ragioni, un processo efficiente di *governance* della rete dovrebbe prevedere il coinvolgimento di tutti gli *stakeholder* interessati - governi, aziende e utenti finali della rete - ed essere basato sul confronto aperto di idee e di ragioni, in modo da produrre cambiamenti condivisi, distribuiti ed ottenuti in base all'autorevolezza, anziché in base all'autorità. La rete è difatti un prodotto collettivo della somma di interessi individuali, e l'unico modo di indirizzarla è quello di orientare nella stessa direzione tale varietà di interessi.

Di conseguenza, la prima raccomandazione del WGIG è quella di creare un *forum* internazionale per la discussione aperta delle questioni legate alla *governance* di Internet, in cui tutti gli *stakeholder* possano partecipare su basi di uguaglianza, sollevare le questioni ed i problemi che essi percepiscono come più importanti, e discutere come e dove affrontarli.
Se difatti in vari casi - dal commercio globale alla proprietà intellettuale - esistono organizzazioni mondiali che, per quanto ancora basate sul modello dell'età industriale e necessitanti di riforme che le mettano in linea con il modello *multi-stakeholder*, possono ospitare le relative discussioni, in altri casi, dallo *spam* ai diritti dei consumatori, non esiste alcuna organizzazione globale, oppure ne esistono diverse che, non parlandosi tra loro, più che risolvere i problemi tendono ad aggravarli e da creare ulteriori conflitti.

Eppure, quasi nessuna delle organizzazioni esistenti è veramente *multi-stakeholder*; visto che il primo passo per risolvere le questioni di Internet è quello di portare allo stesso tavolo tutte le parti coinvolte, l'esistenza di questo forum potrebbe costituire un significativo passo avanti verso la creazione di modelli di *governance* globale efficaci per il ventunesimo secolo.

Va però sottolineato come questo *forum* non possa in alcun modo diventare il "supremo imperatore" della rete o diventarne il controllore; al contrario, deve essere uno dei nodi di una rete di istituzioni formali ed informali, dalle Nazioni Unite fino alle *mailing list* tecniche, che interagendo tra loro affrontano i problemi. Esso deve quindi essere una entità il cui potere non è basato su normative o su autorità conferite dall'alto, ma sull'autorevolezza riconosciuta dal basso.

Nel rapporto, il *forum* è descritto come un modello leggero di consultazione aperta, più che come un gruppo chiuso che prende decisioni; non è chiaro come questo forum giungerebbe a conclusioni formali, e nemmeno come sarebbe finanziato, come

sarebbe composto e come sarebbero selezionati i suoi membri. Si tratta di aspetti che necessitano di opportuni approfondimenti. Per quanto riguarda invece il problema più spinoso, ovvero la funzione di "supervisione" o controllo finale da parte dei governi, non vi è stato né vi poteva essere consenso. A questo proposito, quindi, il WGIG ha presentato quattro diversi modelli: in due di essi – il numero 1 e il numero 4 – il controllo dei governi sull'adozione finale delle politiche è totale ed abbraccia sostanzialmente l'intero campo delle questioni legate a Internet, dall'infrastruttura fino al controllo del suo uso; nel numero 3, il controllo governativo sarebbe limitato a determinate questioni, ipoteticamente quelle attualmente controllate dal governo americano, ma da definirsi; nel numero 2, invece, non vi sarebbe alcun potere speciale attribuito ai governi, il ruolo speciale del governo americano finirebbe, e il forum *multi-stakeholder* sopra descritto assumerebbe il compito di valutare l'andamento dei vari sistemi di *governance.*

Tutti questi modelli rappresentano un cambiamento rispetto al passato; mentre i modelli 1, 3 e 4 vanno nella direzione di un maggior controllo governativo della rete, il modello 2 va nella direzione di un minor controllo governativo della rete.

A fronte di questi modelli, non si può non completare lo scenario con la dichiarazione rilasciata dal sottosegretario americano Gallagher pochi giorni fa, prima ancora della pubblicazione del rapporto, e che ribadisce l'intenzione americana di mantenere lo *status quo*, e di conservare il potere ultimo di approvazione sulla gestione delle risorse uniche della rete, smentendo le dichiarazioni degli anni precedenti in cui il governo americano manifestava l'intenzione di cedere l'intero controllo ad una entità privata (ICANN). Vi è quindi implicitamente un quinto modello, ovvero lo *status quo*.

Tutti questi modelli saranno oggetto[8] delle negoziazioni nel prossimo *PrepCom,* in vista del *summit* finale; al momento non vi è alcuna certezza su quale sarà il risultato. Infine, le raccomandazioni del rapporto del WGIG sono completate con un invito ad un maggior coordinamento, sia tra le varie istituzioni internazionali, sia a livello regionale e nazionale. In particolare, vi è un esplicito invito all'istituzione di comitati nazionali di gestione della *governance* della rete, che coinvolgano tutti gli *stakeholder,* allo scopo di riportare anche a livello nazionale quei ragionamenti e quei meccanismi di *governance* la cui necessità è stata più volte motivata.

Esiste poi una seconda sezione di raccomandazioni, legate alle questioni che il rapporto individua come priorità fondamentali durante la discussione iniziale, e che sono: l'amministrazione del "*root server system*", i costi di interconnessione internazionale, la stabilità e sicurezza della rete, lo *spam*, le possibilità di partecipazione nella *governance* globale, la costruzione di capacità nei paesi in via di sviluppo, l'allocazione dei nomi a dominio, l'allocazione degli indirizzi IP, i diritti di proprietà intellettuale, la libertà di espressione, la *privacy* e protezione dei dati personali, i diritti dei consumatori, il multilinguismo. Vi sono raccomandazioni sulla maggior parte di queste questioni, anche se non su tutte.

Se per i paesi in via di sviluppo questioni come i costi di interconnessione internazionale - che, rovesciando il modello tradizionale delle telecomunicazioni nazionalizzate, creano un flusso di denaro dai paesi in via di sviluppo a quelli sviluppati, e pesano gravemente sui bilanci degli ISP e sulle possibilità di accesso degli

[8] Si legga ora "sono stati oggetto", poiché l'ultima conferenza preparatoria si è svolta a Ginevra dal 19 al 30 settembre 2005.

utenti finali - e come lo sviluppo di capacità sono fondamentali, la società civile ha insistito soprattutto su questioni come la libertà di espressione, la proprietà intellettuale, la *privacy* e i diritti dei consumatori. Si tratta di argomenti che, senza la società civile, sarebbero probabilmente stati dimenticati, e per i quali il contributo da essa apportato è stato fondamentale. Non vi è qui spazio per affrontare nel dettaglio tutte queste raccomandazioni, che peraltro si limitano necessariamente al livello di principio, anche perché in molti casi non esiste ancora un *forum* in grado di raccoglierle; è probabilmente il *forum* suggerito dal WGIG che dovrà, se creato, farsene carico.

Il testo integrale del Rapporto del WGIG è disponibile al sito <http://www.itu.int/wsis/>.

A - ASPETTI GENERALI DELLA *GOVERNANCE*

I. I soggetti coinvolti

La *governance* di Internet può essere definita come "l'azione collettiva che i governi o gli operatori privati di *network* realizzano per raggiungere accordi da applicare a tutte le attività che vengono svolte tramite l'uso della rete"[9]. Si tratta di accordi, che toccano i punti essenziali della standardizzazione tecnica, delle azioni politiche, delle regole e della soluzione delle controversie. Gli aspetti particolari che compongono il quadro complessivo del governo della rete trovano il loro denominatore comune nell'architettura tecnica della rete Internet, la cui struttura chiarisce quanto è stretto il collegamento tra le decisioni che riguardano i temi squisitamente tecnici e le azioni politiche e quanto un intervento sull'una o sull'altra delle due aree produca effetti simmetrici.

Com'è noto Internet (*Interconnected Network*) è un insieme di reti autonome interconnesse tra loro, una cosiddetta "rete di reti" con la caratteristica dell'unitarietà, che permette a tutti gli utenti di scambiarsi informazioni, indipendentemente dalla rete fisica alla quale sono collegati. Affinché questo avvenga è necessario che alcune funzioni siano gestite centralmente. Ciò è reso possibile grazie all'uso di protocolli per mezzo dei quali tutti i computer collegati sono identificati in maniera univoca da un numero IP (*Internet Protocol*). Le risorse sono invece individuate da un nome, espresso da una stringa di caratteri alfanumerici: il nome a dominio.

Quando si digita l'indirizzo di una risorsa in rete lo si fa richiamando il nome a dominio che è automaticamente "risolto"[10] in un indirizzo IP, cioè nella sequenza numerica che permette di collegarsi realmente alla risorsa.

Secondo criteri convenzionalmente accettati, nella formula più comune[11], un nome a dominio è composto da una successione di tre parole, separate da un punto. La prima parola (da sinistra) è l'acronimo "www", uguale per qualsiasi nome; la terza parola - o estensione - corrisponde ad una sigla standard predefinita ed indica l'area tematica o geografica del sito. Essa è detta *Top Level Domain.* La seconda parola (*Second Level Domain*

---

[9] *Internet governance: the state of play*, contributo della *Syracuse University - Georgia Institute of technology* nell'ambito del progetto *Internet governance project* del 2004, disponibile in <http://www.internetgovernance.org>.

[10] Si definisce risoluzione la conversione della stringa alfanumerica del nome a dominio in sequenza numerica.

[11] Una struttura di questo tipo rappresenta solo una modalità di costruzione del nome a dominio. E' infatti possibile inserire dei livelli aggiuntivi al primo ed al secondo od inserire un diverso acrononimo.

Name) è quella compresa tra l'acronimo "www" e la sua estensione ed è scelta liberamente dal titolare del sito che richiede la registrazione.

L'insieme di questi nomi è organizzato in un sistema detto *Domain Name System* (DNS). Il sistema piramidale, parte da una radice e si articola in domini di primo livello (un dominio è un insieme di nomi) e di livelli sottostanti. I domini di primo livello sono a loro volta distinti in domini "generali" (gTLD, *generic Top Level Domain*) e "nazionali" (ccTLD - *country code Top Level Domain*) ovvero contenenti un'indicazione geografica.[12]

> Esempio di composizione di nome a dominio:
>
> Il nome "www.senato.it" è composto dall'estensione ".it" (*Top Level Domain*), che indica la collocazione geografica della risorsa Internet e dalla parola "senato", corrispondente al *Second Level Domain,* ovvero a quella parte del nome a dominio che il Senato della Repubblica ha scelto liberamente per la registrazione della propria risorsa in rete.

I protocolli di comunicazione sono codici numerici usati dagli elaboratori connessi in rete per renderli compatibili. Il protocollo di comunicazione comune o TCP/IP (*Transmission Control Protocol-Internet Protocol*) rappresenta il protocollo principale di Internet cui si richiamano tutti gli altri protocolli, cosiddetti applicativi, tra cui FTP (*File Transfer Protocol*) che consente il trasferimento dei *file* da un computer all'altro, POP3/SMTP con il quale è possibile scambiare posta elettronica, Telnet che permette di effettuare sessioni interattive con terminali remoti e HTTP che consente l'accesso agli ipertesti (pagine *web*)[13].

L'aspetto della standardizzazione tecnica chiama in causa una serie di organizzazioni, con diverso profilo giuridico, cui è demandato il compito di elaborare le norme di armonizzazione che assicurano la compatibilità dei vari protocolli usati per comunicare in rete.

---

[12] S. TRUMPY, *"Internet Governance" in Italia e nel mondo,* COESIN (Comitato esperti di Internet), Roma, 6 novembre 2000.

[13] Per approfondimenti si veda G. PASCUZZI, *Scoperte scientifiche, invenzioni e protocolli relativi a Internet*, «AIDA», n. 5 (1996), pag. 162.

La collocazione e l'assegnazione delle risorse di rete consiste nell'attribuzione e nella registrazione dei nomi a dominio già richiamati (stringhe alfanumeriche associate ad un codice numerico - IP o protocollo Internet)[14] per mezzo dei quali è possibile collegarsi ad un indirizzo Internet. E' questo, senza dubbio, uno degli aspetti più delicati del governo della rete globale del quale si occupano generalmente organizzazioni diverse da quelle cui compete la definizione degli standard. Esiste tuttavia qualche eccezione come ad esempio quella costituita dall'IEEE (*Institute of Electrical and Electronics Engineer*) e dall'ITU (*International Telecommunication Union*), che studiano comunque i due aspetti incaricando diversi dipartimenti. Le organizzazioni di maggiore rilievo in questo settore sono l'ICANN (*International Corporation for Assigned Names and Numbers*), lo IEFT *(Internet Engineering Task Force*) e il NANC *(North American Numbering Council).*

Per quello che attiene all'esame degli interventi politici, l'attenzione va rivolta soprattutto al monitoraggio dell'applicazione delle norme e alla risoluzione delle controversie.

Prima di parlare dei numerosi attori che rivestono ruoli importanti nel controllo della rete, è bene operare una distinzione tra le organizzazioni che vi sono coinvolte. La prima suddivisione va fatta tra organizzazioni governative e non governative. Quelle governative sono ulteriormente suddivisibili in organizzazioni con rappresentatività mondiale o limitata. La limitazione può consistere nella riserva di partecipazione a Stati che appartengano a precise aree geografiche ovvero che abbiano un determinato *status* economico.

1. Organizzazioni governative a rappresentanza universale

Le organizzazioni di questo tipo comprendono anzitutto l'ONU con le sue articolazioni interne. Dalla fine della seconda guerra mondiale, infatti, le Nazioni Unite sono sempre state coinvolte nella questione della regolamentazione di Internet. Oltre agli aspetti generali, l'ONU ha seguìto, nel corso del tempo, attraverso le proprie agenzie, anche questioni particolari collegate al tema della *governance* della rete. Ne sono un esempio la WIPO (*World Intellectual Property Organization*), per quanto attiene alla tutela della proprietà intellettuale, e l'ITU (*International Telecommunication Union*), per la gestione di alcuni aspetti tecnici. Altri

[14] Per approfondimenti si veda G. PASCUZZI, op. cit.

temi, come il commercio o l'educazione e la libertà di espressione, sono seguiti rispettivamente dal WTO (*World Trade Organisation*) e dall'UNESCO (Organizzazione delle Nazioni Unite per l'Educazione, la Scienza, la Cultura e la Comunicazione).

2. Organizzazioni governative a rappresentanza limitata

Come già ricordato queste organizzazioni non hanno una risonanza globale, ma risultano rappresentative solo di una parte del mondo in rete. Nei processi decisionali, quindi, saranno coinvolti solo alcuni Stati, scelti in base all'appartenenza ad una certa area geografica oppure perché rispondenti a precisi parametri economici. In questa categoria rientrano - per citarne solo alcuni - l'OCDE (*Organisation de coopération et de développement économiques*), il G8, l'Unione europea e l'APEC (Cooperazione Economica dei Paesi dell'Asia e del Pacifico). Tutte sviluppano regole cui sono chiamati ad aderire i soli Stati membri.

3. Organizzazioni non governative

Un numero considerevole di temi legati al governo della rete sono affrontati da organizzazioni non istituzionali riconosciute però ufficialmente. Tra quelle di maggiore rilievo sono da menzionare l'ICANN (*International Corporation for Assigned Names and Numers)* assieme alle sue organizzazioni di supporto, allo IETF (*Internet Engineering Task Force*) e al W3C (*World Wide Web Consortium*). L'ICANN si è costituita in California nel 1988, ed è collegata ufficialmente al Dipartimento del Commercio degli Stati Uniti tramite un *Memorandum of Understanding.* E' competente per l'assegnazione degli indirizzi Internet IP. L'IETF è invece chiamato a risolvere problemi tecnici di funzionamento della rete mentre il W3C definisce gli standard del *web* ed individua soluzioni che consentano l'accessibilità di Internet ai disabili. Altri enti coinvolti nella *governance* sono l'ISC (*Internet Systems Consortium),* l'ISOC (*Internet Society*), lo IAB (*Internet Architecture Board*) e l'ARIN (*American Registry for Internet Numbers*), così come vanno anche menzionati il NANOG (*North American Network Operators Group*, lista di discussione, distribuita via *e-mail,* usata per lo scambio di avvisi ed informazioni diretta agli operatori dei servizi Internet ed un certo numero di altri enti che operano in rappresentanza della società civile e che forniscono il loro contributo alla definizione di norme e di *standard*) e l'ASTA (*Anti Spam Technical Alliance*, che include, tra i

suoi membri l'American Online, la British Telecom, la Comcast, la EarthLink, la Microsoft, la Yahoo). Per concludere va detto che, in alcuni casi, gli stessi governi nazionali sono da considerare come attori multilaterali, in quanto le loro decisioni possono influenzare globalmente il governo della rete. E' questo il caso del già richiamato Dipartimento del Commercio USA (si veda ICANN) o della Commissione federale per le comunicazioni o del Dipartimento della giustizia e del Dipartimento della sicurezza nazionale.

4. Schede illustrative sulle organizzazioni

Organizzazioni governative

La **WIPO**, istituto specializzato dell'ONU, è un'organizzazione intergovernativa che ha il compito di promuovere in tutto il mondo la tutela della proprietà intellettuale attraverso l'elaborazione di trattati internazionali e con azioni di cooperazione finalizzate a garantire assistenza tecnica ai Paesi in via di sviluppo. La WIPO riveste una posizione di assoluto rilievo per la tutela dei marchi e dei segni distintivi che possono coincidere o venire lesi da un nome a dominio. L'organizzazione collabora anche con i privati per la risoluzione delle controversie internazionali, nonché con altre organizzazioni internazionali. Si consideri a questo proposito l'Accordo con il WTO entrato in vigore il 1° gennaio 1996 con il quale è stabilita la collaborazione delle due organizzazioni sulla questione dell'applicazione delle norme sulla tutela della proprietà intellettuale (TRIPS). A questo, nel 1998, è seguito il lancio di un'iniziativa comune di sostegno all'applicazione della normativa, rivolta ai paesi in via di sviluppo. Per quanto riguarda specificamente la *governance* di Internet si ricorda che presso la WIPO è istituito un Centro di arbitraggio internazionale per la risoluzione delle controversie che riguardano l'assegnazione dei nomi a dominio.

Per approfondimenti si veda <http://www.wipo.org>.

Sono disponibili, inoltre, i trattati (linkabili) amministrati dalla WIPO, il testo della convenzione istitutiva, il testo dell'Accordo con l'ONU, il testo dell'accordo con il WTO (si veda <http://www.wipo.int/treaties/fr/>).

L'**IEEE** (*Institute of Electrical and Electronics Engineer*) è stato fondato nel 1884 da Edison e Bell. Fra le sue attivita' più note si annoverano la definizione di *standard* in campo elettronico ed elettrico, l'organizzazione di conferenze a livello mondiale e la pubblicazione di prestigiose riviste tecnico-scientifiche. Attualmente l'organizzazione conta più di 370.000 iscritti, distribuiti in 10 regioni geografiche. Conta anche l'iscrizione di 50.000 studenti, organizzati in circa 1100 *student branches*.

Per approfondimenti si veda < http://www.ieee.org>.

L'**ITU** (*International Telecommunications Union*) è la più antica organizzazione intergovernamentale del mondo. Ha competenza nella gestione di tutte le attività ed i servizi attinenti alle tecnologie di telecomunicazione. Costituitasi nel 1865 con il nome originario di "Convenzione Telegrafica Internazionale" è divenuta, nel 1934, la *International Telecommunications Union* seguendo l'intera evoluzione della storia delle telecomunicazioni, dal telegrafo al telefono, fino alle trasmissioni radio, via etere, su cavo o tramite i recenti sistemi ottici e satellitari. Nel 1947 è diventata un'agenzia specializzata delle Nazioni Unite che abbraccia la quasi totalità dei paesi industrializzati del mondo intero. Collabora con diverse organizzazioni europee come il CEN (Comitato Europeo di Normalizzazione) e l'ETSI (*European Telecommunications Standardization Institute*) ed internazionali (ISO - *International Organization for Standardization*). Nell'ambito delle iniziative finalizzate allo sviluppo della società dell'informazione l'ITU ha partecipato attivamento allo svolgimento del WSIS.

Per approfondimenti si veda < http://www.itu.org>

<http://www.itu.int/osg/spu/wsis-themes/ict_stories/index.html>.

Il **WTO** *(World Trade Organisation)* è l'organizzazione mondiale del Commercio. Nasce nel 1994 a Marrakech a completamento dell'*Uruguay Round* (1986-1994) e diviene operativa nel 1995. Raccoglie l'eredità del *General Agreement on Tariffs and Trade* (GATT) ed è un'istituzione nata per regolare il processo di liberalizzazione commerciale iniziato nel secondo dopoguerra. Il processo decisionale del WTO si sviluppa in tre livelli distinti di creazione del consenso. Il primo è rappresentato dal supremo organo decisionale, la Conferenza ministeriale[15], che si riunisce almeno una volta ogni due anni. Il secondo livello riguarda il Consiglio generale, l'organo di regolamentazione delle controversie[16] e quello di esame delle politiche commerciali che sono in realtà fusi nel Consiglio generale del quale costituiscono le diverse articolazioni corrispondenti a distinte funzioni. Il terzo livello include il Consiglio del commercio delle merci, il Consiglio del commercio dei servizi e il Consiglio che esamina gli aspetti dei diritti di proprietà intellettuale che riguardano il

[15] Le riunioni della Conferenza ministeriale svolte sinora sono state quelle di Singapore nel 1996, di Ginevra nel 1998, di Seattle nel 1999, di Doha nel 2001 e di Cancun nel 2003.

[16] In seno a questo si distinguono i "gruppi speciali" incaricati di regolamentare le controversie e composti da esperti e l'organo di appello.

commercio (Consiglio degli ADIPC o TRIPS). In seno al Consiglio generale esistono poi numerosi comitati specializzati, gruppi di lavoro e gruppi di esperti incaricati di analizzare aspetti specifici e particolari. Vi sono infine due altri organi sussidiari che si occupano dei temi affrontati dagli accordi multilaterali (e che non sono stati sottoscritti da tutti i membri del WTO). Questi rendono conto regolarmente della loro attività al Consiglio generale. Il quarto livello di ricerca del consenso riguarda gli organi di base, ovvero organi sussidiari di ciascun consiglio di livello superiore. Per esempio al Consiglio per il commercio delle merci afferiscono ben undici comitati che si occupano ciascuno di un aspetto specifico (agricoltura, accesso ai mercati, sovvenzioni, misure antidumping, ecc). Anche nei comitati è assicurata la rappresentanza di tutti gli stati membri. Il quinto livello è quello che si concretizza attraverso le riunioni informali dei capi delegazione o di altri gruppi di delegazioni. E' questo il momento più interessante della ricerca del consenso che spesso si realizza proprio durante questo tipo di consultazioni che giocano un ruolo cruciale per raggiungere accordi votati nelle sedi proprie. Le questioni più delicate vengono affrontate da gruppi ristretti di persone. E' ricorrente il caso di un presidente di delegazione che conduce personalmente delle negoziazioni e tenta di raggiungere compromessi con le delegazioni dei vari paesi prese singolarmente, oppure di piccoli gruppi scelti tra le rappresentanze maggiormente interessate agli aspetti in discussione. Il punto delicato di questo tipo di consultazioni è la trasparenza, da assicurare tramite un'informazione adeguata fornita a tutte le delegazioni, anche quelle non coinvolte direttamente nei colloqui. Secondo alcuni osservatori esterni questo punto è centrale e non del tutto risolto.

L'**UNESCO** è l'Organizzazione delle Nazioni Unite per l'Educazione, la Scienza, la Cultura e la Comunicazione. E' stata fondata a Parigi il 16 novembre 1945. Nel 1990, al suo interno, è stato creato il settore dell'informazione e della comunicazione con sede principale a Parigi ed uffici periferici in 27 Paesi. La finalità del settore è la promozione della libera circolazione delle idee attraverso le parole e le immagini ed in particolare anche facilitando l'accesso alle tecnologie informatiche. Il settore comunicazione partecipa all'attuazione di numerosi progetti di dimensione interregionale, regionale o nazionale in diverse aree geografiche come l'Africa, l'Asia, gli Stati arabi, il Pacifico, l'America Latina e i Caraibi. Collabora inoltre con numerose

altre agenzie delle Nazioni Unite, ovvero con agenzie non governative internazionali e regionali. L'UNESCO contribuisce all'implementazione del Piano di azione, elaborato durante la prima fase del WSIS (*World Summit on the Information Society*), svoltasi a Ginevra nel 2003. Si tratta dell'UNESCO WSIS *Action Directory* con la quale si intende sostenere lo sviluppo di una società dell'informazione aderente ai principi della libertà di espressione, dell'accesso universale, della non discriminazione, della salvaguardia della cultura della diversità. In particolare nell'area dello sviluppo delle tecnologie informatiche le azioni dell'UNESCO comprendono la costruzione di un portale per il *software* libero nonché la realizzazione di un partenariato per incoraggiare l'uso di questo nuovo tipo di *software* che è considerato molto importante per la crescita dei processi formativi e dell'educazione. In preparazione del secondo *summit* del WSIS, che si è tenuto Tunisi a novembre 2005, l'UNESCO sta inoltre predisponendo una serie di eventi atti a focalizzare i temi di maggiore rilievo riguardanti lo sviluppo della società dell'informazione. A tale proposito si sono svolti dal 1° gennaio 2005 quattro *meeting* durante i quali sono stati affrontati i temi della libertà d'espressione, del multilinguismo e multiculturalismo e degli aspetti critici che influiscono sullo sviluppo della diffusione delle ICT. Si ricorda, infine, che dal 1998, in seno all'UNESCO, è stato istituito un osservatorio permanente sulla società dell'informazione che ha dei punti di monitoraggio regionale in Africa, negli Stati arabi, nell'area dell'Asia-Pacifico, in America Latina/Caraibi e nelle aree geografiche di lingua portoghese.

Per i documenti dei *meeting* si veda

<http://portal.unesco.org/ci/en/ev.php-URL_ID=17637&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

Per altri approfondimenti si veda < http://www.un.org>.

Per il settore della comunicazione si veda

<http://portal.unesco.org/ci/fr/ev.php-URL_ID=1645&URL_DO=DO_TOPIC&URL_SECTION=201.html>.

Per il tema della *e-governance* si veda

<http://portal.unesco.org/ci/fr/ev.php-URL_ID=3038&URL_DO=DO_TOPIC&URL_SECTION=201.html>

ed in particolare ***Renforcement des capacités pour l'e-gouvernance (News).***

Per il tema del portale *free software* si vedano

<http://www.unesco.org/cgi-bin/webworld/wsisdirectory/cgi/page.cgi?g=Detailed%2F108.html&d=1>;

<http://www.unesco.org/cgi-bin/webworld/wsisdirectory/cgi/page.cgi?g=Detailed%2F121.html&d=1>.

L'**OCDE** (*Organisation de coopération et de développement économiques*), che raggruppa oggi 30 paesi membri, nasce il 14 dicembre 1960, con la firma della Convenzione da parte di venti Paesi fondatori. In realtà, grazie all'attività di cooperazione svolta dal Centro per la cooperazione con i Paesi non-membri, l'OCDE è oggi in relazione con un'area geografica molto più vasta che coinvolge oltre 70 Paesi, ONG ed altre forme di aggregazione rappresentative della società civile.

L'OCDE gioca un ruolo molto importante riguardo all'attuazione di politiche di buon governo nel settore pubblico e privato, finalizzate in special modo a mantenere competitivi i settori chiave dell'economia dei governi dei Paesi membri. L'organizzazione promuove la cooperazione tramite l'adozione di decisioni e raccomandazioni, strumenti elaborati dal Consiglio, adottati internazionalmente, sulla base dei quali viene promossa l'adozione di nuove regole tramite la firma di accordi multilaterali. La creazione del consenso avviene attraverso un dialogo continuo che si realizza anche con i Paesi non membri attraverso i *forum* internazionali a tema (*Global Forum*). Sul tema delle politiche in materia di telecomunicazioni e di servizi opera, in seno all'organizzazione, un gruppo di lavoro *ad hoc*, il GTPTSI. Questo gruppo sostiene lo scambio di esperienze tra i membri dell'OCDE e analizza l'evoluzione delle infrastrutture della comunicazione, soffermandosi anche specificamente sugli aspetti legati ad Internet. Il Gruppo procede periodicamente ad un rilevamento comparativo dei prezzi dei servizi delle telecomunicazioni e di Internet ed all'analisi delle ricadute economiche e sociali dell'uso della rete. Assieme ad altre organizzazioni, l'OCDE ha fortemente contribuito a rilevare gli aspetti critici delle politiche pubbliche legate ad Internet quali quelli della sicurezza, della protezione della *privacy*, dell'accesso universale, della difesa dei consumatori, del commercio elettronico.

Per approfondimenti si veda il sito

<http://www.oecd.org/document/40/0,2340,fr_21571361_34590630_34682216_1_1_1_1,00.html>

ed i documenti di studio allegati in documentazione.

Il **G8** non si può annoverare propriamente tra le organizzazioni internazionali, non esistendo alcun trattato istitutivo che ne disciplini la struttura, le modalità di riunione, i fini e gli scopi perseguiti, nonché le procedure attraverso le quali adottare le risoluzioni finali. Si tratta di un vertice, a cadenza periodica, dove i Capi di Stato e di Governo degli Stati maggiormente industrializzati cercano di giungere ad un coordinamento effettivo delle politiche internazionali tra gli Stati partecipanti. Le intese raggiunte non sono giuridicamente vincolanti, ma danno notevole impulso alle attività istituzionali svolte dalle diverse Organizzazioni Internazionali, amplificandone la funzione di indirizzo politico ed economico. La prassi seguita per le singole riunioni dei vertici, prevede una rotazione annuale tra i Paesi aderenti.

Fino al 1998 partecipavano agli incontri anche i Ministri finanziari e i Ministri degli affari esteri. In seguito, al fine di puntualizzare in anticipo i temi all'ordine del giorno, i due gruppi di Ministri decisero di incontrarsi subito prima della riunione del vertice. Tali riunioni interministeriali, di natura preparatoria, si sono recentemente intensificate.

L'agenda del vertice è frutto del lavoro portato avanti da diversi soggetti, quali i rappresentanti personali dei capi di Stato e di Governo, noti anche come *"sherpa"*, (alti funzionari degli Stati membri che rappresentano personalmente il loro Esecutivo); i *"sous-sherpa"* (funzionari di alto livello specializzati in affari esteri e in questioni finanziarie) ed infine i direttori politici dei Ministeri degli esteri, per i temi di politica estera. Gli *"sherpa"* compiono i lavori preparatori al vertice attraverso riunioni che si svolgono nel corso dell'anno. Essi predispongono, oltre all'agenda, anche il progetto del comunicato finale. Tra una riunione e quella successiva, essi restano in stretto contatto al fine di definire le priorità e le compatibilità tra le esigenze nazionali e quelle degli altri Paesi. Gli *sherpa* sono coloro che sostengono il peso delle trattative e devono il loro nome proprio all'impegnativo ruolo che rivestono; quest'appellativo, infatti, caratterizza e richiama i portatori nepalesi che accompagnano le scalate dell'Himalaya. L'individuazione dello *sherpa* avviene in base a criteri diversi per ogni Paese; in Italia tale ruolo, che prende il nome di Rappresentante personale del Presidente del Consiglio Italiano per il G8, è conferito, tradizionalmente, ad un diplomatico di rango elevato che più volte generalmente ricopre anche l'incarico di Consigliere diplomatico del Presidente del Consiglio. Il progressivo allargamento

dell'agenda dei vertici ha comportato la formazione di gruppi di esperti con professionalità *ad hoc*, quali, ad esempio il *working group* o la *task force*. Essi hanno il compito di assistere l'attività di preparazione del vertice riguardo a specifiche materie e di verificarne gli esiti. La Comunità Economica Europea, per le materie di sua competenza, ha iniziato a prendere parte ai Vertici sin dal *summit* di Londra del 1977.

L'**Unione europea** è un'istituzione sovranazionale che nasce alla fine della seconda guerra mondiale. Riunisce i Paesi europei democratici che si riconoscono nell'impegno comune di realizzare uno spazio di pace e di prosperità condivise. Inizialmente, l'UE comprendeva solo sei Paesi: il Belgio, la Germania, la Francia, l'Italia, il Lussemburgo e i Paesi Bassi. La Danimarca, l'Irlanda e il Regno Unito hanno aderito nel 1973, la Grecia nel 1981, la Spagna e il Portogallo nel 1986, l'Austria, la Finlandia e la Svezia nel 1995. Nel 2004 è avvenuto il più grande allargamento mai realizzato con l'adesione contemporanea di dieci nuovi Paesi. Gli Stati membri - ormai divenuti 25 - hanno creato una serie di istituzioni comuni a cui delegano una parte della loro sovranità in modo che le decisioni su questioni specifiche di interesse comune possano essere prese democraticamente a livello europeo.

Le istituzioni dell'UE sono cinque, ognuna delle quali svolge un ruolo specifico**:**

- Il Parlamento europeo (eletto dai cittadini degli Stati membri);
- Il Consiglio dell'Unione europea (che rappresenta i governi degli Stati membri);
- La Commissione europea (motore ed organo esecutivo);
- La Corte di giustizia (che garantisce la conformità con il diritto);
- La Corte dei conti (che verifica che la gestione del bilancio dell'Unione europea sia sana e corretta).

A tali istituzioni si affiancano altri cinque organi importanti:

- Il Comitato economico e sociale europeo (che è il portavoce delle opinioni della società civile organizzata su questioni economiche e sociali);
- Il Comitato delle regioni (che è il portavoce delle opinioni degli enti regionali e locali);
- La Banca centrale europea (che è responsabile della politica monetaria e della gestione dell'euro);

- Il Mediatore europeo (che tratta le denunce presentate dai cittadini contro i casi di cattiva amministrazione nell'azione di un'istituzione o di un organo dell'Unione europea);
- La Banca europea per gli investimenti (che contribuisce al conseguimento degli obiettivi dell'Unione europea tramite il finanziamento di progetti di investimenti).

Tutte le decisioni e le procedure dell'UE hanno la loro base giuridica nei trattati che sono approvati da tutti i Paesi membri.

L'**APEC** (*Asia-Pacific Economic Cooperation*), creata nel 1989, è diventata il principale strumento regionale di promozione del libero scambio e di attività concrete di cooperazione economica dei Paesi dell'area dell'Asia-Pacifico. La Regione comprende diciotto Stati membri, molto diversi tra loro per economia, struttura politica e storia. Il *forum* APEC si propone il raggiungimento di tre obbiettivi principali: la liberalizzazione degli scambi e degli investimenti; l'agevolazione degli stessi; la cooperazione economica e tecnica. I membri del *forum* si sforzano affinché non siano attuate politiche economiche protezionistiche e, contemporaneamente, auspicano di contribuire ad individuare uno strumento valido per risolvere i contenziosi economici attuali e futuri tra paesi che operano nel commercio internazionale.

L'**Unione Africana (UA),** che riunisce 53 Stati del continente africano, nasce dalla trasformazione dell'OUA, il 26 maggio 2001, data dell'entrata in vigore dell'Atto costitutivo. La firma dell'Atto è l'evento conclusivo di un lunghissimo processo evolutivo che ha caratterizzato la storia dell'Africa degli ultimi decenni. Si ricorda che verso la fine degli anni '50 per l'Africa sono stati elaborati numerosi programmi internazionali, volti a favorirne lo sviluppo economico e sociale e ad accompagnarne l'indipendenza, man mano proclamata dai 53 Paesi che ora compongono l'Unione. Nei cinquanta anni successivi i vari Paesi africani hanno gradualmente preso coscienza delle loro potenzialità di sviluppo e si sono indirizzati verso la creazione di un fronte unitario. L'UA sostituisce quindi l'OUA (Organizzazione per l'Unità Africana) secondo le modalità stabilite dal Vertice dei Capi di Stato Africani tenutosi a Lusaka (Zambia) dal 9 all'11 luglio 2001. Modellata istituzionalmente sull'Unione Europea, l'Unione Africana

esplica la sua attività attraverso la Conferenza dell'Unione, il Consiglio esecutivo, il Parlamento panafricano, la Corte di giustizia, la Commissione, il Comitato dei Rappresentanti permanenti, il Consiglio economico, sociale e culturale, i comitati tecnici specializzati e le istituzioni finanziarie.

Il **Partenariato Euromediterraneo** consiste in un'iniziativa politica di integrazione tra i 12 paesi che si affacciano sul bacino del Mediterraneo: Algeria, Malta, Cipro, Turchia, Israele, Egitto, Territori Autonomi Palestinesi, Giordania, Libano, Marocco, Siria e Tunisia, legati all'Unione Europea da Accordi di vario tipo ed intensità. Dopo 20 anni di intensi scambi commerciali su base bilaterale, questi 12 paesi del Mediterraneo ed i 15 Stati membri dell'Unione Europea, in seno alla conferenza di Barcellona (27-28 novembre 1995) hanno dato vita ad un vero e proprio "Spazio Euromediterraneo", una politica globale che riguarda tutti questi Paesi concepiti come un unico insieme politico geografico. La peculiarità del Partenariato Euro-Mediterraneo risiede nella circostanza che è realizzato su due livelli complementari: uno a carattere regionale e l'altro a carattere bilaterale, la cui politica si concretizza attraverso la stipulazione di Accordi di associazione e di cooperazione tra i Paesi dell'UE e quelli dell'area mediterranea.

Attualmente i Paesi che hanno già firmato tali accordi sono: Tunisia (firmato nel 1995 ed entrato in vigore nel 1998), Israele (firmato nel 1995 ed entrato in vigore nel 2000); Marocco (firmato nel 1996 ed entrato in vigore nel 2000); Territori Autonomi Palestinesi (firmato ed entrato in vigore nel 1997); Giordania (firmato nel novembre 1997 ed entrato in vigore nel 2002) e Libano (firmato nel giugno 2002 ed entrato in vigore il 1° marzo 2003).

Il **MERCOSUR** (*Mercado Comun del Sur*) è l'accordo cui il primo gennaio 1995 hanno aderito Argentina, Brasile, Uruguay e Paraguay con l'obiettivo di realizzare la libera circolazione di beni, servizi e fattori produttivi tra gli Stati membri, la fissazione di una tariffa esterna comune, il coordinamento delle politiche macroeconomiche e settoriali per assicurare una libera e regolare competizione tra i sistemi economici degli Stati membri e l'impegno alla modifica delle legislazioni interne in contrasto con il processo di integrazione.

Il **NAFTA** (*North American Free Trade Agreement*) consiste in un accordo di libero scambio stipulato da Stati Uniti, Canada e Messico, modellato sul già esistente accordo di libero commercio tra Canada e Stati Uniti (Fta) firmato alla fine del 1993, ed entrato in vigore il primo gennaio del 1994. L'aspetto che maggiormente caratterizza il Nafta è sicuramente legato alla progressiva eliminazione di tutte le barriere tariffarie fra i Paesi che aderiscono all'accordo.

Organizzazioni non governative

L'**ICANN** (*International Corporation for Assigned Names and Numbers)* è un'associazione internazionale *non-profit* avente la responsabilità di assegnare gli indirizzi IP (*Internet Protocol*) e l'identificatore di protocollo e di gestire il sistema dei nomi a dominio di primo livello (*Top-Level Domain*) generici (gTLD) e del codice internazionale (ccTLD) nonché i sistemi di *root server*. Si tratta dell'organizzazione più importante in tema di collocazione ed assegnazione delle risorse disponibili in Internet. Prima del 1998, anno della costituzione per decisione del Governo USA, la collocazione e la registrazione degli indirizzi Internet (il cosiddetto sistema DNS)[17] era affidata ad altre organizzazioni tra cui IANA (*International Assigned Numbers Authority*). All'ICANN si deve la liberalizzazione delle attività di registrazione dei nomi a dominio di primo livello (TLD, *Top Level Domain*) come ".org", ".com" e ".net"[18]. Questo processo ha fatto sì che non esistesse più una singola Authority di registrazione, ma che si costruisse un vero e proprio sistema (SRS, *Shared Registrations System*) che comprende le diverse *Registration Authority* nazionali. L'ICANN ha inoltre creato un *forum* di arbitraggio internazionale sui contenziosi nell'attribuzione dei nomi a dominio di primo livello (quelli generali, cioè privi di indicazione geografica).

L'**IETF** *(Internet Engineering Task Force*) è un ente *non-profit* che, dal 1986, cura la definizione e lo sviluppo degli *standard* e dei protocolli Internet. Ha una composizione mista che comprende tecnici progettisti di rete, operatori, venditori e ricercatori interessati all'evoluzione della rete.

Per approfondimenti si veda <www.ietf.org>.

[17] *Domain Name System.*

[18] Nel 2000 ICANN ha presentato sette nuovi gTLD: .aero, .biz, .coop, .info, .museum, .name e .pro.

Il **W3C** (*World Wide Web Consortium*) è un consorzio, nato nel 1994 con lo scopo di definire gli *standard* del *web*. Si tratta di un ente senza fini di lucro, autofinanziato, che conta ad oggi più di 500 membri. Nel finanziamento - oltre ai membri - intervengono anche organizzazioni esterne, per realizzare progetti specifici. La finalità dell'ente è quella di "portare il *Web* al massimo del suo potenziale, sviluppando protocolli comuni in grado di promuovere la sua evoluzione e assicurare la sua interoperabilità". Tra gli *standard* più noti creati dal W3C è il linguaggio HTML, cioè quello utilizzato per creare i cosiddetti "ipertesti". Il W3C considera possibile la diffusione massima del *web* solo con il raggiungimento di alcune tappe, quali la costruzione del cosiddetto "*Web* semantico" e di un *Web* accessibile a tutti. Il Consorzio ha iniziato a camminare in questa direzione sin dal 1997 con il lancio dell'iniziativa "*Web Accessibility Initiative*" (WAI).

Per approfondimenti si vedano <http://www.w3c.it> e l'articolo di L. PUCCI, *Le linee guida per l'accessibilità del World Wide Web Consortium*, in P. RIDOLFI (a cura di), *I disabili nella società dell'informazione*, Milano, Angeli, 2002.

L'**ISC** (*Internet Systems Consortium*) è un'organizzazione senza fine di lucro, che ha il compito di coordinare il *server* generale della *root* e di predisporre il *software* principale per implementare il protocollo DNS (*Domain Name System*). I *Root Name Server* sono centrali nel funzionamento del sistema DNS. Nel mondo esistono solo 13 *Root Name Server* globali, chiamati da *a.root-servers*.net fino a *m.root-servers.net.* In Europa ne esistono solo due, uno in Gran Bretagna ed uno in Svezia. ISC ha scoperto ed adottato un sistema che permette di replicare i *Root Name Server* in modo da renderli più accessibili a località fisicamente lontane dai 13 *Root Server* globali.

Per approfondimenti si veda <http://www.isc.org>.

L'**ISOC** *(Internet Society*) è un'organizzazione internazionale non governativa volontaristica che si occupa della crescita e dell'evoluzione di Internet. In particolar modo affronta il tema della ricaduta sociale, politica e tecnica conseguente all'uso della rete. Nel 1999 si è costituita la sezione italiana dell'organizzazione, *Società Internet*, che si occupa della diffusione della cultura Internet sul territorio nazionale.
Per approfondimenti si veda <http://www.isoc.org>.

Lo **IESG** (*Internet Engineering Steering Group)* è un gruppo di lavoro dell'ISOC che cura l'organizzazione tecnica delle attività dello IEFT ed responsabile del processo di formazione degli *standard* le cui specifiche tecniche deputato ad approvare in via definitiva.
Per approfondimenti si veda <http://www.iesg.org>.

Lo **IAB** (*Internet Architecture Board*) è una commissione consultiva dello IETF alla quale sono riconosciute diverse attribuzioni: conferma le cariche di presidente dello IEFT e dei direttori di area dello IESG; supervisiona l'architettura dei protocolli e delle procedure di Internet; organo di appello per le decisioni contestate dell'IESG (di cui nomina i membri scelti tra una rosa di candidati proposti dall'IEFT); coordina l'edizione e la pubblicazione della serie di documenti RFC (*Request for Comments*) nonché l'amministrazione e l'assegnazione dei protocolli IETF; rappresenta ufficialmente lo IEFT nelle relazioni con organizzazioni esterne del *world-wide Internet*; elabora documenti di indirizzo per l'ISOC concernenti questioni tecniche; seleziona i candidati alla presidenza dell'IRTF (*Internet Research Task Force*).
Per approfondimenti si veda <http://www.iab.org>.

L'**ISO** (*International Standardization Organization*) è la prima organizzazione internazionale che produce norme di standardizzazione applicate in tutto il mondo. Le norme ISO - attualmente 15.036, raccolte in collezione - sono elaborate ricercando il più largo consenso possibile Giuridicamente l'ISO è una federazione di organismi nazionali di normalizzazione di 149 Paesi compresi in tutte le regioni del mondo ed individuati negli organismi di standardizzazione di maggiore rilievo di ogni paese. Tutti i membri partecipano alla stesura delle norme in collaborazione con il Segretariato generale e con il sostegno di 3.000 gruppi tecnici di lavoro incaricati di redigere concretamente le norme. I membri dell'ISO nominano inoltre delle delegazioni nazionali presso i comitati di normalizzazione. Globalmente circa 50.000 esperti contribuiscono ogni anno ai lavori dell'organizzazione. L'ISO coopera con molte altre organizzazioni specializzate nel settore della normalizzazione internazionale quali la CEI (*Commission électrotecnique internationale*) e l'ITU (*International Telecommunication Union*) per quanto riguarda il settore delle tecnologie dell'informazione. L'ISO ha inoltre realizzato un partenariato strategico con il WTO per promuovere un sistema mondiale di equo e libero scambio. L'organizzazione collabora inoltre con la maggior parte delle agenzie specializzate dell'ONU.

Per la struttura dell'organizzazione si veda
<http://www.iso.org/iso/fr/aboutiso/isostructure/isostr.html>.

II. L'assegnazione dei nomi di dominio. Cenni storici sull'evoluzione del sistema di gestione centralizzato internazionale[19]

L'esigenza di creare una sede centralizzata per amministrare globalmente la telefonia e le trasmissioni via cavo viene percepita già a partire dal 1865, anno in cui nasce l'ITU (*International Telecommunication Union*), che permetterà di gestire la comunicazione tra le reti telegrafiche sorte un po' in tutto il mondo. Per le reti di telecomunicazione, dunque, questa necessità di centralismo appare subito chiara. Così non è stato per Internet la cui diffusione è apparsa per diverso tempo agli operatori delle telecomunicazioni dettata da una scelta del mercato. Internet nasce come una realtà localizzata sia rispetto all'area geografica sia rispetto al *target* di utenza. Si tratta infatti di un progetto nato negli USA e finanziato in grossa parte dalla DARPA (*Defense Advanced Research Project Agency*). I finanziamenti statali americani erano anche destinati ad una infrastruttura di trasmissione: la NSF *(National Science Foundation).* In questa prima fase di sviluppo della rete, che parte dagli anni '80 e termina nel 1992, la gestione centralizzata fu di competenza di due organismi, anche essi finanziati dal governo statunitense. Si trattava di IETF *(Internet Engineering Task Force*) per la standardizzazione tecnica e di IANA *(Internet Assigned Numbers Authority*) per l'allocazione delle risorse. La catena degli organismi regolatori e di quelli sovvenzionatori si identificava semplicemente in IANA-NSF/DARPA-Governo USA. IANA fungeva sia come gestore di indirizzi[20] sia come gestore del sistema DNS, il che comportava il controllo diretto del *Root server primario*[21]. Nel 1992 il Governo americano propone l'autofinanziamento di Internet e chiarisce l'intenzione di allontanarsi gradualmente dal sostegno della rete. Allo scopo di favorire un passaggio morbido al totale disinpegno finanziario dello Stato, nasce - nel medesimo anno - l'ISOC (*Internet Society*) cui era demandato il compito di coordinare le attività centralizzate di Internet. Nonostante le intenzioni, nel periodo dal 1992 al 1995, non si arrivò ad un

---

[19] Per l'elaborazione della parte introduttiva del capitolo sono stati utilizzati ampi stralci (poi sintetizzati) dello studio di F. GUADAGNI, *Nomi e indirizzi Internet: rivoluzione in vista?* già disponibile all'indirizzo <http://www.telecomitalialab.com/ libri/internettouch/aree/guadagni2.pdf >.

[20] La distribuzione degli indirizzi Internet agli utenti finali avveniva inizialmente (anni '80) secondo il seguente schema: IANA assegna grossi tagli di indirizzi ai "registri regionali" che a loro volta li affidano agli utenti finali. Attualmente gli utenti finali non si rivolgono più in modo diretto ai registri regionali ma passano attraverso gli ISP (*Internet Service Provider*). Sono questi ultimi che ricevono le assegnazioni in un numero limitato di indirizzi ed in modo proporzionale alla loro grandezza. Provider piccoli ricevono un insieme di 8.912 indirizzi IP, mentre quelli grandi hanno tagli da 65.536 indirizzi

[21] E' il *server* che controlla l'elenco mondiale dei domini di primo livello.

trasferimento vero di competenze all'organismo internazionale. Al contrario IANA continuò a svolgere i medesimi compiti fino ad allora riconosciutigli. Nel 1993 il Governo USA - sempre attraverso il finanziamento di NSF - affianca a IANA una piccola azienda commerciale (la NSI - *Network Solutions Incorporated*) con lo scopo di risolvere l'accresciuto carico di lavoro. Nel 1995 viene finanziato, sempre dal Governo, il progetto InterNIC con lo scopo di autorizzare la vendita dei nomi di dominio di secondo livello del dominio ".com" e del quale era principale contraente la NSI. Negli anni successivi il contratto tra InterNIC ed NSF si modifica e consente alla NSI di vendere i nomi dominio nelle aree ".com", ".org" e ".net". La situazione viene quindi a configurarsi come un monopolio in mano ad un'azienda tutelata dal Governo USA. Proprio a seguito di questa situazione da più voci viene chiesta la soluzione di due questioni fondamentali del governo della rete: il superamento della fase di monopolio nell'assegnazione dei nomi a dominio di primo livello e l'esaurimento dei nomi utilizzabili all'interno dell'area ".com" che vedeva già in quel momento un totale di registrazioni pari a circa due milioni. Nel 1996 - dopo che furono accantonate numerose proposte - si arrivò a costituire un comitato tecnico presieduto dal presidente di ISOC. Si trattava dello IAHC *(International Ad Hoc Committee*) costituito da 11 membri provenienti da diversi enti specifici del mondo Internet. Il Comitato prevedeva la progettazione e l'avvio di un nuovo sistema di *Top Level Domains*. La struttura e le norme applicative del nuovo sistema, il gTLD (*generic TPL*) furono descritte inizialmente nel *Final Report* del Comitato e poi in un accordo firmato nel 1997 a Ginevra da più di 50 organizzazioni tra cui Telecom Italia, che è stato tra i primi firmatari. Hanno continuato il compito del Comitato, negli anni successivi, altri due organismi: l'IPOC *(Interim Policy Oversight Committee*) e il PAB *(Policy Advisory Board*). Ne facevano parte alcuni firmatari del cosiddetto movimento MoU che si poneva l'obiettivo di eliminare il regime di monopolio di NSI. Nella coalizione gTLD-MoU[22] confluirono diversi enti che erano interessati a divenire *registrars*[23] e che si raggrupparono nel CORE *(Council of Registrars).* La NSI che si vedeva sfuggire il controllo assoluto del mercato reagì, con l'appoggio di un certo numero di multinazionali, chiedendo al Governo americano il prolungamento del contratto di monopolio. In ragione dell'onda di malcontento che, per una molteplicità di ragioni, si

[22] La sigla riunisce l'acronimo che individua il movimento, cosiddetto MoU, con l'oggetto di cui si sollecitava la riforma cioè l'assegnazione e la registrazione dei nomi a dominio generici di primo livello, i gTLD.

[23] Organizzazioni commerciali, tra di loro concorrenti, che gestiscono le richieste di registrazione degli utenti e che trasferiscono queste ultime all'interno di banche dati (*registry*).

stava sollevando anche nell'opinione pubblica americana, nel 1997 il presidente Clinton incaricò il Dipartimento del Commercio di risolvere il problema. Nel febbraio 1998 fu pubblicato un documento, il *Green Paper,* nel quale era affrontato il tema del ruolo di IANA ed in generale di cosa dovesse diventare la *governance* di Internet e con il quale veniva di fatto riproposto il modello precedente a quello indicato dal gTLD-MoU. Si tendeva a favorire, nei fatti, una supremazia americana nel controllo della rete, problema al quale divenne attenta in quegli anni anche la Comunità europea che cercò di sostenere in qualche modo l'iniziativa gTLD-MoU rendendosi conto che il governo della rete era un tema su cui valeva la pena di vigilare con la massima attenzione. In ogni caso il tentativo di traslare in ambito internazionale la gestione di Internet seguendo le linee indicative del movimento MoU fallì, e nel giugno 1998, dopo diverse modifiche, il *Green Paper,* ridefinito nel frattempo *White Paper*, viene pubblicato come documento ufficiale del Dipartimento del Commercio americano. In esso sono descritte le modalità ed i tempi per la costituzione di una nuova agenzia internazionale. Si tratta di ICANN - in un primo momento denominata *New IANA* - alla quale, sulla base di un *Memorandum of Understanding*[24] firmato con il Dipartimento del Commercio, vengono affidati i seguenti compiti:

- definizione della politica di assegnazione degli indirizzi IP e successivo controllo;
- supervisione del *Root server* primario;
- controllo dell'ammissibilità dell'inserimento dei nuovi nomi a dominio di primo livello nel sistema DNS;
- coordinamento dell'assegnazione dei parametri necessari a mantenere l'unitarietà di Internet;
- individuazione delle altre attività necessarie per il coordinamento delle funzioni DNS.

1. L'ICANN e l'attuale sistema internazionale di governo della rete

L'ICANN (*International Corporation for Assigned Names and Numbers*) è un'associazione *non-profit* internazionale, avente la responsabilità di assegnare gli indirizzi IP (*Internet Protocol*), l'identificatore di protocollo e di gestire il sistema dei nomi a dominio di primo livello (*Top-Level Domain*) generico (gTLD) e del codice internazionale (ccTLD - *country code Top Level Domain*), nonché i sistemi di *root server*. Si tratta

[24] Si veda in <http://www.ntia.doc.gov/ntiahome/domainname/icann-memorandum.htm>.

dell'organizzazione più importante in tema di collocazione ed assegnazione delle risorse disponibili in Internet. Prima del 1998, anno della sua costituzione, per decisione del Governo USA, la collocazione e la registrazione degli indirizzi Internet (il cosiddetto sistema DNS)[25] erano affidate ad altre organizzazioni tra cui - come già ricordato - IANA (*International Assigned Numbers Authority*)[26]. All'ICANN si deve la liberalizzazione delle attività di registrazione dei nomi a dominio di primo livello (TLD, *Top Level Domain*) come ".org", ".com" e ".net"[27]. Questo processo ha fatto sì che non esistesse più una singola *authority* di registrazione, ma che si costruisse un vero e proprio sistema (SRS, *Shared Registrations System*) comprensivo delle diverse *Registration Authority* nazionali. L'ICANN ha inoltre creato un *forum* di arbitraggio internazionale sui contenziosi nell'attribuzione dei nomi a dominio di primo livello (quelli generali, cioè privi di indicazione geografica). All'interno dell'organizzazione, i governi dei diversi Paesi membri sono rappresentati tramite il GAC (*Governmental Advisory Committee*), organo consultivo funzionale alla creazione del consenso tra gli Stati. E' opinione di alcuni che negli ultimi anni i governi dei diversi Paesi così come l'Unione europea stiano svolgendo un'azione sempre più incisiva sulle iniziative di ICANN.[28] L'Unione europea, in modo particolare, è molto attenta a tutti gli aspetti che investono la *governance* della rete. Questo interesse si manifesta attraverso diversi tipi di azioni: l'elaborazione di documenti strategici, la politica di armonizzazione della partecipazione europea al GAC, la messa in opera di un nuovo nome a dominio sovranazionale europeo (".eu") come strumento per promuovere il commercio elettronico[29].

1.1 La struttura e il funzionamento dell'organizzazione

L'ICANN si articola al suo interno in commissioni. Oltre al GAC (*Governmental Advisory Committee*) ne esistono altre quattro di tipo consultivo: la *President's Standing Committee on Privacy*, la *At-large*

---

[25] Acronimo di *Domain Name System.*

[26] IANA ha continuato ad esercitare queste funzioni sino al 2000 per effetto di un regime transitorio.

[27] Nel 2000 ICANN ha presentato sette nuovi gTLD: .aero, .biz, .coop, .info, .museum, .name e .pro.

[28] S. TRUMPY, *Internet governance in Italia e nel mondo*, relazione per la Giornata di lavoro *Internet: quale futuro per l'Italia*, a cura del Comitato di Esperti Internet della Presidenza del Consiglio dei Ministri, Roma, 6 novembre 2000.

[29] Cfr. S. TRUMPY, op. cit.

Advisory Committee, la *DNS Root Server System Advisory Committee* e la *Security and Stability Advisory Committee*.

Vi sono poi sette commissioni afferenti al Consiglio di amministrazione (*Committees of the Board of Directors*): la *Audit Committee*, la *Board Governance Committee*, la *Committee on Conflicts of Interest*, la *Committee on Reconsideration*, la *Executive Committee*, la *Finance Committee* e la *Meeting Committee*.

Fanno parte dell'ICANN[30] anche commissioni diverse, *task forces* e gruppi di lavoro, quali la *International Domain Names* (IDN) *Committee*, la *New TLD Evaluation Process Planning Task Force*, la *Nominating Committee* e la *Committee on ICANN Evolution and Reform*.

1.2 La *Nominating Committee*

Tra tutte le Commissioni citate è opportuno - per la rilevanza che la sua competenza ha nell'influenzare la democraticità ed il pluralismo dell'ICANN - descrivere brevemente la struttura e le funzioni della *Nominating Committee*. La Commissione è responsabile della selezione dei *directors* del Consiglio di amministrazione dell'ICANN, eccezion fatta per il presidente e per quei membri che devono essere proposti da parte delle organizzazioni di supporto.

La *Nominating Committee* è così composta:

1. un presidente proposto dal Consiglio, senza diritto di voto;
2. il presidente uscente senza diritto di voto, in qualità di consigliere;
3. tre membri non votanti (*liaisons*) proposti rispettivamente dalla *Root Server System Advisory Committee*, dalla *Security and Stability Advisory Committee* e dalla *Governmental Advisory Committee*;
4. cinque membri con diritto di voto proposti dalla *At-large Advisory Committee*;
5. due delegati votanti rappresentanti rispettivamente del settore del piccolo e del grande commercio, proposti dal *Business*

[30] Per approfondimenti sulla struttura interna dell'ICANN si veda <http://www.icann.org/committees/.>.

Users Constituency del GNSO (*Generic Names Supporting Organization*);

6. dieci delegati votanti in rappresentanza di diverse organizzazioni di supporto, dei consumatori e delle associazioni della società civile selezionate dal *Non-commercial Users Constituency* del GNSO, dell'*Internet Engineering Task Force* e dell'*ICANN Technical Liaison Group*;
7. un vice-presidente senza diritto di voto proposto dal presidente che non rivesta altra carica nella commissione.

La durata in carica dei membri con diritto di voto è di un anno, rinnovabile per due volte. L'incarico dei membri senza diritto di voto dura per il tempo indicato dai propositori, mentre il presidente ed il vice-presidente durano in carica sino al *meeting* successivo. I criteri per la scelta dei membri sono gli stessi indicati per quelli del Consiglio di amministrazione. Tra le cause di ineleggibilità si distinguono quelle inerenti la selezione (che esclude coloro che ricoprono qualsiasi altro incarico all'interno dell'ICANN) e quelle inerenti lo svolgimento del servizio che riguarda chiunque abbia contatti con l'ICANN[31] anche in qualità di consulente.

1.3 Il Consiglio di amministrazione

L'organo decisionale dell'ICANN è il Consiglio di amministrazione[32] (*Board of Directors*) composto da **15 membri elettivi (*Directors)* e da 6 aggiuntivi senza diritto di voto (*Liaisons*).** Per la determinazione del numero legale sono considerati solo i *Directors*. **I membri elettivi vengono proposti in numero di 9 dalla *Nominating Committee* ed in numero di 6 dalle organizzazioni di supporto** (2 dalla *Address Supporting Organization*, 2 dalla *Country-Code Names Supporting Organization* e 2 dalla *Generic Names Supporting Organization*). La scelta avviene in base a dei criteri esplicitati nella Sezione 3 dello Statuto

---

[31] Per approfondimenti sulla *Nominating Committee* si veda <http://www.icann.org/committees/nom-comm/>.

[32] L'attuale Consiglio di amministrazione è così composto: Raimundo Beca, Vinton G. Cerf, Steve Crocker, *Security and Stability Advisory Committee Liaison*; Mouhamet Diop, Roberto Gaetano, *At Large Advisory Committee Liaison*; Demi Getschko, Hagen Hultzsch, Joichi Ito, Veni Markovski, Thomas Narten, *IETF Liaison*; Thomas Niles, Michael D. Palage, Alejandro Pisanty, Hualin Qian, Njeri Rionge, Vanda Scartezini, Mohamed Sharil Tarmizi, *Governmental Advisory Committee Liaison*; Peter Dengate Thrush, Richard Thwaites, *TLG Liaison*; Paul Twomey, Suzanne Woolf, *Root Server System Advisory Committee Liaison.*

dell'ICANN. Secondo tali criteri i *Directors,* oltre a rappresentare il più ampiamente possibile le diversità culturali e geografiche della comunità di Internet[33], devono essere persone di acclarata integrità, obiettività ed intelligenza, con spiccate capacità manageriali e competenze tecniche specifiche in materia di registri gTLD, ccTLD, IP, *standard* tecnici di Internet e protocolli. Devono inoltre dimostrare di conoscere le politiche di sviluppo, le tradizioni normative e gli interessi pubblici dei vari Paesi aderenti nonché il panorama globale degli utenti di Internet, di quelli che lo utilizzano a scopi commerciali ovvero non commerciali, individuali o accademici. I *Directors* devono inoltre risultare pienamente coscienti delle finalità perseguite da ICANN e del potenziale impatto che le decisioni prese in tale consesso produrrebbero sull'intera comunità della rete. Devono infine essere disposti a prestare la loro opera volontariamente e senza alcun compenso (ad eccezione di un rimborso per le spese sostenute). Lo statuto elenca le incompatibilità con la carica di *Directors*: questi ultimi non dovranno rivestire una carica ufficiale ed elettiva di governi nazionali o di un'organizzazione multinazionale costituita con trattato o in base ad accordi tra Stati. I membri del Consiglio di amministrazione - anche quelli senza diritto di voto - non devono essere contemporaneamente membri delle organizzazioni di supporto di ICANN. Il Consiglio inoltre, tramite un'apposita commissione, dovrà accertare che non sussistano per i candidati *Directors* conflitti di interesse con ICANN o con altre organizzazioni correlate. La confliggenza è valutata in base a quanto disposto dalle Sezioni 5233 e 5227 della CNPBCL (*California Nonprofit Public Benefit Corporation Law*). In aggiunta a tutto questo il Consiglio adotta delle misure, potremmo dire, precauzionali non riconoscendo diritto di voto ai *directors,* ai consiglieri e alle organizzazioni di supporto in quelle materie in cui potrebbero delinearsi interessi finanziari di natura personale in grado di influenzare il voto. I *directors* durano in carica tre anni. La data di inizio dell'incarico si calcola a partire da quella conclusiva del *meeting* annuale dell'ICANN. Il rinnovo delle cariche si realizza secondo la seguente procedura:

- un mese prima del *meeting,* la *Nominating Committee* dà notizia della rosa di candidati prescelta al Segretariato dell'ICANN;

[33] Ogni area geografica dovrà essere rappresentata da almeno un *Director*. Le aree geografiche considerate sono l'Europa, l'Asia/Australia/Pacifico, l'America Latina/Isole caraibiche, l'Africa e il Nord America. Il criterio per la rappresentatività geografica può essere di volta in volta rivisto in ragione dei mutamenti che rendano necessari degli aggiustamenti.

- non oltre cinque mesi dopo la conclusione del *meeting* ogni organizzazione di supporto comunica per iscritto i nomi dei candidati selezionati.

Nessun membro del Consiglio può essere rieletto per più di tre mandati consecutivi.

Tra i componenti del Consiglio senza diritto di voto (*non-voting liaisons*) sono inclusi:

- un membro designato dal GAC;
- un membro designato dal *Root Server System Advisory Committee;*
- un membro designato dal *Security and Stability Advisory Committee;*
- un membro designato dal *Technical Liaison Group;*
- un membro designato dall'*At-Large Advisory Committee*
- un membro designato dall'*Internet Engineering Task Force.*

I *liaisons* possono essere riconfermati nell'incarico fino alla designazione del successore. Essi possono intervenire nelle discussioni o in sede di deliberazione, avere accesso (a determinate condizioni) ai documenti sui quali si articolano i dibattiti, le deliberazioni ed i *meeting* sebbene il loro *status* non sia paragonabile a quello dei *directors*. Sia i *directors* che i *liaisons* possono rassegnare in qualsiasi momento le loro dimissioni oralmente - in occasione dei *meeting* periodici del Consiglio - o per iscritto, dandone notizia al Presidente o al Segretario generale dell'ICANN. La rimozione dall'incarico avviene - informandone sia l'interessato sia le organizzazioni di supporto dell'ICANN - qualora ne facciano richiesta una maggioranza di almeno ¾ dei *directors*. Ad eccezione dei membri proposti dal GAC anche i *non-voting liaison* possono essere rimossi con un voto pari ad un maggioranza di almeno ¾ dei *directors*. Per quanto riguarda i membri proposti dal GAC il Consiglio può solo invitare (sempre con maggioranza minima di ¾) alla rimozione dei membri. Ogni posto che si rendesse vacante sia per la carica di *director* sia per quella di *non-voting liaison* va coperto tramite una nuova selezione da parte della *Nominating Committee*, a meno che non si tratti di rimpiazzare *directors* proposti dalle organizzazioni di supporto le quali sarebbero, in questo caso, protagoniste per la nuova scelta. Della nuova selezione è data notizia scritta al Segretariato.

1.4 La commissione consultiva governativa

Il GAC (*Governmental Advisory Committee*) è l'organo interno maggiormente rappresentativo ed orientativo della politica dell'ICANN. Recentemente il GAC ha esaminato diverse delicate questioni riguardanti la politica pubblica dell'ICANN sulla selezione di nuovi nomi a dominio generici di primo livello, l'elaborazione di nomi a dominio multilingue, la tutela della proprietà intellettuale e la protezione dei consumatori, i princìpi per la gestione e l'amministrazione dei ccTLD (nomi a dominio con indicazione geografica).[34]

Il GAC è composto da un presidente e dai rappresentanti accreditati[35] dei governi nazionali, delle organizzazioni governative internazionali o costituite per trattato e da altre autorità pubbliche (uno per ogni soggetto), tutte investite di un mandato elettivo.

A discrezione del presidente, con un mandato annuale, possono essere eletti, dai rappresentanti aderenti, anche due vice-presidenti.

Il presidente ha potere su tutte le questioni procedurali inerenti la convocazione, lo svolgimento delle riunioni e la moderazione del dibattito. In caso di parità di voti è il voto del presidente a determinare l'esito della votazione. L'elezione dei rappresentanti avviene ogni due anni. L'espressione del voto può avvenire per corrispondenza (postale, telegrafica, corriere elettronico, fax) o direttamente nella sede di riunione della commissione. Le modalità di scrutinio vengono scelte dalla maggioranza con voti espressi per appello nominale o per alzata di mano dai rappresentanti presenti accreditati. Nel caso di voto per corrispondenza è a disposizione dei rappresentanti presenti un bollettino di voto mentre ai non presenti è notificato l'esito della votazione. Le medesime modalità di voto e di comunicazione sono adottate anche per il voto in merito ad una determinata questione. Per l'espressione del voto per corrispondenza il presidente del GAC fissa un termine di 30 giorni a partire dalla data di notifica oltre il quale l'aderente è considerato non votante. Per ciò che riguarda l'esito della votazione, oltre alla notifica da inoltrare a chi vota per corrispondenza, è prevista la comunicazione ufficiale in sede di prima

---

[34] A tale proposito si veda il documento *Principles for the Delegation and Management of Country Code Top Level Domain* reperibile all'indirizzo: <http://www.icann.org/committees/gac/>.

[35] L'elenco dei rappresentanti attuali è disponibile all'indirizzo <http://194.78.218.67/web/contact/reps/index.shtml>.

riunione. Il numero legale per la validità delle riunioni in cui avvengono votazioni è la maggioranza semplice dei rappresentanti degli aderenti. Il dibattito in linea può svolgersi su iniziativa di qualsiasi aderente, previo accordo con il Presidente, e può vertere su qualsiasi argomento. Nella pratica è il segretariato del GAC ad aprire la discussione alla quale tutti i membri possono partecipare e dare il loro contributo entro un limite di tempo che è stabilito dal Presidente in 60 giorni. Conclusa la discussione il Presidente ne trae le conclusioni di cui può mettere al corrente il Consiglio di amministrazione dell'ICANN. Delle eventuali diverse posizioni evidenziate nell'ambito della discussione il Presidente del GAC dovrà informare il Consiglio che avrà così modo di valutare la pluralità delle opinioni degli aderenti. Indipendentemente dalle questioni sulle quali il Consiglio è chiamato a deliberare, il GAC può esprimere comunque le proprie valutazioni tramite comunicati, raccomandazioni o altro su tutte le questioni rilevanti dell'attività dell'organizzazione e delle quali in ogni caso il Consiglio è tenuto a prendere visione. Le riunioni del GAC non sono generalmente aperte al pubblico anche se il Presidente ha potere di renderle tali interamente o parzialmente. Delle riunioni non pubbliche è data informazione tramite un comunicato. Il regolamento del GAC può essere modificato dagli stessi aderenti. Le proposte emendative sono sottoposte al voto entro 60 giorni dalla presentazione e, in più, nel corso della prima seduta successiva alla scadenza del termine con voto segreto, per appello nominale o per alzata di mano a maggioranza semplice degli aderenti. L'articolo 55 del regolamento prevede che, in caso di divergenze interpretative sui princìpi, debbano prevalere le norme statutarie e regolamentari dell'ICANN. Possono essere rappresentati anche gli enti autonomi riconosciuti internazionalmente. L'invito all'adesione viene rivolto dal presidente del GAC o dal Consiglio di amministrazione, che è - in caso di disaccordo, l'organo deliberante. L'accredito può essere richiesto preventivamente dai governi e dalle organizzazioni che non sono rappresentate al GAC. L'elenco degli aderenti è aggiornato periodicamente e pubblicato. A discrezione del presidente anche i rappresentanti delle autorità pubbliche e di altri organismi interessati che non siano aderenti possono assistere alle riunioni del GAC in qualità di osservatori. Il diritto di voto è riservato ai soli rappresentanti accreditati. Il presidente del GAC (ad eccezione della prima elezione) viene eletto dagli aderenti, in conformità alle procedure previste dall'articolo IX delle linee guida. Il presidente può autorizzare la costituzione di comitati *ad hoc* per lo studio di questioni di interesse per i governi nazionali.

Il GAC è convocato per iniziativa del Presidente su domanda di un aderente quando vi sia un'esigenza manifestata da almeno un terzo dei componenti attuali di ICANN, ovvero per decisione del Consiglio di amministrazione. La convocazione deve avvenire con un preavviso minino di 28 giorni, anche con modalità informatiche. Le riunioni *on line* o elettroniche vengono convocate dal presidente almeno 10 giorni prima della data fissata così come quelle di urgenza. Il dibattito interno al GAC si svolge sia attraverso l'organizzazione di *meeting* periodici sia tramite *forum on line* (dal 1999 ad oggi sono stati tenuti 21 *meeting* per ognuno dei quali è data informazione all'ICANN tramite un comunicato e 5 *regional forum*).

Le linee guida per il funzionamento del GAC sono delineate in un documento adottato ufficialmente dall'ICANN il 25 maggio 1999 (in <http://194.78.218.67/web/docs/principes_de_fonctionnement.htm>). Il testo, composto da 55 norme di principio raccolte in 15 Titoli, fissa anzitutto (Titolo I) le competenze dell'organo, quale commissione con funzioni consultive, di analisi e di divulgazione delle attività dell'organizzazione. La funzione informativa è svolta prevalentemente per le decisioni dell'organizzazione con ricaduta sulle politiche interne degli Stati e sulle attività delle altre organizzazioni internazionali, specialmente in riferimento ad aspetti dove risultano evidenti le possibili interazioni tra le deliberazioni dell'ICANN e le norme contenute in trattati o in convenzioni internazionali.

1.5 Il dialogo interno all'ICANN

La comunicazione tra il GAC ed il Consiglio di amministrazione dell'ICANN, così come quella con gli altri organi dell'organizzazione o con le organizzazioni di supporto, avviene tramite l'invio di comunicati. Le conclusioni e le raccomandazioni sono inoltrate al Consiglio di amministrazione tramite il Presidente. In seno al GAC vengono dibattute tutte le questioni di interesse generale o che riguardano i governi. Le riunioni della commissione si svolgono almeno una volta all'anno e comunque tutte le volte che lo si ritenga utile. Al di là del peso che può esercitare ogni singolo governo, comunque, la partecipazione a ICANN è aperta a tutti i soggetti che vogliano avere voce nel governo globale di Internet. Ciò è possibile partecipando alle tribune in linea, accessibili dal sito *web* o attraverso i contributi dati dalle organizzazioni di supporto e dai

comitati consultivi (*mailing list* attive per i partecipanti) o intervenendo alle assemblee pubbliche[36].

1.6 Lo svolgimento dell'attività dell'ICANN

L'ICANN svolge annualmente dei *meeting* per eleggere i suoi *officers* o per discutere temi diversi. L'intervallo di tempo massimo che intercorre tra due *meeting* è di 14 mesi. Del *meeting* si dà notizia in tempo reale (qualora il Consiglio lo stabilisca) tramite collegamenti video ed audio. Vi sono poi incontri definiti *Regular meeting* (la cui cadenza è stabilita dal Consiglio) e gli *Special meeting.* Questi ultimi - dei quali dà notizia il Segretariato generale dell'ICANN - sono fissati qualora ne facciano richiesta ¼ dei membri del Consiglio o il Presidente. La modalità di convocazione è quella del contatto diretto con i membri del Consiglio (per via telefonica o informatica, con preavviso di almeno 48 ore ovvero per posta con un preavviso di almeno 14 giorni). I *meeting* si svolgono alla presenza della maggioranza di tutti i *directors* quando si affrontano questioni che riguardano il commercio, e della maggioranza dei *directors* presenti quando si debba deliberare su qualsiasi altro tema. Se il *quorum* non è raggiunto le sedute sono rinviate per un massimo di 24 ore, trascorse le quali tutti i *directors* non presenti vengono informati. Il processo decisionale può prodursi anche al di fuori del contesto dei *meeting* se tutti i *directors* vi acconsentono per iscritto. In questo caso il consenso raggiunto ha il medesimo valore del voto preso all'unanimità. Qualora sia consentito dalle norme applicative dello statuto, qualsiasi comunicazione inviata per via elettronica è equiparata al consenso scritto.

1.7 Il *forum* di arbitraggio internazionale

La risoluzione delle controversie circa l'assegnazione dei nomi a dominio avviene tramite una procedura arbitrale - attuata interamente via Internet - e predisposta dalla WIPO (*World Intellectual Property Organization*) attraverso il Centro di arbitraggio e di mediazione. Questo organo - dipendente amministrativamente dalla WIPO - è stato creato nel 1994, ha sede a Ginevra, ed è divenuto la principale istituzione per la soluzione extragiudiziale dei litigi. Si pensi che nel solo anno 2003, il Centro ha

[36] I più recenti *meeting* si sono svolti a Roma (2-6 marzo 2004), a Kuala Lumpur (19-23 luglio 2004), a Cape Town (1-5 dicembre 2004, 6° *meeting* annuale), a Mar del Plata (4-8 aprile 2005) ed a Lussemburgo City (11-15 luglio). Per l'anno 2005 in corso il prossimo incontro è previsto a Vancouver, dal 30 novembre al 4 dicembre.

trattato ben 5722 controversie (ripartite in 116 Paesi) relative all'assegnazione dei nomi a dominio e temi assimilati. La procedura adottata è la cosiddetta ADR, ovvero l'*Alternative Dispute Resolution*[37], con la quale vengono risolti i contenziosi commerciali internazionali ed in particolare quelli che vertono sulle questioni tecniche, sullo spettacolo o su altri aspetti della tutela della proprietà intellettuale. La regolamentazione delle controversie avviene in osservanza dei princìpi direttivi contenuti nell'UDRP (*Uniform Domain Name Dispute Resolution Policy* - approvato dall'ICANN il 26 agosto 1999), nel regolamento di applicazione ed in alcune norme supplementari. I princìpi suddetti sono, a loro volta, ispirati a quelli richiamati nelle raccomandazioni formulate dalla WIPO sui nomi a dominio Internet.

L'UDRP è la principale *policy* ovvero la procedura risolutiva più seguita. E' applicabile tra il *registrar*[38] di un indirizzo ed il suo *costumer* o *registrant* (ovvero chi registra materialmente il nome) e riguarda tutti i gTLD ed alcuni ccTLD. Tuttavia, nel corso degli anni, per risolvere casi specifici sono state adottate anche delle *policy ad hoc*. Tra queste è il CEDRP (*Charter Eligibility Dispute Resolution Policy*) per i TLD .aero, .coop, e .mus, l'IPDRCP (*Intellectual Property Defensive Registration Challenge Policy*) per i TLD .pro, la RDRP (*Restrictions Dispute Resolution Policy)* che utilizzable per i TLD .biz ed infine la ERDRP *(Eligibility Requirements Dispute Resolution Policy*) per i TLD .name[39]. I reclami della *policy* ICANN sono presentati dai ricorrenti esclusivamente tramite i *dispute-resolutions service provider* che sono accreditati dallo stesso ente di registrazione. Oltre alla WIPO i *provider* accreditati sono l'*Asian Domain Dispute Resolution Centre,* il CRP (*Institute for Dispute Resolution*) e il NAF *(National Arbitration Forum*).

Per approfondimenti sui princìpi UDRP e sulle norme supplementari si vedano <http://www.arbiter.wipo.int/domains/rules/index-fr.html>;
<http://www.arbiter.wipo.int/domains/rules/supplemental/index-fr.html>.

---

[37] La procedura extragiudiziale non pregiudica in ogni caso lo svolgimento di quella in via giudiziale.

[38] Rappresenta l'ente presso il quale il *respondent*, cioè chi risponde della registrazione del *domain name*, ha registrato il nome per primo.

[39] F. POMARICI, *La risoluzione alternativa delle controversie tramite Internet*, Tesi di laurea non pubblicata, Università "La Sapienza" di Roma, Facoltà di giurisprudenza, Istituto di diritto privato, a.a. 2004-2005.

2. Le organizzazioni di supporto dell'ICANN

Tra le organizzazioni di supporto di ICANN figurano l'**ASA** (*Address Supporting Organization)*, il **ccNSO** (*Country Code Names Supporting Organization*) ed il **GNSO**. Il ruolo delle organizzazioni di supporto è descritto dalle norme del Titolo VIII dello Statuto dell'ICANN[40]. Si tratta di enti *non-profit* che forniscono consulenza al Consiglio di amministrazione dell'ICANN sui temi che riguardano la politica del funzionamento, dell'assegnazione e dell'amministrazione dei nomi di dominio.

L'**ASO**, in particolare, deriva storicamente dall'accordo che nel 1999 venne sottoscritto tra l'ICANN ed alcuni Registri Internet regionali. Il *Memorandum of Understanding,* emendato nel 2000, riguarda l'intesa dell'ICANN con l'*Asia Pacific Network Information Centre* (APNIC), l'*American Registry for Internet Numbers* (ARIN) ed il *Réseaux Ip Européens Network Coordination Centre* (RIPE NCC).

Il **ccNSO** (*Country Code Names Supporting Organization*) è un organismo che ha il compito di sviluppare le politiche di ricerca del consenso sul tema dell'inserimento dei nomi a dominio geografici di primo livello nella struttura globale ICANN.

Il **GNSO** *(Generic Names Supporting Organization*) è un'organizzazione che succede al DNSO (*Domain Name Supporting Organization*) nella promozione della partecipazione internazionale in tema di *management* tecnico di Internet.

III. I Registri regionali

A fianco delle organizzazioni internazionali e delle Autorità di registrazione nazionali esistono attualmente nel mondo cinque Registri Internet cosiddetti regionali (*Regional Internet Registries*). Si tratta di enti *non-profit* che intervengono sulle politiche di assegnazione e registrazione delle risorse Internet e precisamente sugli indirizzi IP. In questo caso l'assegnazione viene delegata da ICANN ai Registri suddetti che provvedono, a loro volta, ad allocarle alle rispettive autorità locali, incaricate di trasferirle agli utenti finali. I Registri regionali sono l'APNIC (*Asia-Pacific Network Information Center*), l'ARIN (*American Registry for*

[40] Si consulti il sito <http://www.icann.org/general/corporate.html>.

Internet Numbers), il RIPE NCC (*Réseaux IP Européens*), la LACNIC (*Latin American and Carribean Internet Addresses Registry*) e l'AfriNIC[41] (*Africain Network Information Center*). L'APNIC serve l'intera area pacifica, comprendente 62 Paesi di Asia e Oceania; l'ARIN registra per Stati Uniti, Canada, isole caraibiche e del Nord Atlantico; il RIPE NCC opera per i Paesi membri dell'Unione, il Medioriente e parte dell'Asia; la LACNIC copre l'America Latina e la regione caraibica. Infine l'AfriNIC serve il continente africano. I Registri regionali lavorano in stretta relazione tra di loro e con le altre organizzazioni nazionali ed internazionali[42].

Per approfondimenti sulle organizzazioni di supporto si vedano <http://www.icann.org>,<http://aso.icann.org>,<http://ccnso.icann.org>, <http://gnso.icann.org>.

Per i Registri regionali Internet <http://www.arin.net/>,<http://www.ripe.net/>,<http://www.apnic.net/>, <http://lacnic.net/en/sobre-lacnic/estatuto/i.html>, <http://www.afrinic.net>.

IV. Il sistema italiano di assegnazione di nomi a dominio ".it"[43]

1. Cenni storici

La *governance* italiana della rete Internet è stata costruita, dal suo esordio sino alla riforma del 2004, sulla separazione delle funzioni di registrazione e di normazione, attribuite a due distinti organismi: la *Naming* e la *Registration Authority*. All'interno di questo sistema la *Naming* rappresentava l'organo legislativo mentre la *Registration Authority* - che materialmente gestiva il registro e l'assegnazione dei nomi - era l'organo esecutivo. Agli enti conduttori spettava la funzione giudiziaria. Questa scelta fu operata in adeguamento alla normativa ISO 6523 che raccomandava espressamente tale separazione. Al termine del 1993 infatti l'ISO aveva sollecitato i vari organismi nazionali - per l'Italia l'UNI e l'UNINFO (normative informatiche) - ad attuare la suddetta normativa. Nel gennaio 1994 il Ministero delle poste e telecomunicazioni ha affidato

---

41 AfriNIC sarà riconosciuta in ottobre 2005 dall'ICANN come il quinto Registro regionale per gli indirizzi Internet, competente per il continente africano finora gestito da ARIN, APNIC e RIPE NCC.

42 ICANN, ASO, IETF, ISOC e NANOG.

43 I paragrafi 1 e 2 sono una sintesi dell'intervento di F. FOGLIANI, *Internet Governance in Italia*, Atti del Convegno dell'Istituto di Ricerca Internazionale, *Tutela del dominio Internet e del marchio*, Milano 19 e 20 marzo 2002 (in <http://www.nic.it/NA/present/fog-milano.html>).

all'UNINFO il compito di costituire un gruppo di lavoro denominato UNINFO-GL per applicare ed estendere la normativa ISO in Italia. Del gruppo furono chiamati a far parte esperti ricercatori e tecnici del settore delle telecomunicazioni. I lavori terminarono a dicembre del 1994 con la decisione di affidare il ruolo di *Naming Authority* al gruppo ITA-PE e di *Registration Authority* allo IAT (oggi ITT) ovvero all'Istituto per le applicazioni telematiche del C.N.R. Lo ITA-PE restò organizzato sino al 1997 come lista di discussione. Nel 1997 - anche in considerazione dell'ampio consenso che si era venuto a creare all'interno della lista sul tema della *governance* di Internet - si decise di elaborare le prime regole per il funzionamento della rete. Così, nel 1998, con l'approvazione dello statuto, l'ITA-PE formalizzò la propria posizione di ente normatore.

Nel settembre 1999 l'Assemblea della *Naming* approvò le nuove regole per i ccTLD.it (*country code Top Level Domain. It)* ovvero per i nomi a dominio di primo livello con indicazione geografica. Rispetto alle vecchie norme dettate dall'ITA-PE, la *Naming* scelse di semplificare la procedura in base alla quale diventava ora possibile l'autocertificazione, l'estensione del diritto alla registrazione a tutti i soggetti dell'Unione Europea, l'eliminazione del limite di un solo nome a dominio per le imprese e gli enti commerciali, l'ammissione alla registrazione anche per le persone fisiche (non più di un nome a dominio)[44]. Il successo fu immediato e la registrazione dei nomi a dominio passò da circa 90 mila nel 1999 ad oltre 400 mila a metà dell'anno 2000. Nell'agosto dello stesso anno 2000 furono introdotte le "procedure di riassegnazione" per la risoluzione delle controversie. In ragione del richiamo esplicito contenuto nel contratto stipulato fra la *Registration Authority* e i singoli *provider* e dell'impegno che gli utenti assumevano nel rispettarle (lettera di responsabilità), le regole della *Naming* assunsero un carattere cogente sia nei confronti della *Registration Authority* sia nei confronti dei *provider* e degli utenti assegnatari.

La *Naming Authority* comprendeva di diritto i *provider,* i tecnici, i professionisti o anche soltanto i privati appassionati di Internet. L'assemblea era anche integrata dai rappresentanti della *Registration Authority* e da altri esperti che potevano essere invitati *ad hoc* per la discussione di temi specifici. Al Presidente della *Naming* erano attribuiti i compiti di garanzia, coordinamento e controllo, esercitato, quest'ultimo, oltre che sul Comitato esecutivo anche sugli Enti conduttori delle procedure di riassegnazione. Questa iniziale grande rappresentatività del mondo di Internet all'interno della *Naming* andò nel tempo scemando poiché i nuovi *maintainer* - in cospicuo aumento - non si iscrivevano più

[44] E. FOGLIANI, op. cit.

all'*Authority*. Ciò produsse anche l'effetto di diminuire le entrate che ben presto non risultarono più adeguate alla gestione del sistema interamente autofinanziato. Durante gli anni 2000 e 2001 si tentò di trasformare la *Registration Authority* in organo amministrativo dello Stato. Nel 2002 la frattura tra le due *authorities* risultò sempre più evidente e si intravide nella creazione della Fondazione Meucci - che avrebbe dovuto riunire in sé le due autorità - una possibile soluzione con la quale si poteva istituzionalizzare il sistema di *governance* della rete Internet. Il progetto non fu però attuato e nel corso del 2003 la *Registration Authority* annunciò che, a partire dal 2004, non avrebbe più riconosciuto le regole della *Naming.* Con il nuovo contratto, valevole dal 1° gennaio 2004, dunque intervengono nuove regole che assoggettano i *maintainer* unicamente alla *Registration Authority.*

2. Il sistema di *governance* attuale

Il nuovo sistema di regole è ora afferente ad un unico organismo normatore: il "Registro del ccTLD.it" che altro non rappresenta se non la vecchia *Registration Authority*. Il Registro è membro attivo del CENTR e dell'ICANN. Al suo interno si articola in una Direzione generale, cui fanno capo cinque unità operative, ed una Commissione per le regole. Quest'ultima è un organo consultivo che propone al Direttore le norme per l'assegnazione e la gestione dei nomi a dominio italiani. Si compone di nove membri che ricoprono il ruolo di «consulenti dell'Istituto di Informatica e Telematica per le attività di registrazione dei nomi a dominio sotto il ccTLD "it"». Di questi nove membri, sei sono designati da associazioni o gruppi ritenuti rappresentativi della LIC *(Local Internet Comunity*) italiana, due dallo IIT-CNR, uno dal Consortium GARR. La composizione della Commissione può essere integrata con altre sette persone, nominate dal Direttore del Registro e scelte per competenza tecnica specifica (2 membri) ovvero perché esponenti governativi o di organismi pubblici nominati da ministeri e da autorità competenti (5 membri). L'incarico dei componenti della Commissione dura un anno e può essere rinnovato. Il Presidente della Commissione è eletto tra i suoi membri.

Tra i sei rappresentanti della LIC entrano a far parte due componenti indicati dai *provider-maintainer*[45], un componente designato dalla sezione

[45] Sono gli operatori che hanno sottoscritto un contratto con il Registro ed in virtù di ciò sono chiamati a registrare e mantenere nomi a dominio per conto proprio o di terzi.

italiana di ISOC (*Internet Society*), un componente suggerito dall'AIIP (Associazione Italiana Internet Provider), uno che viene proposto dall'Assoprovider (Associazione Provider Indipendenti) ed infine uno indicato dal gruppo ITA-PE. Contrariamente a ciò che succede per i membri che provengono dal GARR e dal Registro che vengono direttamente "nominati" a tale carica, i rappresentanti della LIC possono essere, da questa, solo "proposti" al Direttore del Registro che, a sua discrezione, potrà decidere o meno di nominarli.

2.1. La procedura decisionale attuale

Le deliberazioni sono prese a maggioranza semplice dei presenti. Se queste vengono approvate dal Direttore del Registro divengono immediatamente cogenti e sono pubblicate sul sito *web* e sulla lista di discussione dei *maintainer*. Pubblici sono anche i verbali delle riunioni. Le decisioni della Commissione, invece, vengono inviate al Direttore del Registro, tramite del Presidente, entro 10 giorni dalla loro approvazione. Si prospettano a questo punto due possibilità: il Direttore approva le decisioni e provvederà a comunicare alla Commissione, entro un termine massimo di 15 giorni, i tempi di attuazione; ovvero, in caso di disapprovazione, può chiedere un nuovo esame delle decisioni prese. Al Direttore è riconosciuto inoltre un potere decisionale che prescinde dalla consultazione preventiva della Commissione, qualora ricorrano condizioni di urgenza. Su tali decisioni la Commissione è chiamata a deliberare nel corso della prima riunione successiva. Il potere della Commissione non ha in ogni caso valore di vincolo per il Direttore, non potendo le decisioni di quest'ultimo essere annullate. Molto diversa era la rappresentatività della LIC nel vecchio sistema *Naming/Registration Authority.* Il Comitato esecutivo della *Naming* comprendeva ordinariamente 11 membri, di cui 8 eletti dall'assemblea, uno in rappresentanza della *Registration Authority*, uno di Uniinfo ed uno del Ministero delle comunicazioni. Poteva inoltre essere disposta la cooptazione di altri 4 membri scelti fra i rappresentanti di enti statali, giungendo in questo caso al numero massimo di 15 membri. I componenti venivano eletti con voto palese mentre l'attuale regolamento non indica nulla circa le modalità di elezione[46].

[46] Il rappresentante di ISOC è stato designato dal comitato direttivo anziché dall'assemblea (cfr. E. FOGLIANI, op. cit).

Per approfondimento sulle regole e le procedure tecniche previste dal Registro del ccTLD "it" si veda in <http://www.nic.it/RA/CR/>.
Sulla conoscenza e l'uso del dominio Internet ".gov.it" e l'efficace interazione del portale nazionale "italia.gov.it" con le pubbliche amministrazioni e le loro diramazioni territoriali si veda la Direttiva del Presidente del Consiglio dei Ministri del 30 maggio 2002 in
<http://www.innovazione.gov.it/ita/documenti/direttiva_portale.shtml>.

3. I servizi offerti

Il Registro è l'organismo responsabile dell'assegnazione dei nomi a dominio (per la parte riguardante il *country code Top Level Domain* "it") definiti dallo standard ISO 3166 e delle attività relative all'assegnazione di nomi definiti da altri standard (ITU X.400, ITU X.500). Il Registro fornisce inoltre servizi ai *provider/maintainer* che registrano i domini per conto terzi o alle persone fisiche o giuridiche che vogliono gestire direttamente i propri nomi a dominio. In ogni caso è necessario che il richiedente stipuli un contratto con il Registro. Sono poi forniti servizi aggiuntivi tra i quali, ad esempio, l'ospitalità offerta ai *nameserver* secondari ed il mantenimento di liste di discussione su argomenti che interessano la comunità Internet. Riassumendo molto schematicamente i servizi gestiti ed offerti dal Registro del ccTLD ".it" relativamente al *Domain Name System* (DNS) possiamo indicare:

- la gestione del *nameserver* primario del ccTLD "it";
- il coordinamento con i gestori dei *nameserver* secondari del ccTLD "it";
- la gestione del *nameserver* dei domini geografici;
- la gestione del servizio di *nameserver* secondario per i domini registrati nel ccTLD "it" (servizio opzionale).

La gestione del *nameserver* primario del ccTLD "it" è svolto nel rispetto delle regole stabilite da IANA e da ICANN (vedi RFC1591 e ICP-1, attivo su un *server* dedicato esclusivamente a tale compito (dns.nic.it).

Tutti i domini geografici corrispondenti ai nomi, alle traduzioni ed alle abbreviazioni, agli *alias* delle regioni italiane, delle province italiane ed ai nomi dei comuni italiani sono gestiti direttamente dal Registro del ccTLD ".it" sui propri *server*. Attualmente il *nameserver* primario di un dominio geografico viene attivato sul *nameserver* dns.nic.it, mentre il nameserver secondario di un dominio geografico viene attivato sui *server*

dns2.nic.it o dns3.nic.it. Gli attuali *nameserver* secondari del ccTLD "it" distribuiti sia in Italia sia all'estero, sono sette (*nameserver.cnr.it; server2.infn.it ;ns.ripe.net; dns2.it.net; dns2.iunet.it; uth2.dns.cogentco.com; it2.mix-it.net).* Il servizio di *nameserver* secondario per i domini registrati nel ccTLD "it" viene fornito su *server* dedicati esclusivamente a questo compito (dns2.nic.it e dns3.nic.it).

4. Le regole per l'assegnazione di un dominio

Riassumendo a grandi linee quanto è stabilito dal Regolamento, i nomi a dominio vengono assegnati rispetto i seguenti criteri:

- assegnazione in uso ai richiedenti secondo la cronologia delle richieste;
- garanzia di riserva per alcuni nomi a dominio;
- non prenotabilità dei nomi;
- conclusione della procedura con il caricamento del nome assegnato
- nel *database* del Registro dei Nomi Assegnati (RNA).

Tutte le attività del Registro sono svolte dall'Istituto di informatica e telematica del C.N.R. (IIT-CNR), ente pubblico di ricerca al quale sono riconosciute, a livello internazionale, competenze specifiche nel settore della standardizzazione.

5. La risoluzione delle controversie

La procedura di contestazione sull'assegnazione di un nome a dominio ha inizio mediante l'invio di una lettera raccomandata al Registro. Ne consegue un immediato aggiornamento del RNA che comporta l'aggiunta della notazione "valore contestato" al nome a dominio indicato. La notifica dell'avvenuta contestazione è inoltrata dal Registro all'assegnatario del nome contestato entro dieci giorni dalla ricezione della raccomandata che ha in oggetto la controversia. Entrambe le parti sono invitate ad iniziare la procedura arbitrale ovvero quella di riassegnazione del nome. La risoluzione della contestazione non rientra nella competenza del Registro che deve devolverla al Collegio arbitrale, come disposto dall'articolo 15 del Regolamento. Nessun'altra azione può essere condotta dal Registro fin tanto che la controversia non sia risolta. In pendenza di contestazione, il contestante deve confermare ogni sei mesi la sussistenza dell'interesse per l'oggetto contestato (articolo 14.3 Regolamento). Ove non

si ottenesse questa conferma, il Registro riterrebbe la controversia risolta (a meno di aver ricevuto notizia dell'esistenza di un giudizio, di un arbitrato o di una procedura di riassegnazione).

Il Collegio arbitrale è composto di tre arbitri di cui due scelti da ciascuna delle due parti in causa. Il terzo, che ha la carica di Presidente, viene scelto dagli altri due arbitri. Gli arbitri - dei quali si tiene un elenco presso il Registro - sono esperti in materia di nomi a dominio. Dell'elenco fanno parte arbitri già nominati ai sensi del precedente Regolamento (Regole di *naming* versione 3.9). L'accettazione delle nuove proposte di registrazione in elenco è subordinata al parere favorevole della Commissione Regole. La decisione degli arbitri in merito alla contestazione deve essere presa entro il termine di 90 giorni dalla costituzione del collegio. La procedura prevede che il presidente del collegio possa nominare un segretario e che possa regolare lo svolgimento del giudizio nella maniera che ritiene più opportuna purché sia assicurato il rispetto del contraddittorio. In ogni caso le parti dovranno avere a disposizione almeno 10 giorni per presentare le proprie difese e la documentazione, ed un periodo almeno uguale per le repliche. Ove ricorrano gravi motivi, il Collegio può disporre provvedimenti cautelativi per il nome a dominio contestato, che il Registro è tenuto ad attuare immediatamente. Le decisioni del Collegio sono prese nel rispetto delle norme del Regolamento e dell'ordinamento italiano. Il Registro rende pubblici tali atti a meno che il Collegio stesso - su richiesta di una delle parti - non decida diversamente. Le decisioni sono rese esecutive dal Registro entro 5 giorni lavorativi dal ricevimento della comunicazione. Gli effetti della risoluzione della controversia possono tradursi nella cancellazione della notazione di contestazione a fianco del nome assegnato, ovvero nella cancellazione dello stesso dall'RNA e nell'avvio della procedura di riassegnazione che non necessariamente si conclude con l'assegnazione alla parte che ha iniziato la contestazione. Il nome contestato risulta anzi non disponibile per la riassegnazione per almeno 30 giorni. Entro 10 giorni dalla risoluzione della contestazione, la parte contestante è invitata a presentare domanda per la riassegnazione. Trascorsi inutilmente i 30 giorni previsti, il nome a dominio può essere assegnato nuovamente a chiunque ne faccia richiesta (articolo 14.6 Regolamento). La procedura di riassegnazione viene condotta da organizzazioni - denominate enti conduttori - che devono rispondere ai requisiti predisposti dal Registro, ascoltato il parere della Commissione Regole. La scelta dell'ente conduttore spetta a chi contesta il nome a dominio. Qualora su un nome a dominio esista già un giudizio pendente innanzi al giudice ordinario o al collegio arbitrale, il nome non potrà essere riassegnato. Il controllo dei requisiti

richiesti agli enti conduttori è operato dal Registro che può anche decidere di esonerare un ente nel caso di ripetute violazioni di norme procedurali o di merito. Il Regolamento reca precisa indicazione dei casi che comportano il trasferimento del nome a dominio contestato. Essi ricorrono quando:

a) il nome contestato sia identico ad un marchio o al cognome (o nome) del ricorrente;
b) l'assegnatario (resistente) non abbia alcun titolo in relazione al nome ovvero nessun diritto;
c) il nome sia stato registrato e venga usato in mala fede.

Nei casi a) e c), se il resistente non può provare di avere diritto o titolo sul nome, il nome viene trasferito al ricorrente.
Nel caso b) il resistente, per avere diritto o titolo al nome, deve provare la sua buona fede ed il fatto di essere conosciuto con quel nome a dominio (sia personalmente sia come associazione sia come ente commerciale), anche qualora non abbia registrato il marchio. Infine dovrà dimostrare che l'uso del nome - sia a scopo commerciale che non - è legittimo e non ha l'intento di sviare la clientela del ricorrente o violare il marchio registrato (articolo 16.6 Regolamento).

6. Requisiti degli enti conduttori

Ai sensi di quanto disposto dall'articolo 17 del Regolamento, gli enti conduttori possono essere persone giuridiche pubbliche o private ovvero studi professionali costituiti nell'Unione europea. L'accettazione della domanda degli enti presentata al Registro ne comporta l'abilitazione alla conduzione delle procedure. L'inizio dell'attività è subordinato all'apertura alla visibilità pubblica dell'URL (*Uniform Resource Locator*).

V. Registro dei nomi a dominio in altri Paesi

Ai Registri nazionali - istituiti nei vari Paesi a metà degli anni '80 - competono le registrazioni dei cosiddetti ccTLD (*country code Top Level Domain*). Le autorità indipendenti sono classificabili in quattro categorie: le governative, le *non-profit*, le società industriali e le università. Sotto il profilo del rapporto con i governi si potranno avere situazioni in cui esiste

un riconoscimento governativo formale (contratto), uno informale (presenza di un osservatore o un *memorandum*), ovvero l'assenza di esso.
Riguardo al controllo che i governi esercitano sulle *authorities,* in un recente studio di F. Caneschi e S. Trumpy[47] è stato sottolineato che la maggior parte dei registri sono soggetti a scarso o nullo controllo. Sembrerebbe inoltre esistere una relazione inversa tra il controllo esercitato dai governi e il successo del registro (i registri con maggiore successo sarebbero perciò quelli sui quali non è esercitato alcun controllo).

Australia

L'*Authority* nazionale di registrazione ha il proprio riferimento governativo nel NOIE *(National Office for the Information Economy*) che ha attivato un processo per la costituzione di una *corporation,* la ".auDA", incaricata di gestire il DNS sotto il suffisso ".au". La *corporation* è autoregolamentata, si compone di 380 membri rappresentativi degli interessi di piccole e medie imprese, di organizzazioni di tutela dei consumatori, dei *provider* e delle grandi aziende. Il NOIE è rappresentato con un proprio membro - senza diritto di voto - presso il Consiglio di amministrazione dell'*Authority.*

Numero di registrazioni: circa 300 mila

Austria

Il Registro nazionale ".at" nasce dalla *Internet Private Foundation* (associazione di *provider*) ed è regolamentato con legge. Al Consiglio di amministrazione partecipano - a titolo personale - rappresentanti del Ministero dei trasporti e dell'Autorità di regolamentazione.

Numero di registrazioni: circa 300 mila

Belgio

Il Registro nazionale è rappresentato dal DNS.be, associazione senza fini di lucro che ha un collegamento informale con il Governo, consistente - come nel caso austriaco - nella partecipazione di rappresentanti ministeriali (Ministero degli affari economici) e dell'autorità di regolamentazione.

[47] Le informazioni sui vari Paesi sono tratte da S. TRUMPY - F. CANESCHI, *Rapporti tra Registri dei nomi a dominio e relativi governi*, relazione per la Tavola rotonda organizzata dalla Sezione italiana di *Internet Society* (ISOC), *Internet Governance: pubblici poteri e partecipazione della "Local Internet Community"*, 22 maggio 2002, disponibile in <http://www.isoc.it/tavolarotonda4/trumpy-caneschi.html>.

Numero di registrazioni: circa 250 mila

Canada
Il Registro è gestito dalla CIRA *(Canadian Internet Registration Authority*), società *non-profit*, nel cui Consiglio di amministrazione siede, senza diritto di voto, un rappresentante governativo.

Numero di registrazioni: circa 300 mila

Danimarca
Anche in questo caso la gestione è affidata ad un'associazione senza scopo di lucro, la DIFO, riconosciuta ufficialmente nel 1999 dal Ministero della *Information Technology and Research.*

Numero di registrazioni: circa 425 mila

Finlandia
Il Registro viene gestito dalla FICORA, agenzia governativa appartenente al Ministero dei trasporti e comunicazioni.

Numero di registrazioni: circa 40 mila

Francia
Il Registro è gestito dall'associazione senza fini di lucro AFNIC. Il Consiglio di amministrazione è composto di 10 membri: 5 eletti e 5 nominati tra i quali 2 rappresentanti governativi (Ministeri industria, ricerca e telecomunicazioni).

Numero di registrazioni: circa 165 mila

Germania
Il Registro è gestito dalla DENIC, un'organizzazione senza fini di lucro composta sostanzialmente dai *provider*, che non ha un rapporto formale con il Governo (non esiste legislazione specifica) e si limita ad uno scambio di informazioni. La scarsa burocrazia e la regolamentazione "aperta" della Germania hanno fatto sì che il dominio ".de" sia al secondo posto nel mondo per numero di registrazioni.

Numero di registrazioni: circa 6 milioni

Giappone

L'*Authority* di registrazione è il JPNIC riconosciuto dal Governo con il quale non esistono però rapporti diretti. Da parte del Registro vi è comunque l'impegno ad informare il Governo degli atti di maggior rilievo.

Numero di registrazioni: circa 500 mila

Grecia

Il Registro greco è rappresentato da un istituto della Fondazione per la Ricerca e la Tecnologia (*Institute of Computer Science*). Le regole di *naming* sono invece disposte da un ente esterno che è la Commissione nazionale delle poste e telecomunicazioni.

Numero di registrazioni: circa 55 mila

Irlanda

La registrazione è gestita da un'associazione *non-profit* supervisionata dal Governo. L'autorità regolamentare è esterna ed è rappresentata all'interno del *Advisory Group* del Registro.

Numero di registrazioni: circa 35 mila

Lussemburgo

Il Registro è gestito da una fondazione, la RESTENA. I rapporti tra il Registro e il Governo sono stati recentemente oggetto di studio da parte di un gruppo di lavoro *ad hoc*.

Norvegia

L'attuale agenzia di registrazione è la NORID, derivazione della rete per la ricerca norvegese che dipende dunque dal Ministero per l'università e la ricerca. L'attività di controllo è attribuita all'*Authority* per le poste e le telecomunicazioni che agisce di concerto con il relativo ministero.

Numero di registrazioni: circa 165 mila

Nuova Zelanda

Gestisce la registrazione la società InternetNZ, ente *non-profit* a numero di soci illimitato. All'interno del Registro esiste un comitato di supervisione in cui rappresentato il governo.

Olanda

Il Registro è gestito dal SIDN, fondazione senza fini di lucro all'interno della quale il Governo non è rappresentato. Sulla gestione del Registro riferisce comunque al Governo un apposito gruppo di lavoro costituito nel 2000 dal direttorato generale delle telecomunicazioni del Ministero dei trasporti, lavori pubblici e telecomunicazioni.

Numero di registrazioni: circa 860 mila

Portogallo

La registrazione è affidata al FCCN, fondazione privata *non-profit* afferente al Ministero dell'università e della ricerca.

Numero di registrazioni: circa 25 mila

Spagna

Della registrazione si occupa un ente pubblico, il Red.es, collegato al Ministero della scienza e tecnologia.

Numero di registrazioni: circa 45 mila

Svezia

Il Registro è gestito dall'IIS *(Internet Infrastructure Foundation*) che tramite una sussidiaria - la nic.se - svolge questa funzione. Le relazioni formali con il governo, per ora non presenti, sono oggetto di studio. Dopo una specifica raccomandazione governativa è in corso di attuazione la liberalizzazione del Registro.

Numero di registrazioni: circa 100 mila

Svizzera

Il Registro è gestito da una fondazione accademica, la SWITCH. E' in preparazione una relazione formale con il Governo tramite la stipula di un contratto. Nel Consiglio di amministrazione della fondazione sono rappresentate le università associate.

Numero di registrazioni: circa 450 mila

Regno Unito

La registrazione è competenza della Nominet, associazione *non-profit* che ha contatti con il Governo basati sul principio dell'autoregolamentazione. E' allo studio una forma di capacità di intervento governativo solo per il caso di fallimento. Un rappresentante del *Department for Trade&Industry* partecipa, come osservatore, nel *Policy Advisory Board* della Nominet.

Numero di registrazioni: circa 3,7 milioni.

USA

A parte il caso dei nomi a dominio generici di primo livello condivisi con utenti di tutto il mondo, esistono in America anche i registri generici di sola spettanza degli utenti statunitensi. Solo recentemente comunque il Dipartimento del Commercio ha deciso di lanciare il nome ".us", aggiudicando la gestione alla società NeuStar per un periodo di quattro anni.

Numero di registrazioni: circa 165 mila

Per approfondimenti si veda S. TRUMPY - F. CANESCHI, op. cit.

Per i collegamenti ai siti dei registri nazionali si veda <http://www.norid.no/domenenavnbaser/domreg.html>.

VI. L'Autorità di registrazione europea

Di un dominio unico europeo si iniziò a parlare per la prima volta nel 1996, in uno dei primi interventi ufficiali della Commissione europea in tema di *governance* della rete. Negli anni successivi, la Commissione europea si impegnò sempre più frequentemente alla soluzione di disaccordi con il Governo degli Stati Uniti che - in relazione alla regolamentazione dei nomi a dominio di Internet - rivendicava la propria posizione di "inventore" del *web* e pertanto quella di giudice naturale, attraverso l'ICANN, della risoluzione dei conflitti sorti. L'atteggiamento monopolistico degli USA cominciò ad essere criticato e in Europa si avvertì sempre più forte l'esigenza di creare nella rete uno spazio giuridico proprio. Tutto ciò avrebbe dovuto realizzarsi con la creazione di uno specifico dominio e di un'*Authority* europea. Nel 1999 fu elaborato il progetto *eEurope*, illustrato successivamente dalla Commissione in occasione del Consiglio europeo di Lisbona del 23 e 24 marzo 2000. Nella seduta del 2 luglio 2001, il

Parlamento europeo ha approvato una risoluzione legislativa destinata a dare il via all'utilizzo di un *Top Level Domain*, caratterizzato dall'uso del suffisso ".eu", che segnala, rispetto al registrante, l'identità e lo statuto di organismo di diritto europeo. L'iniziativa *eEurope,* inoltre, ha prospettato altre mete da raggiungere con scadenze precise: lo sviluppo di un nuovo tipo di accesso ad Internet, non più via filo ma utilizzando frequenze radio, per aumentare la velocità di trasmissione dei dati; la diminuzione delle tariffe e l'attuazione di una *deregulation* nel campo dei servizi di accesso. Si è arrivati alla messa in opera del dominio europeo di primo livello nel 2002, con l'approvazione del Regolamento n. 733/2002[48]. L'organizzazione, l'amministrazione e la gestione del dominio, nonché la manutenzione delle banche dati e dei servizi correlati di interrogazione destinati al pubblico, il riconoscimento dei *registrars*, la gestione dei *server* e la diffusione dei *file* di zona sono affidati al consorzio EUTid (*European Registry of Internet Domain Names*), con sede in Belgio, che ha già registrato il primo dominio, denominato "www.eurid.eu." In futuro, oltre alla sede principale di Bruxelles, l'EURid avrà altre sedi situate nelle regioni Nord, Sud ed Est d'Europa. Il Consiglio di amministrazione di EURid comprende i rappresentanti dei membri fondatori e di quelli associati. I membri fondatori del consorzio sono: il DNS Belgium vzw/asbl, l'Istituto di informatica e telematica del C.N.R. (IIT-CNR) e il *Network Information Centre Sweeden AB* (NIC SE). I membri associati sono, per il momento, solo l'Arnes (Slovenia) e il CZ NIC (Repubblica Ceca) ma dovranno, in futuro, comprendere i rappresentanti degli Stati membri e di quelli candidati secondo il seguente schema:

- 2 membri rappresentanti dei Paesi candidati (in prima istanza Slovenia e Repubblica Ceca);

- 1 rappresentante di EuroISPA ovvero di altri organismi rappresentativi dei *registrars/ISPs;*

- 1 rappresentante di UNICE o altri organismi di rappresentazione del settore commerciale europeo;

- 1 rappresentante di ISOC o altri organismi rappresentativi della comunità degli utenti Internet;

- 1 rappresentante di EURid;

[48] Per il testo dell'atto normativo si consulti <http://www.europa.eu.int/eur-lex/>.

- 1 rappresentante della comunità accademica e di ricerca (TERENA o simili).

Il Regolamento europeo prevede che il Registro concluda con l'ICANN un contratto che dispone la delega del codice di dominio di primo livello, nel rispetto dei princìpi del GAC. I soggetti abilitati a richiedere la registrazione sono le imprese con sede legale o sede di affari principale nel territorio della Unione europea, le organizzazioni (anche queste con sede nell'Unione europea) e le persone fisiche residenti nel territorio comunitario. Le regole di politica pubblica per la messa in opera e il funzionamento del dominio ".eu" vengono adottate dalla Commissione europea con l'assistenza del comitato per le comunicazioni, istituito dalla direttiva 2002/21/CE del 7 marzo 2002. La Comunità europea mantiene tutti i diritti connessi con il dominio e, in particolare, quelli di proprietà intellettuale e quelli relativi alle banche dati del Registro. Il 28 aprile 2004 la Commissione europea, adottando il Regolamento n. 874/2004, ha disposto le norme applicative per la messa in opera del dominio europeo di primo livello. Secondo tali norme si riconosce ai soggetti legittimati la possibilità di registrarsi con uno o più nomi a dominio. I nomi a dominio, qualora siano disponibili adeguate norme internazionali, devono essere registrati utilizzando tutti i caratteri alfabetici delle lingue ufficiali dell'Unione europea. Il nome ufficiale degli Stati membri può essere registrato nel dominio europeo su richiesta dei governi nazionali. I Paesi candidati e non ancora aderenti all'Unione, alla data di maggio 2004, così come quelli aderenti allo Spazio economico comunitario, possono richiedere di non venire registrati direttamente nel dominio europeo. Il Capo IV del Regolamento introduce un regime transitorio che prevede la registrazione nel dominio "per fasi", tenendo in questo modo conto dei diritti preesistenti. L'inizio della registrazione per fasi è stata realizzata il 1° maggio 2004 per una durata di 4 mesi ed è stata articolata in due bimestri. Le prime registrazioni saranno quelle per i marchi nazionali registrati seguite da quelle riguardanti i titolari di diritti preesistenti. La convalida dei nomi è compito degli agenti di convalida - persone giuridiche con sede nel territorio dell'Unione con accertata reputazione e adeguata competenza - scelti dal Registro che cura anche la pubblicazione, sul proprio sito Internet, delle informazioni che li riguardano. Una copia elettronica del contenuto della base di dati eu. - denominata WHOIS - dovrà essere inviata quotidianamente dal Registro ad un agente depositario che ha concluso con la Commissione un contratto di deposito. Il Registro ha facoltà di bloccare o revocare la registrazione di nomi illeciti che gli organi

giurisdizionali dei singoli Paesi membri ritengano diffamatori, razzisti o contrari all'ordine pubblico. Per la revoca e la risoluzione delle controversie, il Capo IV del Regolamento contempla sia una procedura attivata direttamente dal Registro, per casi specificamente indicati, sia una procedura extragiudiziale dei contenziosi, affidata ad arbitri o a commissioni arbitrali, i cui membri sono designati da fornitori del servizio di risoluzione delle controversie. Questi ultimi sono organismi di accertata reputazione, dotati di appropriate competenze che vengono individuati dal Registro. Ancora in ambito europeo, infine, va segnalata una notizia degli ultimi giorni[49]che riguarda la proposta, avanzata dal Parlamento, di registrare domini con estensione ".kid" riservati ai minorenni. I siti con questa denominazione, interamente dedicati ai bambini e ai ragazzi, sono finalizzati a tutelare la navigazione dei giovani in Internet proteggendoli non solo dai siti a carattere pornografico ma anche da quelli che propongono immagini violente o che, in ogni caso, diffondono contenuti non facilmente elaborabili dai più piccoli. La Commissione, che ha accettato la proposta parlamentare, ha a sua volta suggerito l'istituzione di un'Autorità indipendente deputata al controllo delle richieste e dei requisiti dei siti che vogliono adottare il nuovo suffisso.

RIEPILOGO OBBLIGHI DEL REGISTRO

1. registrazione dei nomi a dominio richiesti;
2. adozione della politica di registrazione per il TLD.eu in consultazione con la Commissione e le parti interessate e in linea con le regole della politica pubblica;
3. applicazione dei diritti connessi ai costi sostenuti;
4. attuazione della politica e della procedura di risoluzione delle controversie in sede extragiudiziale;
5. adozione ed espletamento delle procedure per il riconoscimento dei conservatori di dominio .eu;
6. assicurazione dell'integrità delle banche dati dei nomi a dominio.

Per approfondimenti si veda < http://www.eurid.eu/>.

[49] La notizia è del 13 settembre 2005.

B - L'ACCESSO ALLA RETE: ASPETTI STRUTTURALI

I. Il flusso delle informazioni e la rete[50]

1. L'informazione digitalizzata

La "rivoluzione digitale" determinata dalla possibilità di trasformare un segnale analogico in uno digitale ha realizzato la convergenza tra il mondo delle telecomunicazioni e quello dell'informatica. Si tratta di una realtà ormai consolidata, tanto è vero che oggi possiamo comunemente parlare di *Information and Communication Technology* (tecnologie dell'informazione e della comunicazione) intendendo, con tale espressione, un tutto unico tra informatica e telecomunicazioni. La peculiarità dell'informazione archiviata in formato digitale - utilizzata in via sperimentale negli anni Sessanta - è la sua grande facilità di movimento conseguente alla maggiore velocità con cui viaggia l'energia rispetto alla materia. Come si sa è possibile rappresentare un qualsiasi segnale secondo due modelli: analogico e digitale. Per analogica si intende la rappresentazione continua e simile al reale (*analoga* appunto) di un determinato impulso. Viceversa la rappresentazione digitale è discontinua e l'informazione è codificata in una serie numerica. Ciò è possibile "spezzettando", per così dire, il segnale in tante misurazioni singole ravvicinate nel tempo (introduzione della discontinuità)[51]. Poiché ogni misurazione può essere tradotta in un valore, sarà possibile produrre, da un segnale, una sequenza numerica. La sequenza così ottenuta - poiché non ancora adatta ad essere trasmessa tramite computer - è trasformata in codice binario, cioè in un'alternanza di numeri zero ed uno, che prende il nome di *bit*.

Ogni *bit* è codificato mediante uno o più impulsi discreti e discontinui, denominati elementi del segnale. Naturalmente al numero "zero" corrisponderà una codifica ed al numero "uno" ne corrisponderà un'altra. Dal punto di vista pratico si possono utilizzare diversi generi di segnali: due livelli distinti di tensione elettrica, ad esempio, oppure due

---

[50] Le informazioni tecniche contenute in questo capitolo sono tratte da diversi lavori quali: B. PAVOLETTI, *I concetti fondamentali di Internet*, Regione Liguria, Servizio Sistemi Informatici, 1999; A. SPERLINGA, *Piccolo corso di Internet, edizione minima* in <http://www.alessiosperlinga.it > e <http://encyclopedie-it.snyke.com/articles/rete_telematica.html>.

[51] A. SPERLINGA, op.cit.

frequenze di emissione elettromagnetica, o ancora due impulsi luminosi emessi da un laser[52].

Il passaggio da informazione analogica a digitale e viceversa comporta un processo di **modulazione/demodulazione**. Si tratta in sostanza di modificare (o modulare) alcuni parametri del segnale che trasporta l'informazione (detto portante) in modo tale da codificare opportunamente i numeri 1 e 0 della fonte. In particolare, i parametri che possono essere modulati sono la frequenza e l'ampiezza o fase del segnale analogico. A destinazione si realizzerà il processo inverso, che consente di estrarre dal segnale modulato la codifica binaria originale. Purtroppo un segnale modulato che viaggia lungo una linea è soggetto a notevoli interferenze. Questo limita la quantità di *bit* che può essere trasmessa nell'unità di tempo lungo il canale.

La modulazione e la demodulazione si attuano tramite appositi apparecchi chiamati *modem*[53]. I *modem* rappresentano la più semplice, anche se non la sola, interfaccia di rete. Essi si possono collegare al computer in vari modi. Ve ne sono di esterni, i più diffusi, che si presentano come piccole scatole di plastica, dotate di una presa telefonica e di una presa di tipo seriale. La presa si collega al computer mediante un apposito cavo da inserire nella porta seriale, in dotazione su tutti i moderni *personal computer*. Di recente sono comparsi *modem* che utilizzano un nuovo tipo di porta presente nei computer più evoluti: la porta USB (*Universal Serial Bus*), con caratteristiche di velocità ed efficienza maggiori rispetto a quella tradizionale seriale. Infine esistono anche dei *modem* interni, che possono cioè essere inseriti direttamente in uno degli *slot* di espansione presenti sulla piastra madre del computer. Attualmente i migliori *modem* permettono di ricevere dati con una banda passante teorica di 56 Kbps e di inviare a 32 Kbps[54].

---

[52] Nel caso più semplice, ad ogni *bit* corrisponde un singolo segnale: allo zero corrisponde un livello basso di tensione elettrica e all'uno un livello alto. Una codifica come questa, però, può facilmente generare errori, dovuti ad esempio ad interferenze elettriche che trasformano i segnali corrispondenti al numero uno in segnali corrispondenti allo zero e viceversa. Per questa ragione, nei sistemi di telecomunicazione digitale reali, si usano schemi più complessi, che associano coppie o triplette di elementi del segnale ad ogni *bit*. Questi sistemi di codifica più complessi presentano dei vantaggi in termini di capacità di ricostruzione del segnale e di individuazione e controllo degli errori di trasmissione.

[53] I primi *modem* in grado di svolgere l'operazione di modulazione e demodulazione risalgono alla fine degli anni cinquanta. Essi non superavano i 300 bps. Quelli attuali, più veloci, sono riusciti a raggiungere la velocità di 56 Kbps, anche se tale velocità teorica, e soprattutto può essere raggiunta solo in un verso di trasmissione. Siamo infatti ai limiti fisici che questa tecnologia in grado di conseguire.

[54] Chilo-bit per secondo.

I limiti derivanti dalla velocità di modulazione dei *modem* sono bilanciati dall'opportunità che questi offrono di collegare il computer - sfruttando l'infrastruttura telefonica - ad una rete che ha una diffusione capillare e che arriva direttamente alle abitazioni private. Questo tipo di accesso alla rete si definisce convenzionalmente "ultimo miglio". In genere si tratta di una connessione temporanea, che si prolunga fintanto che l'utente ha necessità di utilizzare i servizi di rete (anche perché in molti paesi la tariffa per l'impiego delle linee telefoniche è calcolata in base al trascorrere del tempo).

2. La tramissione delle informazioni

La trasmissione di dati in formato digitale su una rete avviene generalmente suddividendo il messaggio in "pacchetti" di dimensione fissa o variabile. Questo consente un utilizzo più agevole ed efficiente dei mezzi trasmissivi, la condivisione della rete e l'implementazione di algoritmi per distribuzione della banda tra i vari utenti. La trasmissione dei pacchetti è governata da un insieme di protocolli attivi su tutti gli *host*[55] e su tutti gli apparati che costituiscono la rete. I protocolli fanno in modo che l'informazione giunga correttamente a destinazione e che l'utente possa fruirne.

Un protocollo è un insieme di regole, algoritmi[56] e tecniche per la manipolazione e la trasmissione di dati. I protocolli necessari al funzionamento di una rete come Internet sono moltissimi e in genere risulta utile classificarli rispetto alla cosiddetta "pila ISO/OSI". Questa classificazione, che nella sua definizione originaria faceva riferimento a protocolli ora in disuso, è ormai divenuta molto comune perché consente di classificare con semplicità ed immediatezza qualunque tipo di protocollo individuandone le funzioni e le interfacce.

Sinteticamente la pila ISO/OSI suddivide e classifica i protocolli in 7 livelli[57]:

[55] Da "ospite" (colui che ospita). Unità di elaborazione principale. E' il computer remoto, chiamato anche "end node", attraverso il quale gli utenti possono comunicare con tutte le macchine connesse.

[56] Si tratta di un procedimento che dà vita ad un insieme di regole per la risoluzione di un calcolo numerico.

[57] Si veda S. TANENBAUM, *Reti di calcolatori,* Milano, Pearson Education Italia, 2003.

- Livello 1 - Fisico
  I protocolli di questo livello si occupano dell'interazione con il mezzo fisico di trasmissione realizzando la modulazione/demodulazione delle sequenze binarie 1/0 in segnali adatti al mezzo trasmissivo.

- Livello 2 - Data Link
  A questo livello i protocolli si occupano della trasmissione/ricezione di trame (pacchetti) provenienti dal livello 3. Si compiono inoltre controlli sull'integrità dei pacchetti, si attuano strategie di correzione/individuazione di errori e si gestiscono le connessioni punto-punto o multipunto con altre stazioni che condividono lo stesso mezzo trasmissivo o canale.

- Livello 3 - *Network*
  Comprende protocolli che realizzano il *routing* ossia l'instradamento dei pacchetti dalla sorgente alla destinazione, secondo il percorso più conveniente. E' a questo livello che reti fisiche diverse possono essere interconnesse condividendo un unico protocollo di livello 3 e un unico spazio di indirizzamento (come Internet e il protocollo IP).

- Livello 4 - Trasporto
  I protocolli di questo livello realizzano un collegamento *end-to-end* tra due *host* sulla rete implementando un canale affidabile che provvede a correggere gli errori, ritrasmettere dati persi, controllare e prevenire la congestione della rete e ordinare il flusso di dati ricevuto.

- Livello 5 - Sessione
  I protocolli di questo livello arricchiscono il canale affidabile creato dal livello 4 di ulteriori funzionalità per la sincronizzazione degli *host*, il mantenimento di sessioni di conversazione e la gestione e il controllo dei flussi di dati.

- Livello 6 - Presentazione
  A questo livello si effettuano eventuali conversioni di formato necessarie a far interoperare sistemi eterogenei.

- Livello 7 - Applicazione
  Vi sono classificati tutti i protocolli che realizzano un'applicazione per l'utente finale (trasferimento *file*, terminale remoto, posta elettronica etc.).

I principali protocolli in uso su Internet e, in generale, sulle moderne reti IP possono - rispetto alla pila ISO/OSI - essere così classificati:

Livelli 1 e 2 (questi due livelli sono spesso accorpati in quanto molti protocolli li implementano entrambi)	**Ethernet, Token Ring, ATM** (al 1/2), **Sonet** etc. **PPP** (Prettamente di livello 2 che può utilizzare come livello 1 v35, v90, x25 etc.)
Livello 3	**IP** (Protocollo di livello 3 puro) **ICMP, RIP, OSPF, BGP** (Protocolli di controllo e di scambio informazioni sul *routing*, in aggiunta ad IP)
Livello 4	**TCP** (Trasporto affidabile) e **UDP** (trasporto *best effort*[58])
Livello 5, 6 e 7 (questi livelli sono su Internet tipicamente implementati in un unico protocollo).	**HTTP** (*web*, trasferimento di *file* ipertestuali) **FTP** (trasferimento di *file*), **POP3/IMAP/SMTP** (posta elettronica), **DNS** (risoluzione dei nomi)

Ogni *host*, dotato di un insieme minimo di protocolli necessari, può essere interconnesso alla rete Internet e può potenzialmente scambiare dati con tutti gli altri *host*. Dal punto di vista del protocollo IP (minimo comune denominatore di tutti gli *host* di Internet) tutte le macchine interconnesse in rete e dotate di un indirizzo sono perciò equivalenti. In realtà comunemente gli *host* sono specializzati e svolgono una certa funzione, ad esempio:

- gli *host* specializzati nell'erogare uno specifico servizio sono detti ***Server*** (*Server* di posta elettronica, *server* dei nomi etc.);

[58] Al meglio delle possibilità, ma senza una qualità minima garantita.

- gli *host* che utilizzano i servizi erogati dai *server* sono detti ***Client.*** Spesso i *client* non sono specializzati e possono utilizzare più di un *server*. Un normale pc *desktop* utilizzato da un utente domestico è un perfetto esempio di *client* non specializzato.

Questa modalità di cooperazione è detta comunemente paradigma "*client-server*". Esiste tuttavia una seconda modalità chiamata "*peer to peer*" nella quale un insieme omogeneo di *host* collabora e coopera nell'erogare un servizio. In pratica ogni macchina che partecipa ad una sessione *peer to peer* svolge contemporaneamente sia il ruolo di *client* sia quello di *server*. Questo paradigma è tipicamente usato dalle applicazioni di *file sharing* in cui ogni utente mette a disposizione di tutti gli altri i suoi *file* e contemporaneamente usufruisce di tutti gli altri *file* condivisi.

Tutti i protocolli applicativi citati sino ad ora si basano su comunicazioni di tipo *Unicast*, ossia punto-punto. Tuttavia il protocollo IP prevede la possibilità di realizzare anche comunicazioni *Multicast* ossia da uno a molti.

La comunicazione *multicast* presenta il vantaggio di limitare, ove possibile, la replicazione dei dati sulla rete. Quando i destinatari di un messaggio *multicast* sono più di uno e condividono una parte del percorso dalla sorgente alla destinazione, su questa parte condivisa, il messaggio non è replicato, con ovvi vantaggi sulla velocità di trasmissione e sulla banda occupata. Le comunicazioni *multicast* tuttavia sono, per loro natura, unidirezionali e con una affidabilità di tipo *best effort*; per questo motivo ben si adattano a trasportare su Internet flussi di dati multimediali (*streaming* audio e video) che sono tipicamente unidirezionali, necessitano di *performance* costantemente elevate e sopportano agevolmente la sporadica perdita di qualche pacchetto.

Per poter operare correttamente, una rete *multicast*[59] deve "conoscere" quali siano gli *host* (o gruppi di *host*) interessati a ricevere un determinato flusso. Queste informazioni sono raccolte dai *router multicast* che colloquiano con gli *host* utilizzando un protocollo chiamato IGMP (*Internet Group Management Protocol*).

---

[59] Visto l'interesse suscitato da questa tecnologia, nel *World Wide Web* sono nati numerosi *forum* di discussione cui partecipano anche molte importanti aziende. All'indirizzo www.ipmulticast.com, è possibile recuperare informazioni relative alla Ip *Multicast* Initiative, un *forum* a livello mondiale che si propone di accelerare l'adozione dell'Ip *Multicast*. Presso il sito della IPMI (all'indirizzo <http://www.ipmulticast.com>), è disponibile anche una relazione aggiornata sull'evoluzione dell'Ip *Multicast* fino a oggi.

La tecnologia Ip *Multicast* fu introdotta per la prima volta dall´ingegnere Steve Deering, nel 1988. Fu sperimentata su larga scala durante un convegno dell´*Internet Engineering Task Force* nel 1992, a San Diego, in California. Grazie a questo esperimento gli utenti di 20 siti connessi poterono ascoltare il dibattito di un convegno contemporaneamente. L´interesse suscitato da questa tecnologia spinse matematici e ingegneri a studiare nuovi e diversi algoritmi di *routing*[60], fino a realizzare il precursore della prima rete sperimentale *multicast*, denominata *Multicast Backbone* (Mbone). Un´alternativa a questa metodologia di *routine è* rappresentata dalla scansione ad alberi in cui la rete è vista come un insieme di *link* (alcuni marcati come non accessibili qualora non si fossero precedentemente registrati) che rappresentano i nodi dell´albero e che sono attraversati una sola volta; questo comporta una minore efficienza della struttura, ma garantisce, di contro, che i pacchetti di dati passino una sola volta per ogni nodo.

3. Cos'è una "rete"

Utilizzando un esempio molto semplice possiamo pensare una rete come un collegamento che si realizza già nel normale funzionamento di un singolo PC. I *bit*, infatti, viaggiano continuamente tra i vari componenti dell'elaboratore, attraverso dei canali detti *bus*: l'informazione passa dalla memoria alla CPU[61]; dalla CPU alla scheda grafica; dalla scheda grafica, al *monitor*.

Una vera rete di computer, invece - così come comunemente la intendiamo - non fa altro che estendere questa "capacità di circolazione" dei *bit* tra computer diversi secondo due gerarchie logiche: quelle dei già ricordati paradigmi *client/server* e *peer to peer* (o paritetica).

Riassumendo, una **rete** è dunque un insieme di computer collegati attraverso un sistema di cavi e connessioni o attraverso tecniche di telecomunicazioni radio (o ricetrasmittenti ottici). Il percorso migliore per far comunicare due computer connessi ad una rete è scelto da un dispositivo *hardware* detto *router,* cioè un computer di commutazione che instrada (il nome *router* deriva proprio dal verbo inglese *to rout,* instradare) i pacchetti di dati verso il relativo computer di destinazione, servendosi dell'indirizzo IP. L'indirizzo IP di un pacchetto di dati comunica a quale sottorete, a quale altro *router* o computer devono essere inviati i dati. Una

---

[60] La modalità, cioè, con cui i pacchetti di dati vengono trasmessi da un indirizzo IP ad un altro.

[61] Si tratta del microprocessore del computer, ossia della parte "intelligente" che realizza i calcoli.

volta individuato il percorso, il pacchetto viene spedito ed inizia il flusso dei dati verso la destinazione. Il *router* deve inoltre spedire questi dati nel formato più adatto per il trasferimento delle informazioni. Ciò significa che può "decidere" di reimpacchettare i dati o di frammentarli in pezzi più piccoli, in modo che il destinatario li possa gestire.

4. Le diverse tipologie di reti fisiche

Le reti sono distinte e classificate secondo diversi parametri: estensione, topologia geometrica e logica, mezzi fisici utilizzati per la trasmissione. Sulla base della loro **estensione** si parla di reti LAN, MAN, WAN e GAN. Vediamo di cosa si tratta nel dettaglio:

- la rete **LAN (*Local Area Network*)** è di livello locale costituita da un insieme di computer collegati tra loro e ubicati fisicamente nello stesso luogo, per esempio all'interno di un'area aziendale, un'abitazione privata, una scuola, un centro di ricerca, ecc. Talvolta una rete locale si estende su aree più vaste, spesso collegandosi ad altre reti locali: in questo caso si parla di reti dipartimentali;

- la rete **MAN (*Metropolitan Area Network*)** è di livello o area metropolitana. In questo caso, i computer si trovano all'interno di un'area urbana di grandi dimensioni oppure sono dislocati in più comuni limitrofi. Fra i vari esempi, prendiamo in considerazione quello riguardante più computer interconnessi tra loro e collegati ad un *server* centrale nell'intero territorio comunale e quello relativo ai PC delle segreterie delle facoltà universitarie dislocate in una determinata area metropolitana;

- la rete **WAN (*Wide Area Network*)** copre aree di vaste dimensioni, ad esempio l'intero territorio nazionale o addirittura gli stati con esso confinanti;

- la rete **GAN (*Global Area Network*)** è di livello o area globale o meglio di una rete di reti che collegano computer dislocati in tutti i continenti. Diverse le tecnologie impiegate per interconnettere le macchine: dal cavo in rame del comune doppino telefonico agli avanzati sistemi satellitari. Internet è un tipico esempio di GAN.

Riguardo poi alla **forma o "topologia"** si avranno reti a maglie o reti distribuite, reti a stella, reti a *bus*, reti gerarchiche, reti ad anello[62].

Le reti a maglie o reti distribuite sono reti in cui ogni singolo nodo è collegato con molti altri nodi, al limite con tutti (quest'ultima topologia fornisce la massima efficienza, ma rende veramente complicata e costosa l'aggiunta di nuovi nodi alla rete). In una rete di questo tipo i messaggi sono inoltrati da un nodo all'altro scegliendo uno dei molti percorsi disponibili. La scelta del percorso può avvenire in modo dinamico, secondo le condizioni di traffico. In ogni caso il percorso di un messaggio impegna solo un sottoinsieme dei nodi disponibili, e ciascuno per un tempo limitato. Inoltre, grazie alla ridondanza dei collegamenti tra i nodi, le reti a maglie offrono un alto livello di affidabilità. Infatti, l'interruzione di un collegamento o la rottura di un nodo non pregiudica la funzionalità complessiva del sistema. Per questo la topologia distribuita si presta alla costruzione di grandi reti geografiche con moltissime nodi.

Le reti a stella, come la definizione lascia supporre, sono strutturate su un nodo centrale (detto *hub*) al quale sono connessi tutti gli altri nodi periferici. La comunicazione tra due nodi viene mediata sempre dal nodo centrale. Questo tipo di configurazione è utilizzato spesso nelle reti locali[63].

Nelle reti a *bus* tutti i nodi sono collegati a un cavo lineare (*bus*) mediante delle diramazioni cui sono collegati i computer. In alcuni casi le reti a *bus* possono avere come diramazioni dei *bus* secondari, assumendo una topologia ad albero. In questo tipo di rete tutti i nodi condividono un medesimo canale di trasmissione, ed inoltre ogni messaggio viaggia sempre in tutte le direzioni, ciò che comporta notevoli problemi di controllo della trasmissione e circoscrive l'uso della topologia alla realizzazione di reti locali, dove il numero di nodi è limitato.

Le reti ad anello infine, sono costituite da una serie di nodi interconnessi in modo da formare un anello chiuso. A differenza delle precedenti reti a *bus*, in queste reti i dati viaggiano sempre nella stessa direzione da un nodo all'altro finché non giungono al nodo destinazione.

---

[62] Nel caso delle reti gerarchiche le informazioni si diffondono da un punto centrale verso la periferia e viceversa, mentre nelle reti distribuite (ed è il caso delle reti Internet) esse si muovono liberamente da un punto all'altro su un medesimo livello.

[63] Una topologia ibrida tra rete a stella e rete distribuita (detta anche rete a stella interconnessa) caratterizza invece la rete telefonica: essa infatti è costituita da una costellazione di centrali locali, alle quali afferiscono le linee degli utenti, a loro volta collegate tra loro.

Questo limita i problemi di congestione ma rende meno efficiente l'utilizzo della rete (ogni nodo rifiuta nuovi messaggi finché non ha terminato di ritrasmettere il precedente) e soprattutto può generare dei dati che circolano indefinitamente lungo l'anello.

Per utilizzare le diverse topologie fisiche sopra descritte sono stati sviluppati diversi protocolli (di livello 1 e 2 rispetto alla pila ISO/OSI già descritta)

Tali protocolli determinano le regole per il trasferimento dei dati in rete locale. Le principali sono: Ethernet, Token Ring e FDDI. Tali tecnologie non possono comunicare direttamente tra loro, ma solo attraverso l'ausilio di particolari dispositivi denominati *bridge.* In sostanza esse non possono coesistere sugli stessi cavi o segmenti di rete.

La tecnologia Ethernet è nata nel 1973 e si basa sul sistema è denominato CSMA/CD (*Carrier Sense Multiple Access/Collision Detection* - Accesso multiplo a rilevazione di portante/individuazione delle collisioni) che, seppur molto semplice, è sufficientemente efficace a garantire una discreta velocità di trasferimento dei dati. Il suo funzionamento è, in breve, il seguente: se due computer cercano di trasmettere dati contemporaneamente sullo stesso cavo di rete, si crea una collisione di dati che viene rilevata da entrambi. I computer interrompono pertanto la trasmissione e attendono un intervallo di tempo casuale (misurato in nanosecondi) prima di ritentare la trasmissione. Questa tecnologia, notevolmente perfezionata nel tempo grazie soprattutto al lavoro di standardizzazione effettuato dall'IEEE (*Institute of Electrical and Electronics Engineer*), è attualmente quella predominante per le reti locali e consente di raggiungere velocità di trasferimento considerevoli. Si pensi che dal 1973 ad oggi si è passati da una velocità di 10 Mbit a 1 Gbit su cavo di rame e a 10 Gbit su fibra ottica. Quanto alla standardizzazione si ricorda che per ogni mezzo fisico usato per la trasmissione e per ogni valore di velocità esiste uno specifico protocollo[64].

[64] La standardizzazione IEEE 802.3 prevede per Ethernet i seguenti protocolli:

10BASE5 e 10BASE2	Ethernet su cavo coassiale
10BASE-T	Ethernet su cavo UTP/STP
10BASE-F	Ethernet su cavo in fibra ottica
100BASE-TX	Ethernet a 100 Mbit/s su cavo UTP/STP
100BASE-FX	Ethernet a 100 Mbit/s su cavo in fibra ottica
1000BASE-T	Ethernet a 1000 Mbit/s su cavo UTP/STP
1000BASE-SX (-LX, -CX)	Ethernet a 1000 Mbit/s su cavo in fibra ottica

Nella tecnologia *Token Ring* un particolare segnale elettronico circola sulla rete: si tratta del *token* ("gettone" o "testimone") che passa da macchina a macchina in un circuito chiuso. Per tale motivo questo metodo di trasmissione richiede una topologia fisica di rete ad anello. Il funzionamento di questa rete ricorda la cosiddetta "staffetta" in cui in pratica il computer che deve trasmettere i dati aspetta il passaggio del *token*. Se quest'ultimo è vuoto, la macchina lo carica con il suo pacchetto dati, aggiungendo agli stessi alcune informazioni che contengono l'indirizzo del computer a cui recapitarli. Eseguita tale operazione, il *token* è reinserito in rete e inizia il viaggio verso la macchina designata. Una volta giunto a destinazione, la stazione ricevente preleva i dati in esso contenuti e lo rispedisce vuoto al mittente. Il *token* vuoto funge dunque da "ricevuta di ritorno", a garanzia dell'avvenuta consegna. A conclusione del processo sopra descritto, la stazione mittente reinserisce il *token* nella rete per un utilizzo successivo.

Lo standard FDDI (*Fiber Distributed Data Interface* - Interfaccia a fibra ottica) è basato su una topologia ad anello in fibra ottica che opera attualmente ad una velocità di trasmissione dati pari a 100 MHz. Lo standard FDDI può essere utilizzato per distanze molto lunghe; consente infatti la connessione tra stazioni distanti fino a 2-3 chilometri e offre una copertura dell'intera rete fino a 100 chilometri di distanza. La fibra ottica è costituita da un filamento in vetro rivestito da Kewral, un materiale ad altissima resistenza alla lacerazione e alla corrosione. Utilizza la luce come mezzo per la trasmissione dei dati. Non è percorsa da corrente elettrica ed è insensibile non solo alle radiazioni elettromagnetiche, ma anche a tutte le altre interferenze. Possiede una banda molto larga. Questo tipo di rete dispone inoltre di un doppio anello in fibra ottica. Nel caso in cui l'anello principale si guasti, gli apparati FDDI utilizzano l'anello di riserva.

E' bene in ogni modo precisare che sia la tecnologia *Token Ring* sia la FDDI sono oggi impiegate solo marginalmente.

Affinché le informazioni codificate possano viaggiare lungo una rete telematica, o più in generale lungo un qualsiasi sistema di telecomunicazione, è necessario un mezzo di trasmissione che colleghi il trasmettitore ed il ricevitore. Tale mezzo può essere un cavo (metallico o in fibra ottica) ed in questo caso si parla di reti *wired,* oppure un'onda elettromagnetica che viaggia attraverso l'etere: sono le reti definite

wireless[65]. Ciascuna di queste soluzioni presenta vantaggi e svantaggi, sia dal punto di vista tecnico (larghezza di banda, resistenza ai disturbi, distanza massima raggiungibile) sia in termini di costi e di manutenzione.

Il più diffuso mezzo di trasmissione è - ancora oggi - la coppia intrecciata di cavi, o doppino ritorto. Si tratta di una coppia di fili in materiale conduttore di elettricità (in genere il rame) intrecciati l'uno con l'altro, in modo tale da ridurre gli effetti delle interferenze. Questa soluzione è adottata sia in applicazioni telematiche sia, soprattutto, nei tratti delle reti telefoniche pubbliche che arrivano fino all'utente, ovvero nel cosiddetto "ultimo miglio"[66]. Purtroppo la coppia intrecciata, rispetto ad altri mezzi, è molto sensibile al rumore. Questo ne limita sia la banda passante che la lunghezza massima oltre la quale il segnale diventa inutilizzabile. Per distanze di poche centinaia di metri, ed usando cavi schermati, si possono raggiungere velocità massime di 10 Mbps. Su distanze maggiori le prestazioni diminuiscono notevolmente: i cavi della rete telefonica che collegano le utenze alle centraline con tratti non superiori al paio di chilometri possono arrivare fino a 8 Mbps, ma viaggiando solo in una direzione, e solo grazie allo sfruttamento intensivo delle tecniche di compressione dei dati. Naturalmente prestazioni migliori possono essere ottenute unendo in un unico cavo una serie di doppini: ad esempio la rete Gigabit Ethernet, un'evoluzione della tradizionale rete Ethernet, usa un cavo composto da 4 coppie su cui riesce sviluppare una banda passante di 1000Mbit.

Nell'ambito delle piccole LAN sono utilizzati soprattutto i cavi UTP (*Unshielded Twisted Pair* o doppino ritorto non schermato) e STP (*Shielded twisted pair* o doppino ritorto schermato). Sono costituiti da 4 coppie di conduttori di rame ritorti. Le coppie così intrecciate sono a loro volta ritorte in un unica spirale. Tale disposizione dei cavetti consente di limitare il campo magnetico generato da ogni singolo cavetto che andrebbe a disturbare il segnale dell'intero cavo di rete.

---

[65] Tra le reti *wireless* la più conosciuta in Europa e la più nuova da un punto di vista tecnologico è la 3G nota come UMTS (*Universal Mobile Telecommunications System*). Questa rete trasmette dati ad una velocità massima di 2 megabit al secondo.

[66] Per esaminare i problemi connessi all'"ultimo miglio" e per lo sviluppo della banda larga, è stata costituita una *task force* tra Ministero delle comunicazioni e Dipartimento per l'innovazione e le tecnologie, con l'obiettivo di individuare lo stato di realizzazione delle infrastrutture e le possibili azioni di governo volte al suo rapido ed equilibrato sviluppo. E' stato altresì istituito, con decreto interministeriale del 28 febbraio 2002 del Ministro delle comunicazioni e del Ministro per l'innovazione e le tecnologie, un Comitato tecnico esecutivo con compiti di coordinamento, guida e verifica a livello tecnico, per realizzare un piano nazionale di sviluppo della larga banda.

I cavi UTP e STP presentano ai due estremi i connettori che s'innestano direttamente nelle prese dedicate delle schede di rete o dei concentratori (*Hub*, *Switch*). Tali connettori sono denominati RJ-45 e sono molto simili a quelli utilizzati nei cavi telefonici, ma a differenza di questi ultimi sono leggermente più grossi. La progressiva diffusione di tecniche di cablaggio strutturato per gli edifici ha decretato il definitivo successo dei cavi a 4 coppie UTP e STP che offrono il miglior compromesso tra costi, semplicità di gestione e prestazioni.

Un altro mezzo di trasmissione molto diffuso nella televisione via cavo e praticamente scomparso in ambito di reti locali, è il **cavo coassiale**. Si tratta di un cavo rotondo composto da vari strati: al centro c'è un filo di rame (di diametro variabile), ricoperto da uno strato di materiale isolante, a sua volta rivestito da un conduttore a maglia, il tutto all'interno di una guaina isolante. Rispetto al doppino, questo tipo di cavo presenta una maggiore resistenza al rumore, ed offre un'ampiezza di banda più elevata: si va dai 140 Mbps su distanze brevi ai 20 o 30 Mbps per tratti di alcune centinaia di metri. E' un cavo simile a quello che trasporta i segnali radio e TV su lunghe distanze, adattato alla comunicazione di dati digitali. Si ricorda che, rispetto a quelli analogici, i dati digitali risultano essere più suscettibili non solo al rumore, ma anche alle distorsioni di segnale che si verificano quando i segnali viaggiano lungo grandi distanze. A causa di ciò, le reti che impiegano il cavo coassiale come mezzo trasmissivo possono estendersi solo per distanze limitate: a meno che non vengano utilizzati dei particolari ripetitori di segnale (*repeater*) aventi la funzione di rigenerare periodicamente il segnale.

Oltre ai mezzi sopra descritti - come anticipato - esistono reti in cui la trasmissione avviene per mezzo della luce (infrarossi, laser) od onde radio (*wireless*).

Nelle reti a fibre ottiche si sfrutta la luce visibile. Si può immaginare una fibra ottica come un sottilissimo tunnel rivestito di specchi, in grado di intrappolare un fascio di luce e di condurlo, attraverso una sequenza di riflessioni, da un capo ad un altro. Per essere più precisi, la trasmissione di un impulso luminoso all'interno di un conduttore si basa su un particolare tipo di rifrazione (anche se denominato "riflessione interna totale"). La rifrazione è la deviazione subita da un raggio di luce nell'attraversare il confine tra due mezzi trasparenti diversi. Un classico effetto di questo fenomeno è l'illusione che una matita immersa in un bicchiere d'acqua si spezzi proprio in corrispondenza della superficie del liquido. L'angolo di

questa deviazione si chiama indice di rifrazione. Ora, se un raggio proviene da un mezzo con l'indice di rifrazione maggiore, e se il suo l'angolo d'incidenza (ovvero l'angolo con cui il raggio di luce incontra il confine tra i due mezzi) è minore di un certa grandezza, esso non riesce più ad attraversare il confine tra i due mezzi e viene riflesso totalmente. In questo modo è possibile intrappolare un raggio di luce dentro un cavo. Entrambi i tipi di fibra ottica esistenti, quello *multimodale* e quello *monomodale,* sono costituiti dai due componenti essenziali, ovvero il nucleo (*core*) e il rivestimento (*cladding*). Il primo ha la funzione di trattenere la luce nel secondo. La fibra multimodale presenta diametri di 50, 62.5 e 100 micron. Le dimensioni del nucleo della fibra monomodale variano invece da 5 a 10 micron. Nella fibra ottica la luce è trasportata attraverso il nucleo. Maggiore è la larghezza del nucleo, maggiore è la quantità di luce emanata. La fibra monomodale, benché più costosa rispetto a quella multimodale, copre una distanza superiore rispetto a quella assicurata da quest'ultima. Il suo nucleo di piccole dimensioni e il suo unico fascio luminoso eliminano qualsiasi tipo di distorsione e garantiscono alte velocità di trasmissione.

I vantaggi apportati dalla tecnologia a fibre ottiche, messa a punto solo negli anni '70 (sebbene i principi fossero già noti sin dagli anni '50), sono numerosi. A differenza dei cavi metallici, una fibra ottica può trasportare enormi quantità di informazioni codificate mediante impulsi di luce per lunghissime distanze. Oggi la banda passante di una singola fibra arriva a trasmettere fino a 2,5 miliardi di bit[67] al secondo! E naturalmente i cavi in fibra ottica che vengono posati effettivamente sono composti da un fascio di fibre. Per avere un'idea della quantità di informazioni che possono passare attraverso tali canali di telecomunicazione, si pensi che una banda passante di 1,7 Gbps permette di trasmettere un milione di conversazioni telefoniche contemporanee. E in sede sperimentale sono state sviluppate delle fibre che arrivano alla velocità di 100 Gbps.

Con questi numeri la fibra ottica si candida dunque ad essere il mezzo di trasmissione ideale per il villaggio elettronico digitale. Oltre alla copertura delle lunghe distanze, già accennata, ed all'assenza di fattori distorsivi, la fibra ottica presenta altri vantaggi quali:

- la sicurezza (è facile scoprire eventuali manomissioni operate nei cavi in fibra ottica, considerando che la fuoriuscita di luce da uno di essi causa l'arresto delle attività del sistema);

[67] Il prefisso per indicare valori dell'ordine del miliardo è "giga", abbreviato "G".

- la bassa attenuazione (il segnale luminoso incontra poca resistenza e in questo modo i dati possono viaggiare più lontano);

- la grande larghezza di banda (la fibra ottica è in grado di trasportare un maggior numero di dati rispetto al rame).

D'altro canto però, il passaggio ad un sistema di comunicazione capillare interamente in fibra ottica, comportando la sostituzione di tutti i preesistenti cavi in metallo, determina alti costi di installazione. Se per le lunghe distanze e per i collegamenti transoceanici questa sostituzione ha un rapporto costi/benefici vantaggioso, ciò non è più vero per il collegamento degli utenti finali. La transizione dell'ultimo miglio alla fibra ottica ha dei costi così alti che poche compagnie telefoniche potrebbero essere disposte ad affrontare.

Nelle *wireless*[68] si utilizzano, come già accennato, le **onde radio**. A differenza della luce e dell'elettricità, queste onde non hanno bisogno di essere trasmesse all'interno di cavi, poiché possono viaggiare per lunghe distanze attraverso lo spazio. Grazie a questa caratteristica esse rappresentano oggi il veicolo preferenziale del sistema delle telecomunicazioni mondiali.

I sistemi di telecomunicazione a onde radio sono basati su diverse tecnologie, a seconda delle esigenze che debbono soddisfare. I collegamenti terrestri per distanze brevi (ad esempio tra due edifici non distanti) adottano antenne paraboliche a microonde di bassa potenza, in grado di creare un cosiddetto "ponte radio". Per le distanze geografiche invece sono necessari apparati di trasmissione assai più potenti e costosi. La necessità di ricorrere ad impianti molto potenti è determinata anche dai forti disturbi cui sono soggetti i segnali radio che viaggiano lungo la superficie terrestre. Un problema di cui non soffrono le trasmissioni radio satellitari. Un satellite artificiale per telecomunicazioni è, in effetti, una stazione ripetitrice a microonde, in grado di ricevere e trasmettere verso molte stazioni sulla superficie terrestre. In genere tali satelliti sono posti su un'orbita detta "geostazionaria", a circa 36.000 Km di altezza. Tale orbita consente di assumere la medesima velocità angolare di rotazione della terra e al contempo di bilanciare l'attrazione gravitazionale: ne consegue che il

[68] Standard per le trasmissioni senza fili in ambito di rete locale sono: IEEE 802.11a, IEEE 802.11b e IEEE 802.11g, comunemente indicati dalla sigla **WiFi** sulle apparecchiature.

satellite rimane "parcheggiato" su una perpendicolare, ed è in grado di funzionare da ripetitore per una determinata area del pianeta.

I satelliti geostazionari vengono utilizzati nell'ambito delle telecomunicazioni con tecnologie analogiche sin dagli anni '60. Da circa dieci anni è in atto una massiccia transizione verso le comunicazioni satellitari digitali, che coinvolge in primo luogo la televisione, e che potrebbe in futuro costituire la base per una infrastruttura telematica planetaria. Già oggi è possibile la ricezione di dati mediante una semplice antenna parabolica (identica a quelle adoperata per la televisione satellitare) con una velocità di 400 o 500 Kbps. Tuttavia il processo inverso è ancora impossibile. Infatti per inviare un segnale a microonde verso un satellite geostazionario è necessario sviluppare una notevole potenza (e di conseguenza utilizzare un'antenna parabolica con un diametro dell'ordine delle decine di metri).

Una soluzione potrebbe venire dall'uso di una rete di satelliti a bassa quota (inferiore ai 50 Km), meno costosi per il lancio. Inoltre la loro vicinanza alla superficie terrestre permette di ridurre notevolmente la potenza necessaria per l'invio di segnali, e dunque consentirebbe la diffusione di apparati ricetrasmittenti "domestici".

L'unica difficoltà posta da questa tecnologia è costituita dalla necessità di cambiare satellite appena il precedente esce dallo specchio di visibilità, poiché le basse orbite non sono geostazionarie. Tuttavia, tecnologie di sincronizzazione simili sono oggi ampiamente utilizzate nelle radiocomunicazioni terrestri (ad esempio nelle reti telefoniche cellulari) e non dovrebbero esserci difficoltà eccessive ad estenderle alla comunicazione satellitare.

5. Gli accessi alla rete[69]

Negli ultimi anni, per effetto di molteplici fattori, quali la richiesta di nuovi servizi, le maggiori opportunità tecniche e, allo stesso tempo, il mutamento del quadro regolamentare, funzionale all'evolvere dello scenario competitivo, le reti di telecomunicazione hanno subìto forti cambiamenti sia riguardo all'aspetto del trasporto che a quello dell'accesso all'utenza finale (*last mile* o ultimo miglio). In questa realtà estremamente mutevole i gestori della rete hanno, in

[69] I paragrafi 5 e 6 costituiscono un estratto - in parte sintetizzato - dello studio dell'Autorità per le garanzie nelle comunicazioni, *Le tecnologie xDSL e l'accesso disaggregato alla rete locale*, giugno 2001. Le parti sono evidenziate con l'uso di un carattere più piccolo.

primo luogo, necessità di continuare ad essere competitivi nelle attività tradizionali e, nello stesso tempo, di ampliare l'offerta con nuovi servizi a larga banda rispetto ai quali l'elemento trainante è rappresentato dal successo di quelli forniti via Internet: è infatti in continua crescita sia il numero di utenti che ne usufruiscono che la quantità di banda richiesta per le applicazioni residenziali e per quelle *business*. Per far fronte alle nuove esigenze in tempi brevi e con investimenti contenuti, molti operatori, sia *incumbent*[70] che *new entrant*[71], guardano oggi con molto interesse a un gruppo di tecnologie, dette xDSL, che consentono l'utilizzo della rete di distribuzione in doppino per il trasporto all'utente di voce - come tradizionalmente avviene - e servizi a larga banda. Il termine xDSL (x *Digital Subscriber Line*) sta a rappresentare, al variare della lettera "x", un particolare *modem* che può essere utilizzato per il trasferimento di voce, dati e immagini su doppino telefonico. Le tecniche di ultima generazione più note sono: ADSL, ADSL.Lite, R-ADSL, HDSL, SDSL e VDSL. Il principale vantaggio offerto da tali tecniche sta nell'utilizzo di una rete di distribuzione in doppino che è già capillarmente diffusa sul territorio nazionale. Ciò consente un risparmio sia per gli operatori preesistenti che per quelli alternativi che possono oggi accedere alle linee telefoniche dell'operatore *incumbent* per fornire servizi a larga banda. Tra le diverse tecnologie xDSL utilizzate per l'accesso locale ad alta velocità, il primo esempio che vale la pena di citare è il sistema ISDN che letteralmente significa Rete Numerica Integrata nei Servizi. La chiave di volta dell'ISDN è la realizzazione di una linea numerica d'utente sulle normali centrali telefoniche riutilizzando quindi l'attuale rete di distribuzione (il doppino d'utente). Da un punto di vista trasmissivo è un primo esempio di tecnica DSL in quanto va ad utilizzare il doppino telefonico per trasmissione numerica.

Nella classificazione riportata in figura le tecniche xDSL di nuova generazione vengono suddivise in tre famiglie che fanno capo alla tecnica HDSL (*high-data-rate* DSL) per quanto riguarda sistemi simmetrici (*up-link* e *down-link* hanno la stessa velocità), alla tecnica ADSL (*asymmetrical* DSL) per i sistemi asimmetrici e VDSL (*very-high-rate* DSL) che può essere sia simmetrico che asimmetrico e necessita di un collegamento in fibra ottica dalla centrale ad un terminale remoto per limitare il collegamento in doppino ad una lunghezza non superiore ai 1500 m. Le altre sigle riportate rappresentano variazioni delle tecniche principali menzionate.

---

[70] Fornitore principale presente sul mercato.

[71] Nuovi fornitori concorrenti, definiti anche OLO.

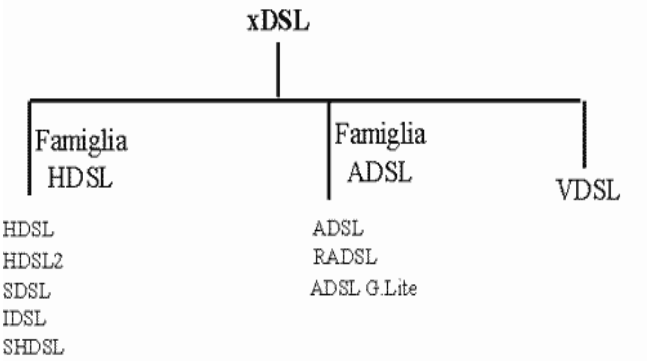


Fig. 1 - Classificazione delle tecniche xDSL

La rete ISDN consente l'*accesso base* che offre tre canali informativi: due canali a 64 Kbit/s utilizzabili come due linee telefoniche indipendenti, denominati canali B, e un canale a 16 kbit/s, denominato canale D, utilizzato per la segnalazione e per la trasmissione di dati a pacchetto. L'accesso primario offre 31 canali informativi, 30 canali B e 1 canale D a 64 kbit/s impiegato solo per la segnalazione utente-rete ed è realizzato con una normale linea PCM a 2 Mb/s. Nella successiva descrizione il riferimento è all'accesso di base.

Nella tecnica ADSL (*Asymmetrical* DSL) la trasmissione avviene su singolo doppino tra centrale e terminazione d'utente, ed è detta asimmetrica perchè la banda dedicata al *down-link* (da centrale a terminazione d'utente) è molto maggiore di quella dedicata all'*up-link*. Ciò risponde bene alle esigenze di un utente che naviga in Internet o accede a servizi del tipo video interattivo.

La tecnica HDSL *(High-data rate DSL)* consente di trasmettere su uno, due o tre doppini, flussi conformi agli *standard* c.d. T1 (1,544 Mb/s) o E1 (2,048 Mb/s). La tecnologia HDSL rappresenta la scelta dominante negli USA per la distribuzione dei servizi T1. L'ETSI (*European Telecommunications Standards Institute*)[72] ha prodotto diversi *standard* per l'HDSL. La tecnica di modulazione può essere di banda-base con codifica di linea 2B1Q o passa-banda con codifica di linea CAP (*Carrierless Amplitude Phase*). Lo standard 2B1Q per 2,048 Mb/s raccomanda la trasmissione *duplex* su singolo doppino o in parallelo su due o tre doppini (nel passare da tre a un singolo doppino la distanza va progressivamente ridotta). L'ETSI ha anche specificato l'uso della tecnica CAP raccomandata per uno o due doppini. L'occupazione di banda varia a seconda della codifica di linea e del numero di doppini utilizzati.

[72] Per tutti gli organismi richiamati, che intervengono nel governo della rete Internet, si faccia riferimento al paragrafo 4 della sezione A - Aspetti generali della *governance*, *Schede illustrative sulle organizzazioni.*

Attualmente si sta mettendo a punto uno *standard* per la tecnica HDSL2 che ha come obiettivo la trasmissione di flussi simmetrici E1 (T1) su singolo doppino con modulazione 16-PAM (*Pulse Amplitude Modulation*) su distanze < 5 Km. Un vantaggio importante della tecnologia HDSL2 rispetto alle tecniche HDSL basate sulla codifica 2B1Q, è la compatibilità spettrale con le altre tecnologie DSL. Infatti l'HDSL2 utilizza una codifica di linea più efficiente del sistema 2B1Q per cui, a parità di velocità trasmissiva, occupa una banda inferiore. In aggiunta, lo spettro HDSL2 è stato progettato per essere "ADSL *friendly*" garantendo in questo modo la compatibilità con altri segnali ADSL all'interno dello stesso cavo.

Ricapitolando, il sistema HDSL2 presenta i seguenti vantaggi rispetto all'HDSL: richiede un solo doppino per il trasporto di servizi E1 (T1), offre prestazioni migliori su distanze maggiori (fino a 4Km), ha una maggiore immunità al rumore. Un altro vantaggio è che gli apparati HDSL2 occupano meno spazio di quelli HDSL e questo aumenta lo spazio disponibile per la co-locazione degli apparati degli operatori licenziatori (spesso chiamati OLO, *Other Licenzed Operator)* o ISP nella centrale del *Local Loop Provider*. La risposta europea all'HDSL2 è rappresentata dallo *standard* SDSL (*Symmetrical single pair* DSL) in cui la scelta della tecnica di modulazione protende verso il PAM a 16 livelli con *Trellis Code Modulation*.

La tecnica VDSL *(Very-high-speed DSL)* è un'estensione dell'ADSL ed è tuttora in corso di standardizzazione in ambito ETSI. Supporta, su singolo doppino, con lunghezze da 300 a 1500 m, velocità (a secondo della distanza) nell'intervallo da 6,1 a 51,8 Mb/s in *down-stream*, 1,6 – 6,5.Mb/s in *up-stream* nel caso di servizi asimmetrici e 6,5 – 25,9 Mb/s per servizi simmetrici. Ad esempio si riesce ad ottenere velocità in *down-stream* fino a 52 Mb/s a 300 m, 26 Mb/s a 1000 m, 13 Mb/s a 1500 m. Le tecniche di modulazione proposte sono M-CAP, M-QAM (*Quadrature Amplitude Modulation)* e DMT (*Discrete Multi Tone*). Generalmente la banda riservata per il VDSL va da 300 kHz a 30 MHz, consentendo in tal modo la trasmissione contemporanea del servizio telefonico analogico POTS (0-4 kHz) o del servizio ISDN (0-80 kHz). Il gruppo di lavoro sul VDSL dell'ANSI, T1E1.4, ha proposto di allocare i servizi VDSL nella gamma 1-2 MHz per *l'up-stream* e 2-18 MHz (e oltre) per il *down-stream*. L'introduzione della tecnologia VDSL pone oggi il problema della compatibilità con i sistemi ADSL soprattutto in considerazione del processo di *unbundling* in corso in Europa. L'altro aspetto dibattuto, volendo realizzare un sistema *full duplex*, riguarda la scelta della tecnica di *duplexing* a divisione di frequenza (FDD) o di tempo (TDD). Citiamo infine il problema delle interferenze con servizi radio all'interno della gamma 300 kHz–30 MHz entro cui è prevista l'allocazione dei servizi VDSL. Va detto che la modulazione DMT presenta un vantaggio rispetto alle altre tecniche a portante singola in quanto consente di

inibire in modo selettivo la trasmissione su quelle sotto-portanti che generano o ricevono segnali interferenti.

6. Accesso disaggregato alla rete locale

Il concetto di accesso alla rete è comunemente inteso come la disponibilità per gli operatori entranti di avvalersi di componenti e servizi di una infrastruttura di rete esistente, al fine di promuovere i propri servizi alla clientela finale. In tal senso, anche l'interconnessione alla rete pubblica commutata di telecomunicazioni costituisce una particolare tipologia di accesso. In ambito internazionale sono state individuate diverse parti e componenti di rete che possono essere oggetto di accesso, quali **ad esempio l'infrastruttura d'accesso a livello locale; l'infrastruttura di segnalazione; la rete commutata di base; la rete intelligente; la rete di trasporto a lunga distanza.** L'attenzione delle Autorità di regolamentazione nelle comunicazioni si è rivolta in particolare all'accesso alla rete locale, per due principali motivazioni:

- gli investimenti e i tempi necessari per la realizzazione di reti locali alternative sono il maggior ostacolo alla costituzione di un mercato pienamente competitivo per i servizi di comunicazione;
- lo sviluppo tecnologico ha consentito l'impiego di tecnologie trasmissive innovative (quali le tecnologie xDSL) che permettono l'offerta di servizi a larga banda su una infrastruttura originariamente installata per supportare servizi telefonici tradizionali.

Il mercato dell'accesso include tre diverse soluzioni tecniche, ovvero l'accesso disaggregato alla rete metallica, l'accesso disaggregato alla sotto rete metallica e l'accesso condiviso. In termini generali, l'accesso disaggregato (o *unbundling*) alla rete locale consiste nella fornitura da parte dell'operatore *incumbent* o dominante (Telecom Italia nel caso italiano) di una serie di servizi di accesso ad altri operatori allo scopo di rendere loro possibile l'offerta diretta di servizi di comunicazione ai singoli utenti[73].

Specificando con maggiore dettaglio è possibile individuare le seguenti principali tipologie di accesso disaggregato:

- accesso di tipo fisico (anche detto *direct access*), ovvero la fornitura di un servizio di accesso, in un punto intermedio della rete di accesso situato tra la terminazione d'utente ed il punto di attestazione lato utente sulla

[73] Secondo i dati forniti dall'Autorità di garanzia nelle comunicazioni, al 31 ottobre 2003, solo una porzione dei siti della rete in rame di Telecom risultava effettivamente accessibile agli operatori alternativi (572 siti operativi su un totale di 1003 in consegna, cioè quelli predisposti da Telecom per la fornitura del servizio).

centrale locale, allo scopo di fornire ad un diverso operatore, da tale punto, l'accesso alla sede d'utente;

- accesso di tipo logico (anche detto *bit stream access*) che include sia il mezzo trasmissivo che i sistemi trasmissivi utilizzati per fornire il servizio e consiste nella fornitura di un flusso numerico con caratteristiche determinate, logicamente dedicato al singolo utente;
- accesso condiviso (*shared access,* anche detto *frequency access*) che è una forma di accesso diretto al doppino del LLP con la differenza che l'operatore *incumbent* e l'altro operatore condividono lo stesso doppino utilizzando diverse porzioni dello spettro.

Le possibili opzioni tecniche individuate per consentire l'accesso alla rete locale sono le seguenti:

1. accesso disaggregato alla rete in rame
2. accesso disaggregato alla rete in fibra ottica
3. canale numerico/virtuale

Mentre le prime due opzioni identificano forme di accesso alla rete locale tramite una disaggregazione di risorse fisiche trasmissive (accesso di tipo fisico o diretto) la successiva consente all'operatore di realizzare l'accesso all'utente finale tramite la fornitura da parte di Telecom Italia di risorse fisiche trasmissive e di sistemi/apparati trasmissivi (accesso di tipo logico).
In linea generale, le diverse tipologie di accesso disaggregato possono avere un carattere complementare (ovvero, coesistono come soluzioni da fornire obbligatoriamente da parte di Telecom Italia, a seconda delle esigenze dell'operatore richiedente l'accesso) oppure sostitutivo (in tal caso, sono utilizzabili esclusivamente nel caso di indisponibilità del servizio richiesto).
A tal riguardo, come confermato dagli stessi operatori, le forme di accesso di tipo fisico appaiono più adatte ad incentivare gli investimenti e l'innovazione tecnologica. D'altro canto, forme di accesso logico possono essere utilizzate come sostitutive in caso di indisponibilità (es. canale numerico) o come strumento transitorio (si veda più avanti il servizio denominato Canale Virtuale Permanente, CVP) per assicurare uno sviluppo immediato e pienamente concorrenziale dei mercati di nuovi servizi. In tal senso, la previsione di tipologie di accesso di tipo logico da parte dell'operatore dominante non va intesa come un sostituto permanente ed equivalente all'accesso di tipo fisico. Sono stati inoltre individuati alcuni servizi che hanno carattere accessorio e sono funzionali alla realizzazione dei servizi di accesso disaggregato sopra elencati.
Si tratta di:

a. servizio di prolungamento dell'accesso;
b. servizio di co-locazione.

7. Caratteristiche strutturali della rete italiana[74]

Nella realtà italiana - come già sottolineato - le reti fisse tradizionali[75] sono ancora il sistema di comunicazione più diffuso, ma le nuove tecnologie di trasmissione in larga banda stanno aumentando la propria quota di mercato. Per quanto riguarda le infrastrutture di rete fissa a grande distanza, la rete nazionale di telecomunicazioni è composta, limitatamente alla fase di trasporto dei dati, essenzialmente da sistemi SDH a 2.5-10 Gbit/s. Le connessioni in fibra ottica continuano a crescere ed hanno toccato quota 6,4 milioni Km/fibra alla fine del 2002 (4,6 milioni di chilometri nella rete dorsale e 1,8 milioni in quella di giunzione) appartenenti a vari operatori quali Telecom, Wind-Infostrada, Albacom, Colt, Fastweb, ecc. La rete di trasporto ha ormai raggiunto dimensioni tali da permettere notevoli potenzialità di sviluppo. Negli ultimi anni sono stati installati i più moderni sistemi utilizzanti la tecnologia WDM, che ha consentito di incrementare la capacità disponibile utilizzando fino a 64 lunghezze d'onda sulla stessa fibra. Per l'accesso finale invece (ultimo miglio), pur essendo aumentato l'utilizzo della fibra ottica, si resta ancora legati al mezzo tradizionale su cavo di rame.

La situazione degli operatori italiani per il trasporto è la seguente:

- l'operatore dominante o *incumbent,* Telecom Italia, sta completando un'evoluzione della propria rete di dorsali, realizzando anelli ottici ad alta capacità di trasporto (80 Tbit/s). L'architettura finale sarà basata su una piattaforma IP con 32 POP che garantirà la gestione integrata di voce e dati, ma non saranno comunque penalizzati gli operatori che vorranno continuare a utilizzare l'attuale infrastruttura ATM per i dati. Tale trasformazione è stata stimolata dalla bassa efficienza e dagli elevati costi gestionali della rete esistente rispetto alle moderne tecnologie, nonché dalla convergenza di tecnologie e reti. A livello di trasporto la situazione

---

[74] Estratto - in parte sintetizzato - del Rapporto del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni, *Strategia e politiche per la larga banda in Italia*, dicembre 2003, integrato con quanto esposto nell'Allegato B alla delibera n. 415/04/CONS dell'Autorità per le garanzie nelle comunicazioni del 1° dicembre 2004 e con la sintesi della normativa vigente.

[75] Nel periodo 2004-2010 si svolgerà in Italia una ricerca nel campo delle reti fisse di nuova generazione con l'obiettivo di creare una rete interamente ottica, anche a livello di accesso. E' prevedibile che anche nel nostro Paese vi sarà presto una saturazione della rete in rame per applicazioni ADSL e che, tra il 2006 e il 2007, inizierà la transizione dalla rete in rame alla rete in fibra ottica. Sicuramente le trasmissioni radio per l'accesso continueranno ad avere un ruolo importante. Tuttavia sarà sempre necessario raggiungere le antenne, con segnali ad alta capacità, e la trasmissione in fibra ottica è quella che permette di soddisfare anche questa esigenza. Questa transizione modificherà anche la rete del trasporto in quanto saranno richieste nuove potenzialità, in relazione al forte incremento di banda e alla natura del traffico, che sarà completamente diversa da quella del traffico telefonico.

può quindi considerarsi soddisfacente pur con qualche disequilibrio territoriale.

- Per gli altri principali operatori[76] si registra quanto segue:

  - **Wind-Infostrada** ha una dorsale nazionale in fibra ottica di 21.000 Km, realizzata per rendersi autonoma da Telecom Italia e che sfrutta parte delle infrastrutture acquistate dalle Ferrovie dello Stato;
  - **Albacom** ha acquistato il 60% di Basictel, società creata dalle Ferrovie dello Stato, attraverso la quale realizzerà oltre 3.800 chilometri di dorsali in fibra ottica sfruttando l'elettrodotto di proprietà delle Ferrovie. In totale Albacom arriverà a posare oltre 8.600 Km di fibra annoverando anche la rete in fibra di proprietà SNAM di cui Albacom ha il diritto di accesso e utilizzo esclusivo e per la quale Albacom paga un affitto annuo;

  - **Edisontel** sta posando 6.300 Km di cavo;

  - **E-Via** sta completando una dorsale in fibra nel Centro Nord composta da circa 2.500 km di cavo;

  - **Interoute** sta completando un anello in fibra ottica tra le città di Milano, Torino, Genova, Roma e Venezia. Tale anello è collegato alla rete europea che connette 45 città in nove Paesi Europei.

Ritornando all'aspetto dell'accesso all'utente finale, la situazione è da considerare soddisfacente solo per le grandi e medie aziende: 110.000 aziende disponevano, alla fine del 2002, di un collegamento con connessione in fibra ottica o con HDSL. Per quanto riguarda l'area residenziale e le piccole aziende e gli utenti SOHO[77], la situazione , invece, è da ritenere meno sviluppata, anche per la quasi totale assenza in Italia di altri portanti a larga banda verso l'utenza domestica, quale la cablatura televisiva. Nuovi operatori italiani offrono la cablatura in fibra ottica per l'utenza residenziale con fornitura di servizi innovativi, ma tali applicazioni rimangono ancora limitate. Viene evidenziato che un notevole progresso in questo senso si potrebbe ottenere con lo sviluppo di un

---

[76] Le informazioni sono riferite al periodo ottobre-novembre 2001. Quelle relative ad Albacom sono state aggiornate su indicazione dello stesso operatore al febbraio 2002 (da *Task force sulla larga banda,* Commissione interministeriale di studio istituita dal Ministro delle comunicazioni e dal Ministro per l'innovazione e le tecnologie, 1° Rapporto, novembre 2001 - Estratto). Si rileva che nell'elenco non compaiono altri operatori di grande rilievo quali Tiscali (nato nel 1998, ora quotato in Borsa, che è stato il primo operatore italiano a lanciare l'Internet gratis), Tele2 e Fastweb, quest'ultimo affermatosi in modo notevole successivamente alla data di pubblicazione del Rapporto citato.

[77] *Small Office Home Office* (sono gli utenti casalinghi o i piccoli uffici).

sistema satellitare a larga banda[78], capace di collegare anche le utenze più decentrate e geograficamente disagiate.

Anche l'Autorità per le garanzie nelle comunicazioni (Allegato B alla delibera n. 415/04/CONS - 1°dicembre 2004) rileva che in Italia l'accesso alla rete telefonica pubblica agli utenti finali viene ancora prevalentemente offerto con tecnologia tradizionale. All'inizio di luglio 2004, secondo la medesima fonte, il numero totale di linee di accesso in rame, residenziali e non, era stimato in circa 27.294.000, di cui 26.596.000 commercializzate direttamente da Telecom Italia. Gli altri operatori risultavano gestire circa 698.000 linee acquisite in modalità *unbundling*. Per la rete di accesso in fibra ottica i dati forniti risalgono al 2001 e fotografano un'estensione della rete - di proprietà di Telecom - pari a 417.000 Km-fibra. Per quanto riguarda le aziende nuove entranti si rileva che, negli ultimi anni, la **Fastweb** ha investito in modo notevole in infrastrutture di accesso in fibra ottica soprattutto nelle aree metropolitane di Roma, Milano, Napoli, Torino, Bologna e Genova tanto è vero che a giugno 2004 il numero di linee di accesso era stimabile in 170.000 unità[79].

Gli accessi in larga banda, secondo le cifre fornite dal Ministero, erano a settembre del 2003 circa 1.920.000 con l'88% attraverso xDSL ed il 12% con altre tecnologie (in prevalenza fibra ottica), a cui vanno aggiunti 300.000 accessi UMTS per un totale di circa 2,2 milioni di accessi.

La generalizzazione dello sviluppo di accessi a banda larga, sia per effetto della politica scelta dall'operatore principale, sia per un'applicazione in Italia abbastanza allargata e relativamente fluida della politica di *unbundling* da parte degli operatori alternativi, è in questo momento essenzialmente affidata allo sviluppo, nella rete di accesso, dei sistemi xDSL (e in particolare ADSL per l'area residenziale), avendo il nostro paese, per tale applicazione, caratteristiche particolarmente favorevoli (cavi a coppie relativamente recenti e circuiti di utente molto corti). Le caratteristiche della rete italiana consentiranno - secondo quanto rileva il Ministero - un forte utilizzo delle tecniche xDSL. Infatti la percentuale dei cavi in doppino della rete utilizzati per l'xDSL è pari al 58,9% e consentirebbe quindi ulteriori sviluppi di utenza; la lunghezza contenuta dei circuiti d'utente (in media 1,5 km) della rete assicura una qualità soddisfacente per i collegamenti in tecnologia xDSL per un'alta percentuale di utenti. La

---

[78] La definizione di larga banda è stata ed è tuttora oggetto di discussione nell'ambito dei corrispondenti gruppi di lavoro istituiti dai governi degli altri paesi. Tale dibattito verte sia sull'ampiezza di banda, sia sui servizi erogabili. La Commissione europea, in considerazione della complessità del fenomeno, ha adottato la seguente definizione: per "larga banda" si intende l'ambiente tecnologico che consente l'utilizzo delle tecnologie digitali ai massimi livelli di interattività.

[79] Per dati di maggiore dettaglio si rinvia alla citata documentazione dell'Autorità segnalata anche in Appendice.

richiesta di nuove installazioni tende ad attestarsi, includendo tutti gli operatori, tra i 10.000 e i 15.000 nuovi impianti al giorno.

Tenuto conto della situazione anzidetta, viene evidenziato che, a livello medio complessivo, pur in presenza di squilibri territoriali, l'accelerazione delle richieste di installazioni xDSL è oggi notevole, anche per le interessanti offerte di commercializzazione che consentono di scegliere tra una molteplicità di contratti (da un'offerta *flat-rate* mensile ad una a consumo senza pagamento di canone fisso).

In aggiunta, il mobile di terza generazione (UMTS) - si sottolinea poi nel Rapporto - potrà avere uno sviluppo sostenibile in termini di infrastruttura e servizi, solo se combinato con la crescita della larga banda *wired*: la necessità di conseguire economie di scala e di esperienza non consente ai due comparti una crescita disgiunta. La diffusione delle infrastrutture delle reti di telecomunicazione è giudicata un fattore decisivo per il superamento del *digital divide* di aree territoriali caratterizzate da un minore sviluppo economico e per la crescita della competitività dell'intero sistema.

In questa prospettiva una problematica di natura sistemica come l'introduzione della larga banda, andrebbe configurata - secondo quanto emerge dal documento - in un quadro chiaro di politica industriale. Si valuta ancora che l'intervento dello Stato in tale ambito può evitare la creazione di un *gap* tecnologico ed economico (ampliamento del *digital divide*, isolamento tecnologico, ecc.) e la conseguente perdita di competitività dell'intero sistema paese. Le applicazioni che potranno essere veicolate attraverso la larga banda avranno impatto su cittadini, imprese e Pubblica amministrazione. Si giudica che quest'ultima avrà un ruolo fondamentale, in quanto le applicazioni in larga banda che essa potrà sviluppare, consentendo un miglioramento dei processi interni ed esterni, avranno ricadute positive anche su imprese e cittadini. Esempi di applicazioni in larga banda sono:

- la *presenza virtuale*, ed in particolare teleconferenza, teledidattica, telemedicina, telelavoro, telesorveglianza. Queste applicazioni sono particolarmente importanti in quanto possono indurre un cambio radicale nel rapporto tra i soggetti coinvolti nella comunicazione, dando così luogo a meccanismi di interazione innovativi. Per quanto riguarda la formazione a distanza, per esempio, si può pensare sia alla trasposizione dell'erogazione di corsi predefiniti in modalità remota, sia, come già sta accadendo, a nuove modalità di apprendimento che prevedono un ruolo attivo degli studenti invece che la semplice fruizione dei contenuti;

- il *peer to peer networking*, che consiste nella creazione di comunità di utilizzatori che scambiano vicendevolmente informazioni e servizi in modo paritetico, talvolta avvalendosi di un coordinamento centralizzato. Analogamente a quanto si è verificato per lo scambio di brani audio,

conosciuto come Napster, che ha svolto il ruolo effettivo di *killer application* finché è stato attivo su Internet in ambiente a "banda stretta".

La diffusione di servizi ASP *(Application Service Providing)* è destinato ad affermarsi come un modello emergente nell'evoluzione dei servizi informatici. L'ASP può essere considerato un aspetto evoluto dell'*outsourcing*, in cui gli strumenti informatici, sia *hardware* che *software*, e le competenze professionali per la loro gestione non sono localizzate necessariamente nella sede degli utilizzatori ma possono risiedere invece nella sede del fornitore del servizio. Gli utilizzatori si avvalgono dei servizi forniti in modalità ASP attraverso i propri elaboratori con un elevato grado di interattività. La modalità di erogazione ASP è da molti ritenuta indispensabile, in particolare per le piccole e medie imprese, che potrebbero in questo modo avvalersi di servizi di elevato livello qualitativo senza dover necessariamente dotarsi direttamente di strumenti e competenze onerose da dedicare ad attività che non rappresentano il *core business*.

Lo sviluppo delle sopra citate applicazioni sarà incentivato dalle caratteristiche delle tecnologie di accesso a larga banda:

- *always on, always available,* caratteristiche *killer* per la rete anche in ambiente *narrowband*, che troveranno un forte potenziamento in ambiente *broadband*;

- *convergenza* su un'unica infrastruttura di servizi di fonia e dati, finora confinati in reti dedicate.

E' in ogni caso importante segnalare - si afferma ancora nel rapporto del Ministero - che tale convergenza non riguarderà se non marginalmente alcuni servizi (quali quelli televisivi), che continueranno a basarsi su uno sviluppo parallelo di infrastrutture dedicate. Saranno inoltre possibili applicazioni avanzate nel campo dell'*e-government*, per disporre, nel rapporto tra cittadino e PA e nell'ambito delle relazioni tra le amministrazioni, dell'utilizzo dei massimi livelli di interattività.

A livello europeo - come evidenzia la Relazione sulle attività del Ministero delle comunicazioni del settembre 2004 - si prevede il sostegno agli investimenti per le infrastrutture a banda larga nelle aree depresse attraverso l'attuazione del piano *e-Europe*. A ciò si concorrerà anche attraverso il Fondo Sociale Europeo. Il piano - che si prefigge l'obiettivo di diffondere, entro il 2005, l'uso delle reti a banda larga in tutta l'Unione - dovrebbe realizzarsi attraverso due categorie di interventi: l'incentivazione di azioni relative ai servizi, alle applicazioni e ai contenuti e lo sviluppo dell'infrastruttura a larga banda e la soluzione di questioni legate alla sicurezza.

8. Evoluzione del quadro regolamentare di riferimento per l'accesso disaggregato alla rete locale

L'attuale sistema regolamentare ha la finalità di creare un quadro competitivo effettivo, attraverso il riconoscimento di diritti ed asimmetrie per gli operatori nuovi entranti. Una misura tipica di asimmetria - come già detto – è l'accesso disaggregato al circuito di utente (*unbundling* del *local loop*): dal 31 dicembre 2000, in attuazione del Regolamento comunitario 2887/2000[80], gli operatori aventi notevole forza di mercato (cioè quelli che detengono più del 25% del mercato della fornitura di reti telefoniche pubbliche) devono accogliere a condizioni eque, trasparenti e non discriminatorie, le richieste ragionevoli di accesso disaggregato alle loro reti locali e alle risorse connesse. Per effetto di tali normative, Telecom Italia ha dovuto mettere a disposizione per l'*unbundling* 1500 centrali in tre *tranche* da 500 centrali ciascuna. Dopo un iniziale elevato interesse all'operazione, trascorso quasi un anno, l'interesse degli operatori licenziatori (**OLO**) è molto calato: l'ultima tranche di 500 centrali ha riscontrato un numero di richieste particolarmente basso, pari a 73. La normativa sancisce che la determinazione dei prezzi per l'accesso alla rete locale deve seguire principi di trasparenza, non discriminazione e orientamento ai costi: in particolare, gli operatori dominanti devono fornire l'accesso disaggregato ai terzi alle stesse condizioni e termini utilizzati per le proprie società consociate o per la fornitura di servizi propri.

I compiti di vigilanza e di intervento sono assegnati alle Autorità nazionali di regolamentazione. Come già precisato, il Regolamento reca disposizioni puntuali in merito alla fornitura di informazioni, alle procedure di ordine e di fornitura dei servizi di accesso disaggregato. In base alle definizioni riportate nel Regolamento, l'«accesso completamente disaggregato alla rete locale» consiste nella fornitura a un beneficiario dell'«accesso alla rete locale o alla sottorete locale (*sub-loop unbundling*) dell'operatore notificato che autorizzi l'uso di tutto lo spettro delle frequenze disponibile sulla coppia in rame». L' «accesso condiviso» (*shared access*) alla rete locale consiste invece nella «fornitura a un beneficiario dell'accesso alla rete locale o alla sottorete locale dell'operatore notificato che autorizzi l'uso della banda non vocale di frequenza dello spettro disponibile sulla coppia elicoidale metallica; la rete locale continua ad essere impiegata dall'operatore notificato per fornire al pubblico il servizio telefonico».

[80] Per i testi degli atti normativi citati consultare <http://www.europa.eu.int/eur-lex/>.

In attuazione del Regolamento, la delibera n. 2/00/CIR dell'Autorità per le garanzie nelle comunicazioni stabilisce le modalità di attuazione dell'*unbundling*. I servizi che l'operatore notificato è tenuto a fornire all'operatore licenziatario nel rispetto delle disposizioni contenute nella delibera 2/00/CIR possono riassumersi come segue:

- *Disaggregazione del mezzo fisico in rame*: rappresenta la possibilità per l'operatore licenziatario (OLO) di accesso alla coppia in rame per servizi POTS, ISDN e in generale per l'utilizzo di sistemi trasmissivi numerici xDSL (*direct access*);
- *Disaggregazione del mezzo fisico in fibra:* rappresenta la possibilità per l'operatore licenziatario di accesso alle fibre posate nella rete di accesso;
- *Canali numerici/virtuali*: rappresenta la possibilità per l'operatore licenziatario di accesso in generale non al mezzo fisico ma al canale logico (*bitstream access*);
- *Prolungamento dell'accesso:* è la possibilità per l'operatore licenziatario di raccolta a livello centralizzato (SGU, stadio di gruppo urbano) degli accessi realizzati a livello di sito periferico (SL, stadio di linea). Può essere realizzato mediante un mezzo fisico (fibra), un canale numerico o soluzioni alternative (ad es. ponte radio);
- *Co-locazione*: è la possibilità per l'operatore entrante di co-locare i propri apparati nei siti di Telecom Italia.

Per quanto riguarda i soggetti beneficiari, l'articolo 3 della delibera n. 2/00/CIR dispone che i soggetti legittimati a richiedere la fornitura di servizi di accesso disaggregato a livello di rete locale sono gli operatori licenziatari ai sensi del D.M. 25 novembre 1997, recante *Disposizioni per il rilascio delle licenze individuali nel settore delle telecomunicazioni*.

Inoltre, con l'articolo 2 della delibera n. 467/00/CONS[81], è disposta la disciplina in materia di autorizzazioni generali che si applica ai servizi di telecomunicazioni offerti al pubblico diversi dalla telefonia vocale e dall'installazione e dalla fornitura di reti pubbliche di telecomunicazioni, comprese quelle basate sull'impiego di radiofrequenze. In tale contesto, accogliendo anche gli orientamenti espressi dalla Comunità Europea,

[81] Per i testi delle delibere si consulti il sito <http://www.agcom.it/attivit_.htm> segnalato anche in Appendice.

l'Autorità ha successivamente inglobato nell'area dei soggetti beneficiari di alcuni servizi di accesso alla rete locale anche i soggetti muniti di autorizzazione generale (come gli ISP). Infatti la delibera n. 3/01/CIR integra l'articolo 3 della delibera n. 2/00/CIR al fine di riconoscere ai soggetti titolari di autorizzazione generale l'accesso all'offerta *wholesale* del servizio di "canale virtuale permanente". Infine, l'articolo 4 della delibera n.15/01/CIR estende agli operatori autorizzati l'accesso ad offerte *wholesale* di servizi di accesso formulate da parte di OLO (*Other Licensed Operator*). Va infine evidenziato che, con delibera 5/00/CIR dell'8 giugno 2000, l'Autorità ha istituito l'Unità per il monitoraggio del processo d'implementazione dei servizi di accesso disaggregato, preselezione e portabilità del numero. In relazione ai temi dell'accesso disaggregato alla rete locale, l'Unità ha inoltre proceduto al monitoraggio delle attività di sperimentazione, di negoziazione ed all'avvio dell'operatività dei servizi, riscontrando e segnalando all'Autorità eventuali possibili interventi correttivi ed integrazioni della disciplina.

Oltre alla determinazione dei prezzi e delle modalità di attuazione dell'*unbundling*, un altro elemento fondamentale in grado di favorire lo sviluppo delle infrastrutture e, quindi, della competizione, **è l'armonizzazione sul territorio nazionale delle modalità di concessione dei diritti di passaggio a livello locale.** Secondo la normativa europea, i diritti di passaggio sul suolo pubblico devono essere concessi a condizioni non discriminatorie. In Italia la materia dei diritti di passaggio è regolata dalla legge n. 249 del 31 luglio 1997[82] e dal D.P.R. 318 del 1997, nei quali sono affermati gli stessi principi di non discriminazione.

La legge n. 249 prevede l'adozione da parte dell'Autorità per la garanzie nelle comunicazioni di un regolamento sulla disciplina delle installazioni e transito su beni pubblici delle reti di telecomunicazione nelle aree urbane e del rilascio dei diritti di passaggio per la realizzazione di reti dorsali.

Nel citato Rapporto ministeriale del 2003 si sottolinea che nel corso delle audizioni che si sono svolte per effettuare l'indagine in oggetto, sono emerse alcune difficoltà che gli operatori nuovi entranti incontrerebbero nell'ottenere le autorizzazioni degli enti locali per la posa delle infrastrutture. In particolare, tali difficoltà riguarderebbero soprattutto:

[82] Per i testi degli atti normativi citati e non presenti nella documentazione allegata si consulti http://www.parlamento.it/leggi/home.htm> e <http://www.agcom.it/attivit_.htm>.

a) i lunghi tempi di attesa delle concessioni;
b) i presunti eccessivi requisiti richiesti dalle autorità locali in materia di lavori di scavo comuni, condivisione delle strutture e riapertura delle strade pubbliche;
c) la scarsa chiarezza sulle regole applicabili;
d) la difficoltà di coordinamento tra i vari servizi pubblici coinvolti nei procedimenti di concessione dei diritti di passaggio;
e) la forte variabilità dei canoni richiesti dalle amministrazioni locali, in dipendenza delle aree geografiche interessate.

E' stato inoltre evidenziato che alcune difficoltà nel realizzare reti in fibra ottica metropolitane potrebbero derivare dalla circostanza che alcune amministrazioni locali, oltre a detenere l'autorità per la gestione del suolo pubblico, sono anche azioniste di *public utilities*, che potrebbero decidere di operare come fornitori di servizi di telecomunicazione a livello urbano. La richiesta ai Comuni di scavare e realizzare una rete di connessione ai siti si scontrerebbe, in questi casi, con un palese conflitto di interessi tra il governo locale e le società di telecomunicazioni che richiedono le autorizzazioni.

Il documento passa poi ad esaminare la gerarchia dei livelli di competizione degli operatori di telecomunicazioni che può riscontrarsi in diversi comparti del mercato e che è attinente sia allo strato infrastrutturale sia ai servizi erogati attraverso di esso.

Nella scala gerarchica, se si sceglie di partire dal livello più lontano dall'utente finale, il primo livello è rappresentato dalle **opere civili** (per esempio scavi e tralicci), che vengono messe a disposizione per la posa di infrastrutture di comunicazione proprietarie. In uno stesso scavo possono venire alloggiati, per esempio, tubi diversi appartenenti a soggetti diversi. Il secondo livello è rappresentato dai **tubi**, che vengono messi a disposizione dei soggetti interessati per il passaggio dei cavi. In uno stesso tubo possono venire così alloggiati cavi appartenenti a soggetti diversi. Il terzo livello è rappresentato dai **cavi**, sia in fibra che in rame, sui quali è possibile realizzare un sistema trasmissivo proprietario. In questo caso nello stesso cavo vengono alloggiati circuiti trasmissivi appartenenti a operatori differenti. Il quarto livello, infine, è rappresentato dai **circuiti trasmissivi completi** sui quali transitano flussi numerici appartenenti a soggetti diversi: a questo livello di condivisione appartengono per esempio i sistemi xDSL offerti in *unbundling*. Per i primi due livelli - si evidenzia nel Rapporto - non sono richiesti né le capacità tecniche, né la struttura organizzativa tipiche degli operatori delle telecomunicazioni. La gestione potrebbe pertanto essere realizzata anche da pubbliche amministrazioni locali o da soggetti analoghi che hanno come obiettivo l'infrastrutturazione del territorio. In questo caso la condivisione di infrastrutture costituisce

un'importante opportunità di ottimizzazione delle risorse che potrebbe essere stimolata tramite l'individuazione di una serie di regole da utilizzarsi come riferimento sul territorio nazionale da parte delle Pubbliche amministrazioni locali. Tali regole possono prevedere ad esempio che, in occasione della richiesta di effettuazione di uno scavo da parte di un soggetto, l'amministrazione verifichi l'eventuale interesse da parte di altri soggetti a condividere la realizzazione dello scavo.

Al contrario, per i livelli superiori (terzo e quarto), è necessario l'intervento di soggetti specializzati, che devono disporre della necessaria competenza ed esperienza nel campo delle telecomunicazioni. Ciò dunque si traduce nell'esistenza di un'elevata barriera all'ingresso dovuta alla necessità di tempi molto lunghi per la realizzazione delle reti e alla capacità di investire molto denaro in costi non recuperabili in caso di uscita dal mercato (*sunk cost*).

Secondo quanto individuato dall'Autorità garante per le comunicazioni (Allegato B alla delibera 415/04/CONS[83]) nei criteri aggiuntivi per la valutazione del significativo potere di mercato vanno annoverate anche le *economie di scala* presenti sul mercato dell'accesso che "costituiscono un ulteriore disincentivo all'investimento da parte dei nuovi operatori". La struttura dei costi dell'accesso - prosegue l'Autorità - "basata su elevate immobilizzazioni e costi variabili contenuti, rende il costo unitario decrescente. Peraltro, tali economie non sono ancora completamente sfruttate in quanto la rete di Telecom Italia ha, in media, un tasso di occupazione pari a circa il 54,5% e quindi non necessita, nel medio periodo, di investimenti per adeguare la capacità produttiva a fronte di un eventuale significativo aumento della domanda. La presenza di una domanda concentrata in determinate aree consente lo sfruttamento anche di economie di densità".

Altre problematiche - segnala il Rapporto del Ministero - sono emerse sui cosiddetti meccanismi di *pricing*[84] dei servizi di telecomunicazione, che possono rappresentare ostacoli al manifestarsi di un'effettiva competizione di mercato.

Per quanto riguarda l'Italia l'attenzione si è focalizzata sia sul tema della rete di accesso (*unbundling*), sia su quello della rete di distribuzione, sia sui punti di accesso internazionali del *backbone*. In riferimento alla rete di accesso il punto nodale parrebbe rappresentato dalle tariffe praticate agli OLO dall'operatore telefonico principale.

Gli OLO hanno infatti espresso la convinzione che le tariffe praticate da Telecom Italia non osservino un reale orientamento ai costi. Peraltro tali tariffe

[83] Per il testo della delibera si veda riferimento in Appendice.
[84] Determinazione delle tariffe.

sono state verificate dall'Autorità e certificate. Un ulteriore problema sollevato riguarda la mancata differenziazione delle tariffe traffico voce e traffico dati, elemento questo che discosta il nostro Paese dai principali paesi europei. Se a livello complessivo (voce + dati), infatti, le tariffe vigenti in Italia sono all'incirca allineate con quelle medie UE, la mancanza della separazione tra voce e dati, porta a pagare un prezzo molto elevato la sola richiesta di dati. Quanto alla rete distributiva la problematica più significativa è invece rappresentata dalle linee affittate, le linee CDN (Circuito Diretto Numerico) di Telecom Italia, necessarie per collegare i siti degli OLO con quelli dell'*incumbent* in cui viene fornito l'*unbundling*. L'attuale situazione di *pricing*, relativamente alle CDN, è stata considerata da diversi operatori come un forte vincolo alla competizione.

Si è poi posto l'accento sul conflitto di interessi che si realizzerebbe internamente all'*incumbent*. Questi infatti fornendo due tecnologie con analoghe capacità di banda (xDSL e CDN), sarebbe indotto a difendere il proprio mercato sulla tecnologia consolidata, la CDN, che costituisce, grazie al mantenimento di prezzi di vendita molto elevati, una porzione ingente dei ricavi. Anche in relazione al *pricing* delle CDN, gli OLO e gli ISP (*Internet Service Provider)* hanno espresso la convinzione che le tariffe praticate da Telecom Italia non osservino un reale orientamento ai costi. E' stato inoltre rilevato come anche la qualità offerta dall'*incumbent* sul servizio xDSL sia "bloccata" dall'interesse di contrastare l'apertura del mercato e difendere il *business* delle CDN.

L'Autorità garante per le comunicazioni ha recentemente varato la Delibera 393/01/CONS "Offerta *wholesale* di linee affittate da parte della società Telecom Italia S.p.A.[85]." L'offerta *wholesale* di linee affittate entrerà in vigore dalla data di notifica delle relative condizioni economiche da parte dell'Autorità stessa. Nel corso delle audizioni si è inoltre esaminata la questione dei vincoli alla competizione concernenti i punti di accesso internazionali della rete dell'*incumbent*. Alcuni operatori hanno dichiarato di preferire quindi l'utilizzo di altre reti internazionali, in quanto più convenienti.

Sulla base di quanto evidenziato - prosegue il Rapporto ministeriale del 2003 - la liberalizzazione del mercato delle telecomunicazioni su rete fissa ha particolarmente penalizzato gli *Internet Service Provider* (ISP), favorendo gli operatori di rete fissa (*Incumbent* e OLO) nell'introduzione della filosofia dell'accesso "libero" alla rete (senza la necessità di sottoscrivere un abbonamento). Gli operatori (*Incumbent* e OLO) hanno potuto introdurre questa strategia estendendo gli introiti previsti per l'interconnessione del traffico voce al traffico dati. Se i benefici per i cittadini sono stati evidenti (in molti si sono avvicinati ad Internet per questa ragione), per gli ISP si è venuta a creare una

[85] Per il testo della delibera si consulti <http://www.agcom.it/provv/d_393_01_CONS.htm>.

condizione di disparità. Questi ultimi non hanno tuttora accesso ad alcun ritorno di tipo economico, alternativo e/o sostitutivo degli stessi abbonamenti.

Un ulteriore vincolo che svantaggia gli ISP, emerso nel corso delle audizioni, riguarda il numero minimo di numeri telefonici attualmente acquistabili, che è pari a 10.000, anche nel caso in cui gli ISP siano interessati ad utilizzare un solo numero per l'accesso. Oltre a costituire un aggravio di costi per gli ISP, tale condizione non consente di fornire un accesso locale agli ISP laddove, per varie circostanze, non siano disponibili almeno 10.000 numeri liberi.

Riguardo ai possibili assetti infrastrutturali il documento informa che, come negli anni '80 il settore dell'*information technology* ha visto la fine dei modelli basati sulla piena integrazione verticale (IBM, Digital, Honeywell, Bull) e l'apparire di leader di singoli *layer* tecnologici (Intel, Sun, Microsoft, Cisco), anche nelle telecomunicazioni si potrà assistere ad evoluzioni analoghe nel medio/lungo periodo. Più precisamente, il riferimento è alla separazione dei *business* della gestione della rete e delle infrastrutture di accesso da quello dell'erogazione dei servizi.

La rete di trasporto nazionale, in particolare quella dell'*incumbent*, è tecnologicamente datata e prevalentemente orientata alla fonia. Infatti gli operatori alternativi, dopo la liberalizzazione del mercato, hanno significativamente investito in reti concorrenti con criteri di progettazione e tecnologie aggiornate, pur se tali reti non sono ancora complete e non ancora distribuite in tutto il territorio nazionale. Questi investimenti troveranno prima o poi un punto di rottura con la convenienza ad affittare circuiti per la lunga distanza da chi possiede i *backbone* nazionali con tecnologie tradizionali. Dove invece la concorrenza non si è ancora sviluppata - fatta eccezione per la proposta imprenditoriale del gruppo e.Biscom - è sulla costruzione di una rete di accesso alternativa a quella dell'*incumbent*. Quest'ultima - segnatamente quella di Telecom Italia - il cui costo di sostituzione è per la sua capillarità elevatissimo, sarà nel tempo posta a raffronto/concorrenza con l'ultimo miglio in fibra ottica degli operatori che adotteranno questa soluzione.

La rete in rame è da considerarsi una *essential facility*, e quindi come tale, sul piano economico, non avrebbe senso la sua duplicazione da parte degli altri operatori con altre reti di accesso con la stessa tecnologia. Con riguardo ai servizi che vengono offerti tramite la rete si è in presenza di *business* a valore aggiunto con ampie possibilità di differenziazione. E' significativo notare che la rete è un bene strategico per l'erogazione dei servizi e per l'effettiva liberalizzazione del mercato. Pertanto la tempestività della messa a disposizione della rete e dei prezzi e servizi per il suo accesso (*unbundling*), è fondamentale per l'efficace sviluppo della concorrenza.

Questa problematica di un *asset* di rete di tipo *commodity* è stata affrontata dalle varie autorità regolatorie - sia in Italia che all'estero - con soluzioni a diverso grado di complessità: da un lato, la contabilizzazione separata di costi e ricavi inerenti alla rete, dall'altro la societarizzazione, ovvero l'istituzione di un

soggetto giuridicamente separato il cui *asset* principale è proprio costituito dalla rete. Si può notare che, in entrambi i casi, il concetto sottostante è quello della separazione. Esistono inoltre considerazioni di fondo sulla profonda differenziazione dei modelli di *business* che caratterizzano la gestione della rete di accesso rispetto a quelli che sono propri dell'erogazione dei servizi. La rete di accesso ha cicli di vita e sviluppo tipicamente lunghi: Telecom Italia ha spiegato che il valore fisico/tecnico dell'infrastruttura in rame si aggira sui 40 anni di durata massima e quindi il ritorno dell'investimento è tipicamente di lungo termine.

La gestione della rete necessita di competenze tecniche elevate, consolidate e certificate (gestione degli apparati, interventi di manutenzione, scelta dei cablaggi, ecc.). Caratteristiche fondamentali nell'attività di gestione di una rete sono: l'ottimizzazione architetturale e la conservazione nel tempo di massimi livelli di esercizio, la distribuzione territoriale, la distanza minima e massima delle utenze dagli stadi di linea urbani e la progettazione geografica in sintonia con lo sviluppo degli insediamenti produttivi ed abitativi. Il livello di esercizio dipenderà dall'impegno dedicato alla manutenzione e dal livello di efficienza di quanto concerne la gestione degli incidenti, giunzioni, nuovi allacciamenti, ecc. La gestione della rete obbliga infine ad un'attenzione continua alla realtà locale e geografica nella quale essa è insediata. L'offerta di servizi è invece caratterizzata da cicli di sviluppo molto più brevi, intensi e con un ritorno atteso sull'investimento a breve termine. Trattasi di iniziative che possono avere un profilo di rischio elevato, e le competenze distintive sono meno tecniche e più di *marketing*, e di aggregazione di contenuti o *bundling* di servizi. Tipicamente, l'offerta di servizi tramite reti di telecomunicazioni ha un panorama competitivo di riferimento di tipo internazionale: ad esempio, per rimanere su un servizio "datato" come la voce, la comunicazione a gruppi (*conference call*) ha profili di *pricing* e di servizio che si confrontano con quelli di altri operatori, anche a livello internazionale.

Inoltre la competizione sui servizi richiede una capacità di segmentazione dell'offerta sulla base dei profili e dei fabbisogni dei clienti (p.e. *business* verso utenza domestica, grandi imprese verso piccole e medie imprese, imprese verso Pubblica amministrazione, ecc.). Invero, la separazione della rete di accesso dalla gestione dei servizi presenta opportunità ma anche rischi. In termini regolamentari, la gestione del *local loo,* separato dal resto della struttura aziendale dell'operatore *incumbent*, avrebbe l'effetto di sollevare quest'ultimo da buona parte dei gravami derivanti dalle misure asimmetriche poste in essere dalle autorità di controllo, lasciandolo più libero di concentrarsi sull'innovazione di servizio per la sua vasta base di clienti. Si lascerebbe quindi ad un solo attore - in assenza di "conflitto di interessi" sulle proprie linee di *business* - il compito di manutenere, gestire e sviluppare la rete attuale. In termini competitivi, il tema della separazione permetterebbe agli altri operatori di accedere a condizioni di servizio in misura non asimmetrica. Il modello di integrazione verticale attuale (rete + servizi), invece, tende a ridurre il ruolo degli operatori alternativi a quello

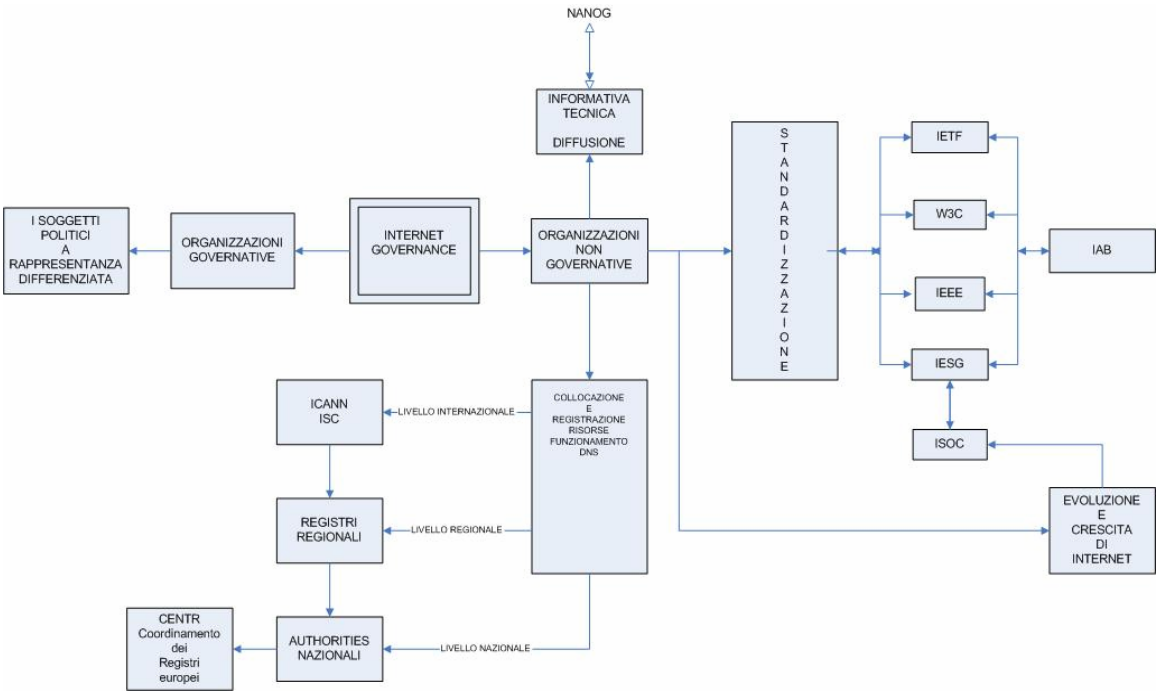
di semplici trasportatori di dati, che operano in aree oggi marginali del mercato utilizzando infrastrutture non proprie. E' invece probabile che al mercato serva proprio qualcuno che svolga la funzione di assumersi il rischio connesso alla titolarità della sola infrastruttura, offrendo elevata efficienza in cambio di alti volumi di servizio e rischi contenuti sul ritorno dell'investimento.

E' opportuno menzionare che, in tema di accesso, il 24 aprile 2002 le Istituzioni europee hanno adottato un nuovo quadro regolamentare, composto da cinque direttive, da una Raccomandazione e dalle Linee guida della Commissione. Le direttive comprendono: la c.d. direttiva quadro (2002/21/CE), quella per le autorizzazioni (2002/20/CE)[86], quella per l'accesso (2002/19/CE) e quella relativa al servizio universale (2002/22/CE). Tutte sono state recepite in Italia dal D. Lgs. 259 del 1° agosto 2003, recante "Codice delle comunicazioni elettroniche" (cosiddetto "Codice"). La Raccomandazione è relativa alle notificazioni, ai termini ed alle consultazioni (di cui all'articolo 7 della direttiva quadro) mentre le Linee guida illustrano alcuni criteri di cui le autorità nazionali di regolamentazione devono tenere conto nell'ambito delle analisi dei mercati di cui agli artt. 14, 15 e 16 della direttiva quadro. In particolare, con l'articolo 14 è attribuito alle autorità nazionali il compito di monitorare lo stato di sviluppo della concorrenza nei mercati per accertare il potere di mercato delle imprese che vi operano, sia singolarmente che congiuntamente.

Secondo quanto rilevato recentemente dall'Autorità per le garanzie nelle comunicazioni (allegato B alla delibera n. 415/04/CONS) il nuovo quadro regolamentare così delineato "riconosce il termine della fase di liberalizzazione dei mercati e sancisce la convergenza tra disciplina regolamentare e disciplina *antitrust*, in primo luogo attraverso la definizione dell'analogia tra significativo potere di mercato e posizione dominante. Infatti la direttiva quadro (considerando 25) indica che "la definizione di quota di mercato significativa di cui alla direttiva 97/33/CE (...) si è dimostrata utile nelle prime fasi di liberalizzazione dei mercati in quanto soglia che fa scattare alcuni obblighi *ex ante*, ma essa deve essere adattata per tenere conto di realtà di mercato più complesse e dinamiche. Per tale motivo la definizione di cui alla presente direttiva è equivalente alla nozione di posizione dominante enucleata dalla giurisprudenza della Corte di giustizia e del Tribunale di primo grado delle Comunità europee", laddove per posizione dominante si intende la "situazione di potenza economica grazie alla quale un'impresa che la detiene è in grado di

[86] Per i testi degli atti normativi comunitari e dell'Autorità garante per le comunicazioni non presenti nella documentazione allegata si consultino i siti segnalati in Appendice.

ostacolare la persistenza di una concorrenza effettiva sul mercato di cui trattasi e ha la possibilità di tenere comportamenti alquanto indipendenti nei confronti dei suoi concorrenti, dei suoi clienti e, in ultima analisi, dei consumatori".



Nota: Per soggetti politici a rappresentanza differenziata si intende fare riferimento sia alle organizzazioni con rappresentanza universale sia a quelle con rappresentanza limitata.

Elaborazione ed ideazione a cura di L. Stendardi (Servizio Studi).

C - PARTICOLARI QUESTIONI DEL GOVERNO DELLA RETE

I. La tutela della proprietà intellettuale e il diritto di autore nella Ue: il contrasto tra la Commissione e il Parlamento in merito alla proposta di brevettabilità del *software*.

Il 7 marzo 2005 il Consiglio europeo dei ministri sulla competitività ha adottato una posizione comune sulla proposta di direttiva che riguarda la brevettabilità "delle invenzioni realizzate tramite calcolatore". Ciò ha prospettato la concreta possibilità di introdurre un significativo cambiamento nel mercato del *software* europeo. Si ricorda che sulla brevettabilità del *software* si era espresso negativamente il Parlamento europeo, con la posizione del 24 settembre 2003. Il testo conteneva una serie di emendamenti con i quali si intendeva modificare profondamente il testo originario di proposta di direttiva presentata dalla Commissione europea.

1. Cosa disponeva la proposta di direttiva

La proposta di direttiva (articolo 2) spiega innanzitutto cosa debba intendersi con l'espressione "invenzione messa in atto per mezzo di un elaboratore o apparecchio analogo", recitando che si tratta di "un'invenzione la cui esecuzione implica l'uso di un elaboratore, di una rete di elaboratori o di un altro apparecchio programmabile e che presenta, a prima vista, non soltanto una o più caratteristiche di novità che sono realizzate, in tutto o in parte, per mezzo di uno o più programmi per elaboratore". Definisce inoltre "contributo tecnico" un contributo giudicato non ovvio da una persona competente in materia. Secondo il commento fornito nel medesimo testo della proposta di direttiva, l'espressione "a prima vista" significa che non è "necessario stabilire la novità effettiva" - anche a mezzo di indagine - per determinare se una invenzione può essere giudicata tale. Ai sensi dell'articolo 3 (che riprende la norma dell'articolo 27, paragrafo 1 dell'accordo ADPIC/WTO), il brevetto può essere concesso per ogni invenzione di prodotti o di processi in tutti i campi della tecnologia, purché essa implichi un'attività inventiva e sia atta ad un'applicazione industriale. Un'invenzione attuata per mezzo di elaboratori elettronici è considerata "appartenente a un settore della tecnologia". Per essere brevettabile essa deve arrecare - come già ricordato - un contributo tecnico. Questo va valutato considerando "la differenza tra l'oggetto della rivendicazione di brevetto nel suo insieme, i cui elementi possono comprendere caratteristiche tecniche e non tecniche, e lo stato dell'arte".

Nella presentazione di commento all'articolato della proposta, la Commissione tiene a sottolineare che quanto disposto dall'articolo 4, paragrafo 2 (ossia la presenza della condizione di contributo tecnico) è da considerare come un'integrazione e non come una sostituzione di quanto disposto dall'articolo 56 della CBE (Convenzione sul brevetto europeo). Il contributo tecnico deve essere valutato nel suo insieme (articolo 4, paragrafo 3), conformemente alle decisioni della commissione tecnica di ricorso dell'UEB (Ufficio europeo brevetti), dove si afferma che non si deve procedere ad una "ponderazione" tra caratteristiche tecniche e non tecniche per stabilire quale delle due componenti dia il contributo più rilevante al successo dell'invenzione. L'articolo 4 dispone ancora - sempre in conformità a quanto stabilito dall'articolo 27, paragrafo 1 dell'accordo TRIPs (*Trade – Related Aspects of Intellectual Property Rights,* WTO) - che un'invenzione attuata per mezzo di elaboratori è brevettabile sotto il duplice profilo del prodotto e del processo, ovvero sia come elaboratore (o apparecchio simile) sia come processo eseguito dall'elaboratore. La Commissione, nel suo commento, sostiene di operare in modo difforme riguardo alla prassi dell'Ufficio europeo brevetti che ammette invece la brevettabilità del *software* di per se stesso o su un vettore.

2. Le proposte emendative del Parlamento europeo in prima lettura

Nel corso della prima lettura il Parlamento europeo ha largamente emendato il testo proposto dalla Commissione, per quanto riguarda la definizione di invenzione e di contributo tecnico. In particolare, in riferimento alla definizione di invenzione, si fa esplicito richiamo alle caratteristiche non tecniche che devono comparire nelle applicazioni dell'invenzione perché questa abbia carattere di "novità". Riguardo al "contributo tecnico" si chiarisce che "il trattamento, la manipolazione e la presentazione di informazioni non rientrano in un settore tecnico, anche se per effettuarli sono utilizzati apparecchi tecnici". Ciò è anche ribadito nell'articolo 3 dove non si riconosce l'elaborazione dei dati come settore tecnico. Il Parlamento ha poi stabilito delle norme che individuano le cause di esclusione della brevettabilità, disponendo che "non sono brevettabili le invenzioni implicanti programmi per elaboratori che applicano metodi per attività commerciali, metodi matematici o di altro tipo e non producono alcun effetto tecnico, oltre a quello delle normali interazioni fisiche tra un programma e l'elaboratore, la rete di elaboratori o un altro apparecchio programmabile in cui viene eseguito". Non sono altresì brevettabili le soluzioni di problemi tecnici realizzate per mezzo di elaboratori elettronici,

quando queste migliorino semplicemente l'efficacia nell'impiego delle risorse del sistema. Largamente modificato appare anche l'articolo 7 inerente la "forma delle rivendicazioni", con il quale si impone di operare una scelta tra brevettabilità del prodotto o del processo tecnico di produzione. Viene poi ulteriormente ribadito che un programma per elaboratore, relativo al solo programma o esistente su un supporto dati, non è brevettabile, come pure è escluso che l'uso di un programma per scopi che non riguardano l'oggetto del brevetto costituisca una violazione di brevetto diretta o indiretta. Nessuna violazione è inoltre ravvisata nell'uso di una tecnica brevettata, se questo uso sia necessario per la realizzazione di un fine importante, come ad esempio la conversione delle convenzioni utilizzate in due diversi sistemi o reti di elaboratori.

3. La posizione comune adottata dal Consiglio

Il 7 marzo 2005 - come già ricordato - il Consiglio ha adottato, a maggioranza qualificata, una posizione comune che ha incorporato circa 25 emendamenti formulati dal Parlamento europeo in prima lettura e che è stata ricevuta dal Parlamento, per la seconda lettura, in data 14 aprile 2005. Conformemente alla Convenzione sul brevetto europeo, il Consiglio ha stabilito che un programma per elaboratore in quanto tale non può costituire un'invenzione brevettabile. Non sono brevettabili le invenzioni implicanti programmi per elaboratori, in codice sorgente, in codice oggetto o in qualsiasi altra forma, che applicano metodi per attività commerciali, metodi matematici o di altro tipo e non producono alcun effetto tecnico oltre a quello delle normali interazioni fisiche tra un programma e l'elaboratore, la rete o un altro apparecchio programmabile in cui viene eseguito.

E' stata introdotta una nuova disposizione per chiarire quali siano le circostanze e le condizioni che permettono la brevettabilità per programmi di elaboratori, da soli o su vettore (articolo 5, comma 2). Sulla nuova proposta la Commissione si è dichiarata favorevole all'accoglimento, ritenendola un compromesso accettabile tra gli interessi dei titolari del diritto e quelli dei concorrenti e dei consumatori (compresa la *open source community*). La Commissione, nel testo della comunicazione[87] di

[87] COM (2005) 83 def del 9 marzo 2005. Il testo della comunicazione e della posizione comune del Consiglio sono disponibili all'indirizzo: <http://www.europa.eu.int/prelex/detail_dossier_real.cfm?CL=it&DosId=172020> (scheda prelex rispettivamente ai *link* COM(2005)83def e GU C E /2005/144/ 9 a pagina n. 9).

commento a quello della posizione comune, ha comunque ritenuto necessario sottolineare l'opportunità di una formulazione più chiara sull'esclusione di brevettabilità per i programmi di elaboratori in quanto tali.

Per il tema degli *standard* aperti si veda <http://www.fsfeurope.org/>.

4. Il Parlamento europeo in seconda lettura: la Raccomandazione relativa alla posizione comune adottata dal Consiglio

In data 21 giugno 2005 il Parlamento europeo ha votato una risoluzione legislativa con la quale si è espresso in merito alla posizione comune adottata dal Consiglio ed ha inteso emendare nuovamente e profondamente il testo adottato dalla Commissione europea sulla brevettabilità del *software.*

Sono state riproposte molte delle osservazioni critiche formulate in prima lettura. Il concetto fondamentale contenuto nel testo della Raccomandazione è la contrarietà alla brevettabilità dei programmi per elaboratore elettronico: "il *software* infatti - dichiara il Parlamento nella motivazione della risoluzione - non è brevettabile più di quanto non lo siano un accordo musicale o un insieme di parole. Essendo formato da un insieme di formule matematiche collegate fra loro, il *software* è una produzione dello spirito umano nell'ambito delle idee. E la libera circolazione delle idee è un principio basilare per la nostra civiltà".

Tra gli altri punti di rilievo si evidenziano quello dell'emendamento 4 (che introduce il nuovo considerando 10 *bis*) con il quale è nuovamente sottolineata la necessità che la direttiva contenga una definizione la più chiara possibile del termine "contributo tecnico", emumerando sempre quelle interpretazioni che devono escludersi dall'ambito di applicazione, o l'indicazione delle condizioni di brevettabilità (emendamento 5) che deve includere "l'applicabilità industriale dell'invenzione".

II. La tutela della proprietà intellettuale

Il sistema di tutela della proprietà intellettuale ha il suo riferimento in tre sottoinsiemi normativi che attengono rispettivamente all'oggetto, al contenuto ed alla fattispecie costitutiva della protezione[88]. Sul piano

[88] M.BERTANI, *Proprietà intellettuale, antitrust e rifiuto di licenze,* «Quaderni di AIDA», n. 10 (2004), pagg. 12-54.

dell'oggetto l'articolo 52, comma 1[89] della **CBE** [90](Convenzione europea dei brevetti) prevede che siano brevettabili le invenzioni, in tutti i settori della tecnica, con carattere di novità e suscettibili di applicazione industriale. In base al successivo comma 2 è consentita l'appropriazione di un insegnamento diverso dal sapere puramente teorico. Recita infatti la norma che non sono da considerare invenzioni "le scoperte, le teorie scientifiche, i metodi matematici, le creazioni estetiche, i piani, principi e metodi per attività intellettuale, per gioco o per attività commerciali, i programmi per elaboratori e le presentazioni di informazioni". Circa l'ampiezza dell'esclusione si ricorda che la CBE all'articolo 52, comma 3, specifica che non è esclusa la brevettabilità delle entità elencate se non nella misura in cui la domanda di brevetto o il brevetto vi faccia riferimento come creazioni considerate "in quanto tali". Secondo qualcuno questa condizione presuppone ragionevolmente che l'entità in sé non brevettabile possa essere connessa ad un'altra che può invece essere protetta e che è rappresentata da qualsiasi insegnamento diverso da quelli espressamente richiamati nella norma.[91]

Riguardo ai programmi per elaboratori, sia il Comitato "Diritto dei brevetti", sia il Consiglio di amministrazione dell'EPO (Ufficio europeo brevetti) si sono espressi per la loro espunzione dalle categorie escluse. In questo modo il *software* sarebbe definibile come "invenzione" e come tale brevettabile. Del resto - viene ancora evidenziato nel documento di lavoro - questo sarebbe in sintonia con quello che è sempre stato l'orientamento giurisprudenziale secondo il quale i programmi di elaboratore che producono un effetto tecnico sono, in via generale, da considerare oggetti brevettabili. E' però anche vero, si sottolinea, che la nuova stesura dell'articolo 52 rende inequivocabile che la protezione brevettuale deve essere riferita ad invenzioni afferenti al settore della tecnica, cioè che per essere brevettabile un oggetto deve possedere un "carattere tecnico" o meglio deve produrre "un insegnamento pratico in materia tecnica". Per quanto riguarda il diritto vigente comunitario, si ricorda che la Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore, prevede che questi siano da considerare come opere letterarie ai sensi della **Convenzione di Berna** sulla tutela delle opere letterarie e artistiche. Nel termine "programma per elaboratore" è compreso il materiale preparatorio per la progettazione. Inoltre, ai sensi dell'articolo 2 della direttiva, la tutela si applica a qualsiasi

---

89 Trasfonde la norma dell'articolo 27, paragrafo 1 dell'Accordo TRIP's sulla proprietà intellettuale.

90 Il testo degli articoli citati è compreso nella documentazione allegata.

91 M. BERTANI, op. cit.

forma di espressione di un programma per elaboratore. Non sono invece da comprendere nella tutela le idee e i princìpi basilari di qualsiasi elemento di un programma per elaboratore, compresi quelli riguardanti l'interfacciabilità. L'unico criterio considerato legittimo per determinare il diritto alla tutela, consiste nell'accertamento dell'originalità dell'opera frutto della creazione intellettuale dell'autore. Autore del programma è definito la persona fisica o il gruppo di persone fisiche che ha creato il programma o, qualora la legislazione degli Stati membri lo permetta, la persona giuridica è designata da tale legislazione come titolare del diritto. Qualora la legislazione di uno Stato membro riconosca le opere collettive, la persona considerata creatrice dell'opera dalla legislazione di tale Stato ne è ritenuto l'autore. Dal riconoscimento del diritto discende una serie di autorizzazioni, quali:

a) la riproduzione, permanente o temporanea, totale o parziale di un programma per elaboratore con qualsivoglia mezzo, in qualsivoglia forma. Nella misura in cui operazioni come il caricamento, la visualizzazione, l'esecuzione, la trasmissione o la memorizzazione del programma per elaboratore richiedono una riproduzione, tali operazioni devono essere sottoposte ad autorizzazione da parte del titolare del diritto;

b) la traduzione, l'adattamento, l'adeguamento e ogni altra modifica di un programma per elaboratore e la riproduzione del programma che ne risulti, fatti salvi i diritti della persona che modifica il programma;

c) qualsiasi forma di distribuzione al pubblico, compresa la locazione, del programma per elaboratore originale e di copie dello stesso. La prima vendita della copia di un programma nella Comunità da parte del titolare del diritto o con il suo consenso esaurisce il diritto di distribuzione della copia all'interno della Comunità, ad eccezione del diritto di controllare l'ulteriore locazione del programma o di una copia dello stesso.

Ai sensi dell'articolo 8 della direttiva, la tutela è riconosciuta per tutta la vita dell'autore e per cinquant'anni dopo la sua morte o dopo la morte dell'ultimo autore sopravvissuto; qualora il programma per elaboratore sia un'opera anonima o pseudonima, o qualora una persona giuridica sia considerata autrice del programma dalla legislazione nazionale, conformemente all'articolo 2, paragrafo 1, la durata della tutela è di cinquant'anni, a decorrere dalla data alla quale il programma per elaboratore è stato per la prima volta messo legittimamente a disposizione del pubblico.

Anche in ambito **WTO, l'accordo TRIPs** sulla tutela del diritto di proprietà intellettuale[92] che riguarda il commercio prevede (articolo 10, Parte II, Sezione 1, Allegato 1C) - conformemente a quanto disposto dalla Convenzione di Berna - che i programmi per elaboratore (sia che siano espressi in codice sorgente sia in codice oggetto) siano protetti come opere letterarie. Il campo di applicazione delle norme internazionali è esteso, secondo l'Accordo, anche ai diritti di noleggio, il che consente agli autori del *software* di esercitare il diritto di impedire il noleggio commerciale delle loro opere.

Si rammenta infine che nel giugno 2000 è stato firmato il ***Patent Law Treaty*** **(PLT),** trattato di armonizzazione internazionale delle norme in materia di brevetti, entrato in vigore il 28 aprile 2005.

1. Il sistema di brevettazione europeo

Il brevetto europeo è un titolo giuridico rilasciato dall'Ufficio europeo di brevetti, organo dell'Organizzazione europea dei brevetti. Conferisce al suo titolare un'esclusività temporanea di utilizzazione dell'invenzione, per un territorio determinato. Il possesso del titolo impedisce quindi a terzi di fabbricare, vendere o utilizzare l'invenzione senza la preventiva autorizzazione. Il brevetto europeo permette di ottenere la tutela in tutti gli stati membri dell'Organizzazione europea dei brevetti sulla base di una domanda depositata in una delle tre lingue ufficiali (tedesco, inglese e francese). Gli effetti giuridici del titolo si producono anche in quei Paesi con il quali l'Organizzazione ha concluso accordi in tal senso ed in cui i brevetti non vengono registrati (c.d. brevetto "forte"). Va però puntualizzato che questo tipo di protezione della proprietà intellettuale non si basa su uno strumento giuridico comunitario bensì su due sistemi complementari: il sistema nazionale e quello europeo.
Il brevetto nazionale ha formato l'oggetto di un'armonizzazione *de facto* in seguito alla conclusione di diverse convenzioni internazionali, inclusa la Convenzione sul rilascio dei brevetti europei (Convenzione di Monaco) del 1973, alla quale tutti gli Stati membri dell'UE hanno aderito.

---

[92] Per approfondimenti si veda <http://www.wto.org/english/docs_e/legal_e/legal_e.htm> e M. BERTANI, *Proprietà intellettuale, antitrust e rifiuto di licenze,* «Quaderni di AIDA», n. 10, 2004, pagg. 12-54. Sintesi degli accordi sulla proprietà intellettuale e diritto di autore in:
<http://www.wto.org/french/thewto_f/whatis_f/tif_f/agrm7_f.htm>.
Si veda anche P. ZOCCOLI, *Il WTO e la regolazione della liberalizzazione del commercio mondiale per la costruzione del vantaggio competitivo della nazione e delle imprese,* in «Economia e diritto del terziario», n. 2 (2004), pagg. 396-413.

La Convenzione di Monaco stabilisce una procedura unica di rilascio del brevetto europeo ed ha istituito l'Ufficio europeo dei brevetti, il quale rilascia i brevetti che diventano in seguito brevetti nazionali disciplinati dalle norme nazionali. L'esistenza di un unico *iter* procedurale non deve però confondersi con l'introduzione nell'ordinamento giuridico comunitario di un vero e proprio brevetto europeo che è ancora solo un'idea da concretizzare. Ci si riferisce ad una proposta di regolamento che è il risultato delle discussioni avviate con la pubblicazione del Libro verde sul brevetto comunitario ed il sistema dei brevetti in Europa, avvenuta in data 24 giugno 1997. Gli orientamenti del Libro sono stati presentati nella comunicazione della Commissione del 5 febbraio 1999 ("*Promuovere l'innovazione tramite il brevetto - Il seguito da dare al Libro verde sul brevetto comunitario e sul sistema dei brevetti in Europa*") e l'importanza di una rapida attuazione del brevetto comunitario è stata risottolineata dal Consiglio europeo di Lisbona del 23 e 24 marzo 2000. Secondo il testo proposto i sistemi nazionali e quello europeo dovranno continuare a coesistere creando però una sorta di simbiosi tra il sistema del brevetto comunitario e quello della Convenzione di Monaco. Dopo l'adozione del regolamento, la Comunità avrà la competenza esterna esclusiva per quanto riguarda il brevetto comunitario che avrà un carattere unitario ed autonomo e produrrà gli stessi effetti nell'intero territorio europeo.
Riguardo allo stato dell'*iter* della proposta di regolamento si ricorda che il **10 aprile 2002** il Parlamento europeo ha approvato la proposta della Commissione con alcuni emendamenti che riguardano in particolare le disposizioni linguistiche, il ruolo degli uffici nazionali dei brevetti nei confronti dell'Ufficio europeo dei brevetti ed il sistema giudiziario.

Il **3 marzo 2003** il Consiglio ha raggiunto un accordo su un approccio politico comune che concerne i princìpi e le caratteristiche di base del sistema giudiziale, del regime linguistico, dei costi, del ruolo degli uffici nazionali dei brevetti e della ripartizione delle entrate.
In particolare è stato deciso che, a partire dal 2010, le controversie relative ai brevetti comunitari saranno esaminate in primo grado dinanzi ad una camera giurisdizionale, istituita con decisione del Consiglio, e denominata **Tribunale del brevetto comunitario**. Tale camera sarà associata al Tribunale di primo grado delle Comunità europee. Sino ad allora i tribunali nazionali continueranno ad essere competenti per le controversie sui futuri brevetti comunitari. Per quanto riguarda il regime linguistico, le rivendicazioni dovranno essere presentate in una delle tre lingue ufficiali dell'Ufficio europeo dei brevetti (inglese, tedesco o francese), che sarà la lingua di lavoro, e tradotte a spese dell'Ufficio in altre due lingue (italiano e

spagnolo). Una volta rilasciato il brevetto, tali rivendicazioni dovranno essere tradotte in tutte le lingue comunitarie. I **diritti** risultanti dalla concessione dei brevetti dovrebbero essere suddivisi in parti uguali fra l'Ufficio europeo dei brevetti e gli uffici nazionali, secondo criteri da stabilire.

Il **26 novembre 2003** il Consiglio ha esaminato le questioni rimaste in sospeso, raggiungendo un ampio accordo su un testo di compromesso presentato dalla presidenza italiana. Non è stato però possibile trovare consenso unanime su tutti i temi in discussione. Allo stato attuale il principale scoglio politico sembra essere costituito dalla traduzione della domanda di rivendicazione del brevetto. Il testo proposto prevede, infatti, che tali rivendicazioni - che sono la parte più breve ma la più importante, in quanto attinente alla definizione dei limiti della protezione - vadano tradotte in tutte le lingue ufficiali dell'UE. Ne consegue che il nodo essenziale da sciogliere è quello dell'individuazione dei soggetti che dovranno giudicare della validità giuridica della traduzione e della definizione delle modalità di gestione degli effetti di una traduzione errata. Un secondo punto di disaccordo riguarda la definizione del termine di deposito delle traduzioni. Anche questa è una questione fondamentale in quanto, secondo il regime proposto, se le traduzioni non verranno depositate entro i limiti fissati, il brevetto comunitario sarà giudicato privo di effetto.

2. Il brevetto internazionale

Il PCT o Trattato di Cooperazione in materia di Brevetti (*Patent Cooperation Treaty*) è un trattato multilaterale gestito dall'OMPI (Organizzazione Mondiale della Proprietà Intellettuale) che ha sede a Ginevra. La procedura PCT facilita l'ottenimento di una protezione per le invenzioni negli Stati membri del Trattato. Un'unica domanda internazionale ha gli stessi effetti di una domanda nazionale per gli Stati designati; è anche possibile effettuare una designazione di "brevetti regionali" (cioè validi in un gruppo di Stati). Attualmente le Organizzazioni regionali sono:

- l'OEB (Organizzazione Europea dei Brevetti)
- l'ARIPO (*African Regional Industrial Property Organization*)
- l'OAPI (*Organisation Africane pour la Propriété Intellectuelle*)
- l'EAPO (*Euroasian Patent Office*)

Il PCT non elimina la necessità di continuare singolarmente la procedura per il rilascio in ogni Stato (o organizzazione regionale) designato, però ne facilita il proseguimento. L'esame formale, la ricerca documentale internazionale e (facoltativamente) l'esame internazionale preliminare, sono effettuati una volta sola per tutti i Paesi durante la fase internazionale della procedura. Il rilascio del brevetto resta però di esclusiva competenza dell'ufficio nazionale (o regionale) designato.

ORGANIZZAZIONE EUROPEA DEI BREVETTI

L'**Organizzazione europea dei brevetti** (OEB) è stata istituita dalla Convenzione di Monaco (Convenzione sul brevetto europeo - CBE) per rafforzare la cooperazione tra i paesi europei in materia di protezione delle invenzioni. E' costituita da un Consiglio di amministrazione - che ne rappresenta l'organo legislativo - e dall'Ufficio europeo dei brevetti (organo esecutivo). Il Consiglio di amministrazione vota il bilancio e conferisce l'incarico al presidente per la sua esecuzione o per modificare il regolamento relativo alle tasse di iscrizione. L'OEB è strutturata in cinque direzioni generali: le DG1 e DG2 che hanno competenza per l'esame delle domande di brevetto fino al suo rilascio ed alla procedura di ricorso. L'esame è sia di tipo formale, sia attinente al monitoraggio dello stato della tecnica. L'OEB è inoltre competente per la pubblicazione delle domande e per l'esame del finanziamento. La DG1 raccoglie la documentazione di ricerca. La DG3 si occupa dei ricorsi e su di essi si esprime. La DG4 è competente per l'amministrazione generale, la gestione del personale, dei finanziamenti e dell'informazione sui brevetti.

La DG5 ha competenza per le questioni giuridiche e gli affari internazionali. L'OEB è un ente autonomo sul piano finanziario e degli investimenti. L'autofinanziamento si attua attraverso l'introito delle tasse di registrazione dei brevetti rilasciati annualmente. Queste vengono pagate direttamente dai titolari del brevetto agli uffici nazionali. La definizione dell'ammontare del pagamento è assoggettata al diritto nazionale dei differenti Stati. Per il 2004 il *budget* è risultato superiore a 1,1 miliardi di euro (cfr. cronologia delle tappe sul sistema di brevettazione europeo nella brochure di presentazione dell'Ufficio europeo dei brevetti).

Attualmente nel mondo sono in vigore più di 4 milioni di brevetti ed ogni anno vengono depositate circa 700 mila domande. Dopo la pubblicazione, i *dossier* sulle domande di brevetto sono soggetti ad

ispezione pubblica, ovvero chiunque può prendere visione delle notificazioni, delle risposte dei richiedenti e delle eventuali modifiche apportate alle domande. Le informazioni sono accessibili non soltanto in forma cartacea, ma anche tramite Internet o altri supporti. La loro pubblicizzazione ha lo scopo di stimolare l'innovazione, gli investimenti e il trasferimento di tecnologie, permettendo di evitare la ripetizione di ricerche parallele sui medesimi prodotti. Più dell'80 per cento dei brevetti mondiali sono rilasciati dall'OEB, dall'Ufficio dei brevetti giapponese e da quello statunitense. I tre uffici - al fine di gestire meglio il volume delle domande - hanno instaurato a partire dal 1983 una cooperazione per i progetti di automatizzazione delle banche dati. La Convenzione europea dei brevetti è collegata al Trattato di cooperazione in materia di brevetti, trattato internazionale che definisce una procedura di deposito uniforme e semplificata, valida in 100 paesi che è seguita da una procedura di ricerca internazionale e, a richiesta, anche da un esame preliminare internazionale. L'attuazione del Trattato è di competenza dall'Organizzazione mondiale della proprietà intellettuale di Ginevra (OMPI). Nel quadro degli accordi conclusi con questa organizzazione, l'OEB agisce come esecutore del Trattato in qualità di ufficio ricevente, di amministrazione incaricata della ricerca internazionale e di amministrazione incaricata dell'esame preliminare internazionale. I brevetti europei possono essere rilasciati sulla base di domande internazionali depositate ai sensi delle norme del Trattato.

L'Accademia internazionale dell'Ufficio europeo dei brevetti è stata fondata nel 1997. Ha il compito di garantire il collegamento tra gli Stati membri, le agenzie internazionali (WIPO, OHIM) le università, gli istituti di ricerca[93] ed i professionisti esperti nel campo della proprietà intellettuale. Assieme agli esperti dell'Ufficio europeo brevetti e dei vari uffici nazionali, l'Accademia promuove corsi di aggiornamento e formazione in tema di proprietà intellettuale. Ha organizzato un totale di 22 seminari, *forum* e simposi. L'attività principale nel 2003 ha riguardato il tema del brevetto del *software*.

[93] In particolare l'Accademia collabora con WIPO, OHIM, BBM (*Benelux trademark office*), uffici nazionali per la proprietà intellettuale dei vari stati europei, EPI (*Institute of Professional Representative before the EPO*), CEIPI *(Centre for International Industrial Property Studies at the Robert Schuman University*), EIPIN *(European Intellectual Property Institutes Network)*, MPI *(Max Planck Institute for intellectual property, Competition and Tax Law)*, ISI *(Fraunhofer Institute for Systems and Innovation Research)*, LESI (*Licensing Executives Society International*), UNICE *(The Voice of Business in Europe).*

UFFICIO EUROPEO DEI BREVETTI

L'**Ufficio europeo dei brevetti,** istituito nell'ambito dell'Organizzazione europea dei brevetti, svolge attività di cooperazione tra i vari Paesi e le regioni dell'Europa centrale ed orientale, dell'Africa, dell'America Latina e dell'Asia. I progetti, in taluni casi commissionati dalla Commissione europea, sono finalizzati a realizzare l'ammodernamento dei sistemi di protezione della proprietà industriale, allineandoli alle disposizioni stabilite dagli accordi TRIP's sulla proprietà intellettuale, definiti dalle Conferenze ministeriali del WTO. Lo scopo è quello di creare le condizioni per migliorare gli investimenti ed il trasferimento di tecnologia nel quadro delle relazioni commerciali ed economiche con l'Unione europea e con gli altri Stati europei. L'Ufficio concorre poi all'attuazione del *"common software*" destinato alla gestione dei brevetti e dei marchi. In origine questo *software* era stato sviluppato nel quadro del programma di assistenza regionale dell'Unione europea per gli uffici dei brevetti dei Paesi dell'Europa centrale e orientale. Tutte le domande presentate all'Ufficio europeo dei brevetti vengono pubblicate in *dossier*, costituendo in questo modo sia un'opportunità di osservazione dei mercati sia una fonte informativa delle più recenti innovazioni tecniche, utile anche ad evitare sviluppo di ricerche parallele.

Per approfondimenti si veda <http://www.european-patent-office.org/index.en.php>.

III. La *open source*

Nel corso degli ultimi anni il tema dell'*open source* è stato molto dibattuto nei diversi contesti pubblici e privati e da parte di molti si è fatto notare che questa soluzione potrebbe costituire un elemento fondamentale per risolvere i problemi attinenti all'uso ed alla valorizzazione delle tecnologie informatiche, soprattutto nel mondo della Pubblica Amministrazione.

Con l'espressione *"open source"* ci si riferisce ad un programma per elaboratore che deve includere il codice sorgente e deve consentire la distribuzione sia sotto forma di codice sorgente, sia in forma compilata. Nei casi in cui il *software* non includa il codice sorgente questo deve essere comunque scaricabile via Internet senza costi aggiuntivi. Il codice sorgente deve essere la forma privilegiata in cui il programmatore modifica il

programma. Spesso il termine *open source* ne richiama un altro, quello di *free software.*

Secondo la definizione data dalla *Free Software Foundation*[94] (FSF) il *software* libero (o *free software*) "si riferisce alla libertà dell'utente di eseguire, copiare, distribuire, studiare, cambiare e migliorare il *software*". Più precisamente, esso consente che gli utenti siano liberi in quattro aspetti:

1. libertà di eseguire il programma, per qualsiasi scopo;
2. libertà di studiare come funziona il programma ed adattarlo alle proprie necessità. L'accesso al codice sorgente ne è un prerequisito;
3. libertà di ridistribuire copie in modo da aiutare il prossimo;
4. libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti, in modo tale che tutta la comunità ne tragga beneficio. L'accesso al codice sorgente ne è un prerequisito.

Va evidenziato che - sempre secondo le definizioni date dalla FSF - i termini "*open source*" e "*software* libero" sono molto spesso usati come fossero sinonimi anche se individuano approcci concettuali diversi. Mentre il *software* libero va considerato tale in relazione alle motivazioni etiche e di principio dalle quali scaturisce la tutela di una serie di diritti dell'utente (quelli richiamati nei punti sopra elencati), l'*open source* trova le proprie motivazioni in considerazioni tecnico-economiche. Né il "*free software*" né *l'open source* implicano comunque l'obbligatorietà della gratuità. Nel rapporto[95] conclusivo dell'indagine conoscitiva sul *software* libero, condotta recentemente (maggio 2003) da una commissione ministeriale istituita *ad hoc* presso il Ministero per l'innovazione e le tecnologie, vengono sintetizzate le informazioni sui principali prodotti *open source* disponibili oggi sul mercato. Si fa anzitutto distinzione tra prodotti OS[96] lato *server*[97] e prodotti OS lato *client*[98], evidenziando come sia decisamente più trainante il mercato del *software* OS dedicato al lato *server*. Secondo uno studio IDA (*Interchange of Data between Administrations*)[99], citato nel Rapporto, l'utilizzazione dell'OS nelle strutture pubbliche dei Paesi considerati è pari al 63% (in maggior parte riferibile alle applicazioni *web* e *file*). Relativamente alle applicazioni destinate ai *server*, le soluzioni

---

94 La *Free Software Foundation* (FSF), nata nel 1985, promuove una politica di sostegno per il diritto ad usare, studiare, copiare, modificare e redistribuire i programmi per elaboratori.

95 Ministero per l'innovazione e le tecnologie, *Indagine conoscitiva sul sofware a codice sorgente aperto nella Pubblica Amministrazione,* Rapporto della Commissione, maggio 2003.

96 *Open Source.*

97 Fornitore di servizi Internet.

98 Utilizzatore della rete Internet.

99 Si veda <http://europa.eu.int/idabc/>.

software più utilizzate sono il sistema operativo Linux e il *web server* Apache (quest'ultimo è diffuso per il 68% nelle applicazioni della pubblica amministrazione). Quanto a Linux si sottolinea che questo è stato il sistema operativo che ha avuto la più rapida espansione nel periodo 1999/2000 (crescita del 132 per cento)[100] pur essendosi ormai stabilizzata la diffusione. Per quanto concerne il mercato del *sofware* OS lato *client* - più dimensionato, come ricordato, rispetto al precedente - l'indagine fornisce dettagliate informazioni circa i principali fornitori di soluzioni e di servizi e le tipologie di supporto (installazione, fornitura di pacchetti, contratti, realizzazione di progetti, consulenza gratuita). Il documento illustra inoltre un quadro dei prodotti OS, operando una distinzione tra sistemi operativi, *software* di infrastruttura e *software* applicativi. Interessante è pure il quadro comparatistico che richiama la situazione di diffusione dell'OS nei principali Paesi europei, il capitolo dedicato alle prospettive di sviluppo (e alla valutazione dell'impatto) dell'OS nel mondo dell'istruzione, dell'industria e della ricerca e, da ultimo, il capitolo dedicato alle proposte per incrementare la diffusione del *software* libero.

Per approfondimenti:

<http://www.fsf.org/>,<http://www.openitalia.net/>,<http://www.linux.it/>,<http://www.linux.it/GNU/articoli/index.shtml>,<http://www.linux.it/GNU/opinioni/index.shtml>.

La ***Free Software Foundation*** è nata nel 1985 per promuovere una politica di sostegno del *software* libero ed in particolare del sistema operativo GNU. La sezione europea della Fondazione, la FSF *Europe*, ha partecipato ai lavori del *World Summit on the Information Society* (WSIS) assieme ad altri rappresentanti della società civile, per assicurarsi che i princìpi fondamentali dell'era digitale non siano determinati solo dall'industria dei media e dai governi e che i diritti umani non incontrino, nella fase applicativa, limiti di tipo tecnologico. Nel corso del primo appuntamento del WSIS è stato istituito un Gruppo di lavoro dell'ONU sulla *Internet governance* (WGIG), con il fine di poter dare voce in seguito a tutti i soggetti che operano nel mondo della rete globale. Tuttavia il tema del *software* libero, pur rientrando nella lista degli argomenti di lavoro, non è stato affidato - come oggetto di riflessione specifica - ad alcun gruppo. La FSF *Europe* è riuscita comunque, in collaborazione con l'organizzazione associata spagnola *Fundaciòn Via Libre*, a commentare almeno due dei più importanti documenti sui quali il WGIC ha lavorato: quello dedicato alla *cyber security* e al *cybercrime* e quello sui diritti

[100] Fonte IDC, azienda sussidiaria di IDG (*International Data Group*), *leader* nel campo della ricerca delle tecnologie di comunicazione.

della proprietà intellettuale. La *Free Software Foundation Europe* sta lavorando convintamente contro l'introduzione dei brevetti *software* in Europa adducendo la motivazione che i sostenitori dei brevetti sul *sofware* non fornirebbero alcuna ragione scientifica né alcun supporto empirico per giustificare gli appelli all'innovazione e alla competitività legati alla brevettabilità. Esisterebbero, al contrario, molte buone ragioni per opporvisi, riassumibili:

- nel pericolo di monopolizzare le idee astratte;
- nell'ostacolo all'innovazione, in quanto i brevetti possono essere rilasciati senza aver prodotto alcuna implementazione (codice sorgente) ed impedendo anche la ricerca;
- nell'ostacolo alla concorrenza di mercato, garantendo un potere squilibrato ai soggetti dominanti;
- nell'ostacolo alla rivelazione delle idee, che poi è la motivazione originaria per giustificare l'introduzione del sistema brevettuale;
- nella riduzione della competitività europea;
- nell'ostacolo all'interoperabilità, aumentando la dipendenza da un singolo fornitore;
- nella diffusione degli effetti negativi in molte altre aree dell'economia.

Per visionare i lavori del WGIG (Gruppo di lavoro del WSIS sulla *Internet governance*) si veda <http://www.wgig.org/working-papers.html>

Per informazioni sulle organizzazioni associate alla *Free Software Foundation* si vedano i siti:
<http://www.fsfeurope.org/projects/wsis/wsis.it.html>.
<http://www.fsfeurope.org/associates/associates.fr.html>.

IV. Tutela della *privacy* e sicurezza della rete[101]

1. Il quadro italiano e sovranazionale

Le moderne tecnologie possono costituire, attraverso il monitoraggio della vita sociale, una minaccia della riservatezza della vita privata degli individui. Gli strumenti che favoriscono tale monitoraggio sono molteplici (telecamere, documenti di identità elettronici, *card* magnetiche). Tra le possibilità offerte dalla navigazione in Internet si ricordano i *cookies*, i *log*, i *web bugs*, gli *spyware*, la c.d. *persistence* e gli *adware*. Si intende per *log* un *file* di testo dove è registrata e documentata l'attività delle applicazioni

[101] Il testo esplicativo di questo argomento è una sintesi dei capitoli I e IX della pubblicazione di G. PASCUZZI, *Il diritto dell'era digitale - Tecnologie informatiche e regole privatistiche*, Bologna, il Mulino, 2002 integrato dalla lettura della normativa comunitaria e nazionale di riferimento.

software che sono installate sul computer. In questo modo il gestore di un sito è in grado di conoscere il numero dei visitatori, la loro provenienza, il tempo speso e le pagine consultate. I *cookies* (biscottini) sono *file* molto piccoli che contengono informazioni di base sull'utente in relazione al *server*. Si tratta in genere di dati che riguardano il *login*, gli acquisti in linea, le eventuali registrazioni con i quali è possibile ricostruire un profilo dell'utente. I *web bugs*, o cimici *web*, sono etichette elettroniche che permettono ai siti *web* ed alle imprese pubblicitarie di seguire la navigazione dell'utente sulla rete. Nel caso degli *spyware* si tratta di codici che raccolgono dati e li inviano al produttore del *software* o a società di *telemarking*. Infine la *persistence* e gli *adware* sono rispettivamente una tecnologia con la quale si riducono le comunicazioni tra sito *web* e *browser* e che consente di archiviare le ricerche effettuate dall'utente, e programmi che si scaricano gratuitamente ma che impongono la visualizzazione di *banner* pubblicitari[102]. Per contrastare questo fenomeno di intrusione nella vita privata degli utenti sono state sviluppate tecnologie che permettono di ovviare in parte a tali inconvenienti. Si tratta delle cosiddette *privacy enhancing technologies* o PET da distinguere in:

- tecnologie che consentono di limitare la riconoscibilità del soggetto da parte di terzi, definite *subject-orientend PETs*;
- tecnologie che permettono la protezione dell'identità, definite *object-oriented PETs*;
- tecnologie che assicurano la protezione dei dati relativi alle transazioni, denominate *transaction-oriented PETs*;
- tecnologie che creano zone di interazione dove è possibile nascondere l'identità dei soggetti, definite *system-oriented PETs*.

Altre tecniche di difesa sono la crittografia e la steganografia. Nel primo caso la protezione è assicurata dalla cifratura dei messaggi, mentre la steganografia è in realtà non una tecnica, ma un insieme di tecniche con le quali due persone possono comunicare tra di loro senza che altri sappiamo dell'esistenza stessa della comunicazione[103].

L'avvento dell'era digitale ha comportato notevoli cambiamenti sul piano delle regole giuridiche che tutelano il diritto alla riservatezza. Anzitutto si è assistito ad una trasformazione ed un ampliamento di tale diritto di tutela, attuati con la transizione dal "diritto ad essere lasciati soli al diritto sul controllo sulle informazioni che riguardano l'individuo"; è poi

---

[102] G. PASCUZZI, op. cit.
[103] G. PASCUZZI, op. cit.

intervenuta una diversificazione delle ragioni della tutela e l'evidenziazione della inidoneità di un controllo territoriale per una realtà aterritoriale come quella di Internet. Si è infine utilizzato un approccio alternativo per disciplinare il trattamento dei dati personali, costituito dai codici di autoregolamentazione, dalla certificazione di qualità e dalla negoziazione diretta tra le parti.

La normativa sovranazionale è emanata sia in ambito UE sia presso il Consiglio d'Europa e l'OCSE. In riferimento al Consiglio d'Europa è senz'altro degna di menzione la Raccomandazione n. R. (99)5 per la tutela della *privacy* su Internet[104].

Tra gli atti normativi comunitari vanno invece ricordate le direttive[105] 95/46/CE del 24 ottobre 1995 e 97/66/CE del 15 dicembre 1997[106] con le quali si è intervenuti a tutela delle "persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" e "sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni".

Secondo quanto sottolineato da Pascuzzi nell'opera citata in nota, la convergenza tra le direttive sopra indicate sarebbe da ravvisare su tre punti: il primo riguarda la canonizzazione dei princìpi generali in ordine alle modalità di trattamento dei dati; il secondo è inerente al riconoscimento di posizioni tutelate in capo ai titolari dei dati ed il terzo è attinente alla disciplina specifica dei cosiddetti dati sensibili. Con riferimento al metodo è stato stabilito che i dati personali siano trattati in modo lecito e corretto, che vengano raccolti e registrati per finalità specifiche, legittime ed esplicite, che siano esatti, pertinenti e completi e non eccedenti rispetto agli scopi di utilizzo. Per quanto riguarda invece le posizioni tutelate di cui al secondo punto, il riferimento è al diritto di conoscenza, di accesso ai dati, di modifica ed aggiornamento di dati incompleti o superati, al diritto all'oblio (cancellazione delle informazioni quando non più necessarie) e a quello di opposizione al trattamento[107]. Per i dati particolarmente delicati (ultimo punto) è disposta, come già accennato, una disciplina particolare

---

[104] Tra le altre si ricorda: a) la Raccomandazione n. R. (2002)9 sulla protezione dei dati personali raccolti e trattati per scopi assicurativi, b) la Raccomandazione n. R. (99)14 sul servizio universale, relativa ai nuovi servizi di comunicazione ed informazione, c) la Raccomandazione n. R. (95)4, sulla protezione dei dati personali nel settore dei servizi di telecomunicazione, con particolare riguardo ai servizi telefonici.

[105] Per i testi degli atti normativi citati consultare <http://www.europa.eu.int/eur-lex/ >.

[106] Sostituita dalla direttiva 2002/58/CE del 12 luglio 2002.

[107] Articolo 13 della legge n. 675 del 1996. Per i testi delle direttive si consulti il sito <http://www.europa.eu.int/eur-lex/>.

per evitare possibili discriminazioni in base all'etnia, alle convinzioni religiose o filosofiche, alle opinioni politiche, sindacali od altro.

Tra gli atti normativi più recenti vanno menzionate la direttiva 2000/31/CE (*Direttiva sul commercio elettronico*) e la direttiva 2002/58/CE (*Direttiva relativa alla vita privata e alle comunicazioni elettroniche).* Quest'ultima fa parte del cosiddetto "Pacchetto Telecom" che, dal 24 aprile 2002, disciplina il settore delle comunicazioni elettroniche. Il "Pacchetto Telecom" comprende altre direttive concernenti il quadro generale, l'accesso e l'interconnessione, le autorizzazioni e le licenze, il servizio universale (2002/19/CE, 2002/20/CE e 2002/22/CE).

La direttiva 2002/58/CE è abrogativa della direttiva 97/66/CE del Parlamento europeo e del Consiglio del 15 dicembre 1997. Tratta di molteplici temi come la conservazione dei dati di collegamento da parte degli Stati membri per scopi di sorveglianza di polizia, la spedizione di messaggi elettronici indesiderati, i marcatori (*cookies*) e l'inclusione dei dati personali negli elenchi pubblici. Il fenomeno dell'invio di comunicazioni non richieste ad indirizzi di posta elettronica (cosiddetto *spam*) è stato costantemente all'attenzione dell'Autorità di garanzia sulla *privacy* anche in virtù del fatto che le comunicazioni non hanno solo contenuto commerciale ma anche politico (c.d. *marketing* politico). Nella Relazione che l'Autorità ha presentato per l'anno 2004 si evidenzia una accresciuta sensibilità degli utenti verso questo problema, desumibile "dall'intenso contenzioso e dalle azioni che sono state proposte dinanzi all'autorità giudiziaria ordinaria". Per arginare il fenomeno, il Garante ha partecipato ad alcuni incontri tenuti presso il Ministero delle comunicazioni, cui sono intervenuti operatori di telefonia fissa e mobile, e associazioni di fornitori dei servizi Internet e dei consumatori. In tali incontri si è dialogato circa la possibile stesura di un codice di autoregolamentazione da realizzare con la collaborazione di questa Autorità, che fornirà il proprio contributo tenendo però presente il valore cogente delle norme che saranno contenute nel codice di deontologia e di buona condotta per Internet. Proprio su questo tema gli organi di informazione hanno dato grande rilievo alla vicenda dell'indagine giudiziaria curata dalla Guardia di finanza nei confronti di una società quotata in Borsa che ha utilizzato migliaia di indirizzi *e-mail* per finalità di *marketing*, senza il consenso informato degli interessati. Sulla vicenda, per la quale due responsabili della società sono stati indagati per reati che vanno dall'illecito trattamento dei dati personali alla frode informatica ed all'accesso abusivo a sistemi informatici, il Garante ha ricevuto di recente

copia di alcuni atti e valuterà a breve l'eventuale adozione dei provvedimenti di competenza.

Non di rado viene rappresentata da parte di utenti dei servizi gratuiti di accesso ad Internet ed alla posta elettronica l'impossibilità di esprimere un consenso specifico e differenziato con riferimento alle diverse finalità del trattamento operato dai fornitori dei medesimi servizi. In particolare, è talvolta negata la stessa opportunità di usufruire dei predetti servizi nel caso in cui l'utente non presti il consenso al trattamento dei dati per finalità pubblicitarie e commerciali.

In occasione della trattazione di uno specifico ricorso (Provv. 12 ottobre 2004) il Garante ha chiarito che è improprio richiedere un ampio e generalizzato consenso - peraltro anche quando il Codice in materia di protezione dei dati personali[108] permette di prescindere dal medesimo consenso, come, ad esempio, per l'eventuale comunicazione dei dati all'autorità giudiziaria (cfr. art. 24, comma 1, lett. *a)*, del Codice) - associandovi finalità pubblicitarie e di profilazione per le quali non è lasciata all'utente alcuna libertà nella manifestazione di volontà. La mancata richiesta di consensi differenziati (e limitatamente ai casi in cui sono necessari) determina un quadro confuso che non permette all'utente di esprimere scelte libere, consapevoli e non contraddittorie fra loro. In questa prospettiva, l'Autorità ha riaffermato la necessità che il consenso sia realmente espresso senza condizionamenti che ne influenzino sotto vari profili la libera manifestazione (art. 23, comma 3, del Codice). Quanto all'eventuale trattamento dei dati dell'interessato per finalità di profilazione, è stato precisato che tale trattamento potrebbe risultare lecito in determinate circostanze qualora, per i rapporti contrattuali, la società preveda l'assegnazione di un accesso gratuito ad Internet dietro "corrispettivo" di una profilazione lecita, corretta e proporzionata dell'interessato medesimo"[109].

In concomitanza dell'affermarsi del commercio elettronico - nella seconda metà degli anni '90 - vi è stata una progressiva presa di coscienza della necessità di garantire sicurezza sulla rete e precisamente di garantire una diffusione controllata delle informazioni riguardanti la sfera privata. Ciò sarebbe dovuto avvenire soprattutto - come auspicato nella citata Raccomandazione n. R. 99(5) del Comitato dei Ministri agli Stati membri per la protezione della *privacy* su Internet - essenzialmente mediante l'adozione di codici di condotta o linee guida direttamente applicabili sia ai

[108] D. Lgs n. 196 del 2003 (compreso nella documentazione allegata).
[109] Relazione del Garante per la *privacy*, anno 2004 (estratto).

navigatori-utenti sia ai fornitori di servizi di accesso. In ciò è da ravvisare una novità significativa: l'appello non è infatti più diretto ai soggetti che tradizionalmente sono scelti come interlocutori, ovvero alle istituzioni nazionali, ma a coloro che sono direttamente interessati a vedere garantita una gestione corretta dei dati. Si ricorda in proposito che l'articolo 27 della direttiva 95/46/CE sulla *privacy* incoraggia l'elaborazione di codici di condotta da parte di professionisti.

In ambito normativo nazionale l'articolo 31 della legge 675 del 31 dicembre 1996, ora abrogata dal D.Lgs. 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), attribuiva al Garante della *privacy* il compito di stimolo all'elaborazione di codici deontologici di buona condotta in determinati settori, codici poi effettivamente scritti e contenuti del T.U. approvato nel 2003.

Se si osserva l'evoluzione storica di tali codici è evidente che, applicando la citata disposizione della legge sulla *privacy*, nonché le norme contenute nel D. Lgs. 30 luglio 1999, n. 281 (*Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica*) - in base alle quali il Garante ha promosso la redazione del Codice di deontologia e di buona condotta per il trattamento dei dati personali per scopi storici (provvedimento n. 8/P/2001 del 14 marzo 2001) - ed in riferimento a quella di cui all'articolo 20 del D. Lgs. 28 dicembre 2001, n. 467 (*Disposizioni correttive ed integrative della normativa in materia di protezione dei dati personali*) si è potuto assistere, dal 1996 al 2001, ad una progressiva accentuazione dell'influsso delle regole e dei princìpi comunitari su questi testi di autodisciplina[110].

Secondo la dottrina più recente si può parlare di codici di prima, seconda e terza generazione. Tra i codici di prima generazione merita di essere citato il codice deontologico dei giornalisti che costituisce in Italia fonte rilevante di bilanciamento e raccordo tra il diritto all'informazione e quello alla tutela della riservatezza. Di seconda generazione sono classificati il D. Lgs. 11 maggio 1999, n. 135 e il D. Lgs. 30 luglio 1999, n. 281 che hanno come caratteristica comune quella di aver delineato l'evoluzione della sfera di efficacia che non è più solo intercategoriale ma diviene ultracategoriale, ovvero fonte di diritto oggettivo. Ai codici di terza generazione appartiene il D.Lgs. 467/2001 che amplia ulteriormente l'efficacia e la rilevanza delle norme precedenti. Il decreto prevede che nella stesura dei codici si tenga conto sia degli atti comunitari

---

[110] G. SANTANIELLO, *I codici di deontologia nel trattamento dei dati personali* in «Interlex, diritto tecnologia informazione», rivista *on line*, consultabile sul sito <http://www.interlex.it/675/santaniello3.htm>.

(specificamente delle Raccomandazioni del Consiglio d'Europa, citate nella legge delega n. 676 del 31 dicembre 1996), sia dei poteri propulsivi e di indirizzo del Garante, sia delle regole di autodisciplina elaborate dai soggetti interessati, realizzando così il policentrismo delle fonti di sistemi giuridici avanzati, ordinati su più livelli (c.d. "ordinamenti binari")[111].

L'entrata in vigore del già menzionato "Codice in materia di protezione dei dati personali"(D. Lgs. 30 giugno 2003, n. 196, di seguito, semplicemente, "Codice"), avvenuta il 1° gennaio 2004, ha rappresentato una tappa fondamentale per la tutela dei diritti della persona ed ha concluso il processo di recepimento delle direttive europee in materia (95/46/CE e 2002/58/CE). E' stata così attuata la razionalizzazione della disciplina inizialmente introdotta con la legge 31 dicembre 1996, n. 675, riunendo in un unico testo una normativa che si era, nel tempo, stratificata a seguito di numerosi interventi modificativi ed integrativi. Già nel primo anno di vigenza del Codice, infatti, sono stati introdotti alcuni, seppur circoscritti, interventi modificativi in settori di rilievo, e segnatamente in relazione al regime dei dati relativi al traffico telefonico, nel contesto sanitario e con riferimento alle ripetute proroghe dei termini per adottare le misure minime di sicurezza e i regolamenti sul trattamento dei dati sensibili da parte dei soggetti pubblici.

Si rammenta che, con Regolamento n. 460/2004, in data 10 marzo 2004, il Parlamento ed il Consiglio hanno approvato l'istituzione dell'Agenzia europea per la sicurezza delle reti e dell'informazione. L'istituto ha il compito di assistere e fornire consulenza alla Commissione ed agli Stati membri su tutte le questioni connesse con la sicurezza delle reti e dell'informazione offrendo, in particolare, collaborazione nei lavori tecnici preparatori di aggiornamento e di sviluppo della normativa comunitaria. L'Agenzia è inoltre chiamata a favorire la cooperazione tra gli Stati ed a promuovere attività di valutazione dei rischi. Organi dell'Agenzia sono il consiglio di amministrazione, il direttore esecutivo ed il gruppo permanente di parti interessate. Quest'ultimo è composto da esperti rappresentanti dell'industria delle tecnologie dell'informazione e della comunicazione, delle organizzazioni dei consumatori e da esperti universitari in materia di sicurezza delle reti e dell'informazione.

Oltre che sui codici deontologici l'incremento della fiducia dei consumatori - come già accennato - si stimola anche attraverso la realizzazione di marchi di tutela e con la contrattazione diretta tra le parti. Riguardo al primo aspetto sappiamo che numerose aziende dell'industria *on*

---

[111] G. SANTANIELLO, op. cit.

line hanno puntato sui *privacy seals*, ovvero sui marchi che nascono nell'ambito di specifiche iniziative gestite da organizzazioni indipendenti. I *privacy sel programs* certificano con specifici marchi distintivi la sicurezza di un determinato sito riguardo alla *privacy*. Tra i principali programmi - che prevedono anche meccanismi semplificati per la risoluzione dei conflitti - si ricordano TRUST, BBB *On line* e CPA *Webtrust.* Vi è poi - come già detto - la disciplina che discende dal contratto tra le parti che si stipula al momento del loro incontro sulla rete[112].

Si rammenta infine che l'OCSE ha elaborato delle linee guida[113] in materia di sicurezza dei sistemi e delle reti di informazione il cui scopo è quello di promuovere una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti d'informazione. Nel documento sono indicati nove princìpi tra di loro complementari rivolti a tutte le parti interessate, sia in ambito politico che operativo. Si tratta dei princìpi della sensibilizzazione (consapevolezza della necessità di tutelare la sicurezza dei sistemi e delle reti d'informazione), della responsabilità, della risposta (necessità di operare con tempestività per prevenire incidenti di sicurezza), dell'etica, della democrazia, della valutazione dei rischi, della concessione e applicazione della sicurezza, della gestione della sicurezza e della rivalutazione.

2. Lo stato di recepimento delle direttive comunitarie negli Stati membri dell'Unione europea[114]

Il 2004 è stato l'anno dell'allargamento dell'Unione europea con l'ingresso di dieci nuovi Stati (Cipro, Estonia, Lettonia, Lituania, Malta, Polonia, Repubblica Ceca, Slovenia, Slovacchia, Ungheria).

Nei nuovi Stati membri, **le disposizioni delle direttive europee in materia di protezione dei dati (95/46/CE) e comunicazioni elettroniche e vita privata** (2002/58/CE) trovano applicazione integrale a partire dalla data di adesione all'Unione europea, ossia dal 1° maggio 2004. Guardando più in dettaglio alla situazione esistente al 31 dicembre 2004 nei venticinque Paesi dell'UE, lo stato di recepimento nella legislazione nazionale rende opportune alcune precisazioni. Tutti i quindici Paesi dell'Unione europea avevano recepito la direttiva prima del 1° maggio

---

[112] G. PASCUZZI, op. cit. Per i testi degli atti normativi comunitari citati si consulti il sito <http://www.europa.eu.int/eur-lex/>.

[113] Il testo delle Linee guida è compreso nella documentazione allegata.

[114] Garante della *privacy*, op.cit. (Estratto in parte sintetizzato).
Per i testi degli atti normativi citati si consulti <http://www.europa.eu.int/eur-lex/>.

2004, anche se la Francia aveva notificato la legislazione adottata nel 1978, perdurando l'*iter* parlamentare (iniziato nel 2001) per l'adozione della normativa specifica. La nuova legge francese "*Informatique et libertés*", di recepimento della direttiva 95/46/CE, è stata poi adottata il 6 agosto 2004 ed è entrata in vigore il giorno successivo. Rispetto alla precedente legge, il nuovo testo aumenta i poteri sanzionatori dell'autorità di protezione dei dati, la *Commission Nationale de l'Informatique et des Libertés* (CNIL); elimina l'obbligo di notificazione alla CNIL per i titolari che designano (su base facoltativa) un "referente per la protezione dei dati" (il cosiddetto "*correspondant à la protection des données*"). Questi è incaricato di vigilare sull'applicazione della normativa da parte del titolare e di monitorare la liceità e le modalità dei trattamenti di dati personali effettuati da quest'ultimo (ai sensi dell'art. 18 c.2 della direttiva); la legge infine, dispone l'obbligo di sottoporre a valutazione preliminare da parte della CNIL qualsiasi trattamento che comporti il ricorso a tecniche biometriche ed inasprisce anche le sanzioni previste in caso di inadempimento. Il nuovo quadro normativo sarà completato attraverso l'adozione di atti di legislazione secondaria che preciseranno le procedure di valutazione preliminare ed altri aspetti concernenti, ad esempio, i requisiti da soddisfare per svolgere la funzione di "referente per la protezione dei dati". La valutazione della qualità del recepimento per i quindici Paesi membri è in corso da parte della Commissione, secondo un programma di lavoro fissato nel Primo rapporto sull'applicazione della direttiva.

I nuovi Stati membri sono tutti provvisti di una legge nazionale in materia di protezione dei dati, che in alcuni casi è stata adottata *ex novo*, mentre in altri ha subìto vari emendamenti dopo l'adozione della direttiva 95/46/CE, in particolare al fine di istituire un'autorità per la protezione dei dati incaricata di vigilare sull'applicazione delle disposizioni a livello nazionale. Va sottolineato che dal 2001 alcuni dei nuovi Stati membri (Estonia, Lettonia, Lituania, Polonia, Repubblica Ceca, Repubblica Slovacca e Ungheria) hanno stabilito forme più strette di collaborazione e scambio di informazioni, anche attraverso un apposito sito *web* (*www.ceecprivacy.org*) e l'organizzazione di due conferenze semestrali per discutere di tematiche di interesse comune. La Commissione sta valutando l'effettiva conformità delle disposizioni nazionali con l'*acquis* comunitario.

La situazione relativa al recepimento della direttiva sulla vita privata e le comunicazioni elettroniche è più articolata. Nella Relazione 2003 si è fatto cenno alle iniziative preliminari adottate dalla Commissione europea nei confronti di alcuni Stati, per omessa comunicazione delle misure nazionali di trasposizione, ovvero per l'incompleta trasposizione della direttiva (con particolare riguardo all'art. 13, relativo alle comunicazioni

indesiderate). Dopo il parere motivato emesso il 1° aprile 2004 nei confronti di Belgio, Finlandia, Francia, Germania, Grecia, Lussemburgo e Paesi Bassi, e dopo l'adesione dei nuovi Stati membri, alla fine del mese di giugno 2004 la Commissione ha deciso di adire la Corte di giustizia nei confronti di tre Paesi (Belgio, Grecia, Lussemburgo) per la mancata adozione della legislazione primaria di recepimento. Gli altri Paesi (Finlandia, Francia, Germania e Paesi Bassi) hanno provveduto nel frattempo a notificare le misure nazionali adottate. Tuttavia la Commissione ha segnalato anche ad altri Paesi l'imperfetta trasposizione delle norme della direttiva 2002/58/CE.

Ciò riguarda, in particolare:

- il recepimento delle disposizioni dell'art. 13, che vieta le comunicazioni indesiderate (quindi anche lo *spam*) in assenza del consenso preventivo dell'abbonato *(opt-in)*. Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato le misure nazionali adottate;

- il recepimento degli articoli 5, 6 e 9 che riguardano, rispettivamente, i dati di traffico e di ubicazione e le relative modalità di trattamento e conservazione. Belgio, Repubblica Ceca, Estonia, Grecia e Lussemburgo non hanno notificato alla Commissione le misure adottate in materia.

Anche riguardo alla direttiva 2002/58/CE, la Commissione sta valutando la piena conformità della legislazione nazionale in vigore nei Paesi dell'Unione europea.

3. Le iniziative delle istituzioni europee per una migliore applicazione delle direttive comunitarie [115]

Sia il Primo Rapporto della Commissione europea sullo stato di attuazione della direttiva 95/46/CE (pubblicato il 15 maggio 2003), sia i risultati dell'Eurobarometro, pubblicati nel febbraio 2004, evidenziano una realtà caratterizzata da luci ed ombre riguardo all'effettiva trasposizione dei princìpi comunitari ed alla percezione dell'efficacia di tali princìpi da parte di imprese e cittadini europei. Nel rapporto della Commissione viene delineato un programma di lavoro articolato in dieci punti per giungere ad una migliore applicazione della direttiva tra i Paesi dell'Unione. Su molti di

[115] Garante della *privacy*, op. cit. (estratto in parte sintetizzato). Per i testi degli atti normativi citati si consulti <http://www.europa.eu.int/eur-lex/>.

essi la Commissione ha previsto e richiesto iniziative comuni da parte delle autorità di protezione dei dati, le quali hanno quindi deciso di integrare, a partire dal 2004, le azioni richieste anche nel loro programma di lavoro. Del resto, le stesse autorità avevano da tempo indicato fra le priorità del proprio mandato il potenziamento dell'attuazione delle norme in materia di protezione dei dati attraverso numerose strategie. Queste ultime sono state sistematizzate in un documento che il **Gruppo dei Garanti europei,** istituito dall'art. 29 della direttiva 95/46/CE (di seguito, semplicemente, "Gruppo art. 29"), ha adottato nel settembre 2004 allo scopo di indicare alcune linee comuni di attività.

Per quanto concerne, in particolare, il potenziamento dell'attuazione dei princìpi comunitari in materia di protezione dei dati, le autorità garanti dei vari paesi hanno posto l'accento soprattutto:

- sulle strategie per migliorare il rispetto e l'applicazione pratica delle normative nazionali, che contemplano l'elaborazione di approcci comuni comprendenti anche indagini ed accertamenti ispettivi "sincronizzati" in alcuni settori che risultano essere particolarmente problematici nella maggioranza dei venticinque Paesi Ue (si veda, in proposito, la "*Declaration on Enforcement*" approvata dal Gruppo il 25 novembre 2004);

- sulla semplificazione degli adempimenti connessi alla notificazione dei trattamenti, attraverso la creazione di una *task force* incaricata di individuare gli spazi di armonizzazione (soprattutto in tema di deroghe all'obbligo di notificazione) e di elaborare un possibile modello di notificazione "unica" per i soggetti stabiliti in più Stati membri dell'Unione europea. Sulla base delle risposte pervenute ad uno specifico questionario, la *task force* ha inoltre operato una ricognizione delle disposizioni e prassi vigenti in ciascun paese riguardo all'obbligo di notificazione dei trattamenti di dati personali; ha curato altresì la predisposizione di un *vademecum* da mettere a disposizione di tutti i soggetti interessati (principalmente le società private che intendono operare in più di un Paese dell'Unione) mediante la pubblicazione sul sito *web* della Commissione specificamente dedicato alla protezione dei dati ed all'attività del Gruppo art. 29;

- sull'armonizzazione delle previsioni in materia di informativa, in particolare attraverso l'elaborazione di un modello redatto in termini chiaramente comprensibili ed utilizzabili da tutti i titolari di trattamento, secondo un approccio "multilivello". Il Gruppo, anche sulla scorta della

risoluzione adottata in materia dalla Conferenza internazionale tenutasi a Sydney nel 2003 (v. Relazione 2003, p. 116) e del dibattito svolto a Wroclaw, durante la Conferenza internazionale del 2004 (v. *infra*), ha elaborato un parere, pubblicato il 25 novembre 2004, che individua le caratteristiche di tale "informativa-modello". Le decisioni assunte dal Gruppo, volte a favorire ed incrementare le forme di cooperazione al fine di pervenire a soluzioni interpretative uniformi, sono in linea di continuità rispetto a scelte compiute da diversi anni. La collaborazione internazionale fra le autorità di protezione dei dati (compreso il Garante), prevista anche dalla Convenzione n. 108 del Consiglio d'Europa, è operativa da molto tempo ed ha sistemi di scambi di informazioni sia a livello bilaterale, sia a livello multilaterale. Oltre agli ambiti istituzionalizzati attraverso la creazione del Gruppo art. 29 ed alle Conferenze delle autorità di protezione dei dati, si segnalano brevemente alcuni significativi esempi di tale collaborazione, rimandando ai paragrafi successivi per maggiori dettagli sull'attività svolta;

- sulla trattazione di segnalazioni e ricorsi che hanno carattere transnazionale e lo scambio di informazioni e buona prassi che sono oggetto dei seminari organizzati fin dal 2000 con cadenza semestrale nel quadro della cosiddetta *Complaints Handling Network*;

- sulle questioni attinenti al settore delle telecomunicazioni che sono oggetto dell'analisi condotta dall'*International Working Group on Data Protection inTelecommunications*, che si riunisce con cadenza semestrale;

- sulla lotta allo *spam* che è oggetto della specifica cooperazione prevista dalla rete istituita fra le autorità competenti in materia di *spam* (*Contact Network of Spam Authorities*, CNSA - che inizia la sua attività alla fine del 2003).

Gli aspetti della direttiva 95/46/CE che presentano maggiori difficoltà nell'armonizzazione delle modalità applicative riguardano innanzi tutto la conservazione dei dati di traffico (art. 6) ed il principio del consenso preventivo per l'invio di comunicazioni non sollecitate (art. 13).

Sul primo aspetto il Gruppo art. 29 è intervenuto per ricordare agli Stati la necessità del rispetto dei tempi e dei modi previsti dalla direttiva. Nel parere 1/2003, adottato il 29 gennaio 2003, i Garanti hanno precisato che i dati memorizzati ai fini della fatturazione e dei pagamenti di interconnessione possono essere conservati soltanto per un periodo di

tempo limitato e non su base routinaria per lunghi periodi, come peraltro già indicato nella Raccomandazione n. 3/99 del Gruppo. Il Gruppo art. 29, sulla scorta dell'applicazione del principio di proporzionalità e tenendo conto che, conformemente all'art. 6, par. 2, della direttiva 2002/58/CE, i dati relativi al traffico possono essere sottoposti a trattamento "sino alla fine del periodo durante il quale può essere legalmente contestata la fattura o preteso il pagamento", ha ritenuto che i dati dovrebbero essere conservati solo per il periodo necessario a consentire il pagamento delle fatture e la composizione delle controversie. Normalmente ciò implica un periodo di memorizzazione massimo di 3-6 mesi - e non più lungo - nei casi in cui le fatture sono state pagate e non sembrano essere state oggetto di contestazione o di richieste di delucidazioni (tenuto conto del diritto alla tutela della vita privata dei singoli abbonati).

Pertanto, considerato che i diversi sistemi giuridici degli Stati membri contemplano varie disposizioni in merito all'estensione del periodo durante il quale possono essere avviate iniziative nell'ambito del diritto contrattuale, i Garanti hanno ritenuto che tali disposizioni debbano essere applicate in conformità al principio per cui il trattamento dei dati personali deve essere limitato a quanto è strettamente necessario per conseguire i fini per i quali i dati sono stati rilevati e successivamente trattati, considerato inoltre che, di regola, il pagamento dei servizi resi effettuato entro i termini di conservazione. Il secondo importante aspetto, cui si è già accennato, concerne l'applicazione uniforme del principio dell'*opt-in* per le comunicazioni commerciali. La direttiva 2002/58/CE sulla vita privata e le comunicazioni elettroniche ha disciplinato in particolare, armonizzandole, le condizioni alle quali le comunicazioni elettroniche (ad esempio la posta elettronica, gli *sms*, il fax, il telefono) possono essere utilizzate a fini di commercializzazione diretta. A partire dalle legislazioni introdotte in alcuni Stati (tra cui l'Italia) che prevedevano in materia la necessità di un consenso esplicito dell'interessato, l'art. 13 della direttiva ha introdotto un regime generale basato sul consenso preventivo ai fini dell'invio di questo tipo di comunicazioni. La novità e la complessità del principio hanno indotto sia le istituzioni comunitarie, sia il Gruppo art. 29, ad intervenire per evitare divergenze applicative nei diversi Stati membri. L'urgenza di un tale intervento risiede nell'enorme recente sviluppo dell'invio di comunicazioni indesiderate (cd. *spam*) e la necessità di presentarsi nella lotta a questo fenomeno, che si manifesta ormai in tutto il mondo, con un quadro giuridico realmente armonizzato a livello europeo. Da qui: i richiami del Consiglio ad una puntuale applicazione della direttiva, le linee d'azione disegnate dalla Commissione nella sua comunicazione del 22 gennaio 2004 e la definizione di elementi per una cooperazione tra le

autorità nazionali incaricate dell'attuazione dell'art. 13 (per l'Italia, il Garante) attraverso la rete *spam* CNSA, cui si è fatto riferimento, e l'adozione di regole comuni per la trattazione di casi di *spam* transfrontaliero. Il Consiglio dell'Unione, proprio in considerazione del grande impegno da assumere per contrastare lo *spam,* ha adottato nel mese di novembre alcune conclusioni che impegnano gli Stati ad un recepimento puntuale della direttiva 2002/58/CE ed in particolare del suo art. 13; ha richiesto poi alla Commissione di valutare se alcune disposizioni nazionali introdotte in attuazione della direttiva possano ritenersi confliggenti con l'applicazione armonizzata del principio del consenso preliminare (*opt-in*) da parte del destinatario e pertanto incidere sull'efficacia delle misure di contrasto allo *spam* transfrontaliero. Analoga attenzione è stata posta all'intensificazione della collaborazione internazionale - in particolare, come ricordato, in sede OCSE ed *International Communication Union* (ITU) - finalizzata alla presentazione, attraverso la Commissione europea, di una posizione unitaria dei Paesi dell'Unione. Infatti, in altri Paesi la legislazione vigente si fonda sul diverso principio del cd. *opt-out* (la possibilità, cioè, per il destinatario di chiedere di non ricevere le comunicazioni commerciali) e pertanto quello che nell'Unione europea dall'entrata in vigore della direttiva 2002/58/CE (e nei singoli Paesi dalla data di trasposizione) è assoggettato a sanzione, in altri paesi può non costituire un comportamento vietato. In tale contesto, il contributo del Gruppo art. 29 assume una notevole rilevanza. In particolare, il parere n. 5/2004 del 27 febbraio 2004 offre indicazioni su specifici elementi che riguardano le nozioni di "posta elettronica", "previo consenso" da parte degli abbonati e "commercializzazione diretta"; si prendono altresì in considerazione l'eccezione alla norma del previo consenso ed il regime per le comunicazioni indirizzate alle persone giuridiche. Tra le attività svolte a livello europeo[116] si segnala la **Conferenza di primavera dei Garanti europei** che si è svolta a Rotterdam dal 21 al 23 aprile 2004 ed è stata dedicata alle politiche finalizzate a garantire l'efficacia della protezione dei dati. I temi centrali dell'incontro sono stati il ruolo e l'azione di intervento delle autorità, le comunicazioni elettroniche, il rispetto delle norme sulla protezione dei dati personali e la cooperazione giudiziaria a livello europeo. Il segretario generale dell'Autorità ha affrontato il tema delle strategie da mettere in atto per garantire l'effettiva attuazione delle norme in materia di *privacy*, non solo attraverso verifiche e controlli, ma anche mediante una costante azione di sensibilizzazione. Per quanto riguarda in particolare l'attività di verifica, soprattutto alla luce della direttiva 95/46/CE, si è altresì evidenziata l'opportunità di potenziare la collaborazione fra le

[116] Garante della *privacy*, op.cit.

autorità nazionali della protezione dei dati, anche in considerazione del carattere transnazionale delle problematiche che investono il settore della *privacy* (esempio tipico lo *spam*).

V. Il *digital divide*[117]

Il *digital divide* (letteralmente divario digitale) è definibile, sinteticamente, come la distanza tra chi è in grado (o ha la possibilità) di usare i nuovi strumenti informatici e di comunicazione e chi invece non lo è. Ciò crea una frattura di sviluppo principalmente tra aree ricche e povere del mondo, ma anche all'interno di una medesima realtà geografica. Certamente non sarebbe corretto individuare in questo fenomeno la sola o la principale causa del ritardo dello sviluppo ma è indiscutibile che l'accesso alle tecnologie dell'informazione costituisce un'opportunità notevole per la crescita socio-economica di un paese. Negli ultimi anni molte agenzie internazionali ed organizzazioni non governative hanno cominciato a discutere del problema ed a prospettare possibili soluzioni. Ripercorrendo le principali tappe cronologiche degli eventi più significativi sono da segnalare in ambito internazionale: il *summit* G8 di Okinawa, del luglio 2000, durante il quale è stata creata la *Digital Opportunity Task Force* con la finalità di analizzare e descrivere le linee di intervento sul *digital divide*; la creazione della ICT *Task Force* in ambito ONU nel marzo 2001; l'approvazione - durante il G8 di Genova, nel 2001 - del *Genoa Action Plan* con il quale si chiariscono le linee di intervento mondiali sulla questione; la definizione degli obiettivi per lo sviluppo della società dell'informazione avvenuta durante il primo *summit* mondiale del WSIS[118] tenuto a Ginevra nel 2003.

1. Il quadro europeo ed internazionale

Secondo i dati conclusivi di un'indagine condotta dalla Commissione europea e riferiti all'anno 2001, in media il 55% dei servizi pubblici di base dei paesi membri è ormai accessibile in linea. Inoltre la maggior parte dei siti *web* esaminati fornisce un'interattività superiore al semplice scaricamento dei programmi. I servizi amministrativi in linea aumentano più rapidamente per le imprese (68%) rispetto a quanto non lo siano per i

---

[117] Per approfondimenti si veda T. PUCCI, *Il diritto all'accesso nella società dell'informazione e della conoscenza. Il* digital divide, in «Informatica e diritto», marzo 2005, pagg. 119-153.

[118] Per i lavori preparatori del *summit* si visiti il sito <http://www.itu.int/wsis/>.

cittadini (47%). Primi fra tutti quelli che consentono pagamenti al settore pubblico (il tasso maggiore - pari all'88% - rappresentato da dichiarazioni IVA)[119]. La medesima realtà è fotografata dal Rapporto annuale[120] dell'Istat, anno 2003, secondo il quale Internet è la rete di comunicazione elettronica più diffusa tra le imprese europee medio-grandi (con accesso al *web* in più del 90 per cento dei casi). Più contenuta è la percentuale di diffusione nelle piccole imprese, che risulta comunque in crescita rispetto all'anno 2002. Sono ancora poco utilizzate le reti Intranet che raggiungono un valore percentuale superiore al 40 per cento solo in Lussemburgo. Per quanto riguarda la diffusione nei nuclei domestici la Commissione rende noto che, a metà del 2002, il 40% di essi aveva accesso ad Internet. In valore assoluto è stato rilevato che gli utenti europei della rete sono circa 150 milioni, cifra pari a quella degli Stati Uniti. Si consideri che in tutto il mondo il numero di utenti è pari a 404 milioni, cifra suscettibile di aumento sino a 550 milioni nel 2005[121]. Per quanto riguarda la diffusione della larga banda i dati riportati dal Ministro per l'innovazione e le tecnologie evidenziano che, durante il primo trimestre 2004, le nuove sottoscrizioni sono state, nel mondo, pari a 9,5 milioni. Prima fra tutti è la Cina con circa 14 milioni di linee DSL, seguita da Giappone e Stati Uniti (11 e 10 milioni rispettivamente). L'Italia compare al settimo posto con circa 3 milioni di linee. Considerando le utenze telefoniche totali, la Corea del Sud - che si attesta in quarta posizione nella classifica degli abbonati - è invece prima nella diffusione della DSL.

---

[119] Commissione europea, *Verso un'Europa basata sulla conoscenza. L'Unione europea e la società dell'informazione*, Ufficio delle pubblicazioni ufficiali delle Comunità europee, Bruxelles 2003.

[120] Il testo del Rapporto è compreso nella documentazione allegata.

[121] *Idem.*

CLASSIFICA MONDIALE LINEE DSL (Q1 2004) MLN DI LINEE	
Cina	13,995
Giappone	11,196
Stati Uniti	10,584
Corea del Sud	6,580
Germania	4,840
Francia	4,116
Italia	2,875
Taiwan	2,590
Canada	2,340
Regno Unito	2,272

fonte: DSL Forum/Point Topic

DIFFUSIONE DSL / 100 LINEE TELEFONICHE (%) (Q1 2004)	
Corea del Sud	28,3
Taiwan	19,8
Belgio	16,7
Hong Kong	16,1
Giappone	15,7
Israele	14,5
Danimarca	14,2
Finlandia	13,6
Singapore	13,4
Francia	12,1

fonte: DSL Forum/Point Topic

Sulla diffusione di Internet nel mondo sono proposte - poiché giudicate molto accurate - le analisi di dati di fonte *Network Wizards* rielaborati dalla società di ricerca italiana "Gandalf"[122]. Secondo i dati di questo studio - ampiamente stralciato, in parte sintetizzato e riportato di seguito - la crescita del numero di *host* Internet dal 1981 al 2004 è la seguente:

1981 – 213
1982 – 235
1983 – 562

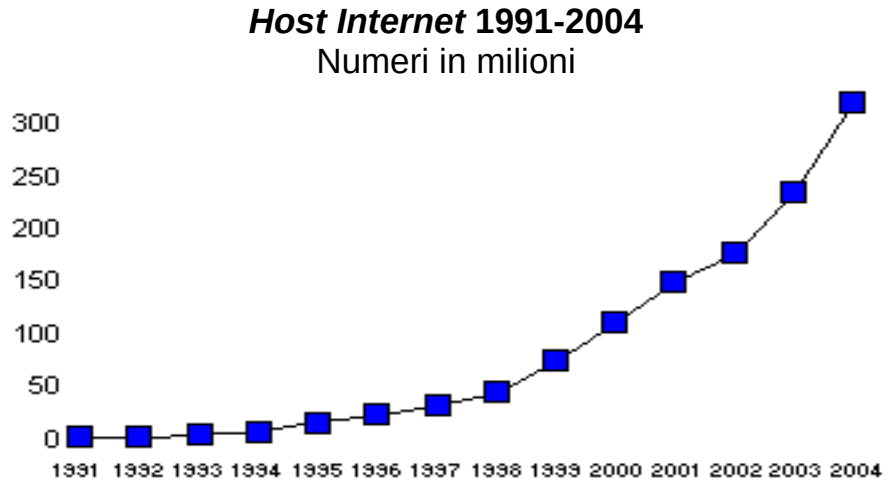
[122] Si veda il sito <http://www.gandalf.it/dati/>. (Lo studio illustra i criteri seguiti per la raccolta e l'elaborazione dei dati, di cui si offre una sintesi:

I dati di *hostcount* su scala mondiale pubblicati nell'appendice 1 di *La coltivazione dell'internet* e *on line* nella rubrica *Il mercante in rete* sono basati sulle statistiche pubblicate da *Network Wizards*. L'ultimo aggiornamento di quella serie è stato pubblicato nel marzo 2005 (i dati sono aggiornati al dicembre 2004). In passato erano state usate, per verifica, anche altre fonti. Ma non sono più disponibili – oppure sono diventate così sporadiche e imprecise da non offrire aggiornamenti attendibili. Comunque la fonte qui usata è l'unica disponibile che permette un confronto storico coerente dal 1981 al 2004. Per *hostcount* si intende un calcolo del numero di *host* Internet, cio di "indirizzi IP" permanenti e attivi, cioè di nodi connessi alla rete, suddivisi per paese. Non c'è una correlazione diretta fra il numero di *host* e il numero di persone collegate alla rete in ciascun paese; il dato di *hostcount* è un indice rilevante del livello di attività nell'uso di Internet. Naturalmente l'appartenenza al paese dipende da dove è registrata la proprietà del *domain* e non dalla collocazione fisica del *server*. Alcuni operatori, anche in Italia, usano *domain* "americani" (classificati come ".com" o ".org" o ".net") ma questo fenomeno non ha dimensioni tali da modificare in modo rilevante il significato dei dati e i termini di confronto fra i diversi paesi. Tuttavia nell'analisi dei dati sono stati introdotti alcuni correttivi per neutralizzare l'effetto di questo fattore).

1984 – 1.204
1985 – 1.961
1986 – 5.089
1987 – 28.174
1988 – 80.000
1989 – 130.000
1990 – 376.000
1991 – 727.000
1992 – 1.313.000
1993 – 2.217.000
1994 – 5.846.000
1995 – 14.352.000
1996 – 21.819.000
1997 – 29.760.000
1998 – 43.230.000
1999 – 72.398.000
2000 – 109.574.000
2001 – 147.345.000
2002 – 171.638.000
2003 – 233.101.000
2004 – 317.646.000

Nota: Le discontinuità nella serie numerica sono dovute ai cambiamenti di metodo avvenuti nel 1987 e nel 1997.

L'andamento negli ultimi 14 anni è riassunto nel grafico seguente



Lo studio[123] di *Network Wizards* evidenzia che:

[123] L'elaborato derivante da una sintesi di estratti degli studi citati in nota è evidenziato in carattere più piccolo.

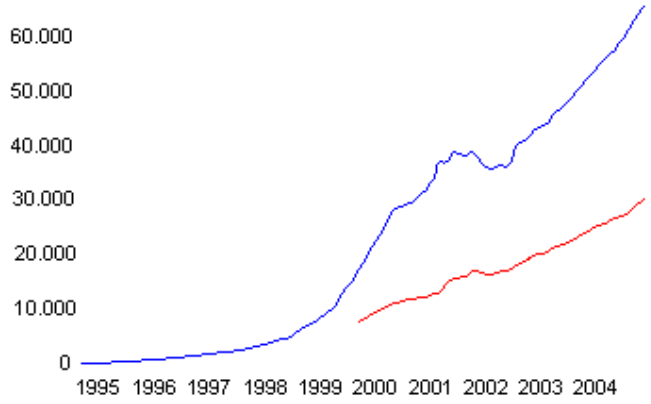
"in vari periodi ci sono stati tentativi di individuare un'immaginaria «crescita esponenziale» oppure una tendenza che somigliasse a una «curva logica» o «gaussiana», ma non c'è mai stato un andamento che confermasse quelle ipotesi. Da cinque o sei anni la crescita si sviluppa su un percorso quasi «lineare» – con un'accelerazione nel 2003-2004 di cui non è ancora possibile valutare la portata. I fatti confermano che questa evoluzione, influenzata da una varietà di fattori, non permette di tracciare proiezioni coerenti".

Ancora si afferma che, pur essendo la crescita continua, essa è il risultato di molte diverse tendenze. Da ciò la difficoltà di definire una linea coerente di sviluppo. In ogni caso si riscontra una crescita veloce con una dimensione complessiva delle attività nell'Internet decuplicata in sette anni e più che raddoppiata negli ultimi tre.

Da uno studio pubblicato da Netcraft si rileva che, nei primi mesi del 2005, si sono registrati quasi 65 milioni di siti *web*, con un veloce aumento rispetto ai periodi precedenti. Di questi circa 30 milioni sono quelli che risultano avere un'attività rilevante, come si vede nel grafico di seguito riportato.

Siti *web* nel mondo – 1995-2005

numeri in migliaia



(La linea rossa indica i siti che risultano "attivi")

Lo studio evidenzia inoltre che attualmente, dopo una fase di cedimento fra il 2001 e il 2003, è in atto una vigorosa crescita, certamente più dimensionata se si contano i soli siti "attivi". Da altre fonti, come, ad esempio, l'*Online Computer Library Center*, risulta che circa il 40 per cento delle presenze *web* è rappresentato da siti provvisori, incompleti o privi di contenuti (semplici "occupazioni di posizione"). Fra quelli attivi, due terzi sono siti pubblicamente aperti e accessibili a tutti, mentre un terzo ha qualche (totale o parziale) limitazione di accesso.

Per quanto riguarda il numero di persone che usano Internet - si prosegue nel *dossier* - i dati sono incerti, contradddittori e imprecisi – specialmente quando si tratta di fare confronti internazionali.

Nella tabella seguente è riassunto l'andamento di crescita dal 1994 al 2004.

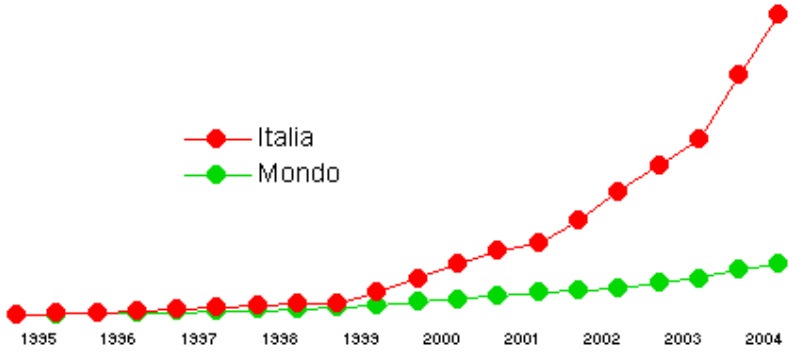
	Numero di *host*	**% di crescita**	
		semestrale	**annuale**
Dicembre 1994 *	5.846.000	51,1	118,9
Giugno 1995 *	8.200.000	40,3	106,8
Dicembre 1995 *	12.881.000	57,1	120,3
Giugno 1996 *	16.729.000	30,5	104,0
Dicembre 1996 *	21.819.000	30,4	52,0
Giugno 1997 *	26.053.000	19,4	55,7
Dicembre 1997	29.670.000	13,9	36,0
Giugno 1998	36.739.000	23,8	41,0
Dicembre 1998	43.230.000	17,7	45,7
Giugno 1999	56.218.000	30,0	53,0
Dicembre 1999	72.398.000	28,8	67,5
Giugno 2000	93.047.800	28,5	65,5
Dicembre 2000	109.574.400	17,8	51,4
Giugno 2001	125.888.200	14,9	35,3
Dicembre 2001	147.344.700	17,0	34,5
Giugno 2002	162.128.500	10,0	28,8
Dicembre 2002	171.638.300	5,9	16,5
Dicembre 2003	233.101.500	n.a.	35,8
Giugno 2004	285.139.100	22,3	n.a.
Dicembre 2004	317.646.000	11,4	36,3

* Il metodo di analisi cambiato a partire dal dicembre 1997.
I dati per gli anni 1994-1997 sono "ponderati"
per adeguare la vecchia metodologia alla nuova.
Le percentuali del 1994 riferite al 1993 sono basate sulla "vecchia" serie di dati.
La crescita nel dicembre 1993 rispetto a un anno prima era del 138 %
e negli anni precedenti le percentuali erano ancora più alte.
Dal 1987 al 2004 i dati di *hostcount* internazionali sono stati diffusi ogni sei mesi,
ma per il 2003 solo una volta, alla fine dell'anno.

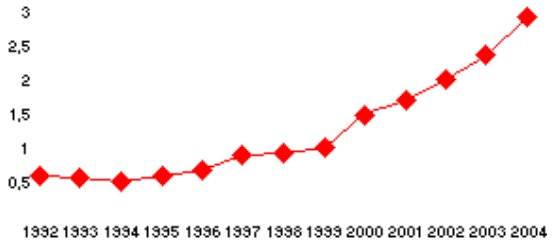
Come è prevedibile con l'aumentare delle quantità di *host*, le percentuali di crescita risultano progressivamente diminuite fino al 1997. Dal 1999 sembra essersi innescata una fase più veloce, seguita da un (relativo) rallentamento nel 2001-2002. Ma nel 2003 e nel 2004 si riscontra di nuovo uno sviluppo più forte.

Per quanto riguarda l'Italia lo studio segnala l'opportunità di usare cautela nella valutazione dei dati di crescita nel 2002-2004[124], anche se non è in discussione un cambiamento di tendenza, a partire dal 1999-2000, che risulta evidente in questi grafici dove viene proposto un confronto fra l'andamento di crescita del *hostcount* italiano e quello mondiale dal 1995 al 2004.

Host Internet 1995-2004
fine 1994 = 100
dati semestrali



Host Internet italiani come % del totale mondiale 1992-2004



Per alcuni anni la crescita di Internet in Italia ha avuto uno sviluppo analogo a quello medio mondiale. Dopo una leggera crescita nel 1997 la percentuale di crescita italiana resta pressoché costante rispetto al totale (fra 0,8 e

[124] Si veda a questo proposito la sintesi di un estratto del Rapporto 2003 del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni, riportata più avanti (paragrafo 2), che sottolinea invece il *gap* informatico ancora esistente tra il nostro Paese ed altre nazioni europee.

0,9 %). A partire dal secondo semestre del 1999 si rileva un cambiamento significativo e sembra che l'attività *on line* in Italia continui a crescere più velocemente della media.
Come già osservato, i dati del 2002-2004 indicano una crescita talmente accelerata da far insorgere più di un dubbio sull'esattezza delle cifre. Ripetute rilevazioni, in vari periodi, confermano invece - si sottolinea nella ricerca - che **la posizione dell'Italia è effettivamente significativamente migliorata e che il Paese si attesta ormai fra i primi cinque o sei al mondo per attività di rete.** Anche nel resto del mondo si riscontrano alcuni cambiamenti rilevanti, con una crescita particolarmente veloce in alcuni paesi.

La tabella seguente analizza i dati per i 52 paesi (su 240) con più di 100.000 *host* Internet.

	Numero di *host* dicembre 2004	Crescita % in un anno	% su totale	Per 1000 abitanti
Stati Uniti	191.000.000	+ 29,9	62,0	679,1
Giappone	19.543.040	+ 50,1	6,2	153,1
Italia	9.343.663	+ 70,1	2,9	161,4
Olanda	6.443.558	+ 88,5	2,0	397,2
Germania	6.127.262	+ 79,1	1,9	74,2
Gran Bretagna *	6.000.000	n.a.	1,9	100,9
Francia	4.999.770	+ 80,4	1,6	83,7
Australia	4.820.646	+ 69,3	1,5	242,5
Brasile	3.934.577	+ 24,4	1,2	22,2
Canada	3.839.173	+ 19,6	1,2	121,4
Taiwan	3.516.215	+ 26,6	1,1	155,9
Spagna *	2.800.000	n.a.	0,9	66,9
Svezia	2.668.816	+ 73,3	0,8	298,0
Polonia	2.482.546	+ 91,4	0,8	65,0
Belgio	2.012.283	+ 38,4	0,6	194,0
Finlandia	1.915.506	+ 52,1	0,6	367,0
Danimarca	1.908.737	+ 30,1	0,6	354,6
Messico	1.868.583	+ 40,1	0,6	18,2
Svizzera	1.785.472	+ 75,3	0,6	244,0
Austria	1.594.059	+ 62,3	0,5	197,4

	Numero di *host* dicembre 2004	Crescita % in un anno	% su totale	Per 1000 abitanti
Norvegia	1.367.973	+ 35,0	0,4	298,8
Russia	1.157.677	+ 44,7	0,4	8,0
Argentina	1.050.639	+ 41,5	0,3	28,4
Israele	1.004.141	+ 58,4	0,3	148,8
Hong Kong	856.244	+ 44,6	0,3	127,6
Corea (Sud) *	800.000	n.a.	0,3	16,7
Rep. Ceca	724.631	+ 100,1	0,2	71,0
Nuova Zelanda	651.065	+ 37,2	0,2	162,4
Ungheria	611.887	+ 67,5	0,2	60,5
Turchia	611.557	+ 70,1	0,2	8,6
Singapore	610.655	+ 26,0	0,2	177,5
Portogallo	605.648	+ 101,9	0,2	58,0
Tailandia	514.228	+ 395,9	0,2	8,0
Sudafrica	451.500	+ 56,4	0,1	9,7
Grecia	377.221	+ 53,6	0,1	34,2
Colombia	324.889	+ 181,4	0,1	7,3
Irlanda *	300.000	n.a.	0,09	75,6
Cile	294.575	+ 45,5	0,08	19,6
India	276.293	+ 218,0	0,09	0,26
Romania	276.201	+ 95,6	0,09	12,7
Estonia	237.461	+ 109,9	0,07	175,1
Slovacchia	188.352	+ 69,4	0,06	35,0
Perù	177.948	+ 171,0	0,06	6,6
Cina	163.626	+ 2,0	0,05	0,13
Ucraina	151.366	+ 15,9	0,05	3,2
Islanda	144.636	+ 36,1	0,05	541,8
Malesia	139.932	+ 30,7	0,04	5,6
Indonesia	130.600	+ 57,8	0,04	0,6
Marocco	128.695	n.a.	0,04	4,3
Emirati Arabi	117.573	+ 21,0	0,04	29,5

Uruguay	112.640	+ 28,5	0,04	33,2
Lituania	106.458	+ 70,6	0,03	30,8
Totale	317.646.084	+ 36,3		21,4

I dati per gli Stati Uniti sono "ponderati" per tener conto del fatto
che una parte dei *domain* "apparentemente americani" ha sede in altri paesi.
Lo stesso correttivo introdotto nei grafici che seguono.
L'indice di densità "mondiale" calcolato escludendo gli Stati Uniti.* I dati disponibili per la Gran Bretagna, la Spagna, la Corea e l'Irlanda appaiono "sottostimati"
e perciò qui i numeri sono arbitrariamente, ma non irragionevolmente, aumentati.

I dati riportati evidenziano una forte crescita avvenuta non solo in Italia, ma anche in diversi paesi europei ed extraeuropei. Come sempre, le evoluzioni dovranno essere verificate su periodi più lunghi. Ma ci sono in ogni caso alcune notevoli variazioni, come quella della Francia che, per la prima volta, nel 2004, ha superato l'Australia, o della Polonia, che già in periodi precedenti, aveva superato "in cifra assoluta" alcuni dei paesi tradizionalmente più forti. Nello studio si fa inoltre rilevare che vi sono forti indici di crescita anche in paesi a densità molto elevata e ciò confermerebbe che si è ancora lontani da ogni possibile "livello di saturazione". Nel 1999 solo sei paesi nel mondo registravano più di un milione di *host* Internet (di cui due in Europa). Nel 2000 ve ne erano dieci (quattro in Europa), nel 2001 tredici (sei in Europa), nel 2002 diciassette (nove in Europa). Nel 2003 gli *host* sono saliti a venti e nel 2004 si è passati a ventiquattro, di cui quindici in Europa, cinque nelle Americhe, tre in Asia e uno in Oceania.

Nel 2001 i paesi con oltre tre milioni di *host* erano due e otto nel 2003. Diventano undici nel 2004. Otto paesi, di cui cinque in Europa, contano oltre quattro milioni di *host*. L'Italia ha superato il milione di *host* nel 2000, due milioni nel 2001, tre nel 2002 e cinque nel 2003.

Se non si tiene conto unicamente dei confini politici ma si accorpano i dati in base alla condivisione della lingua e dell'omogeneità etnica si possono evidenziare altre due grandi collettività con oltre 5 milioni di *host*. Si tratta della **comunità di lingua spagnola** (di cui il 40 % in Spagna e il 60 % nell'America Latina) e dell'**area etnica cinese** (per il 96 % fuori dalla Cina continentale).

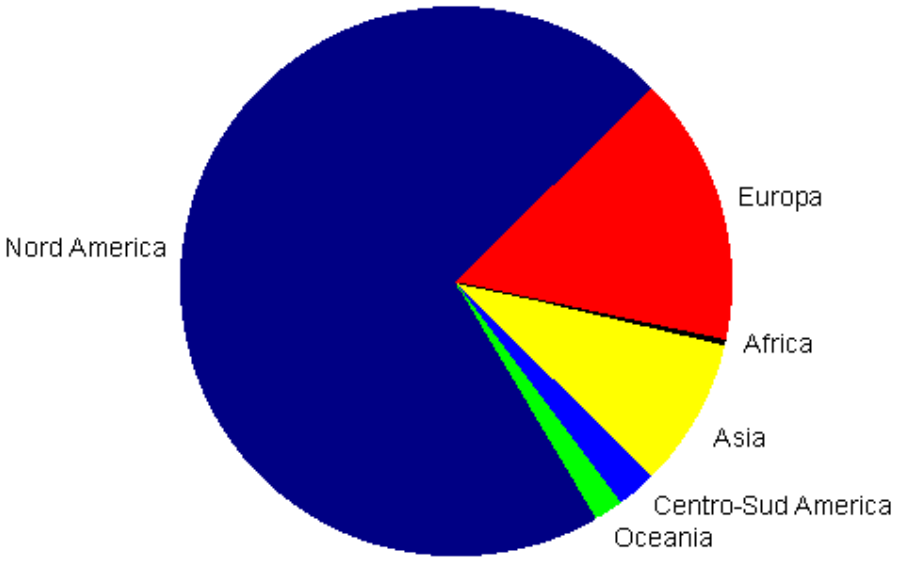
Nel 2002 la Cina[125] (esclusa Hong Kong) è comparsa, per la prima volta, tra i paesi con più di 100.000 *host*. Da allora la crescita è stata continua e velocissima. Si calcola che attualmente, con i suoi 103 milioni di utenti Internet, la Cina è seconda solo agli Stati Uniti. Secondo previsioni pubblicate recentemente, entro la fine dell'anno 2005, gli *user* arriveranno a 125 milioni e la Cina diverrà la prima *cyber*-potenza del mondo entro il 2007.

[125] Per approfondimenti sul *digital divide* in Cina si veda G. ROSATI, *Il Digital Divide in Cina*, 15 gennaio 2003, in <http://www.unarete.org> al *link* "Documenti", in cui sono raccolti riferimenti al *digital divide* nei diversi Paesi del mondo.

In ogni caso in questo Paese continua ad esistere un forte controllo sociale che limita il libero accesso all'uso della rete insieme ad una severa censura esercitata su tutti i mezzi di informazione e di comunicazione. Si pensi che Baidu (ovvero il *Google* cinese) deve tenere conto delle restrizioni politiche imposte dal governo. Ad esempio se si digitano le parole "*Free* Tibet" o "Radio *Free* Asia" come oggetto di ricerca non si ottiene alcuna risposta. A maggio del 2005 il governo cinese ha reso obbligatoria l'iscrizione di ogni *blog* al ministero dell'informazione e dell'industria cinese, con multe fino a un milione di *yuan* (circa 100 mila euro) [126].

Per quanto riguarda l'India, dove da anni si prospetta l'impegno per una più ampia diffusione della rete, la situazione è ancora molto insoddisfacente (nonostante la diffusa conoscenza dell'inglese e l'alto livello di cultura informatica in alcune parti del paese ci sono solo 276.000 *host* Internet pari a 0,26 per mille abitanti) anche se, nel 2004, rispetto agli anni precedenti, si è riscontrata una crescita notevole (per la prima volta ha superato la Cina). La situazione non è migliore nel resto del "subcontinente" indiano.

Graficamente la situazione per **"grandi aree geografiche**" risulta così illustrata:



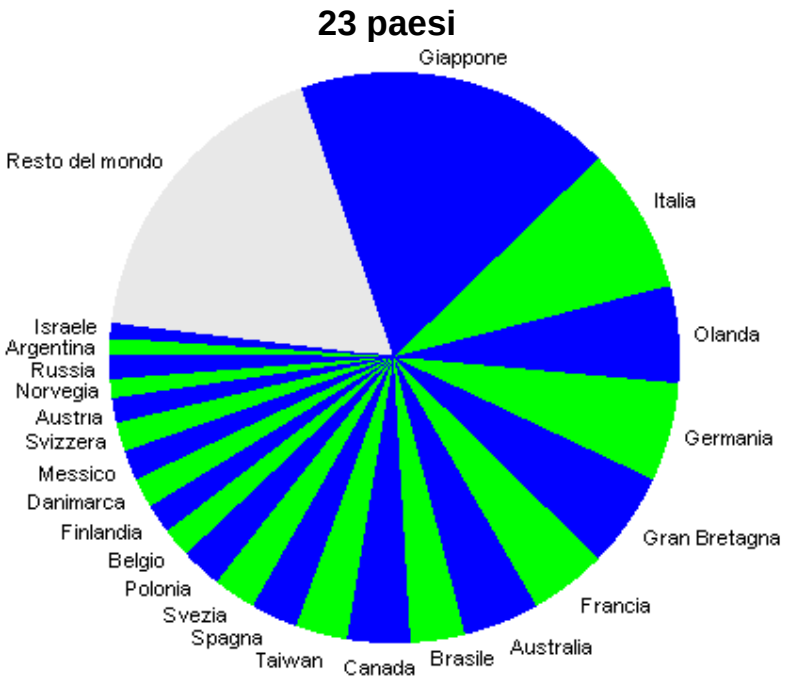
La situazione generale, in questa prospettiva, rimane simile a quella che avevamo visto nei periodi precedenti. La "globalità" è molto relativa. **Una grande parte del mondo è ancora isolata da Internet**. Il Nord America e

[126] C. MAGNANINI, *Net economy made in China* in « L'espresso », n. 33, agosto 2005, pp. 40-45.

l'Europa, con il 19 % della popolazione, realizzano l'80 % dell'attività in rete. Negli ultimi tre anni la crescita è risultata molto più veloce in Europa, in Asia e nell'America centro-meridionale che non in America settentrionale e in Oceania. L'Africa ha uno sviluppo proporzionalmente simile alla media mondiale, ma rimane ancora - come gran parte dell'Asia - molto arretrata. **Il continente con la densità più alta rispetto alla popolazione è l'Oceania,** che ha più di 160 *host* Internet per 1000 abitanti, mentre la media in Europa è di 82, quella dell'America latina di 16, quella asiatica di 8 e quella africana di 0,8 cioè, rispettivamente, un decimo e un centesimo del livello europeo.

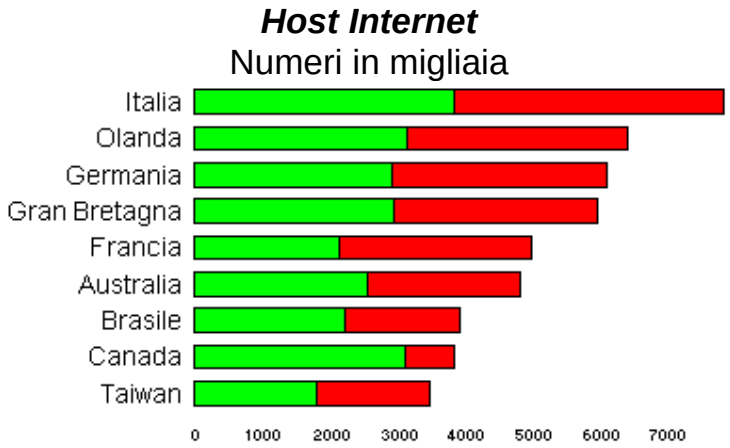
Anche all'interno di ciascuna delle zone geografiche si evidenziano forti squilibri. Il 97 % della rete nel Nord America è concentrata negli Stati Uniti. In Oceania il 99 % dell'attività risulta ascrivibile a due paesi: Australia e Nuova Zelanda. Il 68 % dell'attività Internet in Asia è in Giappone (il 18 % nell'area etnica cinese). Il 68 % dell'attività di rete africana è concentrata in Sudafrica, mentre l'82 % di quella dell'America centro-meridionale è in Brasile e in Argentina. Solo in Europa il quadro appare abbastanza omogeneo poiché nessun paese ha più del 17 % del totale, anche se rimangono, anche nel nostro continente, forti differenziazioni, come risulta dall'analisi dei dati europei. La percentuale di crescita di attività statunitense continua a diminuire gradualmente nel corso degli anni rispetto a quella degli altri paesi.

Se per una lettura più chiara togliamo gli Stati Uniti dal grafico, questa è la presenza in rete degli altri 23 paesi con più di un milione di *host* Internet.



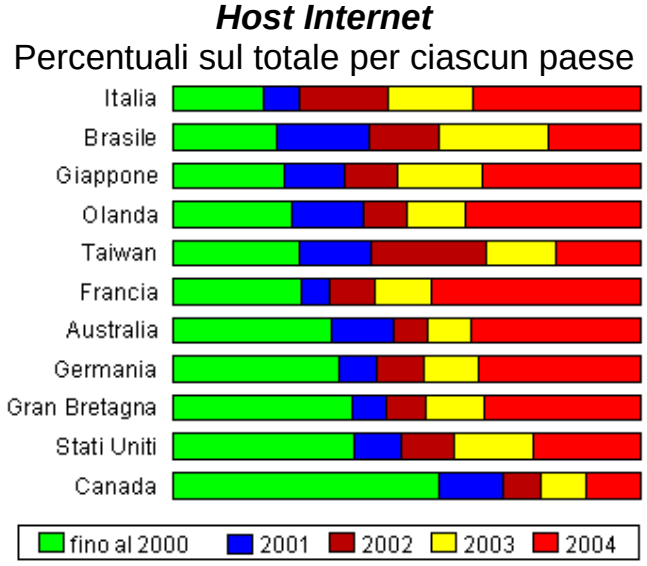
Attualmente si riscontrano cambiamenti rilevanti rispetto al passato, con la crescita di alcuni paesi europei e con una più forte presenza di Brasile, Taiwan e Messico (tre nuovi "milionari" nel 2004 sono la Russia, l'Argentina e Israele). Più di metà di tutta la rete al di fuori degli Stati Uniti è ancora concentrata in sette paesi che possiedono meno del sette per cento della popolazione mondiale. La novità degli ultimi tre anni è che tra essi compare l'Italia.

Le velocità di crescita registrate sono molto diverse nei vari paesi, come è evidente nel grafico riportato di seguito. I dati riguardano 9 degli 11 paesi nel mondo con più di tre milioni di *host* Internet (per maggiore facilità di lettura sono esclusi gli Stati Uniti e il Giappone).

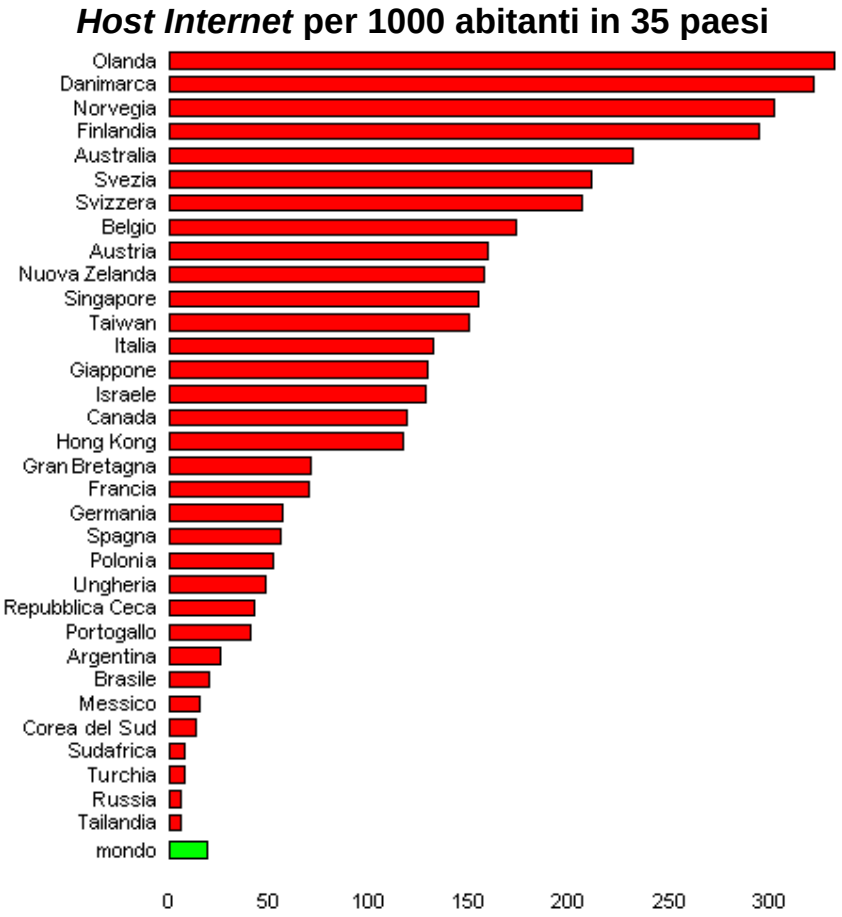


La parte rossa delle barre rappresenta l'aumento in due anni (dal 2002 al 2004). La crescita dell'Italia è intenzionalmente, quanto arbitrariamente, attenuata in questo grafico e in quello che segue.

Le differenze di velocità di crescita sono ancora più evidenti nel grafico seguente, dove le fasi di sviluppo sono espresse come percentuali del totale.



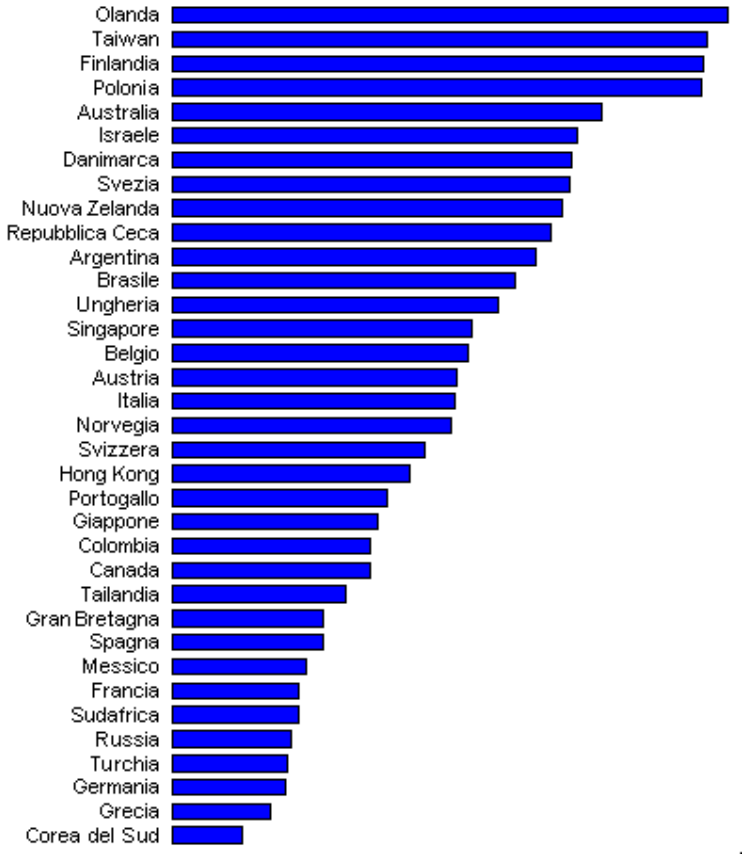
Un cambiamento di tendenza è registrato in Francia, ma si rileva una crescita veloce anche in paesi che erano già notevolmente avanzati, come l'Olanda. Un confronto interessante è mostrato dal grafico seguente in cui il numero di *host* Internet espresso in rapporto alla densità di popolazione nei 35 paesi (con più di 300.000 *host* Internet).



Anche in questo caso è dominante la presenza degli Stati Uniti (che già nel 1998 avevano superato il "primato" tradizionale della Finlandia). Si rileva ancora una volta un forte progresso dell'Olanda, che ha superato il livello dell'area scandinava. La posizione dell'Italia è molto migliorata, anche se ancora lontana da quella dei paesi più avanzati. **Si è registrata una nuova accelerazione in paesi tradizionalmente forti come l'Australia e confermata la crescita del Giappone**, che ha quasi raggiunto il livello di densità di Taiwan. **Fra i paesi dell'Europa centro-orientale è evidente un forte sviluppo della Repubblica Ceca e della Polonia mentre, nell'area mediterranea, è rilevante la crescita di Israele.**

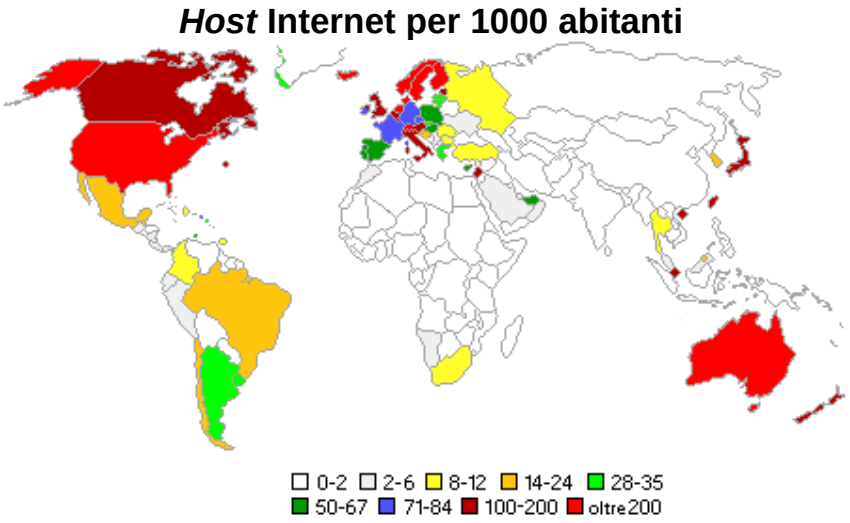
Nello studio di Gandalf i dati vengono anche rapportati al reddito (prodotto interno lordo) e delineano il seguente quadro:

Host Internet in rapporto al reddito (PIL) in 35 paesi



Come si era già notato nelle analisi precedenti, è rilevante il livello di attività in rete in alcuni paesi dell'Asia, dell'Europa orientale e dell'America latina. Anche da questo punto di vista è notevole il progresso dell'Olanda, che si colloca al quarto posto sulla scala mondiale (dopo gli Stati Uniti, l'Estonia e l'Islanda) e della Polonia che ha quasi raggiunto la Finlandia.

Di interesse anche la distribuzione geografica della densità di uso di Internet illustrata di seguito



Un po' arbitrariamente in questa mappa l'area "gialla"
estesa solo a una parte della Federazione Russa
poiché ragionevole pensare che l'attività *on line*
sia concentrata soprattutto nella Russia europea

Non compaiono nella mappa alcuni paesi "piccoli"
con una densità relativamente elevata
(per esempio alcune isole del Pacifico).
Sono, comunque, pochi e non influiscono
significativamente sul quadro generale.

Si ricorda che, nel 1996, nessun paese al mondo, all'infuori degli Stati Uniti, aveva un milione di *host* Internet. Il Giappone non aveva ancora raggiunto l'*hostcount* della Gran Bretagna e della Germania. L'Olanda e la Francia non avevano superato il totale, tradizionalmente alto, della Finlandia. L'Italia, che aveva da poco sorpassato la Norvegia, era ancora molto lontana non solo dalla Finlandia, ma anche dalla Svezia. Solo otto anni fa l'Italia era al quattordicesimo posto del mondo "in cifra assoluta" e al trentesimo per densità (*host* per mille abitanti). In Europa risultava al settimo posto per *hostcount* totale e tredicesima per densità.

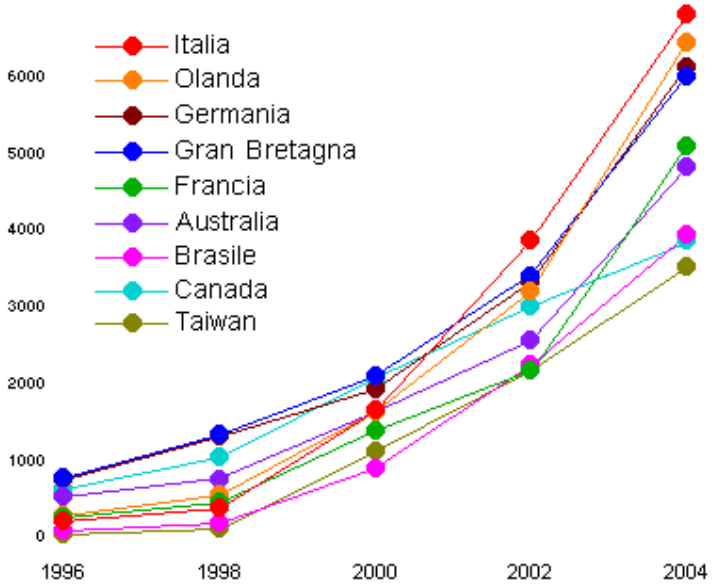
La tabella allegata di seguito mostra l'evoluzione del numero di *host* avvenuta dal 1996 al 2000 e dà conto del fattore di moltiplicazione nel 2004, rispetto agli anni 1996, 1998 e 2000.

	migliaia di *host*			**crescita 2004 su**		
	1996	**1998**	**2000**	**1996**	**1998**	**2000**
Mondo	16.729	36.739	109.574	x 18,9	x 8,8	x 2,9
Stati Uniti	10.110	23.800	72.457	x 18,9	x 8,0	x 2,6
Gran Bretagna	764	1.322	2.291	x 7,9	x 4,5	x 2,6
Germania	743	1.309	2.163	x 8,2	x 4,7	x 2,8
Giappone	734	1.352	4.641	x 26,6	x 14,5	x 4,7
Canada	603	1.028	2.364	x 6,4	x 3,7	x 1,6
Australia	515	750	1.616	x 9,4	x 6,4	x 3,0
Finlandia	328	514	772	x 5,8	x 3,7	x 2,5
Olanda	277	533	1.624	x 23,2	x 12,1	x 4,0
Francia	252	447	1.376	x 17,9	x 11,2	x 3,6
Svezia	246	381	764	x 10,8	x 7,0	x 3,5
Italia	193	358	1.631	x 48,4	x 26,1	x 5,7
Norvegia	177	312	525	x 7,7	x 4,4	x 2,6
Svizzera	135	216	461	x 13,2	x 8,3	x 3,9
Spagna	119	258	664	x 23,5	x 10,9	x 4,2
Danimarca	111	200	436	x 17,2	x 9,5	x 4,4
Austria	99	152	504	x 16,1	x 10,5	x 3,2
Sudafrica	99	141	185	x 4,6	x 3,2	x 2,4
Nuova Zelanda	85	178	310	x 7,7	x 3,6	x 2,1
Brasile	77	164	623	x 51,1	x 24,0	x 6,3
Russia	69	176	335	x 16,8	x 6,6	x 3,5

Dai dati si può notare che, anche nei paesi con un fattore di crescita relativamente più basso, lo sviluppo non si può definire “lento”. Infatti, **su scala mondiale, Internet cresciuta di 19 volte in otto anni, di quasi 9 in sei ed è triplicata negli ultimi quattro.** Nei paesi meno veloci la dimensione attuale quintuplicata rispetto al 1996 e più che triplicata dal 1998. In alcuni paesi, fra cui

l'Italia, il cambiamento è stato, come già ricordato più volte, molto più evidente. Fra i paesi non citati in questa tabella rilevante la crescita di Taiwan, che è fra le più veloci del mondo. La Polonia ha avuto un'evoluzione paragonabile, in proporzione, a quella italiana (negli ultimi quattro anni il paese con il più veloce sviluppo in Europa).

Il grafico seguente riassume l'evoluzione di nove paesi (esclusi gli Stati Uniti e il Giappone) con più di 3 milioni di *host* Internet nel 2004.



In questo grafico la crescita dell'Italia nel 2003-2004
intenzionalmente, quanto arbitrariamente, ridotta

In tutti - ad eccezione del Canada - si nota una forte crescita nell'ultimo periodo ed in particolar modo in Olanda, Brasile e Taiwan. Analoghe variazioni si rilevano in molti paesi con un *hostcount* inferiore a tre milioni anche se non rappresentanti nel grafico.

Dallo studio citato è sembrato utile estrarre anche dati più dettagliati che riguardano aree del mondo particolarmente svantaggiate rispetto alla possibilità di accedere alle nuove tecnologie dell'informazione, come l'Africa e l'Asia.

Africa

Dai dati che riguardano il continente africano due fatti risultano chiari: il primo è che quasi tutta l'Africa, insieme a una larga parte dell'Asia, rimane fortemente arretrata. L'altro è che, come rilevato nell'analisi dei dati internazionali, otto decimi dell'attività *on line* di tutto il continente si trovano concentrati in un solo paese: il Sudafrica (che ha il 5 % della popolazione).

Nella tabella seguente è riassunta la situazione nei 14 paesi africani con più di 1.500 *host* Internet.

	Numero di *host* dicembre 2004	% su Africa	Per 1000 abitanti
Sudafrica	451.500	68,4	9,7
Marocco	128.695	19,5	4,3
Egitto	23.407	3,5	0,34
Kenya	10.848	1,6	0,35
Tanzania	9.444	1,4	0,26
Zimbabwe	8.055	1,22	0,69
Mozambico	7.670	1,16	0,80
Namibia	4.632	0,70	2,4
Swaziland	2.642	0,40	2,5
Zambia	2.610	0,40	0,23
Angola	2.480	0,38	0,18
Nigeria	2.498	0,38	0,02
Botswana	2.097	0,31	1,20
Ruanda	1.744	0,26	0,21
Africa	664.000		0,79

Come risulta dai dati internazionali la densità media
su scala mondiale è di 21 *host* Internet per mille abitanti.

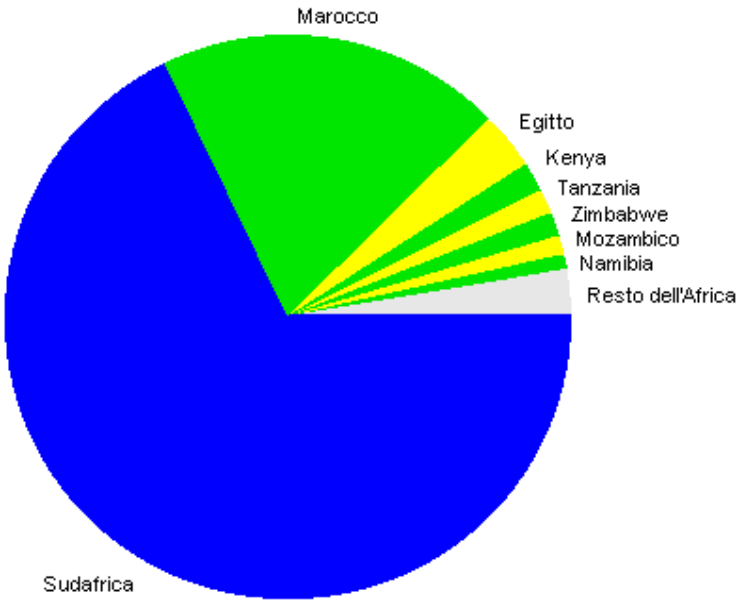
In un quadro generale di scarsissima densità esistono differenze rilevanti. **Il più forte cambiamento riguarda il Marocco**, che (anche se è ancora molto lontano dalla realtà sudafricana) sembra aver raggiunto una presenza *on line*

nettamente superiore a quella degli altri paesi africani. Peculiare è comunque anche la situazione dell'Egitto che spicca tra gli altri paesi, in cui l'attività *on line* rimane a livelli estremamente bassi. Si veda ad esempio la Libia che, in rapporto alla popolazione, ha una densità inferiore alla Nigeria e la Tunisia che non verte in condizioni migliori. L'Algeria, tra tutti, è notevolmente più indietro.

Anche nell'Africa sub-sahariana i segnali di crescita riguardano solo alcuni paesi, come il Kenya, il Mozambico e la Tanzania. Una densità relativamente elevata (rispetto al basso livello del continente) è riscontrabile in alcuni piccoli paesi come Namibia, Swaziland e Botswana.

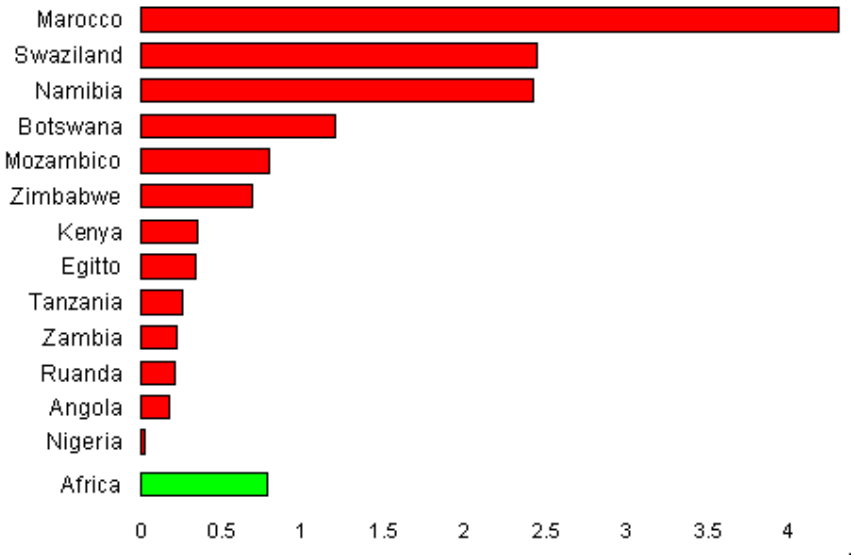
I dati seguenti illustrano la situazione degli otto paesi africani con più dl 3000 *host* Internet.

8 paesi africani

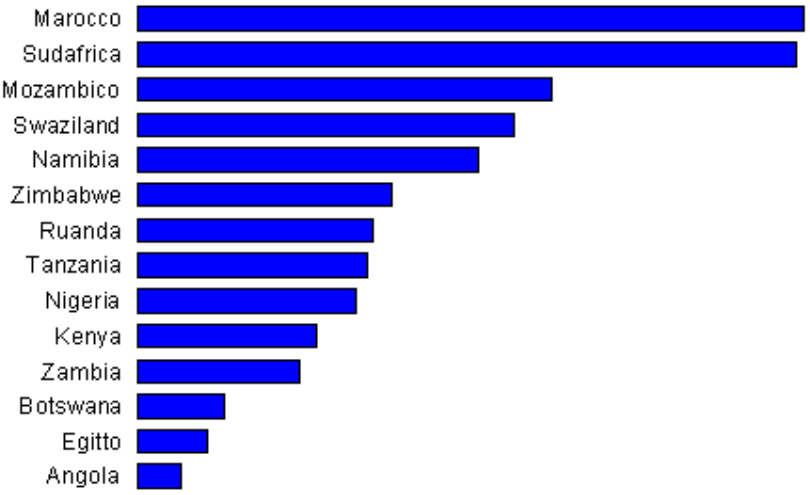


Il Sudafrica rimane, nella ripartizione, dominante, anche se la situazione in mutazione con la recente consistente crescita fatta registrare dal Marocco. Con i grafici che seguono vengono illustrati rispettivamente la densità (*host* per mille abitanti) nei 13 paesi africani (escluso il Sudafrica) con più di mille *host* Internet e la distribuzione in rapporto al reddito.

Host Internet per 1000 abitanti
in 13 paesi africani



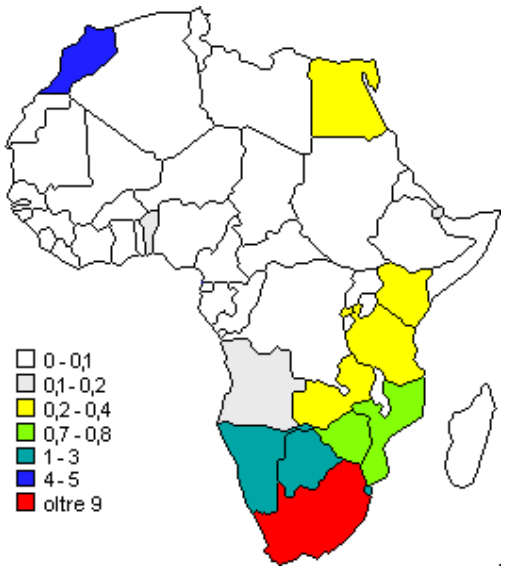
_Host Internet i_n rapporto al reddito (PIL)
in 14 paesi africani



Relativamente a questo parametro il Marocco ha raggiunto, se non superato, il livello del Sudafrica. La maggior parte del continente africano rimane comunque in una situazione di arretratezza. In un precedente studio che prendeva come riferimento i "grandi paesi a bassa densità" erano state rilevate la scarsissima diffusione di Internet in Congo ed in Etiopia. Non migliore appariva la situazione in Somalia e in Eritrea, così come in Sudan e nello Zaire (dove non risulta rilevata alcuna attività *on line*).

E' illustrato di seguito la distribuzione geografica della densità di diffusione.

Host Internet per 1000 abitanti



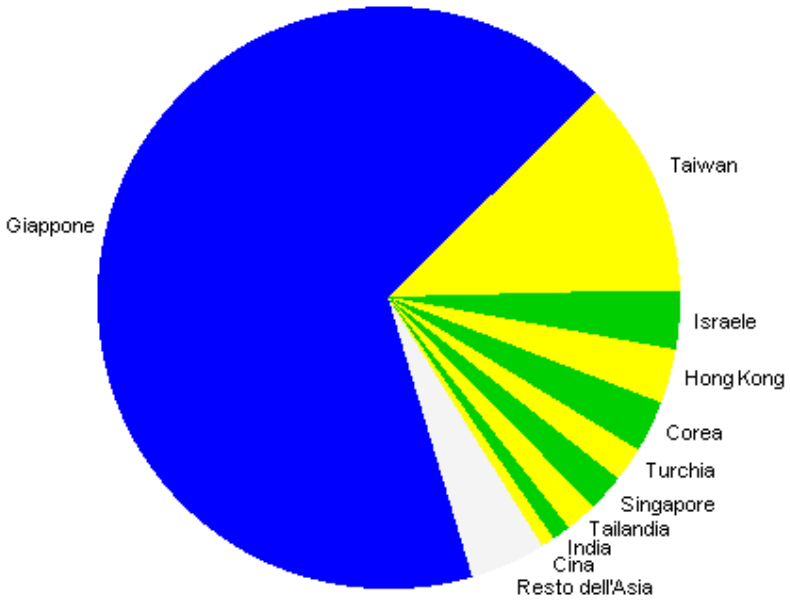
Tre “punti” blu comparirebbero al largo delle coste africane se in questa carta fossero comprese le isole Seichelle, Mauritius e São Tomé e Principe, che hanno fra tre e sei *host* Internet per mille abitanti. Ma naturalmente su numeri molto piccoli la significatività incerta.

Asia

Con oltre 28 milioni di *host* Internet **l'Asia è al terzo posto nel mondo**, dopo il Nord America e l'Europa, **per attività in rete**. Ha una crescita più veloce della media mondiale. Ma anche qui con enormi differenze fra paese e paese. Come si evidenzia dalla tabella allegata - riferita ai 19 paesi asiatici con più di 10.000 *host* Internet - **il Giappone ha un ruolo dominante** in Asia, analogo a quello che hanno gli Stati Uniti su scala mondiale. I primi cinque paesi, che rappresentano meno del 6 % della popolazione, realizzano l'87 % dell'attività in rete.

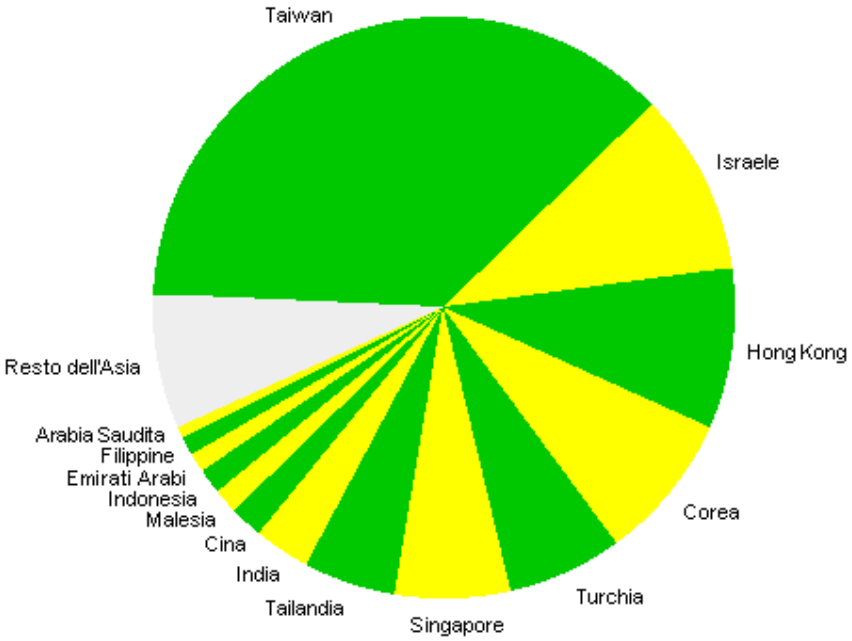
	Numero di *host* dicembre 2004	% su Asia	Per 1000 abitanti
Giappone	19.543.040	68,5	153,1
Taiwan	3.516.215	12,3	155,9
Israele	1.004.141	3,5	148,8
Hong Kong	856.244	3,0	127,6
Corea (Sud)	800.000	2,8	16,7
Turchia	611.557	2,1	8,6
Singapore	610.655	2,1	177,5
Tailandia	514.228	1,8	8,0
India	276.293	0,97	0,26
Cina	163.626	0,57	0,13
Malesia	139.932	0,49	5,6
Indonesia	130.600	0,46	0,6
Emirati Arabi	117.573	0,41	29,5
Filippine	93.345	0,33	1,14
Arabia Saud.	52.091	0,18	2,18
Cipro	39.366	0,14	55,0
Pakistan	32.038	0,11	0,22
Kazakistan	13.557	0,05	0,9
Libano	13.264	0,05	3,6
Asia	28.570.000		7,5

10 paesi



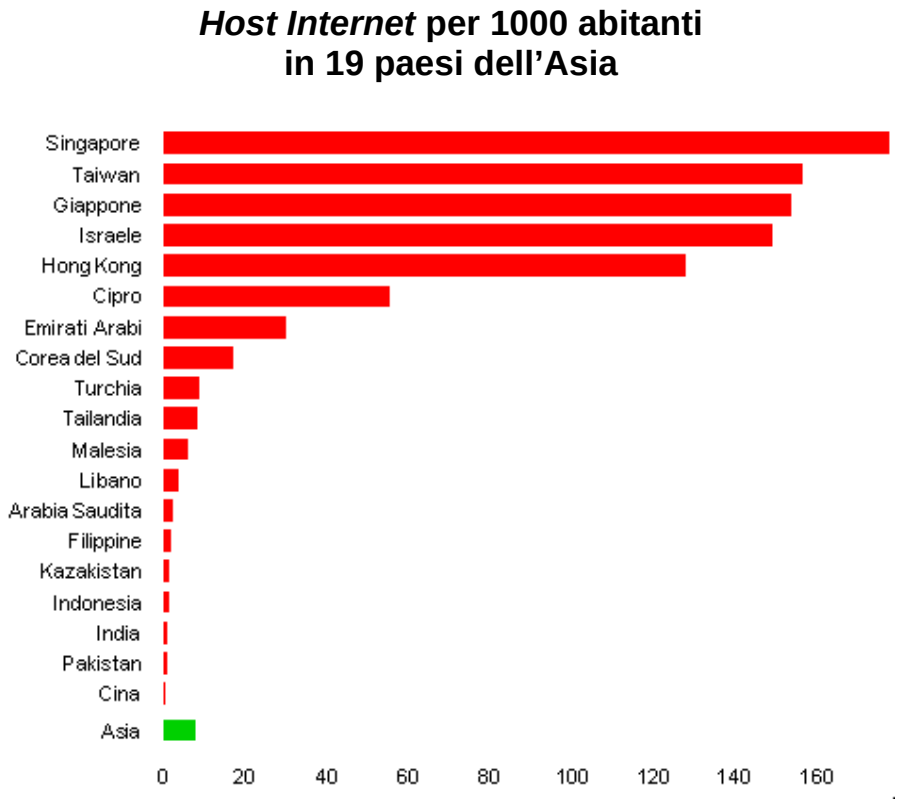
Se togliamo il Giappone dal grafico, questa è la situazione degli altri 15 paesi asiatici con più di 50.000 *host*.

15 paesi



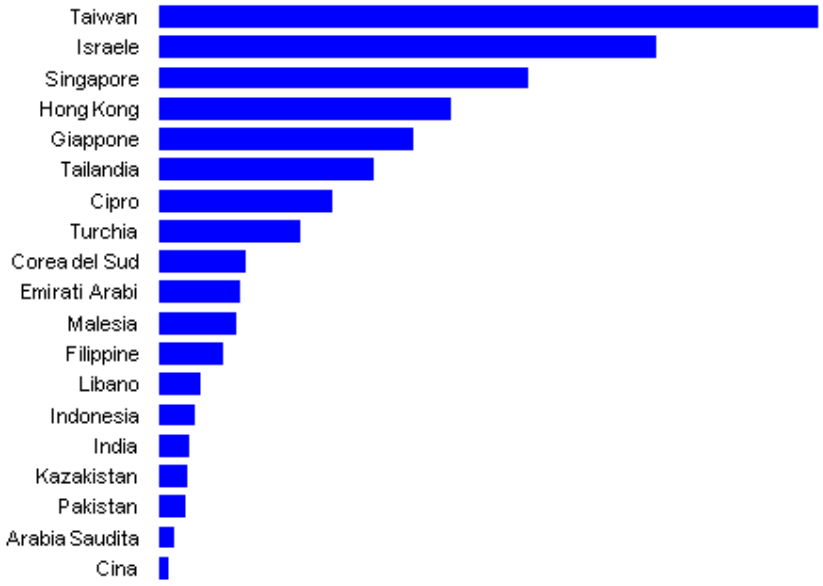
"Piccoli" paesi con meno di sette milioni di abitanti, come Israele e Hong Kong (che mantiene una identità nell'Internet separata dalla Cina) o con meno di quattro milioni, come Singapore, hanno un'attività *on line* molto superiore a quella di paesi enormemente più grandi.

Le differenze sono evidenti in questo grafico della densità (*host* per mille abitanti) negli stessi 19 paesi elencati nella tabella all'inizio.



Si confermano forti differenze, ma con un profilo diverso, nell'analisi del *hostcount* in rapporto al reddito (prodotto interno lordo).

Host Internet in rapporto al reddito (PIL) in 19 paesi dell'Asia



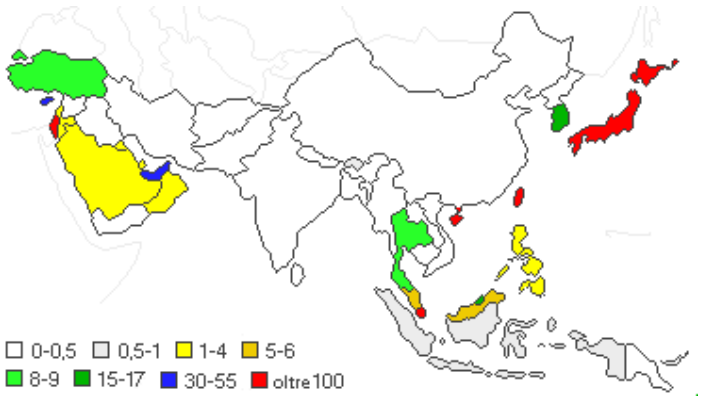
Il quadro è diverso da quello della densità rispetto alla popolazione – ma conferma enormi differenze fra i diversi paesi asiatici.

In Cina rispetto ad altri Paesi dell'area etnico-cinese si registra - sia in relazione alla densità di popolazione sia in relazione al reddito - una bassissima attività di rete, causata, come già ricordato, anche dal rigido controllo sociale tuttora esistente in quel Paese.

Critica appare pure la situazione dell'India, nonostante l'impegno profuso negli ultimi anni per sostenere lo sviluppo della rete e nonostante, nel 2004, si sia evidenziata una notevole crescita. La densità è ancora molto bassa e la situazione non è migliore nel resto del "subcontinente" indiano.

La distribuzione geografica riassunta di seguito:

***Host Internet* per 1000 abitanti**



Sono pochi i paesi con una densità elevata e localizzati solo in alcune parti del continente. Se si potessero isolare alcune aree urbane ci sarebbero piccoli "punti", anche in paesi a bassa densità, di non trascurabile attività nell'Internet. Ma il quadro generale conferma una situazione di grandi squilibri".

2. La situazione italiana[127]

Il Rapporto 2003 del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni *(Strategia e politiche per la larga banda in Italia)* sottolinea che "rispetto ai Paesi europei di maggiore dimensione e rispetto alla media dei paesi dell'Unione, l'Italia presenta un *gap* in termini diffusione di Internet. Infatti, in base alle più recenti rilevazioni comparate sulla penetrazione Internet (Aprile 2001), tra i paesi con caratteristiche omogenee, si registra un distacco rispetto a UK e Germania, che hanno una penetrazione del 50% superiore a quella italiana ed uno scarto di circa il 25% rispetto alla media di penetrazione Internet dei paesi UE. Il passaggio alla larga banda ci vede pertanto in una posizione di partenza diversa rispetto ad altri Paesi europei".

Anche secondo l'Istat l'Italia risulta tra i paesi con minore diffusione Intranet e non ottimale è anche la diffusione del commercio elettronico anche se "in generale nei paesi dell'Unione la pratica delle vendite via Internet è meno diffusa di quella degli acquisti" e pari ad un percentuale

[127] La descrizione del quadro italiano deriva da ampi stralci del Rapporto del Ministro per l'innovazione e le tecnologie e del Ministro delle comunicazioni, anno 2003. Questi sono evidenziati con l'uso di un carattere più piccolo.

variabile tra il 17% ed il 12% soltanto in alcuni Paesi quali i Paesi Bassi, la Finlandia, la Danimarca, il Belgio, la Norvegia e l'Irlanda (Italia tra l'1% ed il 9%). Complessivamente nel quadro sull'uso delle tecnologie informatiche l'Italia si pone in una posizione intermedia rispetto ai Paesi europei sia rispetto all'accesso al *web* sia rispetto all'uso delle reti Internet[128].

La carenza di diffusione di una cultura tecnologica di base non colpisce solo il ramo *consumer,* ma anche il ramo *business*. Il sistema produttivo italiano, caratterizzato dal prevalere delle PMI, necessita di supporto e indirizzo per incrementare e ottimizzare il proprio livello di utilizzo delle ICT, che anche in questo caso ha alla base interventi significativi sulla formazione e per la creazione di professionalità specifiche. Si pone inoltre in rilievo che il fenomeno del *digital divide* appare molto più complesso di una semplice differenziazione tra quanti si connettono abitualmente alla rete e quanti no.

Accanto alla divisione tra coloro che usano Internet e quelli che non lo fanno (the *first divide*), recenti studi evidenziano che il gruppo di coloro che non usano Internet non è omogeneo ma si divide (*dual digital divide*) tra coloro che sono interessati ad Internet, ma non sono in grado di connettersi (*near-users*) per varie ragioni (economiche e di alfabetizzazione) e quelli che non hanno interesse a connettersi (*distant-users*). Mentre le modalità di intervento sul *digital divide* dei cosiddetti *near users* sono facilmente individuabili, più complesso individuare gli interventi necessari a ridurre quello dei cosiddetti *distant-users*. Infatti per questi ultimi non basta superare le barriere all'accesso (costo, alfabetizzazione), ma occorre rendere loro evidente anche la necessità di utilizzare la rete. E' riconosciuto che una delle cause della resistenza alla rete dei *distant users* va ricercata oltre che nella mancanza di alfabetizzazione "tecnologica" nella scarsa consapevolezza della necessità di utilizzare la rete come indispensabile moltiplicatore delle proprie capacità sociali.

Accanto a questi tipi di *digital divide* - prosegue il Rapporto - "ne esiste anche un altro, più strettamente legato a problemi di accesso e più specificatamente alla difficoltà di realizzare infrastrutture a larga banda in determinate aree, dove gli operatori ritengono antieconomico effettuare investimenti in infrastrutture. Questo tipo di *digital divide* può realizzarsi a diversi livelli.

Il primo di essi è quello che discrimina tra aree più o meno sviluppate del Paese dal punto di vista economico, come ad esempio il Nord e il Sud del Paese (*digital divide* geografico).

Il secondo livello è quello che discrimina tra tipi diversi di zone, come ad esempio tra aree rurali ed aree urbane (*digital divide* tipologico). La maggiore densità di popolazione e di imprese rende infatti la redditività dell'investimento più elevata nelle aree urbane rispetto a quelle rurali.

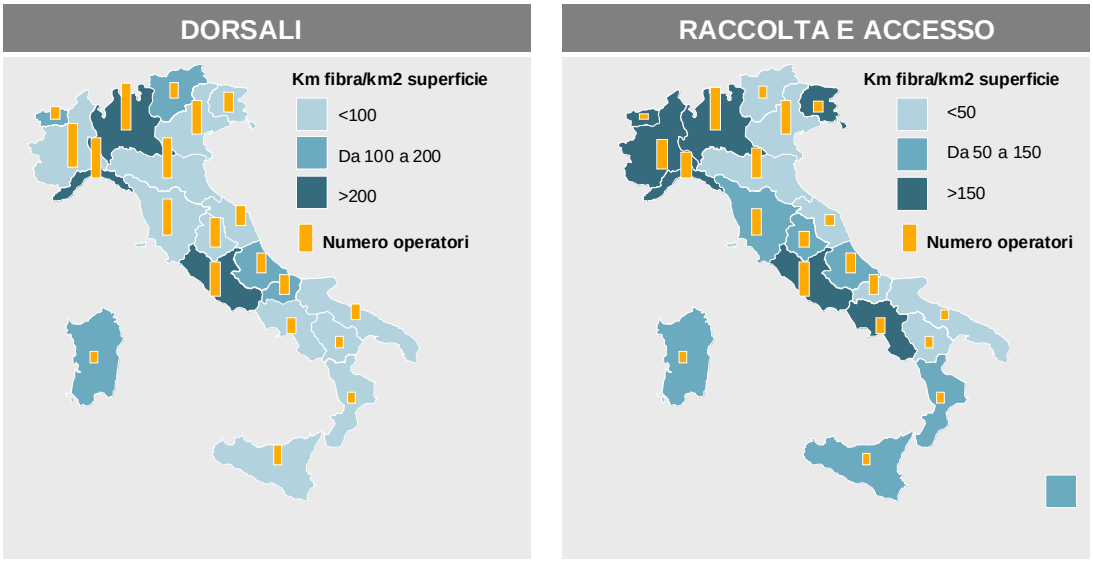
Il terzo livello può verificarsi addirittura all'interno della stessa area, nel caso in cui, ad esempio, strade o addirittura palazzi contigui ospitino o meno

[128] Per approfondimenti si veda ISTAT, op. cit., pag. 153 (documentazione allegata).

clienti ritenuti remunerativi dal soggetto che realizza l'infrastruttura (*micro digital divide*)".

Telecom Italia è attualmente l'operatore principale (o *incumbent*) nel mercato delle telecomunicazioni e circa il 57% delle sue centrali sono oggi raggiunte in fibra ottica, con una concentrazione prevalente nelle città più grandi.

Densità regionale delle reti di comunicazione e livello di competizione



Fonte: Osservatorio Banda - Betwee, elaborazione Roland Strategy

A seguito della liberalizzazione e della conseguente concorrenza sul mercato, oggi circa il 70% dei capoluoghi di provincia è ***raccordato in fibra ottica*** da due o più operatori (nel 50% dei casi vi sono almeno tre operatori presenti). La ridondanza si riduce, però, in modo significativo, passando dalle città del Centro-Nord a quelle del Sud: la densità di fibra per superficie, anche in rapporto al traffico, è doppia, infatti, nelle grandi regioni settentrionali rispetto a quella delle regioni del Mezzogiorno.

Nonostante la diffusione della fibra sul territorio sembri abbastanza omogenea se vista a livello di macroregioni (Nord Ovest, Nord Est, Centro e Sud/Isole), in realtà la situazione è diversa se la si esamina più in dettaglio. Dai 122 chilometri di fibra per mille abitanti del Centro si passa ai 107 del Nord Ovest, ai 103 del Nord Est per scendere decisamente ai 65 di Sud/Isole. In sostanza, esiste una disparità nella disponibilità di banda potenziale per abitante. Tale disparità è legata alle politiche di sviluppo delle reti seguite dagli operatori concorrenti dell'operatore ex-monopolista (presente in maniera omogenea sul territorio), i quali hanno ovviamente privilegiato le aree a maggior densità di utenza potenziale. Per quanto riguarda specificamente **l'area di accesso** - che rimane il collo di bottiglia della rete italiana a banda larga - il contesto italiano, come già accennato, è oggi proiettato ad una estesa presenza della tecnologia xDSL che, sfruttando la capillare infrastruttura del tradizionale cavo telefonico,

consente la copertura (potenziale) di oltre il 70% della popolazione, con una diffusione tuttavia non uniforme sul territorio nazionale. La potenzialità di accesso in tecnologia xDSL, infatti, è ormai distribuita nella totalità dei capoluoghi di provincia e nella stragrande maggioranza dei comuni con più di 10.000 abitanti, località in cui sono stati effettuati dall'operatore principale i necessari investimenti in apparati di raccolta DSLAM (*Digital Subscriber Line Access Multiplex*) nell'ambito delle centrali terminali. E' invece inferiore nei comuni con meno di 10.000 abitanti, dove risiede circa un terzo della popolazione italiana, in ragione di differenti prospettive di ritorno degli investimenti che hanno condizionato le scelte di tutti gli operatori. Si registra inoltre un graduale peggioramento man mano che si procede da Nord a Sud: mentre in Lombardia ed Emilia Romagna si raggiungono percentuali superiori al 50 %, man mano che si scende verso Sud i valori si riducono progressivamente (Toscana 34%, Lazio 23 %), fino a raggiungere livelli compresi tra l'11% e il 15% in Puglia, Molise, Calabria e Basilicata, penalizzate dall'alta percentuale di residenti in piccoli centri.

Solo gli *Internet Service Provider* (di seguito ISP) e *Application Service Provider* (di seguito ASP) possono giocare il ruolo di "soggetti attivatori" dell'innovazione attraverso la loro rete commerciale e di concerto con gli attori istituzionali (Ministero delle comunicazioni, Ministero delle attività produttive, Dipartimento innovazione e tecnologie). Al centro del progetto vi è la netta convinzione che vada sostenuto e potenziato il ruolo fondamentale che in questo contesto evolutivo è svolto dagli ISP. Questi, infatti, non si limitano più ad assicurare il collegamento all'universo di Internet, ma si trasformano progressivamente in ASP, valorizzando la loro diffusa rete commerciale per offrire, principalmente alle PMI (Piccole e Medie Imprese), ma anche alle pubbliche amministrazioni locali, specie a quelle di piccole dimensioni, ai professionisti e ai cittadini una serie di pacchetti applicativi *web-based*.

Dal punto di vista dei ***settori di applicazione***, si può affermare che per la pubblica amministrazione locale e la Sanità/*Education*, tali tecnologie sono impiegate da poco più del 30% del totale dei soggetti considerati, di cui il 22% tramite servizi xDSL (nella quasi totalità in modalità ADSL) e poco più dell'8% con collegamento in fibra ottica. Fra le altre tecnologie di accesso, prevale l'ISDN base e si registra un primo – ma significativo – processo di adozione del satellite, utilizzato da circa il 5% delle aziende del segmento considerato.

Il valore di penetrazione della banda larga cala però drasticamente nelle aziende con meno di 50 addetti ed per questo che il Governo italiano è impegnato in una campagna di ***promozione verso le PMI*** dei vantaggi competitivi derivanti dall'uso efficace (non solo *e-mail* ma impiego di *Internet Business Solutions*) delle nuove tecnologie. In particolare, il Ministero delle Comunicazioni ha avviato il progetto ***Agire Digitale*** allo scopo di valorizzare il nuovo ruolo degli ISP i quali, offrendo ormai non solo connessioni Internet ma anche pacchetti applicativi, operano come *Application Service Provider*. La loro rete commerciale, già consolidata presso l'ambiente delle PMI, potrà quindi

costituire uno straordinario veicolo per accelerare nelle imprese l'uso delle nuove tecnologie *web-based,* ma, affinché tale uso risulti efficiente ed efficace, sarà necessario attivare un accesso a larga banda. Il progetto sarà svolto in collaborazione con il Dipartimento dell'innovazione e le tecnologie e il Ministero delle attività produttive. L'attuale basso livello di utilizzo, in realtà, non dipende soltanto da elementi culturali, ma soprattutto dalle conseguenze del *digital divide*, in quanto in Italia permane una situazione atipica rispetto alla maggioranza degli altri Paesi europei: le PMI costituiscono infatti il 99,5% del totale delle aziende e danno lavoro ad una percentuale degli occupati nettamente superiore rispetto agli altri paesi sviluppati. Le PMI sono distribuite abbastanza uniformemente su tutto il territorio nazionale, anche in prossimità di quei centri con meno di 10.000 abitanti che, per motivi orografici e/o di mercato, non dispongono delle infrastrutture necessarie.

L'utilizzo delle tecnologie a banda larga, analizzato in base al settore merceologico di attività, evidenzia che nel settore della finanza (che include le banche, ma anche le imprese del mondo assicurativo) quasi la metà delle aziende è già dotato di una modalità di connessione a reti a larga banda con una lieve prevalenza dell'ADSL rispetto alla fibra. Ottima è la diffusione per la larga banda anche nel comparto dei Servizi, mentre buona quella relativa al comparto Educazione. La debolezza della pubblica amministrazione locale è probabilmente anch'essa dovuta al fenomeno del *digital divide*, in quanto per esse valgono considerazioni analoghe a quelle fatte per le PMI.

L'estensione della copertura dei servizi xDSL complementata dallo sviluppo dell'offerta della tecnologia satellitare è, a breve-medio termine, la base principale per ridurre il *digital divide* negli accessi a banda larga.

In conclusione si può affermare che, per accelerare i processi innovativi, è necessaria la disponibilità di ***diverse piattaforme tecnologiche*** soprattutto nelle reti di accesso. Comunque, dal punto di vista della dotazione infrastrutturale, il fenomeno del *digital divide* appare meno critico. Infatti, il 79% della popolazione italiana e il 92% delle imprese sono coperti da centrali predisposte per i servizi xDSL, mentre tali percentuali nel Mezzogiorno si attestano rispettivamente al 74 % ed al 90%. A parte le infrastrutture, la maggiore criticità è costituita da un *cultural divide* che sta alla base del minor livello di domanda da parte del Mezzogiorno. E' quindi necessario uno sforzo notevole per rendere disponibile ***un'ampia gamma di servizi*** su più piattaforme distributive, accompagnata da programmi di alfabetizzazione, in particolare per le PMI e per l'universo SOHO, centrati sull'importanza di questi servizi per aumentare l'efficienza delle aziende e la possibilità di operare delle famiglie.

3. Le politiche per favorire il superamento del *gap* digitale

Unione europea[129]

Uno degli obiettivi dell'Unione europea è assicurarsi che le imprese, le amministrazioni pubbliche e i cittadini europei continuino a svolgere un ruolo guida nello sviluppo dell'economia globale basata sulla conoscenza e sull'informazione, partecipandovi a pieno titolo. A tal fine intende:

- promuovere la ricerca per lo sviluppo e l'impiego di nuove tecnologie dell'informazione e della comunicazione;
- istituire e conservare un quadro di norme e di *standard* che stimolino la concorrenza;
- promuovere lo sviluppo di applicazioni e di contenuti, sostenendo iniziative volte ad incoraggiare i cittadini europei a fruire della società dell'informazione
- e a parteciparvi.

La politica dell'UE nel settore della società dell'informazione si articola nella politica delle telecomunicazioni, il cui fondamento giuridico contenuto negli articoli 95 (armonizzazione del mercato interno), 81 e 82 (concorrenza) nonché negli articoli 47 e 55 (diritto di stabilimento e servizi) del trattato sulla Comunità europea; nel sostegno allo sviluppo tecnologico nel settore delle tecnologie dell'informazione e delle comunicazioni (TIC), basato sugli articoli da 163 a 172 (ricerca e sviluppo) del trattato CE; nel contributo alla creazione delle condizioni necessarie per la competitività dell'industria della Comunità, ai sensi dell'articolo 157 del trattato CE e nella promozione di reti transeuropee (TEN) nei settori dei trasporti, dell'energia e delle telecomunicazioni, come sancito dagli articoli 154, 155, 156 del trattato CE.

Le due principali componenti della strategia comunitaria relativa alla società dell'informazione risalgono alla metà degli anni '80 e sono:

- le attività di ricerca e di sviluppo nel settore delle TIC sono state avviate nel 1984 con il programma ESPRIT (tecnologia dell'informazione), seguito a ruota nel 1986 dai programmi

[129] Quadro tratto dalla sintesi della scheda Scadplus, consultabile sul sito <http://www.europa.eu.int/scadplus/>, ai *link* "Sintesi della legislazione dell'Unione", "Società dell'informazione", "Introduzione".

concernenti in modo specifico le applicazioni telematiche (trasporti, sanità e formazione a distanza) e dal programma RACE (tecnologie avanzate delle telecomunicazioni);

- la politica delle telecomunicazioni che è stata varata nel 1987 con il libro verde sulla liberalizzazione delle telecomunicazioni. Esso perseguiva tre obiettivi rimasti validi a tutt'oggi:

  - liberalizzare i segmenti di mercato ancora in regime di monopolio;
  - armonizzare il settore delle telecomunicazioni in Europa mediante norme e standard comuni;
  - applicare con rigore le norme sulla concorrenza ai segmenti di mercato liberalizzati per evitare accordi collusivi e l'abuso o la costituzione di posizioni dominanti.

La Commissione, nell'ambito di una strategia volta ad incoraggiarne e ad accrescerne l'utilizzo, ha avviato alcuni programmi che mirano non solo ad ottimizzare l'accesso ad Internet, ma anche a sostenere lo sviluppo di contenuti di qualità elevata nel rispetto del retaggio linguistico e culturale europeo ed a consentire alle imprese europee di svolgere un ruolo guida nel costante sviluppo di applicazioni Internet.

Tra le iniziative di maggior rilievo strategico è senz'altro da annoverare il piano *eEurope.* Il primo piano d'azione in questa direzione - *eEurope 2002* - era imperniato su tre punti prioritari:

- rendere Internet un sistema sicuro, meno costoso e più rapido;
- investire nelle persone e nelle loro competenze;
- promuovere l'utilizzo di Internet.

L'attuale piano 2005 insiste invece principalmente sulla diffusione dell'accesso a banda larga a prezzi concorrenziali, sulla sicurezza delle reti e sullo sviluppo dell'uso delle tecnologie dell'informazione da parte delle Comunità pubbliche.

Altro programma - il MODINIS - adottato nel novembre 2003, punta a garantire un seguito al piano d'azione eEurope 2005 attraverso la diffusione di buone pratiche, la comparazione tra le prestazioni dei vari Stati membri e il sostegno ad azioni di sensibilizzazione destinate a rendere più sicure le reti e l'informazione.

Come già ricordato è considerato di grande interesse il progresso tecnologico che rappresenta il nocciolo duro della società dell'informazione. Per garantire la coerenza e l'efficacia della strategia europea è considerata quindi fondamentale l'articolazione tra ricerca e sviluppo nel campo delle TIC.

Nel Quinto programma quadro (1999-2002) tutte le attività di ricerca, sviluppo tecnologico e dimostrazione (RST) concernenti le tecnologie dell'informazione e delle comunicazioni, precedentemente ripartite in programmi distinti, sono state riunite nel programma TSI, cui è stata attribuita una dotazione di bilancio di 3,6 miliardi di euro fino al 2002. Il programma TSI integra la RST e le misure di diffusione ed opera sulla base di un programma di lavoro che viene aggiornato ogni anno per adattare tempestivamente le attività di ricerca della Comunità al progresso tecnologico e all'evoluzione dei mercati.

Il Sesto programma quadro (2002-2006), adottato nel giugno 2002, comprende anche un aspetto "Tecnologie per la società dell'informazione" dotato di un bilancio di 3,625 miliardi di euro.

Accanto alle principali strategie politiche vi sono poi da ricordare importanti iniziative che fungono da misure specifiche di accompagnamento, quali:

- la *politica per la sicurezza e la privacy*, volta ad individuare soluzioni giuridiche e tecnologiche in materia di autenticazioni, integrità, riservatezza, tutela dei dati personali, sicurezza in rete, ecc.;
- il *completamento del mercato interno* per quanto concerne il commercio elettronico, il cui obiettivo assicurare servizi *on-line* gratuiti su tutto il territorio dell'Unione europea e offrire a consumatori e imprese le garanzie giuridiche necessarie per intraprendere attività in rete;
- il *programma eContent* per lo sviluppo di contenuti culturali e linguistici europei multimediali destinati ad Internet;
- il *piano d'azione e-Learning* che coordina le attività comunitarie correlate all'istruzione nell'era digitale.

Quadro italiano

La promozione dell'uso di Internet si sta sviluppando in Italia sia lungo la direttrice più generale della liberalizzazione del mercato delle telecomunicazioni, sia attraverso politiche specifiche di finanziamento atte a rimuovere ostacoli di accesso alla rete, che sono in parte strutturali ed in parte di altra natura (culturale e sociale).

Con la **legge 8 aprile 2002, n. 59**[130] si è inteso promuovere l'uso di Internet attraverso un maggiore grado di libertà nel mercato dell'interconnessione. La legge consente agli operatori autorizzati ai servizi di trasmissione dati e accesso ad Internet - gli *Internet Service Provider* (ISP) - di erogare servizi di trasmissione dati in competizione con gli operatori licenziatari, attraverso l'equiparazione delle condizioni di accesso all'interconnessione, e configura una vera e propria libertà di accesso al mercato della connettività Internet, soprattutto laddove i grandi operatori non raggiungono determinate aree del territorio nazionale con servizi evoluti e di qualità. Con il **D.M. 28 maggio 2003**[131] sono state fissate le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso alle comunicazioni in rete locale mediante radiofrequenze (*access point*). I soggetti autorizzati - obbligati all'iscrizione presso il registro degli operatori di comunicazione - a fornire questo tipo di servizio in locali aperti al pubblico o in aree confinate a frequentazione pubblica (aereoporti, stazioni ferroviarie e marittime, centri commerciali), possono avere sede in Italia o all'estero, in Paesi appartenenti allo spazio economico europeo o dell'OMC (Organizzazione Mondiale del Commercio) o comunque in Paesi con i quali vi siano accordi di reciprocità nel settore.

Per ciò che riguarda i contributi alla larga banda la legge finanziaria 2003, sostituendo una precedente disposizione della legge n. 57 del 2001, alla quale non era stata data attuazione, ha disposto un contributo statale pari a 75 euro alle persone fisiche o giuridiche che acquistano o noleggiano o detengono in comodato un apparato di utente per la trasmissione o la ricezione a larga banda dei dati via Internet. Questi contributi sono stati rifinanziati dall'articolo 1, comma 212 della legge finanziaria 2005 (L. 30 dicembre 2004, n. 311) per i contratti stipulati a decorrere dal 10 dicembre 2004. Rispetto alle leggi finanziarie precedenti (2003 e 2004) che prevedevano un'unica tipologia di contributo pari a 75 euro, da

[130] Il testo della legge è compreso nella documentazione allegata.
[131] Il testo del decreto è compreso nella documentazione allegata.

corrispondere per ogni contratto di abbonamento, la legge finanziaria 2005 ha differenziato il contributo: 50 euro per l'abbonamento alla larga banda, elevato a 75 euro qualora l'accesso alla rete fissa o mobile UMTS ricada nei comuni delle regioni obiettivo 1 o in quelli con popolazione inferiore a 10.000 abitanti. Nella Relazione sulle attività del Ministero delle comunicazioni presentata nel settembre 2004, si evidenzia che le leggi finanziarie 2003 e 2004 hanno stanziato, per facilitare l'accesso ad Internet in banda larga e per i *decoder* della televisione digitale terrestre, un importo complessivo di 171 milioni di euro di cui circa 61 milioni per il solo accesso ad Internet. Nella medesima Relazione si evidenzia poi che, per favorire lo sviluppo delle infrastrutture anche nelle regioni dove il *digital divide* si è progressivamente aggravato, è stato siglato nel 2003 un *Memorandum* d'intesa tra il Ministro delle Comunicazioni, il Ministro dell'Economia e delle Finanze e il Ministro per l'Innovazione e le Tecnologie, da un lato, e la Società Sviluppo Italia dall'altro, per la realizzazione di un programma finalizzato a sviluppare, in modo sinergico ed equilibrato, la rete infrastrutturale a larga banda e implementare i nuovi servizi della "società dell'informazione" nel Mezzogiorno d'Italia. Aderendo alle richieste dei Ministeri interessati, il 13 novembre 2003, il CIPE ha approvato uno stanziamento di 270 milioni di euro per lo sviluppo di nuove reti a larga banda (150 milioni di euro) e dei relativi servizi innovativi nel Mezzogiorno (120 milioni di euro).

Le procedure per l'erogazione dei contributi sono definite con un decreto interministeriale emanato dal Ministro delle comunicazioni, di concerto con il Ministro dell'economia e delle finanze: per l'anno 2005 il decreto è stato emanato il 22 febbraio 2005. Per l'attuazione si è evitato di privilegiare un operatore o una tecnologia rispetto ad un'altra. Sono stati quindi ammessi indistintamente operatori di rete e ISP (*Internet Service Provider*) e tra, gli operatori, sia coloro che offrono sistemi con accesso di tipo *wireless* o attraverso satellite. I contributi inoltre sono stati estesi anche ai contratti di abbonamento stipulati con gli operatori di rete mobile UMTS. Il contributo è erogato all'utente sotto forma di sconto effettuato direttamente dall'operatore con cui stipulato il contratto. Il rimborso per l'operatore è invece erogato direttamente dal Ministero. All'iniziativa, avviata con la legge finanziaria 2003, hanno partecipato 33 operatori di rete e ISP, di cui 13 hanno ripresentato domanda nel 2004. La procedura ha il suo punto di forza nella trasparenza. Il Ministero infatti pubblica sul proprio sito Internet una pagina informativa in cui dà conto dei lotti di autorizzazioni preventive assegnati e dell'andamento dei relativi fondi.

Va poi senz'altro menzionata la **legge n. 4 del 9 gennaio 2004**[132] (c.d. Legge Stanca) che reca norme sull'accessibilità per i soggetti diversamente abili. La legge, attuata con D.P.R. n. 75 del 1° marzo 2005, delinea, come "tecnologie assistive" "gli strumenti e le soluzioni tecniche, *hardware* e *software*, che permettono alla persona disabile, superando o riducendo le condizioni di svantaggio, di accedere alle informazioni e ai servizi erogati dai sistemi informatici" (articolo 2, comma 1). I soggetti erogatori sono individuati in capo agli enti pubblici economici, ai privati concessionari di servizi pubblici, "alle aziende municipalizzate regionali, agli enti di assistenza e riabilitazione pubblici, alle aziende di trasporto e di telecomunicazione a prevalente partecipazione di capitale pubbblico e alle aziende appaltatrici di servizi informatici". Ai suddetti soggetti è fatto divieto di stipulare contratti per realizzare o modificare siti Internet se non rispettosi dei requisiti di accessibilità per i diversamente abili. L'articolo 5 della legge dispone l'applicabilità delle norme anche al materiale formativo e didattico utilizzato nelle scuole di ogni ordine e grado.

Più in generale, in relazione al tema complessivo dello sviluppo della società dell'informazione, si rammenta che, con **D.P.C.M. del 19 settembre 2001,**[133] è stato istituito, presso la Presidenza del Consiglio dei Ministri, un Comitato dei Ministri per la Società dell'Informazione cui stato affidato il compito di "coordinare l'azione delle amministrazioni e di assicurare la definizione e la realizzazione di una strategia coerente ed unitaria per lo sviluppo della Società dell'Informazione nel Paese". Con il compito di formulare proposte al Comitato, sempre presso la Presidenza del Consiglio, è stato anche istituito il *Forum* per la Società dell'Informazione cui partecipano rappresentanti delle istituzioni pubbliche, delle parti sociali, delle associazioni, degli operatori di settore e degli utenti nonché delle aziende, delle istituzioni di ricerca e delle università.

Si ricorda inoltre che - sempre in un'ottica di attenzione verso i soggetti meno facilitati all'accesso - con **decreto ministeriale 25 luglio 2003** è stata istituita e regolamentata la commissione interministeriale per l'impiego delle tecnologie dell'informazione e della comunicazione per le categorie deboli o svantaggiate.

Quanto all'attività svolta dal predetto Comitato per la Società dell'Informazione sono da segnalare, tra le iniziative di maggiore rilievo:

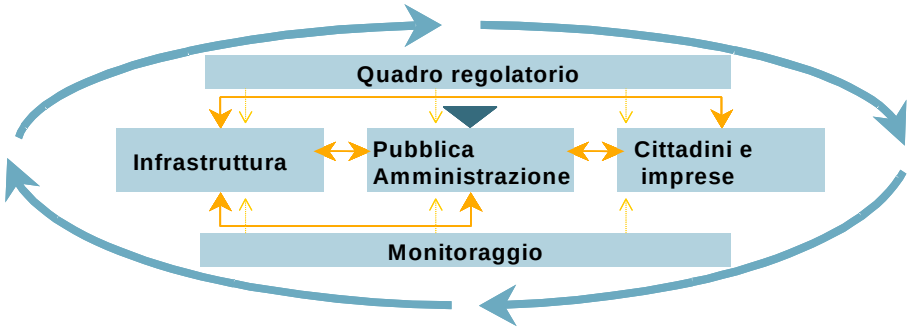
---

[132] Il testo della legge è compreso nella documentazione allegata.

[133] Successivamente integrato, per quanto riguarda la composizione del Comitato, dal D.P.C.M. del 7 febbraio 2002 e dal D.P.C.M. del 5 aprile 2002 (testi compresi nella documentazione allegata).

- l'approvazione del Piano per l'Innovazione Digitale delle Imprese (febbraio 2005);
- l'approvazione del Piano di Innovazione Digitale[134] per il Mezzogiorno (febbraio 2005);
- l'approvazione di 10 progetti assegnati a diversi dicasteri, per uno stanziamento globale di 161 milioni di euro, che hanno per obiettivo la valorizzazione della competitività del Paese, della cultura nazionale, dell'educazione e alfabetizzazione digitale, della telemedicina e dell'*e-Government* (marzo 2003).

Secondo quanto evidenziato nel **Rapporto 2003 del Ministro per l'Innovazione e le Tecnologie e del Ministro delle Comunicazioni** (*Strategia e Politiche per la larga banda in Italia*), le strategie e le politiche adottate dal Governo per la diffusione della larga banda si articolano in interventi per l'infrastruttura, la pubblica amministrazione, i cittadini e le imprese. L'evoluzione di questi interventi monitorata con continuità per assicurarne la congruità con gli obiettivi della Società dell'Informazione.



Meccanismi per lo sviluppo delle strategie governative per la larga banda

il Governo italiano - relativamente all'infrastruttura - intenderebbe raggiungere, nel breve periodo, i seguenti obiettivi:

- "politiche ed incentivi per la banda larga anche come mezzo di abbattimento del *digital divide*, secondo gli obiettivi e-*Europe* 2005;
- diffusione dell'UMTS;
- introduzione del sistema televisivo digitale terrestre DVB-T inteso altresì come strumento per la diffusione di Internet su una piattaforma molto diffusa e capillare quale il ricevitore televisivo domestico;
- introduzione del DAB ("*Digital audio broadcasting*");
- diffusione dell'accesso pubblico ai servizi Wi-Fi".

[134] Il testo del Piano è compreso nella documentazione allegata.

Sempre secondo quanto viene evidenziato nel Rapporto, il Governo "considera, inoltre, la domanda di servizi della pubblica amministrazione un fattore trainante per lo sviluppo della larga banda: infatti, essa crea le condizioni economiche per la domanda di larga banda da parte dei cittadini e delle imprese, mettendo a disposizione nuove applicazioni e servizi. L'allargamento del mercato incentiva lo sviluppo di ulteriori applicazioni tecnologiche anche da parte degli operatori privati".

L'intervento sulla domanda pubblica risulterebbe poi particolarmente efficace nel "contrastare il "*digital divide"* territoriale e sociale in quanto garantisce:

- la copertura di aree svantaggiate, dove le dinamiche di mercato, presenti e future, non garantiscono a priori la presenza della larga banda;
- l'aumento dell'alfabetizzazione digitale dei cittadini".

Sulla questione del miglioramento delle relazioni via Internet delle imprese con la pubblica amministrazione, il **Rapporto 2003 dell'Istat** [135]chiarisce che i servizi *on line* più richiesti dalle imprese sono quelli informativi (pari all'82,6 per cento). Molto richiesto è comunque anche l'accesso alle pratiche amministrative (24,9 per cento), l'effettuazione di pagamenti *on line* (16 per cento) e la partecipazione al servizio di *e-procurement* (10,4 per cento). I servizi pubblici sono utilizzati maggiormente dalle imprese con oltre 250 addetti e da quelle localizzate nel Mezzogiorno (specialmente per l'*e-procurement*). Buone risultano anche le opportunità che Internet offre al miglioramento del rapporto tra banche ed imprese. Oltre al tradizionale *corporate banking* riscuotono infatti molto successo i servizi di incasso e pagamento (utilizzazione superiore al 61 per cento) mentre sono ancora poco diffusi la richiesta di finanziamenti *on line* e il *trading on line*[136].

I principali fattori di freno allo sviluppo del mercato privato sono stati individuati nella disomogeneità della diffusione degli accessi, nella inadeguatezza di applicazioni, contenuti e servizi che richiedono l'impiego di larga banda e nel basso livello di alfabetizzazione informatica. Le azioni identificate per incentivare la larga banda per il mercato residenziale e le imprese sono focalizzate sull'accrescimento della consapevolezza dei benefici da essa indotti e, per le imprese, anche sulla reingegnerizzazione dei processi interni ed esterni necessari per garantire la competitività nel prossimo futuro".

---

[135] Il testo del rapporto è compreso nella documentazione allegata.

[136] ISTAT, op. cit., pag. 160.

D - DOCUMENTAZIONE ALLEGATA

NORMATIVA ITALIANA

Decreto del Ministro delle Poste e Telecomunicazioni 28 febbraio 1997

Tariffe promozionali per comunicazioni verso fornitori di servizi della rete Internet

(Supplemento ordinario n. 50/L GU n. 55, 7 Marzo 1997)

Il Ministro delle Poste e delle Telecomunicazioni
di concerto con il Ministro del Tesoro e del Bilancio e della Programmazione Economica

Visto il Testo Unico delle disposizioni legislative in materiale postale, di bancoposta e di telecomunicazioni, approvato con decreto del Presidente della Repubblica 29 marzo 1973 n.156;

Vista la convenzione stipulata il 1º Agosto 1984 tra il Ministero delle poste e delle telecomunicazioni e la SIP - Società italiana delle telecomunicazioni p.a. approvata con decreto del Presidente della Repubblica 13 agosto 1984, n 523;

Visto il decreto ministeriale del 6 aprile 1990 concernente l'approvazione del piano regolatore nazionale delle telecomunicazioni, e pubblicato nel supplemento ordinario alla Gazzetta Ufficiale n. 90 del 18 aprile 1990;

Visto il decreto ministeriale del 28 febbraio 1997 concernente l'adeguamento delle tariffe telefoniche nazionali, ed in particolare l'art. 22;

Visto il decreto ministeriale del 28 febbraio 1997 concernente l'adeguamento delle tariffe telefoniche internazionali;

Riconosciuta l'utilità di individuare tariffe promozionali per l'offerta sperimentale di pacchetti tariffari a favore degli utenti di categoria B e C e istituti scolastici per le comunicazioni verso fornitori di servizi della rete Internet.

DECRETA:

Art. 1

1. Compatibilmente con la disponibilità degli impianti e con le esigenze del pubblico servizio, consentito agli utenti di categoria B e C ed agli istituti scolastici per le utenze intestate a questi ultimi, l'abbonamento a condizioni promozionali, per un periodo non superiore ad otto mesi a partire dal 1º maggio 1997, alle prestazioni sperimentali di pacchetti tariffari relative alle comunicazioni di accesso e fornitori di servizio della rete Internet.

Art. 2

1. I pacchetti tariffari di cui al presente decreto sono applicati su richiesta di apposito abbonamento da parte dell'utente e degli istituti scolastici interessati.

2. Le riduzioni previste nei pacchetti tariffari di cui al presente decreto, ove richiesta, sostituiscono le altre eventuali riduzioni definite dai decreti tariffari in vigore per le utenze a basso traffico sugli impulsi di contatore non addebitati per consumi compresi tra 110 e 200 scatti/mese e per le tariffe telefoniche ridotte per elevati volumi di traffico.

3. Il richiedente deve fornire alla società concessionaria Telecom Italia, copia del contratto stipulato con il fornitore di servizi della rete Internet.

4. L'attivazione in via sperimentale delle condizioni promozionali previste dai pacchetti tariffari di cui al presente decreto ha corso a partire dal mese successivo a quello di ricezione della richiesta.

Art. 3

1. Le condizioni tariffarie applicate all'abbonato aderente ali pacchetti tariffari di cui all'art. 1, sono stabiliti nelle unite tabelle 1 -- 2 -- 3 che costituiscono parte integrante del presente decreto.

Art. 4

1. Il presente decreto entra in vigore dal giorno successivo a quello della pubblicazione sulla Gazzetta Ufficiale della Repubblica Italiana.

Tabella 1

PACCHETTO TARIFFARIO "AMICI MIEI"

Agli abbonati di categoria B e C sottoscrittori del contratto di abbonamento al presente pacchetto tariffario si applicano le seguenti condizioni:

Condizione tariffaria A):

riduzione del 15% sulle tariffe relative a comunicazioni svolte verso tre numeri telefonici nazionali di fornitori di informazione Internet.
Canone mensile supplementare:
lire 3.000 per comunicazioni svolte sulla Rete Telefonica Generale;
lire 5.000 per comunicazioni svolte sulla rete ISDN.

Condizione tariffaria B):

riduzione del 15% sulle tariffe telefoniche relative a comunicazioni svolte verso due numeri telefonici nazionali ed uno internazionale di fornitori di informazioni Internet.
Canone mensile supplementare:

lire 5.000 per comunicazioni svolte sulla Rete Telefonica Generale;
lire 10.000 per comunicazioni svolte sulla rete ISDN.

Tabella 2

PACCHETTO TARIFFARIO "LONG TIME"

Agli abbonati di categoria B e C sottoscrittori del contratto di abbonamento al presente pacchetto tariffario si applicano le seguenti condizioni:

per ogni comunicazione si applica una riduzione del 50% sulle tariffe telefoniche relative alla parte di comunicazione che eccede i primi 15 minuti di durata della comunicazione stessa.
La riduzione di cui al comma precedente si applica alle comunicazioni urbane e settoriali dalle ore 18,30 alle ore 22,00 dei giorni feriali escluso il sabato, dalle ore 13,00 alle ore 22,00 del sabato; dalle ore 8,00 alle ore 22,00 dei giorni festivi; dalle ore 0,00 alle ore 8,00 e dalle ore 22,00 alle ore 24,00 di tutti i giorni.

Canone mensile supplementare:
lire 1.500 per comunicazioni svolte sulla Rete Telefonica Generale;
lire 3.000 per comunicazioni svolte sulla rete ISDN.

Tabella 3

PACCHETTO TARIFFARIO "LONG STUDY"

Alle utenze telefoniche intestate agli istituti scolastici sottoscrittori del contratto di abbonamento al presente pacchetto tariffario si applicano le seguenti condizioni:

per ogni comunicazione si applica una riduzione del 50% sulle tariffe telefoniche relative alla parte di comunicazione che eccede i primi 15 minuti di durata della comunicazione stessa.
La riduzione di cui al comma precedente si applica alle comunicazioni urbane e settoriali dalle ore 8,30 alle ore 13,00 dei giorni feriali escluso il sabato, dalle ore 8,00 alle ore 8,30 e dalle ore 13,00 alle ore 18,30 dei giorni feriali escluso il sabato; dalle ore 8,00 alle ore 13,00 del sabato.

Canone mensile supplementare:
lire 3.500 per comunicazioni svolte sulla Rete Telefonica Generale;
lire 7.500 per comunicazioni svolte sullla rete ISDN.

D.P.C.M. del 19 settembre 2001

Istituzione del Comitato dei Ministri per la Società dell'Informazione

IL Presidente del Consiglio dei Ministri

VISTO il decreto legislativo 30 luglio 1999, n. 303;

VISTA la legge 23 agosto 1988, n. 400 recante la "Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri";

CONSIDERATO che il Governo ritiene lo sviluppo della Società dell'Informazione un obiettivo fondamentale della propria azione;

DECRETA:

Art. 1

1. Presso la Presidenza del Consiglio dei Ministri è istituito un Comitato dei Ministri per la Società dell'Informazione, con il compito di coordinare l'azione delle amministrazioni e di assicurare la definizione e la realizzazione di una strategia coerente ed unitaria per lo sviluppo della Società dell'Informazione nel Paese.

2. Il Comitato è composto dal Ministro per l'innovazione e le tecnologie, che lo presiede, dal Sottosegretario di Stato alla Presidenza del Consiglio dei Ministri con funzioni di Segretario del Consiglio stesso e dai Ministri per le attività produttive, per l'attuazione del programma di Governo, per i beni culturali, per le comunicazioni, dell'economia e delle finanze, per la funzione pubblica, dell'interno, del lavoro e delle politiche sociali, per le politiche comunitarie, della pubblica istruzione, università e ricerca scientifica, della salute. Alle riunioni del Comitato possono essere invitati a partecipare altri Ministri interessati agli argomenti da trattare.

Art. 2

1. Presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, è istituito il Forum per la Società dell'Informazione con il compito di formulare proposte al Comitato dei Ministri finalizzate allo sviluppo della Società dell'Informazione.

2. Il Forum presieduto dal Ministro per l'innovazione e le tecnologie. Il Comitato dei Ministri di cui all'art.1 definisce la partecipazione al Forum delle istituzioni pubbliche, delle parti sociali, delle associazioni, degli operatori del settore e degli utenti, delle aziende e degli altri soggetti coinvolti, delle istituzioni della ricerca e dell'università e ne specifica le attività e le modalità di lavoro.

Art. 3

1. Al fine di assicurare il necessario supporto tecnico ai lavori del Comitato dei Ministri di cui all'art.1, presso la Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, costituito un gruppo di studio e di lavoro.

2. Il Ministro per l'innovazione e le tecnologie nomina il coordinatore del gruppo di studio e di lavoro, che assume anche le funzioni di coordinatore del Forum. Fa parte del gruppo un rappresentante del Dipartimento per l'informatica, la telematica e la statistica ed un rappresentante di ciascuna delle amministrazioni di cui all'art.1, comma 2. Il gruppo può richiedere la partecipazione e la collaborazione di esperti.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI - DIPARTIMENTO DELLA FUNZIONE PUBBLICA

D.P.C.M. 7 febbraio 2002

Attività di comunicazione delle pubbliche amministrazioni.

Vista la legge 23 agosto 1988, n. 400, recante "Disciplina dell'attivita' di Governo e ordinamento della Presidenza del Consiglio dei Ministri";

Visto il decreto legislativo 30 marzo 2001, n. 165, recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";

Vista la legge 7 giugno 2000, n. 150 "Disciplina delle attivita' di informazione e di comunicazione delle pubbliche amministrazioni";

Visto il decreto del Presidente della Repubblica del 21 settembre 2001, n. 422, recante "Regolamento per l'individuazione dei titoli professionali del personale da utilizzare presso le pubbliche amministrazioni per le attivita' di informazione e comunicazione e disciplina degli interventi formativi";

Visto il decreto del Presidente del Consiglio dei Ministri del 9 agosto 2001, recante "Delega di funzioni del Presidente del Consiglio dei Ministri in materia di funzione pubblica e di coordinamento dei servizi di informazione e sicurezza al Ministro senza portafoglio on. dott. Franco Frattini";

Visto il decreto del Presidente del Consiglio dei Ministri del 31 ottobre 2001, recante "Struttura di missione per la comunicazione e informazione ai cittadini";

Vista la direttiva del Ministro per la funzione pubblica del 13 dicembre 2001, sulla formazione e la valorizzazione del personale delle pubbliche amministrazioni;

E M A N A

la presente direttiva:

Premessa.

Con l'entrata in vigore della legge del 7 giugno 2000, n. 150, e l'emanazione del regolamento di attuazione del 21 settembre 2001, n. 422, le pubbliche amministrazioni dispongono di un nuovo indispensabile strumento per sviluppare le loro relazioni con i cittadini, potenziare e armonizzare i flussi di informazioni al loro interno e concorrere ad affermare il diritto dei cittadini ad

un'efficace comunicazione. La comunicazione pubblica cessa di essere un segmento aggiuntivo e residuale dell'azione delle pubbliche amministrazioni, e ne diviene parte

integrante, cosi' come accade da decenni alle imprese che agiscono nel mercato dei prodotti e dei servizi. Lo sviluppo delle attivita' legate alla comunicazione di impresa e alla pubblicita', in grado di determinare scelte organizzative e strategiche che influiscono positivamente sulla visibilita' e sull'immagine aziendale e che coinvolgono trasversalmente tutto il processo produttivo, attraverso azioni di comunicazione interna, hanno accompagnato nel nostro Paese il percorso e la crescita delle imprese del settore privato e, recentemente, anche di alcune pubbliche amministrazioni. La riforma della pubblica amministrazione, il federalismo e il rafforzamento dei livelli locali di governo, l'attuazione del principio di sussidiarieta' e il conseguente nuovo orizzonte delle missioni delle amministrazioni, possono realizzarsi solo con il pieno consenso dei cittadini e delle imprese, degli operatori del settore pubblico, da coinvolgere attraverso opportuni ed adeguati processi di relazione e comunicazione.

Finalita' e ambito di applicazione.

Con questa direttiva il Dipartimento della funzione pubblica, in linea con la volonta' del Governo di attuare un radicale processo di cambiamento della Pubblica amministrazione, fornisce alle amministrazioni pubbliche, di cui all'art. 1, comma 2, del decreto del Presidente della Repubblica 21 settembre 2001, n. 422, gli indirizzi di coordinamento, organizzazione e monitoraggio delle strutture, degli strumenti e delle attivita' previste dalla normativa in materia di informazione e comunicazione pubblica. La direttiva si propone di contribuire al perseguimento, da parte delle pubbliche amministrazioni, delle seguenti finalita':

sviluppo di una coerente politica di comunicazione integrata con i cittadini e le imprese; gestione professionale e sistematica dei rapporti con tutti gli organi di informazione (mass media tradizionali e nuovi);

realizzazione di un sistema di flussi di comunicazione interna incentrato sull'intenso utilizzo di tecnologie informatiche e banche dati, sia per migliorare la qualita' dei servizi e l'efficienza organizzativa, sia per creare tra gli operatori del settore pubblico senso di appartenenza alla funzione svolta, pieno coinvolgimento nel processo di cambiamento e condivisione nelle rinnovate missioni istituzionali delle pubbliche amministrazioni;

formazione e valorizzazione del personale impegnato nelle attivita' di informazione e comunicazione;

ottimizzazione, attraverso la pianificazione e il monitoraggio delle attivita' di informazione e comunicazione, dell'impiego delle risorse finanziarie.

Questa direttiva, pertanto, richiama e impegna la responsabilita' dei vertici delle amministrazioni pubbliche all'applicazione della legge n. 150/2000 e alla definizione di strutture e risorse necessarie per:

progettare e realizzare attivita' di informazione e comunicazione destinate ai cittadini e alle imprese;

procedere ad una rinnovata ingegneria dei processi di comunicazione interna e adeguare i flussi di informazione a supporto dell'attivita' degli uffici che svolgono attivita' di informazione e comunicazione, e il loro coordinamento, gia' individuati dalla legge n. 150/2000;

produrre e fornire informazioni, promuovere eventi che, tenendo conto dei tempi e dei criteri che regolamentano il sistema dei media, possano tradursi in notizie per i mass media tradizionali e nuovi - come i giornali on-line - e altri mezzi di diffusione di notizie di interesse pubblico.

La direttiva, inoltre, pone all'attenzione dei dirigenti degli uffici stampa e degli Urp, cosi' come delle analoghe strutture previste dalla legge n. 150/2000, la ricerca dell'efficienza e dell'efficacia nei processi di produzione della comunicazione, quale obiettivo della loro attivita'.

1. Gli obiettivi.

Le pubbliche amministrazioni, attraverso gli uffici stampa, i portavoce e gli Urp e le analoghe strutture, devono:

1) garantire un'informazione trasparente ed esauriente sul loro operato;

2) pubblicizzare e consentire l'accesso ai servizi promuovendo nuove relazioni con i cittadini;

3) ottimizzare l'efficienza e l'efficacia dei prodotti-servizi attraverso un adeguato sistema di comunicazione interna.

Per consentire il pieno raggiungimento di questi obiettivi, le pubbliche amministrazioni devono:

1) dare avvio e sviluppo alle strutture deputate alla realizzazione delle attivita' di informazione, portavoce e ufficio stampa, e di comunicazione, ufficio per le relazioni con il pubblico;

2) promuoverne il pieno raccordo operativo sotto forma di coordinamento e attraverso una adeguata struttura organizzativa. Inoltre, nella creazione dei nuovi profili professionali e delle nuove forme di organizzazione del lavoro pubblico e della sua comunicazione interna, deve essere favorita la definizione di adeguati interventi formativi e di aggiornamento che promuovano operatori dell'informazione e comunicazione competenti e motivati. Il Dipartimento della funzione pubblica, con la collaborazione delle associazioni professionali del mondo dell'informazione, della comunicazione e delle relazioni pubbliche, realizzera' un sistema di monitoraggio dell'applicazione della legge n. 150/2000 anche in vista di una programmazione di successivi interventi e direttive che avranno come obiettivo di rendere il settore coerente con la dimensione europea.

2. Tipologia della comunicazione.

La legge n. 150/2000 indica quali figure capaci di realizzare le attivita' di informazione e comunicazione nell'amministrazione pubblica il portavoce e l'ufficio stampa, da un lato, e l'ufficio per le relazioni con il pubblico e analoghe strutture, dall'altro. I due segmenti di attivita' individuati sono importanti, ma non singolarmente esaustivi della funzione di comunicazione la cui complessita' si esprime sia attraverso la previsione di differenti tipologie professionali, sia attraverso attivita' che non si esauriscono nel front-office o nei rapporti con i media. La comunicazione interna e la produzione di messaggi complessi verso l'esterno rappresentano momenti differenti della stessa funzione di informazione e comunicazione delle pubbliche amministrazioni, e pertanto richiedono un coordinamento che ne governi, con efficacia, le interazioni e le sinergie. Questa dimensione complessiva e integrata della comunicazione non puo' essere dimenticata ne' sottovalutata nell'attuazione della legge del 7 giugno 2000, n. 150. Nello svolgimento delle attivita' di comunicazione e informazione, cosi' come nella costruzione degli assetti organizzativi delle loro strutture, le amministrazioni devono, inoltre, considerare centrali e decisivi gli strumenti interattivi della comunicazione on line (Internet-intranet). I processi organizzativi devono, conseguentemente, essere ridisegnati in relazione all'esigenza di sviluppare modalita' interattive di comunicazione interna ed interistituzionale nei confronti dei cittadini. Una buona comunicazione interna, fondata su di un'ampia circolazione delle informazioni sulle attivita' ed i processi lavorativi, e il pieno coinvolgimento del personale nei progetti di cambiamento organizzativo, consente di costruire al meglio l'identita' di un'amministrazione, favorisce la crescita di un senso di appartenenza positivo alla dimensione del lavoro pubblico e contribuisce a porre su nuove basi l'immagine della sfera pubblica.

3. Modalita' operative: il coordinamento degli strumenti della comunicazione.

Le amministrazioni devono assicurare il raccordo operativo tra i segmenti di comunicazione attivati, il portavoce, l'ufficio stampa e l'ufficio per le relazioni con il pubblico e le analoghe strutture, devono prevedere forme organizzative di coordinamento delle loro attivita' per massimizzare l'utilizzo delle risorse umane ed economiche, e creare sinergie ed integrazione tra le azioni di comunicazione per contribuire a rendere efficaci e soddisfacenti le relazioni con i cittadini. Ciascuna amministrazione, quindi, potra' istituire al proprio interno una struttura di coordinamento, costituita dal direttore dell'Urp e delle analoghe strutture ove esistenti, dal direttore dell'ufficio stampa e dal portavoce se presente all'interno dell'amministrazione. La struttura di coordinamento ha funzioni di programmazione, indirizzo e raccordo delle attivita' da realizzare. Alla struttura di coordinamento spetta il compito di presentare al vertice dell'amministrazione, entro il 30 novembre di ogni anno, il programma delle iniziative di comunicazione.

Il programma deve contenere:

la definizione degli obiettivi e della strategia della comunicazione integrata (azioni di comunicazione interna, esterna, on-line, pubblicitaria etc.);

la descrizione delle singole azioni con l'indicazione dei tempi di realizzazione (calendarizzazione per fasi);

la scelta dei mezzi di diffusione e il budget;

la pianificazione delle attivita' di monitoraggio e valutazione dell'efficacia delle azioni (sia in itinere al progetto sia ex post).

3.1. La struttura di missione per l'informazione e la comunicazione con i cittadini. Per soddisfare l'esigenza di raccordo operativo e d'integrazione tra le strutture di informazione e comunicazione previste della legge del 7 giugno 2000, n. 150, il Dipartimento della funzione pubblica ha attivato un'apposita "Struttura di missione", con l'incarico di:

1) integrare le proprie attivita' di comunicazione ed informazione (ufficio stampa, Urp, sito web) coordinandole con l'ufficio del portavoce;

2) supportare le amministrazioni nell'attuazione delle norme per sviluppare e sperimentare azioni e progetti di comunicazione pubblica integrata.

La struttura di missione ha l'obiettivo di garantire l'attuazione della legge del 7 giugno 2000, n. 150, di monitorare l'attivazione di strutture di comunicazione integrata presso le amministrazioni, nonché di fornire consulenza alle amministrazioni anche per l'attivita' di formazione, limitatamente al settore della comunicazione. Presso la struttura, inoltre, operano gruppi di lavoro specializzati sull'applicazione della legge e sull'uso di un linguaggio chiaro e comprensibile da parte delle amministrazioni.

4. Funzioni degli organi dell'informazione e della comunicazione.

Un moderno sviluppo dell'informazione e della comunicazione richiede un decisivo impegno delle amministrazioni. Particolare attenzione deve essere posta ai compiti che la legge affida agli Urp, attraverso la realizzazione delle reti civiche e del sito Internet della pubblica amministrazione, nella loro funzione di relazione verso l'esterno. Essi svolgono infatti compiti di informazione, di garanzia di accesso ai servizi, di ascolto delle esigenze degli utenti, di promozione dell'innovazione e della semplificazione, nonché di verifica della soddisfazione del cittadino rispetto all'erogazione dei servizi stessi. In questo contesto, gli uffici per le relazioni con il pubblico e le analoghe strutture devono poter ricorrere a procedure di comunicazione interna codificate ed efficaci per divenire il terminale di destinazione di atti e documenti che consentano sollecite ed esaurienti risposte alle richieste dei cittadini. Nei casi piu' complessi, gli Urp devono poter disporre della documentazione utile alla soddisfazione dell'utente entro un tempo ragionevole, comunque predeterminato dalle amministrazioni di appartenenza che individueranno, del pari, le sanzioni in caso di inadempienza o di ritardo nella risposta. Al fine di rendere gli Urp strumenti del cambiamento interno della Pubblica amministrazione, attraverso una funzione di marketing istituzionale e di verifica della soddisfazione del cittadino rispetto all'erogazione dei servizi, opportuno che essi siano in grado di progettare e sviluppare azioni di studio e ricerca attraverso risorse umane in possesso delle competenze necessarie. L'incarico di gestione delle reti civiche,

assegnato dalla legge n. 150/2000 agli Urp, e del sito Internet, destinato ad espandere la dimensione di questi uffici da semplice sportello di informazione al cittadino a terminali di banche dati. Gli Urp devono pertanto essere in grado di svolgere piu' funzioni e di corrispondere ad una domanda differenziata di servizi da parte del cittadino. La stessa legge n. 150/2000 attribuisce all'ufficio stampa, prioritariamente, la gestione dell'informazione in collegamento con gli organi di informazione mezzo stampa, radiofonici, televisivi ed on line. In particolare l'ufficio stampa, coordinato da un direttore di servizio, si occupa:

- della redazione di comunicati riguardanti sia l'attivita' dell'amministrazione e del suo vertice istituzionale sia quella di informazione, promozione, lancio dei servizi;

- dell'organizzazione di conferenze, incontri ed eventi stampa;

- della realizzazione di una rassegna stampa quotidiana o periodica, anche attraverso strumenti informatici; del coordinamento e della realizzazione della newsletter istituzionale e di altri prodotti editoriali. Nelle amministrazioni locali di piccole dimensioni, per meglio ottimizzare le loro funzioni, gli uffici stampa, cosi' come gli uffici per le relazioni con il pubblico, possono essere costituiti in forma consorziata tra enti locali che raggruppino una popolazione residente non inferiore a 25.000 unita'. A differenza dell'ufficio stampa e dei suoi compiti istituzionali, la figura del portavoce, presente nelle amministrazioni complesse, sviluppa un'attivita' di relazioni con gli organi di informazione in stretto collegamento ed alle dipendenze del vertice "pro tempore" delle amministrazioni.

5. La formazione.

La legge del 7 giugno 2000, n. 150, e il regolamento del 21 settembre 2001, decreto del Presidente della Repubblica n. 422, e piu' specificatamente la direttiva del Ministro per la funzione pubblica del 13 dicembre 2001, sulla "Formazione e la valorizzazione del personale delle pubbliche ammistrazioni", individuano nella formazione la chiave per migliorare la qualita' delle prestazioni e per incentivare la motivazione del personale. La normativa offre alle amministrazioni i primi strumenti per adeguare, migliorare, selezionare - attraverso la definizione di percorsi di formazione ad hoc - le risorse umane gia' indirizzate o da indirizzare nei settori delle relazioni con i media (ufficio stampa e ufficio del portavoce) e con i cittadini (uffici delle relazioni con il pubblico e analoghe strutture). E' da tenere presente che le attivita' di informazione e comunicazione - svolte all'interno di queste strutture - sono considerate rilevanti per la concreta realizzazione di pratiche di buon governo. Le norme sopraindicate sanciscono una parita' dell'offerta formativa con la presenza di soggetti privati e di una cultura di mercato dal cui confronto e competizione deve derivare un miglioramento complessivo della qualita' della formazione in questo settore. La formazione, oltre ad avere il compito di professionalizzare le risorse umane, dovra' essere la leva primaria per rendere omogeneo il livello di preparazione e la capacita' del personale impegnato nella comunicazione pubblica. In considerazione di cio' le amministrazioni devono adottare programmi formativi per tutto il personale impegnato nell'attivita' di informazione e

comunicazione come previsto dalle norme vigenti e dalla direttiva del 13 dicembre 2001. L'attivita' formativa dei singoli dipendenti svolta nel periodo intercorso tra l'entrata in vigore della legge n. 150/2000 e la pubblicazione del regolamento (decreto del Presidente della Repubblica n. 422/2001), che rispetti i requisiti previsti dalle due norme, su richiesta delle amministrazioni di appartenenza, potra' essere validata da una commissione, istituita presso la struttura di missione del Dipartimento della funzione pubblica.

6. I nuovi profili professionali.

L'individuazione e la regolamentazione delle tipologie professionali che opereranno negli uffici stampa, negli uffici per le relazioni con il pubblico e in strutture analoghe utilizzando strumenti di informazione e comunicazione tradizionali e nuovi, come indicato dall'art. 8, comma 3, ed art. 9, comma 5, della legge del 7 giugno 2000, n. 150, sono affidate alla contrattazione collettiva con le organizzazioni sindacali rappresentative sul territorio nazionale delle categorie professionali.

7. Il monitoraggio delle attivita'.

Il Dipartimento della funzione pubblica ha gia' promosso e sviluppera' in modo costante sondaggi, studi, ricerche e sperimentazioni finalizzate a:

1) monitorare lo stato di attuazione della legge del 7 giugno 2000, n. 150;

2) verificare le inadeguatezze da questa gia' rivelate nel lungo dibattito che ne ha accompagnato la pur necessaria approvazione (dall'esigenza di meglio definire gli ambiti delle singole professionalita', ai rilievi mossi anche in sede europea circa gli accessi a taluni ruoli ed uffici);

3) promuovere modelli e standard di riferimento che favoriscano la nascita e lo sviluppo di una cultura della comunicazione integrata nell'ambito delle pubbliche amministrazioni.

Nell'ambito di tale attivita', che sara' sviluppata in collaborazione con le associazioni di categoria e gli ordini professionali dei comunicatori, delle relazioni pubbliche e dei giornalisti, grande attenzione verra' dedicata alla costruzione di tipologie professionali e modelli di valutazione delle professionalita' della nuova comunicazione pubblica e dell'efficacia del loro agire. Si tratta di tenere sotto osservazione la qualita' dei servizi e delle attivita', di valutare le performance e "validare" i risultati. Le amministrazioni, a tal fine, dovranno verificare, attraverso sondaggi, studi e ricerche, da affidare anche a soggetti privati, l'attuazione del piano di comunicazione annuale e misurarne l'efficacia.

8. Il linguaggio.

Il Dipartimento della funzione pubblica ha gia' promosso e realizzato, a partire dai primi anni '90, progetti dedicati alla semplificazione del linguaggio amministrativo usato nei contatti con i cittadini. L'opinione pubblica, ma anche le amministrazioni, si aspettano ulteriori sforzi per combattere e rendere il cosiddetto "burocratese" piu' chiaro ed

accessibile e la comunicazione tra i cittadini e la pubblica amministrazione piu' snella ed efficace. La comunicazione delle pubbliche amministrazioni deve soddisfare i requisiti della chiarezza, semplicita' e sinteticita' e, nel contempo, garantire completezza e correttezza dell'informazione. Questo obiettivo dovra' essere perseguito anche con l'impiego dei nuovi strumenti informatici. Il Dipartimento della funzione pubblica attivera' nei prossimi mesi, presso la struttura di missione, un servizio di consulenza il cui scopo sara' di assistere le pubbliche amministrazioni e i gestori di servizi pubblici a riscrivere atti e documenti, a migliorare la qualita' della comunicazione per renderla piu' semplice e comprensibile a tutti i cittadini ed utenti dei servizi pubblici. L'obiettivo sara' di quello di rendere ufficiali le regole della semplificazione e di promuoverne la diffusione in tutte le amministrazioni.

9. Le risorse.

Le amministrazioni si impegnano a individuare nel proprio bilancio un capitolo dedicato alle spese complessive per la comunicazione e informazione pubblica in una percentuale non inferiore al 2% delle risorse generali.

10. Osservanza della direttiva.

La dirigenza verra' valutata, ai sensi del decreto legislativo del 30 luglio 1999, n. 286, e del decreto legislativo del 30 marzo 2001, n. 165, anche alla luce dell'applicazione della presente direttiva. Pertanto i vertici dell'amministrazione, in sede di emanazione della direttiva annuale e degli indirizzi strategici, indicheranno le misure di comunicazione istituzionale da adottare e gli obiettivi da raggiungere in linea con il programma di governo dell'Amministrazione pubblica.

DPCM del 5 aprile 2002

Integrazione all'art. 1, comma 2 del decreto del 19 settembre 2001 di istituzione di un Comitato
dei Ministri perla Società dell'Informazione

IL Presidente del Consiglio dei Ministri

Visto il decreto legislativo 30 luglio 1999, n. 303;

Visto il decreto del Presidente del Consiglio dei Ministri 19 settembre 2001 con il quale stato istituito il "Comitato dei Ministri per la Società dell'Informazione" con il compito di coordinare l'azione delle amministrazioni e di assicurare la definizione e la realizzazione di una strategia coerente ed unitaria per lo sviluppo della Società dell'Informazione nel Paese;

VISTO il decreto del Presidente del Consiglio dei Ministri 7 febbraio 2002 di integrazione della composizione del Comitato dei "Ministri per la Società dell 'Informazione con il Ministro degli affari esteri;

CONSIDERATO che il Ministro per gli affari regionali ha avviato un'intensa attività di informatizzazione all'interno dei suoi uffici, e soprattutto lo sviluppo della rete informatica con le Regioni;

CONSIDERATA la necessità di definire le strategie politiche funzionali allo sviluppo della Società dell'Informazione integrando l'attività di Governo con le specifiche esigenze delle autonomie territoriali;

RITENUTO pertanto necessario integrare il decreto del Presidente del Consiglio dei Ministri 19 settembre 2001 con l'inserimento del Ministro per gli affari regionali in seno al Comitato dei Ministri per là Società dell'informazione

DECRETA:

Art. 1

La composizione del Comitato dei Ministri per la Società dell'Informazione di cui al decreto del Presidente del Consiglio dei Ministri 19 settembre 2001 integrata dal Ministro degli Affari Regionali.

L. 8 aprile 2002 n. 59

Disciplina relativa alla fornitura di servizi di accesso ad Internet.

Articolo 1.

1. Gli operatori autorizzati ai servizi di trasmissione dati e accesso ad Internet (Internet service provider) ai sensi del decreto legislativo 17 marzo 1995, n. 103, e del regolamento di cui al decreto del Presidente della Repubblica 4 settembre 1995, n. 420, nonché ai sensi della Del.Aut.gar.com. n. 467/00/CONS del 19 luglio 2000, pubblicata nella Gazzetta Ufficiale n. 184 dell'8 agosto 2000, e delle successive delibere, hanno diritto di fruire delle condizioni economiche applicate agli organismi di telecomunicazioni titolari di licenza individuale sulla base dell'offerta di interconnessione di riferimento pubblicata da un organismo di telecomunicazioni notificato quale avente significativo potere di mercato (SPM), secondo criteri definiti dalla medesima Autorità per le garanzie nelle comunicazioni entro due mesi dalla data di entrata in vigore della presente legge. Entro il medesimo termine l'Autorità per le garanzie nelle comunicazioni è tenuta ad aggiornare l'elenco degli operatori aventi significativo potere di mercato sul mercato dell'accesso ad Internet per gli effetti di cui agli articoli 4, 5, 7, 8 e 9 del regolamento di cui al decreto del Presidente della Repubblica 19 settembre 1997, n. 318 (2).

2. Gli accordi di interconnessione tra i fornitori di servizi Internet e un organismo avente significativo potere di mercato sono stipulati in conformità alla normativa vigente e alle delibere dell'Autorità per le garanzie nelle comunicazioni.

3. Le disposizioni di cui ai commi 1 e 2 si applicano per ogni tipo di tariffa applicata dagli operatori autorizzati ai servizi di trasmissione dati e accesso ad Internet.

4. Le disposizioni di cui ai commi 1, 2 e 3 si applicano per il periodo di tre anni a decorrere dalla data di entrata in vigore della presente legge.

DECRETO 28 maggio 2003

Condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti ed ai servizi di telecomunicazioni

ALLEGATO A

IL MINISTRO DELLE COMUNICAZIONI
Vista la legge 31 luglio 1997, n. 249;

Visto il decreto-legge 23 gennaio 2001, n. 5, convertito, con modificazioni, dalla legge 20 marzo 2001, n. 66;

Visto il decreto-legge 12 giugno 2001, n. 217, convertito, con modificazioni, dalla legge 3 agosto 2001, n. 317;

Vista la legge 1° agosto 2002, n. 166, ed, in particolare, l'art. 41 recante norme di riassetto in materia di telecomunicazioni;

Vista la legge 16 gennaio 2003, n. 3 ed, in particolare, l'art. 41 recante norme in materia di tecnologie delle comunicazioni;

Visto il decreto del Presidente della Repubblica 29 marzo 1973, n. 156;

Visto il decreto del Presidente della Repubblica 19 settembre 1997, n. 318, e successive modificazioni;

Visto il decreto del Presidente della Repubblica 5 ottobre 2001, n.447;

Visto il decreto ministeriale 20 febbraio 2003, recante modifica del Piano nazionale di ripartizione delle frequenze pubblicato nella Gazzetta Ufficiale n. 50 del 1° marzo 2003;

Vista la delibera dell'Autorità per le garanzie nelle comunicazioni (di seguito l'Autorita) n. 467/00/Cons del 19 luglio 2000, «Disposizioni in materia di autorizzazioni generali», pubblicata nella Gazzetta Ufficiale n. 184 dell'8 agosto 2000;

Vista la delibera dell'Autorità n. 236/01/Cons «Regolamento per l'organizzazione e la tenuta del registro degli operatori di comunicazioni» pubblicata nella Gazzetta Ufficiale n. 150 del 30 giugno 2001;

Vista la raccomandazione della Commissione europea relativa alla armonizzazione della fornitura dell'accesso Radio-LAN del pubblico alle reti e ai servizi pubblici di comunicazione elettronica nella Comunità del 20 marzo 2003, che prevede la possibilità di un regime di autorizzazione generale per la fornitura di tali servizi;

Considerato che, secondo quanto previsto dalla citata raccomandazione, non devono esistere discriminazioni tra i vari sistemi Radio-LAN e le altre tecnologie che danno accesso alle reti e ai servizi di comunicazione e che le condizioni di accesso alla proprietà pubblica e privata da parte dei fornitori di servizi di accesso Radio-LAN del pubblico sono subordinate alle norme in materia di concorrenza stabilite dal trattato e, ove pertinente, alle disposizioni della direttiva 2002/21/CE del Parlamento europeo e del Consiglio quadro del 7 marzo 2002 (direttiva quadro);

Tenuto conto delle competenze dell'Autorità per le garanzie nelle comunicazioni in materia di telecomunicazioni stabilite dalla normativa vigente;

Viste le direttive 2002/19/CE, 2002/20/CE, 2002/21/CE e 2002/22/CE, del Parlamento europeo e del Consiglio del 7 marzo 2002 e considerato che il regime dell'autorizzazione generale per la fornitura dell'accesso del pubblico alle reti e ai servizi pubblici di comunicazione elettronica nella Comunità conforme ai principi delle direttive medesime;

Considerato che ai sensi della direttiva 2002/20/CE (direttiva autorizzazioni) ogniqualvolta sia possibile e soprattutto qualora il rischio di interferenze dannose sia trascurabile, l'uso delle frequenze non deve essere subordinato alla concessione di diritti individuali d'uso;

Considerato che le applicazioni Radio-LAN utilizzano frequenze ad uso collettivo che non hanno diritto a protezione e non debbono provocare interferenze ad altri servizi e che, pertanto, l'uso delle relative frequenze non va subordinato alla concessione di diritti d'uso individuali;

Considerata l'opportunità di fissare le condizioni per il rilascio delle autorizzazioni generali per la fornitura al pubblico dell'accesso Radio-LAN alle reti e ai servizi di telecomunicazioni, in accordo con l'art. 1 del citato decreto 20 febbraio 2003 modificativo del Piano nazionale di ripartizione delle frequenze e nelle more dell'adozione della normativa di recepimento delle citate direttive europee prevista dall'art. 41 della legge 1° agosto 2002, n. 166;

Sentiti gli operatori di telecomunicazioni e le associazioni rappresentative del settore in audizione congiunta con l'Autorità per le garanzie nelle comunicazioni in data 17 aprile 2003;

Visto il parere del Consiglio superiore delle comunicazioni espresso nell'adunanza n. 182 del 22 maggio 2003;

DECRETA:

Art. 1
Definizioni

1. Ai fini del presente decreto si intendono per:

a) «Radio Local Area Network (di seguito denominate "Radio LAN" o "R-LAN")»: un sistema di comunicazioni in rete locale mediante radiofrequenze che utilizza apparati a corto raggio secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, nelle seguenti bande di frequenza: 2.400,0-2.483,5 MHz (brevemente banda a 2.4 GHz), 5.150-5.350 MHz, 5.470-5.725 MHz (brevemente bande a 5 GHz)»;

b) «access point»: strumento di accesso per un numero variabile di utenti tra la rete Radio-LAN e la struttura di rete di telecomunicazioni;

c) «codici di abilitazione e identificazione»: codici forniti dall'impresa autorizzata all'abbonato per identificarlo univocamente e verificarne l'abilitazione all'accesso alla rete tramite l'access point;

d) «autorizzazione generale»: un'autorizzazione che ottenuta su semplice dichiarazione di inizio attività.

2. Ai fini del presente decreto si applicano le definizioni di cui all'art. 1, comma 1, del decreto del Presidente della Repubblica 19 settembre 1997, n. 318.

Art. 2

Oggetto ed ambito di applicazione

1. Il presente provvedimento fissa le condizioni per il conseguimento dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio-LAN nella banda 2,4 GHz o nelle bande 5 GHz, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni, in locali aperti al pubblico o in aree confinate a frequentazione pubblica quali aeroporti, stazioni ferroviarie e marittime e centri commerciali.

2. Ai fini della limitazione delle interferenze dannose ad altri servizi previsti dal Piano nazionale di ripartizione delle frequenze, gli *access point* operanti nella banda 5.150-5.350 MHz possono essere installati all'interno di edifici secondo le caratteristiche tecniche di cui alla nota 184 del Piano nazionale di ripartizione delle frequenze come modificato dal decreto del Ministro delle comunicazioni 20 febbraio 2003, pubblicato nella Gazzetta Ufficiale n. 50 del 1° marzo 2003.

Art. 3

Procedura per il conseguimento dell'autorizzazione generale

1. La fornitura del servizio di cui all'art. 2 subordinata ad un'autorizzazione generale secondo le condizioni di cui all'art. 6.

2. Il soggetto che intende fornire il servizio di cui all'art. 2, avente sede in ambito nazionale o in uno dei Paesi dello Spazio economico europeo (SEE), in uno dei Paesi appartenenti all'Organizzazione mondiale del commercio (OMC), o in altri Paesi con i

quali vi siano accordi di reciprocità nel settore disciplinato dal presente provvedimento, farà comunque salva ogni eventuale limitazione derivante da accordi internazionali, tenuto a presentare al Ministero delle comunicazioni, di seguito denominato «Ministero», una dichiarazione comprensiva di tutte le informazioni necessarie a verificare la conformità alle condizioni di cui all'art. 6. La predetta dichiarazione, che deve attenersi a quanto indicato nell'allegato A) al presente decreto, costituisce denuncia di inizio attività e dà titolo ad avviare il servizio contestualmente alla sua presentazione.

3. Il soggetto richiedente allega alla dichiarazione la documentazione di cui all'art. 6, comma 1, lettere a) e b) della delibera dell'Autorità n. 467/00/Cons. Il soggetto che abbia precedentemente ottenuto una o più autorizzazioni all'offerta al pubblico di servizi di telecomunicazioni, puo' presentare la dichiarazione facendo riferimento alla documentazione già esibita, nei limiti della prevista validità.

4. I soggetti autorizzati sono obbligati all'iscrizione al registro degli operatori di comunicazione, previsto dall'art. 1, comma 6, lettera a), n. 5), della legge 31 luglio 1997, n. 249, secondo le disposizioni della delibera dell'Autorità n. 236/0l/Cons e successive modificazioni.

5. I soggetti che hanno presentato la dichiarazione di cui al presente articolo, comunicano entro trenta giorni al Ministero ogni variazione delle informazioni contenute nella stessa e nella relativa documentazione allegata.

Art. 4

Contributi

1. I diritti amministrativi imposti ai soggetti autorizzati ad offrire il servizio di cui all'art. 2 coprono esclusivamente i costi amministrativi sostenuti per la gestione, il controllo e l'applicazione del regime di autorizzazione generale.

2. La misura di tali contributi sarà fissata con apposito provvedimento e resa pubblica ai sensi delle normative vigenti.

Art. 5

Validità e cessione dell'autorizzazione generale

1. L'autorizzazione generale di cui all'art. 3 ha una durata non superiore a nove anni a decorrere dalla data di notifica della dichiarazione di cui al medesimo articolo ed rinnovabile, previa nuova dichiarazione presentata con almeno trenta giorni di anticipo rispetto alla scadenza.

2. La scadenza coincide con il 31 dicembre dell'ultimo anno di validità dell'autorizzazione generale.

3. L'autorizzazione generale non può essere ceduta a terzi senza l'assenso del Ministero volto a verificare la sussistenza dei requisiti in capo all'impresa cessionaria, per il rispetto delle condizioni di cui all'autorizzazione medesima.

Art. 6

Condizioni dell'autorizzazione generale

1. Il soggetto titolare dell'autorizzazione generale per la fornitura, attraverso le applicazioni Radio-LAN, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni, tenuto a soddisfare le seguenti condizioni:

a) l'utilizzazione di apparecchiature conformi a quanto previsto dal decreto legislativo 9 maggio 2001, n. 268, di recepimento della direttiva 1999/5/CE;

b) la sicurezza delle operazioni di rete, il mantenimento dell'integrità della rete, l'interoperabilità dei servizi nonché la protezione dei dati; a tal fine l'interconnessione tra reti Radio-LAN ammessa esclusivamente attraverso reti pubbliche di telecomunicazioni; ammesso il collegamento tra gli access point appartenenti alla medesima Radio-LAN limitatamente all'ambito geografico locale definito all'art. 2, comma 1 e nel rispetto delle caratteristiche tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze;

c) la fornitura delle informazioni necessarie per verificare il rispetto delle condizioni stabilite ed a fini statistici;

d) il rispetto della normativa vigente in materia di tutela della salute pubblica e dell'ambiente, ivi incluso il rispetto dei tetti previsti per le emissioni elettromagnetiche;

e) l'utilizzazione delle frequenze di cui all'art. 1, comma 1, lettera a) esclusivamente secondo le caratteristiche di armonizzazione e tecniche previste dal vigente Piano nazionale di ripartizione delle frequenze, con l'esclusione di utilizzo delle medesime per scopi di interconnessione;

f) l'assenza di interferenze dannose alle altre utilizzazioni previste dal vigente Piano nazionale di ripartizione delle frequenze nelle bande di cui all'art. 1, comma 1, lettera a), senza alcun diritto a protezione dalle medesime utilizzazioni;

g) la pubblicizzazione delle condizioni di offerta del servizio, incluse quelle attinenti alle condizioni economiche, alla qualità e alla disponibilità del servizio nonché le relative variazioni delle condizioni stesse;

h) l'istituzione di una procedura per la trattazione dei reclami;

i) il pagamento dei contributi, ove previsti;

j) la fornitura di fatture dettagliate e documentate, ove applicabile in funzione della tipologia del servizio offerto;

k) l'adozione di opportuni codici di abilitazione e identificazione per identificare univocamente l'abbonato e verificarne l'abilitazione all'accesso alla rete tramite l'access point;

l) il rispetto delle disposizioni vigenti in materia di pubblica sicurezza e tempestiva collaborazione con l'Autorità giudiziaria ai sensi dell'art. 7, comma 13 del decreto del Presidente della Repubblica n. 318 del 1997;

m) il rispetto di ogni ragionevole misura tecnica di mitigazione, come previsto dalle rilevanti raccomandazioni e decisioni dell'ECC;

n) il rispetto delle eventuali disposizioni emanate dall'Autorità in materia di accesso, condivisione degli apparati e delle strutture, garanzie in materia di tutela della effettiva concorrenza.

2. In particolare il soggetto di cui al comma 1 tenuto al rispetto degli obblighi di cui agli articoli 4 e 5 della direttiva 97/66/CE ed alle successive modificazioni di cui alla direttiva 2002/58/CE, quando recepita nell'ordinamento nazionale, che disciplinano gli aspetti legati alla sicurezza ed alla riservatezza delle reti e dei servizi.

Art. 7

Controlli e verifiche - Disposizioni sanzionatorie - Conciliazione e risoluzione delle controversie

1. Il Ministero e l'Autorità, nell'ambito delle rispettive competenze, possono procedere all'attuazione di controlli periodici per la verifica del rispetto delle condizioni di cui al presente decreto.

2. In caso di inosservanza delle condizioni previste per le autorizzazioni generali di cui al presente decreto si applicano le disposizioni di cui all'art. 6, comma 4, del decreto del Presidente della Repubblica 19 settembre 1997, n. 318, e all'art. 25 della legge 24 aprile 1998, n. 128, come modificato dall'art. 13 della legge 21 dicembre 1999, n. 526.

3. Le procedure di conciliazione e risoluzione delle controversie sono disciplinate dall'art. 18 del decreto del Presidente della Repubblica 19 settembre 1997, n. 318.

Art. 8

Disposizioni transitorie e finali

1. Le imprese già autorizzate all'esercizio sperimentale del servizio di fornitura, attraverso le applicazioni Radio-LAN, dell'accesso del pubblico alle reti e ai servizi di telecomunicazioni mediante l'impiego delle frequenze 2.400-2.483,5 MHz, cessano la sperimentazione entro sessanta giorni dalla entrata in vigore del presente decreto.

2. I titoli abilitativi di cui al presente decreto verranno adeguati alla normativa comunitaria in corso di recepimento di cui alle premesse, in materia di comunicazioni elettroniche.

D.Lgs. 30 giugno 2003 n. 196

Codice in materia di protezione dei dati personali.

(omissis)

Articolo 5. Oggetto ed ambito di applicazione.

1. Il presente codice disciplina il trattamento di dati personali, anche detenuti all'estero, effettuato da chiunque è stabilito nel territorio dello Stato o in un luogo comunque soggetto alla sovranità dello Stato.

2. Il presente codice si applica anche al trattamento di dati personali effettuato da chiunque è stabilito nel territorio di un Paese non appartenente all'Unione europea e impiega, per il trattamento, strumenti situati nel territorio dello Stato anche diversi da quelli elettronici, salvo che essi siano utilizzati solo ai fini di transito nel territorio dell'Unione europea. In caso di applicazione del presente codice, il titolare del trattamento designa un proprio rappresentante stabilito nel territorio dello Stato ai fini dell'applicazione della disciplina sul trattamento dei dati personali.

3. Il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali è soggetto all'applicazione del presente codice solo se i dati sono destinati ad una comunicazione sistematica o alla diffusione. Si applicano in ogni caso le disposizioni in tema di responsabilità e di sicurezza dei dati di cui agli articoli 15 e 31.

(omissis)

Articolo 12. Codici di deontologia e di buona condotta.

1. Il Garante promuove nell'àmbito delle categorie interessate, nell'osservanza del principio di rappresentatività e tenendo conto dei criteri direttivi delle raccomandazioni del Consiglio d'Europa sul trattamento di dati personali, la sottoscrizione di codici di deontologia e di buona condotta per determinati settori, ne verifica la conformità alle leggi e ai regolamenti anche attraverso l'esame di osservazioni di soggetti interessati e contribuisce a garantirne la diffusione e il rispetto.

2. I codici sono pubblicati nella Gazzetta Ufficiale della Repubblica italiana a cura del Garante e, con decreto del Ministro della giustizia, sono riportati nell'allegato A) del presente codice .

3. Il rispetto delle disposizioni contenute nei codici di cui al comma 1 costituisce condizione essenziale per la liceità e correttezza del trattamento dei dati personali effettuato da soggetti privati e pubblici.

4. Le disposizioni del presente articolo si applicano anche al codice di deontologia per i trattamenti di dati per finalità giornalistiche promosso dal Garante nei modi di cui al comma 1 e all'articolo 139.

(omissis)

Articolo 26. Garanzie per i dati sensibili.

1. I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato e previa autorizzazione del Garante, nell'osservanza dei presupposti e dei limiti stabiliti dal presente codice, nonché dalla legge e dai regolamenti.

2. Il Garante comunica la decisione adottata sulla richiesta di autorizzazione entro quarantacinque giorni, decorsi i quali la mancata pronuncia equivale a rigetto. Con il provvedimento di autorizzazione, ovvero successivamente, anche sulla base di eventuali verifiche, il Garante può prescrivere misure e accorgimenti a garanzia dell'interessato, che il titolare del trattamento è tenuto ad adottare.

3. Il comma 1 non si applica al trattamento:
a) dei dati relativi agli aderenti alle confessioni religiose e ai soggetti che con riferimento a finalità di natura esclusivamente religiosa hanno contatti regolari con le medesime confessioni, effettuato dai relativi organi, ovvero da enti civilmente riconosciuti, sempre che i dati non siano diffusi o comunicati fuori delle medesime confessioni. Queste ultime determinano idonee garanzie relativamente ai trattamenti effettuati, nel rispetto dei princìpi indicati al riguardo con autorizzazione del Garante;
b) dei dati riguardanti l'adesione di associazioni od organizzazioni a carattere sindacale o di categoria ad altre associazioni, organizzazioni o confederazioni a carattere sindacale o di categoria.

4. I dati sensibili possono essere oggetto di trattamento anche senza consenso, previa autorizzazione del Garante:

a) quando il trattamento è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, a carattere politico, filosofico, religioso o sindacale, ivi compresi partiti e movimenti politici, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, relativamente ai dati personali degli aderenti o dei soggetti che in relazione a tali finalità hanno contatti regolari con l'associazione, ente od organismo, sempre che i dati non siano comunicati all'esterno o diffusi e l'ente, associazione od organismo determini idonee garanzie relativamente ai trattamenti effettuati, prevedendo espressamente le modalità di utilizzo dei dati con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13;

b) quando il trattamento è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2;

c) quando il trattamento è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere in sede giudiziaria un diritto, sempre che i dati siano trattati esclusivamente

per tali finalità e per il periodo strettamente necessario al loro perseguimento. Se i dati sono idonei a rivelare lo stato di salute e la vita sessuale, il diritto deve essere di rango pari a quello dell'interessato, ovvero consistente in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

d) quando è necessario per adempiere a specifici obblighi o compiti previsti dalla legge, da un regolamento o dalla normativa comunitaria per la gestione del rapporto di lavoro, anche in materia di igiene e sicurezza del lavoro e della popolazione e di previdenza e assistenza, nei limiti previsti dall'autorizzazione e ferme restando le disposizioni del codice di deontologia e di buona condotta di cui all'articolo 111.

5. I dati idonei a rivelare lo stato di salute non possono essere diffusi.

(omissis)

Legge 9 gennaio 2004 n. 4

Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici.

1. Obiettivi e finalità.

1. La Repubblica riconosce e tutela il diritto di ogni persona ad accedere a tutte le fonti di informazione e ai relativi servizi, ivi compresi quelli che si articolano attraverso gli strumenti informatici e telematici.

2. È tutelato e garantito, in particolare, il diritto di accesso ai servizi informatici e telematici della pubblica amministrazione e ai servizi di pubblica utilità da parte delle persone disabili, in ottemperanza al principio di uguaglianza ai sensi dell'articolo 3 della Costituzione.

2. Definizioni.

1. Ai fini della presente legge, si intende per:

a) «accessibilità»: la capacità dei sistemi informatici, nelle forme e nei limiti consentiti dalle conoscenze tecnologiche, di erogare servizi e fornire informazioni fruibili, senza discriminazioni, anche da parte di coloro che a causa di disabilità necessitano di tecnologie assistive o configurazioni particolari;
b) «tecnologie assistive»: gli strumenti e le soluzioni tecniche, hardware e software, che permettono alla persona disabile, superando o riducendo le condizioni di svantaggio, di accedere alle informazioni e ai servizi erogati dai sistemi informatici.

3. Soggetti erogatori.

1. La presente legge si applica alle pubbliche amministrazioni di cui al comma 2 dell'articolo 1 del decreto legislativo 30 marzo 2001, n. 165, e successive modificazioni, agli enti pubblici economici, alle aziende private concessionarie di servizi pubblici, alle aziende municipalizzate regionali, agli enti di assistenza e di riabilitazione pubblici, alle aziende di trasporto e di telecomunicazione a prevalente partecipazione di capitale pubblico e alle aziende appaltatrici di servizi informatici.

2. Le disposizioni della presente legge in ordine agli obblighi per l'accessibilità non si applicano ai sistemi informatici destinati ad essere fruiti da gruppi di utenti dei quali, per disposizione di legge, non possono fare parte persone disabili.

4. Obblighi per l'accessibilità.

1. Nelle procedure svolte dai soggetti di cui all'articolo 3, comma 1, per l'acquisto di beni e per la fornitura di servizi informatici, i requisiti di accessibilità stabiliti con il decreto di cui all'articolo 11 costituiscono motivo di preferenza a parità di ogni altra condizione nella valutazione dell'offerta tecnica, tenuto conto della destinazione del bene o del servizio. La mancata considerazione dei requisiti di accessibilità o l'eventuale acquisizione di beni o fornitura di servizi non accessibili è adeguatamente motivata.

2. I soggetti di cui all'articolo 3, comma 1, non possono stipulare, a pena di nullità, contratti per la realizzazione e la modifica di siti Internet quando non è previsto che essi rispettino i requisiti di accessibilità stabiliti dal decreto di cui all'articolo 11. I contratti in essere alla data di entrata in vigore del decreto di cui all'articolo 11, in caso di rinnovo, modifica o novazione, sono adeguati, a pena di nullità, alle disposizioni della presente legge circa il rispetto dei requisiti di accessibilità, con l'obiettivo di realizzare tale adeguamento entro dodici mesi dalla data di entrata in vigore del medesimo decreto.

3. La concessione di contributi pubblici a soggetti privati per l'acquisto di beni e servizi informatici destinati all'utilizzo da parte di lavoratori disabili o del pubblico, anche per la predisposizione di postazioni di telelavoro, è subordinata alla rispondenza di tali beni e servizi ai requisiti di accessibilità stabiliti dal decreto di cui all'articolo 11.

4. I datori di lavoro pubblici e privati pongono a disposizione del dipendente disabile la strumentazione hardware e software e la tecnologia assistiva adeguata alla specifica disabilità, anche in caso di telelavoro, in relazione alle mansioni effettivamente svolte. Ai datori di lavoro privati si applica la disposizione di cui all'articolo 13, comma 1, lettera c), della legge 12 marzo 1999, n. 68.

5. I datori di lavoro pubblici provvedono all'attuazione del comma 4, nell'àmbito delle disponibilità di bilancio.

5. Accessibilità degli strumenti didattici e formativi.

1. Le disposizioni della presente legge si applicano, altresì, al materiale formativo e didattico utilizzato nelle scuole di ogni ordine e grado.

2. Le convenzioni stipulate tra il Ministero dell'istruzione, dell'università e della ricerca e le associazioni di editori per la fornitura di libri alle biblioteche scolastiche prevedono sempre la fornitura di copie su supporto digitale degli strumenti didattici fondamentali, accessibili agli alunni disabili e agli insegnanti di sostegno, nell'àmbito delle disponibilità di bilancio.

6. Verifica dell'accessibilità su richiesta.

1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie valuta su richiesta l'accessibilità dei siti Internet o del materiale informatico prodotto da soggetti diversi da quelli di cui all'articolo 3.

2. Con il regolamento di cui all'articolo 10 sono individuati:

a) le modalità con cui può essere richiesta la valutazione;
b) i criteri per la eventuale partecipazione del richiedente ai costi dell'operazione;
c) il marchio o logo con cui è reso manifesto il possesso del requisito dell'accessibilità;
d) le modalità con cui può essere verificato il permanere del requisito stesso.

7. Compiti amministrativi.
1. La Presidenza del Consiglio dei Ministri - Dipartimento per l'innovazione e le tecnologie, anche avvalendosi del Centro nazionale per l'informatica nella pubblica amministrazione di cui all'articolo 4, comma 1, del decreto legislativo 12 febbraio 1993, n. 39, come sostituito dall'articolo 176 del decreto legislativo 30 giugno 2003, n. 196:

a) effettua il monitoraggio dell'attuazione della presente legge;
b) vigila sul rispetto da parte delle amministrazioni statali delle disposizioni della presente legge;
c) indica i soggetti, pubblici o privati, che, oltre ad avere rispettato i requisiti tecnici indicati dal decreto di cui all'articolo 11, si sono anche meritoriamente distinti per l'impegno nel perseguire le finalità indicate dalla presente legge;
d) promuove, di concerto con il Ministero del lavoro e delle politiche sociali, progetti, iniziative e programmi finalizzati al miglioramento e alla diffusione delle tecnologie assistive e per l'accessibilità;
e) promuove, con le altre amministrazioni interessate, sentita la Conferenza permanente per i rapporti tra lo Stato, le regioni e le province autonome di Trento e di Bolzano, l'erogazione di finanziamenti finalizzati alla diffusione tra i disabili delle tecnologie assistive e degli strumenti informatici dotati di configurazioni particolari e al sostegno di progetti di ricerca nel campo dell'innovazione tecnologica per la vita indipendente e le pari opportunità dei disabili;
f) favorisce, di concerto con il Ministero del lavoro e delle politiche sociali e con il Ministro per le pari opportunità, lo scambio di esperienze e di proposte fra associazioni di disabili, associazioni di sviluppatori competenti in materia di accessibilità, amministrazioni pubbliche, operatori economici e fornitori di hardware e software, anche per la proposta di nuove iniziative;
g) promuove, di concerto con i Ministeri dell'istruzione, dell'università e della ricerca e per i beni e le attività culturali, iniziative per favorire l'accessibilità alle opere multimediali, anche attraverso specifici progetti di ricerca e sperimentazione con il coinvolgimento delle associazioni delle persone disabili; sulla base dei risultati delle sperimentazioni sono indicate, con decreto emanato di intesa dai Ministri interessati, le regole tecniche per l'accessibilità alle opere multimediali;
h) definisce, di concerto con il Dipartimento della funzione pubblica della Presidenza del Consiglio dei Ministri, gli obiettivi di accessibilità delle pubbliche amministrazioni nello sviluppo dei sistemi informatici, nonché l'introduzione delle problematiche relative all'accessibilità nei programmi di formazione del personale.

2. Le regioni, le province autonome e gli enti locali vigilano sull'attuazione da parte dei propri uffici delle disposizioni della presente legge .

8. Formazione.
1. Le amministrazioni di cui all'articolo 3, comma 1, nell'àmbito delle attività di cui al comma 4 dell'articolo 7 del decreto legislativo 30 marzo 2001, n. 165, nonché dei corsi di formazione organizzati dalla Scuola superiore della pubblica amministrazione, e nell'àmbito delle attività per l'alfabetizzazione informatica dei pubblici dipendenti di cui all'articolo 27, comma 8, lettera g), della legge 16 gennaio 2003, n. 3, inseriscono tra le

materie di studio a carattere fondamentale le problematiche relative all'accessibilità e alle tecnologie assistive.

2. La formazione professionale di cui al comma 1 è effettuata con tecnologie accessibili.

3. Le amministrazioni di cui all'articolo 3, comma 1, nell'àmbito delle disponibilità di bilancio, predispongono corsi di aggiornamento professionale sull'accessibilità.

9. Responsabilità.

1. L'inosservanza delle disposizioni della presente legge comporta responsabilità dirigenziale e responsabilità disciplinare ai sensi degli articoli 21 e 55 del decreto legislativo 30 marzo 2001, n. 165, ferme restando le eventuali responsabilità penali e civili previste dalle norme vigenti.

10. Regolamento di attuazione.

1. Entro novanta giorni dalla data di entrata in vigore della presente legge, con regolamento emanato ai sensi dell'articolo 17, comma 1, della legge 23 agosto 1988, n. 400, sono definiti:

a) i criteri e i princìpi operativi e organizzativi generali per l'accessibilità;
b) i contenuti di cui all'articolo 6, comma 2;
c) i controlli esercitabili sugli operatori privati che hanno reso nota l'accessibilità dei propri siti e delle proprie applicazioni informatiche;
d) i controlli esercitabili sui soggetti di cui all'articolo 3, comma 1.

2. Il regolamento di cui al comma 1 è adottato previa consultazione con le associazioni delle persone disabili maggiormente rappresentative, con le associazioni di sviluppatori competenti in materia di accessibilità e di produttori di hardware e software e previa acquisizione del parere delle competenti Commissioni parlamentari, che devono pronunciarsi entro quarantacinque giorni dalla richiesta, e d'intesa con la Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281

11. Requisiti tecnici.

1. Entro centoventi giorni dalla data di entrata in vigore della presente legge il Ministro per l'innovazione e le tecnologie, consultate le associazioni delle persone disabili maggiormente rappresentative, con proprio decreto stabilisce, nel rispetto dei criteri e dei princìpi indicati dal regolamento di cui all'articolo 10:

a) le linee guida recanti i requisiti tecnici e i diversi livelli per l'accessibilità;
b) le metodologie tecniche per la verifica dell'accessibilità dei siti Internet, nonché i programmi di valutazione assistita utilizzabili a tale fine.

12. Normative internazionali.

1. Il regolamento di cui all'articolo 10 e il decreto di cui all'articolo 11 sono emanati osservando le linee guida indicate nelle comunicazioni, nelle raccomandazioni e nelle direttive sull'accessibilità dell'Unione europea, nonché nelle normative

internazionalmente riconosciute e tenendo conto degli indirizzi forniti dagli organismi pubblici e privati, anche internazionali, operanti nel settore.

2. Il decreto di cui all'articolo 11 è periodicamente aggiornato, con la medesima procedura, per il tempestivo recepimento delle modifiche delle normative di cui al comma 1 e delle innovazioni tecnologiche nel frattempo intervenute.

PRESIDENZA DEL CONSIGLIO DEI MINISTRI
DIRETTIVA 6 agosto 2004

Progetti formativi in modalità e-learning *nelle pubbliche amministrazioni.*

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE
e
IL MINISTRO PER LA FUNZIONE PUBBLICA

Visto l'art. 5 della legge 23 agosto 1988, n. 400, recante «Disciplina dell'attività di Governo e ordinamento della Presidenza del Consiglio dei Ministri»;
Visto il decreto legislativo 12 febbraio 1993, n. 39, recante «Norme in materia di sistemi informativi automatizzati delle amministrazioni pubbliche, a norma dell'art. 2, comma 1, della legge 23 ottobre 1992, n. 421» e successive modificazioni ed integrazioni;
Visto il decreto legislativo 30 marzo 2001, n. 165, recante «Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche», ed in particolare l'art. 7-bis introdotto dalla legge 16 gennaio 2003, n. 3, recante «Disposizioni ordinamentali in materia di pubblica amministrazione»;
Visto il decreto del Presidente del Consiglio dei Ministri del 9 agosto 2001, recante «Delega di funzioni del Presidente del Consiglio dei Ministri in materia di innovazione e tecnologie al Ministro senza portafoglio, dott. Lucio Stanca»;
Visto il decreto del Presidente del Consiglio dei Ministri del 29 novembre 2002, recante «Delega di funzioni del Presidente del Consiglio dei Ministri in materia di funzione pubblica al Ministro senza portafoglio, avv. Luigi Mazzella»;
Vista la direttiva del Ministro per la funzione pubblica in data 13 dicembre 2001, recante «Formazione e valorizzazione del personale delle pubbliche amministrazioni»;
Vista la direttiva del Ministro per l'innovazione e le tecnologie in data 21 dicembre 2001, recante «Linee guida in materia di digitalizzazione dell'amministrazione»;
Viste le «Linee guida del Governo per lo sviluppo della societa' dell'informazione nella legislatura», del giugno 2002;
Vista la direttiva del Ministro per l'innovazione e le tecnologie in data 20 dicembre 2002, recante «Linee guida in materia di digitalizzazione dell'amministrazione» per l'anno 2003;
Vista la direttiva del Ministro per l'innovazione e le tecnologie in data 18 dicembre 2003, recante «Linee guida in materia di digitalizzazione dell'amministrazione» per l'anno 2004;

EMANANO
la seguente direttiva
in materia di progetti formativi in modalità *e-learning* nelle pubbliche amministrazioni:

1. Premessa

La presente direttiva rivolta alle amministrazioni dello Stato, ivi compresi gli istituti e scuole di ogni ordine e grado e le istituzioni educative, le aziende ed amministrazioni dello Stato ad ordinamento autonomo, le istituzioni universitarie, gli enti pubblici non economici nazionali, l'Agenzia per la rappresentanza negoziale delle pubbliche amministrazioni (ARAN), le agenzie di cui al decreto legislativo 30 luglio 1999, n. 300; resta ferma, comunque, la competenza dello Stato di cui all'art. 117, secondo comma,

lettera r), della Costituzione. La direttiva 13 dicembre 2001, recante: «Formazione e valorizzazione del personale delle pubbliche amministrazioni» - emanata dal Ministro per la funzione pubblica di concerto con il Ministro per l'innovazione e le tecnologie - in tema di e-learning, evidenzia, tra l'altro, che l'adozione delle nuove tecnologie informatiche comporta notevoli investimenti iniziali e richiede un'accurata pianificazione, in modo da poter tenere nella debita considerazione, oltre agli obiettivi primari della formazione, le esigenze dei destinatari della stessa e l'opportunita' di fare ricorso alle tradizionali metodologie d'aula per un'adeguata integrazione, ove necessaria. La materia, come noto, ha anche formato oggetto del documento con il quale il Ministro per l'innovazione e le tecnologie, nel mese di giugno del 2002, ha impartito le «Linee guida del Governo per lo sviluppo della societa' dell'informazione nella legislatura». Tra i programmati interventi sul sistema Paese é compreso, infatti, l'e-learning, il cui impiego pone l'esigenza di affrontare le problematiche connesse alla formazione con nuove strategie, finalizzate, da un lato a venire incontro alle esigenze di aggiornamento dei singoli destinatari; dall'altro a soddisfare quelle, parimenti rilevanti, di natura organizzativa. Inoltre, gli standard - da definire con il Dipartimento della funzione pubblica - devono assicurare adeguati livelli di servizio, il riutilizzo dei contenuti e l'allineamento ai modelli europei. Piu' recentemente, il decreto del Ministro dell'istruzione, dell'universita' e della ricerca, di concerto con il Ministro per l'innovazione e le tecnologie, in data 17 aprile 2003, ha rappresentato una testimonianza ed una conferma del significativo cambiamento in atto: si fa qui riferimento, in particolare, ai criteri e alle procedure di accreditamento dei corsi di studio a distanza delle universita' statali e non statali e delle istituzioni universitarie abilitate e allo specifico richiamo alle «prescrizioni tecniche» per l'adozione di un'architettura di sistema in grado di gestire e rendere accessibili all'utente i corsi di studio a distanza (articoli 1 e 2). Il Consiglio europeo di Lisbona di marzo 2000 ha invitato i Governi nazionali a favorire una rapida accelerazione informatica che consenta di adottare i livelli formativi e informativi necessari per la Societa' Europa del terzo millennio, fissando come ambizioso obiettivo strategico del successivo decennio, quello di trasformare l'economia europea in quella basata sulla conoscenza piu' competitiva e dinamica del mondo, in grado di realizzare una crescita economica sostenibile con nuovi e migliori posti di lavoro e una maggiore coesione sociale. Connesso a tale obiettivo, stato sviluppato il piano di azione eEurope 2005, che ha inserito l'e-learning tra le proprie azioni prioritarie. Al riguardo si segnala che, in ambito europeo, le pubbliche amministrazioni hanno manifestato in maniera univoca un elevato interesse nei confronti delle nuove tecnologie informatiche; le stesse, infatti, attraverso una rete capillare e pervasiva - quale certamente la rete Internet - offrono l'opportunita' di accelerare e di ottimizzare la diffusione delle informazioni e della conoscenza attraverso soluzioni virtuali, che consentono di abbattere vincoli di tempo e di spazio, difficilmente superabili facendo ricorso unicamente ai tradizionali processi formativi, e informativi, in uso fino ad oggi. In molti Paesi, inoltre, in corso un processo di armonizzazione dei rispettivi sistemi informativi, nella prospettiva di realizzare, sia a livello nazionale che a livello intergovernativo, l'interoperabilita' sotto il duplice profilo dei contenuti e dei servizi offerti; cio' anche come risposta all'invito ai Governi nazionali, rivolto dal Consiglio europeo di Lisbona, ad imprimere una rapida accelerazione al programma di informatizzazione, in vista del raggiungimento dei livelli formativi e informativi di cui la Societa' europea necessita nel terzo millennio.

2. Obiettivi

La direttiva sulla formazione del dicembre 2001, precedentemente citata, indica esplicitamente (punto 6) che i mutamenti organizzativi in atto, l'introduzione di nuove metodologie, l'esistenza di una rete nazionale e il diffondersi del telelavoro devono portare a ripensare i luoghi e le tecniche della formazione. In particolare, la direttiva (punto 3) chiarisce che le metodologie di formazione a distanza consentono di ampliare il numero dei destinatari e di realizzare una formazione continua che garantisca livelli minimi comuni di conoscenze. Pertanto, la presente direttiva intende promuovere una corretta utilizzazione di dette nuove metodologie e tecnologie nel campo della formazione a distanza, fornendo indicazioni metodologiche di carattere generale e rinviando, per il resto, alle allegate «Linee guida per i progetti formativi in modalita' e-learning nelle pubbliche amministrazioni», elaborate dal Centro nazionale per l'informatica nella pubblica amministrazione, che formano parte integrante della presente direttiva. Il sopra richiamato ripensamento delle procedure tecniche attinenti alla formazione, conseguente alle nuove tecnologie comporta, in primo luogo, la necessita' di tener presente che il processo di e-learning non consiste nella sola distribuzione e diffusione in rete di materiale: esso, per contro, esige che vengano messi a disposizione e forniti servizi didattici on-line. La progettazione delle attivita' formative deve quindi prestare attenzione anche agli aspetti relativi alla gestione ed al coordinamento del programma di formazione nel suo complesso, oltre che alle metodologie proprie della formazione a distanza (e-learning), in modo che l'iniziativa venga realizzata nella maniera piu' soddisfacente in termini di efficienza e di efficacia. Il programma di formazione nel suo complesso deve infatti essere esplicitato, come indicato dalla legge n. 3 del 2003, in un piano annuale di formazione del personale, compreso quello in posizione di comando o fuori ruolo, tenendo conto dei fabbisogni rilevati, delle competenze necessarie in relazione agli obiettivi, nonché della programmazione delle assunzioni e delle innovazioni normative e tecnologiche. Il piano di formazione indica gli obiettivi e le risorse finanziarie necessarie, nei limiti di quelle a tale scopo disponibili, prevedendo l'impiego delle risorse interne, di quelle statali e comunitarie, nonché le metodologie formative da adottare in riferimento ai diversi destinatari. I progetti formativi in modalita' e-learning pongono, di fatto, una serie di problematiche, alcune delle quali sono strettamente legate alla vera e propria formazione, mentre altre riguardano i profili organizzativi e tecnici connessi alla realizzazione di un progetto di automazione, che non puo' essere affidato alla sola competenza dell'ufficio preposto alla formazione, ma deve prevedere il coinvolgimento della dirigenza ai piu' alti livelli, dei responsabili delle risorse umane e dei sistemi informativi, nonché degli uffici comunque e a vario titolo interessati.

3. La gestione ed il coordinamento

Il processo di e-learning si inserisce nel piu' ampio quadro del complesso degli interventi formativi e, pertanto si avvale di quelle «strutture [...] che assicurino la pianificazione e la programmazione delle attivita' formative» richiamate dal punto 3 della direttiva del 2001, anche al fine di curare le varie fasi del processo formativo descritte al punto 5 della medesima direttiva. Pertanto, anche con specifico riferimento al processo formativo in modalita' e-learning ed alle sue fasi, l'amministrazione si avvale di dette strutture o, comunque, di una figura di riferimento dotata della necessaria capacita' professionale - presente nella propria organizzazione interna e non necessariamente coincidente con il responsabile della progettazione - che coordini le

attivita' didattiche, garantisca adeguati livelli di servizio, dialoghi con le parti: «la domanda», rappresentata dai discenti, «l'offerta», costituita, ad esempio, dal tutor e dal team tecnico. In caso di affidamento all'esterno, la ditta appaltatrice dovra' fornire un proprio responsabile di progetto che sara' l'interlocutore del coordinatore interno. Quest'ultimo, poi, tenuto conto del compito che chiamato a svolgere, deve necessariamente essere munito di competenza e autorevolezza tali da poter coinvolgere la dirigenza e i discenti in un progetto innovativo che presenti importanti implicazioni organizzative e, nel contempo, controllare l'operato e l'apporto del personale messo a disposizione dalla ditta o dalle ditte esterne all'organizzazione dell'amministrazione committente.

4. L'impatto organizzativo.

I progetti formativi in modalita' e-learning hanno - come accennato - un impatto rilevante sull'organizzazione del lavoro. Sin dalla fase della progettazione pertanto auspicabile il coinvolgimento attivo degli uffici interessati, con particolare riguardo a quelli preposti alla formazione, e agli uffici dei responsabili dei sistemi informativi. L'aggiornamento del personale degli uffici addetti alla formazione e la collaborazione con l'ufficio preposto alla gestione dei sistemi informativi sono, inoltre, presupposti indispensabili per il successo del progetto formativo. Tenuto conto, poi, della circostanza che la modalita' di formazione e-learning permette di erogare la prestazione senza che il dipendente debba allontanarsi dal proprio luogo di lavoro e senza che vengano posti vincoli temporali, per tutta la durata della formazione si rende necessaria anche una ridistribuzione dei carichi di lavoro e la predisposizione di apposite postazioni di lavoro o di piccoli laboratori locali destinati all'utilizzo del materiale didattico ed allo svolgimento di eventuali attivita' di supporto; dovra', inoltre, essere previsto un congruo numero di ore settimanali da dedicare alle attivita' didattiche programmate. Va altresi' considerato che, in molti casi, il dipendente avra' anche bisogno di acquisire la necessaria familiarita' con uno strumento nuovo, o che comunque non usa abitualmente, quindi il percorso formativo dovra' iniziare con l'alfabetizzazione informatica: per tutta la sua durata dovranno essere assicurati un adeguato supporto tecnico ed una sistemazione logistica che consentano di utilizzare a pieno le potenzialita' della modalita' e-learning, oltre che un congruo numero di ore settimanali da dedicare alle anzidette attivita' didattiche.

5. I ruoli.

Le amministrazioni devono porre particolare attenzione nella scelta delle figure che intervengono in un processo di e-learning, sia che esse vengano individuate nell'ambito della singola amministrazione, sia che le stesse vengano reperite presso i possibili fornitori del percorso formativo, che rappresentano l'offerta. Sul versante della domanda, importante la creazione di una figura interna a una o piu' amministrazioni (oppure la riqualificazione di una figura gia' presente nell'area delle risorse umane), che abbia specifica esperienza in materia e adeguata conoscenza delle persone e delle problematiche inerenti il contesto e sia in grado di coordinare gli interventi da effettuare, di dialogare con le parti (che rappresentano, rispettivamente, la domanda e l'offerta), nonché di promuovere un'effettiva innovazione nei processi formativi. Il versante dell'offerta presenta, nell'ambito delle funzioni fondamentali del processo di e-learning (progettazione, realizzazione, erogazione) una serie di fasi complesse, e conseguenti relativi ruoli eventualmente anche sovrapposti, quali: il coordinatore del

progetto complessivo (project manager), il progettista didattico (instructional designer), l'esperto dei contenuti, il gruppo (team) di sviluppo, il docente (mentor), il tutor di processo/animatore ed il gruppo (team) tecnico. Per quanto concerne tutte le anzidette figure si rinvia a quanto riportato nel documento, allegato, che contiene le «Linee guida» sopra richiamate (punto 4).

6. Principi guida per la qualita' dei progetti di e-learning.

La formazione, in tutte le sue modalita', costituisce un processo articolato in piu' fasi che richiede il supporto ed il monitoraggio delle amministrazioni committenti per tutta la sua durata. In previsione di cioè, le «Linee guida» forniscono indicazioni - di ordine metodologico e sotto il profilo tecnologico - per lo sviluppo di progetti di qualita' e ad esse pertanto si rinvia. In questa sede si ritiene, comunque, opportuno richiamare le fasi e le componenti critiche, evidenziando che la consapevolezza della dirigenza ed il responsabile supporto che essa puo' cosi' offrire sono sicuramente due elementi indispensabili per il buon esito di un progetto di formazione in modalita' e-learning. In particolare, l'amministrazione deve:

a) effettuare una preliminare ricognizione dei profili dei destinatari, delle loro esigenze, del loro fabbisogno formativo;

b) valutare il relativo impatto organizzativo nel proprio ambito;

c) individuare, sempre nel proprio ambito, il soggetto che deve promuovere il progetto e successivamente coordinarlo e gestirlo;

d) effettuare una ricognizione del livello di alfabetizzazione informatica dei destinatari della formazione;

e) procedere ad una preliminare ricognizione delle strutture/infrastrutture tecnologiche (server, rete, postazione individuale) disponibili in funzione degli interventi di formazione auspicati e una pianificazione delle spese necessarie per la dotazione;

f) individuare i profili delle figure professionali via via coinvolte nei vari stadi del progetto;

g) adottare la metodologia didattica del processo di e-learning il piu' possibile idonea a realizzare l'interattivita', la multimedialita' e la collaborazione tra i diversi soggetti interessati, tenendo conto del ruolo attivo dell'utente e dell'importanza della classe virtuale;

h) potenziare le strutture tecnologiche (server, rete e postazioni di lavoro), in modo da garantire un'adeguata erogazione e fruizione dei contenuti multimediali;

i) creare e gestire il materiale che viene prodotto, strutturandolo in «unita' autoconsistenti», eventualmente anche riutilizzabili in varie combinazioni da inserire nella piattaforma (learning object);

j) assicurare la piattaforma tecnologica costituita da componenti software interoperabili, in grado di registrare il percorso delle attivita' del discente e di permettere anche l'interazione tra discenti (comunita' virtuale);

k) provvedere al continuo monitoraggio del progetto e del processo di e-learning, nonché alla valutazione del livello professionale dei partecipanti.

Nell'insieme delle attivita' che caratterizzano questo tipo di formazione, l'interoperabilita' delle singole componenti e la «portabilita» dei materiali didattici sono requisiti essenziali a tutela e garanzia degli investimenti a tal fine effettuati, dal momento che rendono possibile la cooperazione tra amministrazioni ed assicurano l'indipendenza dal fornitore. Proprio in previsione di cioè sono stati costituiti gli enti di standardizzazione, con il compito di fornire indicazioni di dettaglio sugli standard che i

fornitori di soluzioni tecnologiche, servizi e contenuti dovrebbero adottare per la propria offerta. A questo proposito non bisogna dimenticare che le attivita' di e-learning sono rivolte a destinatari eterogenei per quanto concerne il ruolo rivestito, le specifiche competenze possedute e il grado di familiarita' acquisito con l'impiego degli strumenti disponibili in rete. Pertanto puo' rendersi necessaria una corretta integrazione tra formazione a distanza e formazione in aula, ovvero anche la realizzazione di un progetto di formazione misto, per il quale comunque essenziale la presenza effettiva (in aula), soprattutto quando il percorso formativo rivolto ad un'utenza che ha scarsa dimestichezza con le pratiche della formazione on-line. Si sottolinea, infine, che il monitoraggio e la valutazione costituiscono le leve per assicurare il livello della formazione e il raggiungimento dei risultati attesi, relativamente ai contenuti, al grado di corrispondenza del progetto e delle azioni intraprese alle concrete esigenze di formazione del personale, nonché agli aspetti qualitativi sotto i profili operativo e gestionale.

7. Componenti di costo di un progetto di e-learning.

L'amministrazione dovra' provvedere ad un'analisi dei costi tenendo conto di tutte le componenti che concorrono a formare un progetto di e-learning. Complessivamente - come viene meglio indicato nelle allegate «Linee guida» (punto 6) - si possono individuare quattro aree principali: 1) l'organizzazione; 2) i servizi (progettazione, erogazione, gestione e monitoraggio); 3) le tecnologie (piattaforme e infrastrutture); 4) i contenuti (produzione e manutenzione).

Per progettare e realizzare un sistema e-learning si devono valutare le varie soluzioni indicate, tra loro integrabili, che comprendono offerte di prodotti differenti o provenienti da diversi fornitori, come indicato nelle «Linee guida» alle quali si rinvia ancora una volta.

8. Ruolo del Centro nazionale per l'informatica nella pubblica amministrazione (CNIPA) e del Dipartimento della funzione pubblica. Il CNIPA e il Dipartimento della funzione pubblica, nell'ambito delle rispettive competenze, assumono un ruolo di coordinamento e di monitoraggio dei progetti di formazione in e-learning delle amministrazioni pubbliche. Il CNIPA ha redatto un vademecum esplicativo delle «Linee guida» e curera' la definizione di un profilo applicativo che consenta di garantire la portabilita' e la riusabilita' dei materiali didattici, nonché la cooperazione applicativa tra i sistemi delle amministrazioni. Al fine di agevolare l'individuazione e l'organizzazione delle risorse pubbliche disponibili in rete e di dare visibilita' ai progetti locali e alle migliori pratiche, prevista - entro il primo semestre del 2005 - la costruzione di un portale sul tema dell'e-learning aperto a tutte le pubbliche amministrazioni. L'iniziativa si propone di favorire il riuso e di ottimizzare l'impiego delle risorse umane e finanziarie prevedendo, tra i contenuti del portale, anche una raccolta digitale di learning objects, realizzati attraverso i progetti formativi delle amministrazioni pubbliche. Il CNIPA, inoltre, sviluppera' attivita' di sperimentazione di soluzioni tecnologiche innovative e mettera' a disposizione delle amministrazioni una piattaforma per l'e-learning sincrono e asincrono che potra' essere utilizzata per valutare l'efficacia didattica dei materiali interattivi e per effettuare una sperimentazione - dell'e-learning stesso - senza investimenti iniziali. La piattaforma sara' disponibile anche per le amministrazioni di medio-piccole dimensioni che intendano sfruttare le economie di scala derivanti dalla soluzione in parola. In attuazione di quanto previsto dall'art. 7-bis del decreto legislativo 30 marzo 2001, n. 165 - come integrato dall'art. 4 della legge 16 gennaio 2003, n. 3 - il

Dipartimento della funzione pubblica, nell'esercizio dei propri compiti di indirizzo e coordinamento, svolgera' un'azione di supporto alle amministrazioni per la redazione dei piani di formazione del personale, fornendo indicazioni specifiche in relazione alla particolare modalita' di erogazione (indicatori di qualita', format dedicati, procedure di elaborazione). La comunicazione, al Dipartimento della funzione pubblica, dei piani formativi delle amministrazioni consentira', poi, la costituzione di una banca dati sulla formazione nel settore pubblico. Tale base informativa, per la quale previsto uno specifico approfondimento sull'e-learning, sara' messa a disposizione delle amministrazioni per favorire la diffusione di modelli, progetti formativi, contenuti. Il Dipartimento della funzione pubblica fornira' strumenti per la valutazione delle attivita' formative, offrendo i mezzi per un approfondito esame dei risultati conseguiti con le varie modalita' di erogazione (aula, e-learning, sistema integrato) e promuovera', nel contempo, «iniziative di accompagnamento e formazione» per l'attuazione della citata direttiva 13 dicembre 2001, nonché iniziative sperimentali, finalizzate all'individuazione di nuove figure professionali. Il Centro nazionale per l'informatica nella pubblica amministrazione e il Dipartimento della funzione pubblica della Presidenza del Consiglio dei Ministri, congiuntamente, cureranno l'organizzazione di seminari informativi e la predisposizione di materiali formativi/informativi multimediali.

Allegato

Linee guida per i progetti formativi in modalita' e-learning nelle pubbliche amministrazioni

1. Obiettivi

Obiettivo primario delle presenti «Linee guida» elaborate dal Centro nazionale per l'informatica nella pubblica amministrazione quello di promuovere in tutte le pubbliche amministrazioni un corretto impiego delle nuove metodologie e tecnologie per la formazione dei propri dipendenti, in sintonia con il percorso individuato dalla direttiva 13 dicembre 2001 - emanata dal Ministro per la funzione pubblica di concerto con il Ministro per l'innovazione e le tecnologie - recante: «Formazione e valorizzazione del personale delle pubbliche amministrazioni». La direttiva in parola ha gia' offerto l'opportunita' di evidenziare che l'introduzione di nuove tecnologie, l'esistenza di una rete nazionale e il diffondersi del telelavoro sono importanti eventi, che richiedono, necessariamente, una riflessione sui luoghi dove la formazione avviene e sulle modalita' tecniche che la disciplinano. In sede di progettazione delle attivita' formative dovranno quindi essere tenute in debita considerazione anche le metodologie di formazione a distanza (e-learning), atte a migliorare l'efficienza e l'efficacia della formazione. La modalita' e-learning non deve, pero', essere vista come alternativa a quella tradizionale, ma piuttosto come una nuova possibilita' che si aggiunge a quelle tradizionali. Un progetto formativo in modalita' e-learning presenta implicazioni di ordine organizzativo, tecnologico e metodologico, che comportano importanti investimenti iniziali e deve, quindi, essere attentamente monitorato e valutato nei vari stadi di sviluppo. Inoltre, gli elevati costi di produzione dei materiali didattici destinati alla formazione a distanza di alta qualita' rendono opportuna la collaborazione tra strutture diverse per un intelligente riuso dei materiali stessi, che, a tal fine, devono essere progettati secondo gli standard internazionali che assicurano la portabilita' su diversi ambienti operativi. La complessita' dei progetti di questo tipo potra' anche comportare il ricorso all'esternalizzazione, ma cioè non esime dalla partecipazione attiva alla fase di

progettazione, di erogazione, di monitoraggio e di verifica. Occorre, quindi, prevedere un'adeguata attivita' formativa del personale degli uffici preposti alla formazione, che dovra' essere posto in grado di operare al meglio nel nuovo contesto ambientale che si formato alla luce delle modificazioni intervenute nel tempo. Questo documento, oltre a fornire indicazioni sulle metodologie e sull'impatto organizzativo, intende anche evidenziare l'importanza delle tecnologie e dei problemi tecnici connessi alla produzione ed all'impiego di materiali didattici conformi agli standard e, quindi - come accennato - portabili e riusabili.

2. La gestione ed il coordinamento

I progetti di formazione in modalita' e-learning, al pari di molti progetti formativi tradizionali, si sviluppano in linea con i processi di cambiamento che spesso comportano la definizione di nuovi obiettivi e di nuovi profili professionali. L'individuazione di questi ultimi, e delle conseguenti necessita' formative, un compito che non puo' essere affidato all'esterno della struttura dell'amministrazione, perché presuppone una profonda conoscenza della missione e del modo di operare della stessa, delle varie attribuzioni di competenze esistenti e dei rapporti interni tra le diverse unita' operative. Il ruolo attivo dell'amministrazione non deve, tuttavia, limitarsi alla sola fase progettuale - nella quale devono comunque essere previste anche le attivita' di gestione ed i relativi costi - ma occorre un controllo continuo e vigile durante tutte le fasi del processo. In particolare, nella fase di erogazione del servizio la gestione operativa richiede una puntuale attivita' di coordinamento, nonché una scrupolosa azione di verifica del raggiungimento degli obiettivi e di monitoraggio. A tal fine necessario prevedere una figura manageriale interna all'amministrazione - non necessariamente coincidente con il responsabile della progettazione - che coordini le attivita' didattiche, garantisca i livelli di servizio, dialoghi con le parti: la domanda, rappresentata dai discenti, e l'offerta (tutor, team tecnico, ecc.). Nel caso, poi, di affidamento all'esterno la ditta appaltatrice dovra' garantire un proprio responsabile di progetto, che sara' l'interlocutore del coordinatore interno, che una figura, per quanto detto, di grande rilievo, come del resto evidenziato nella direttiva che precede. Si sottolinea, da ultimo, che le tradizionali attivita' di monitoraggio possono essere svolte sia utilizzando risorse interne, sia facendo ricorso a societa' specializzate esterne all'amministrazione; in ogni caso le risorse umane e quelle economiche ritenute necessarie devono essere adeguatamente valutate nell'ambito dei costi da sostenere per la realizzazione del progetto.

3. L'impatto organizzativo

La direttiva del 13 dicembre 2001 - sopra-richiamata - ha sottolineato l'esigenza che i piani formativi nascano nell'ambito organizzativo al quale sono destinati ed ha anche evidenziato che detti piani, a loro volta, hanno un impatto sull'organizzazione del lavoro. Questa considerazione , a maggiore ragione, vera e fondata per quanto concerne i progetti formativi in modalita' e-learning. Negli enti pubblici molto spesso questa tipologia di progetti viene avviata e gestita dall'area preposta alla formazione, che - anche in relazione all'evoluzione legislativa e tecnologica che sta coinvolgendo la pubblica amministrazione nel suo complesso - si tende, ora, a dotare in maniera sempre piu' consistente di autonomia gestionale, tecnico/operativa e finanziaria. In buona sostanza, l'attivita' svolta nel campo della formazione genera interventi innovativi che, a loro volta, poi, producono ulteriori elementi di innovazione. Negli enti caratterizzati da una struttura e da una organizzazione particolarmente solide, la competenza in materia

di attivita' formative affidata ad un apposito nucleo - costituito nell'ambito dell'area preposta alla formazione - che svolge compiti di coordinamento e di assistenza sul piano metodologico e si occupa, inoltre, di rilevare le esigenze che, sotto questo profilo, interessano l'intera struttura dell'ente. Esiste, poi, una rete di referenti, distribuiti nelle diverse aree dell'ente stesso, che svolgono un ruolo fondamentale di rilevazione delle esigenze formative - anche di settore - di programmazione delle relative attivita', di valutazione del grado di apprendimento e dell'impatto che ne deriva. Nell'ampio scenario organizzativo sinteticamente delineato, risulta evidente che l'attivita' di formazione in e-learning contribuisce certamente a creare una conoscenza condivisa su temi specifici che interessano diverse competenze e rappresenta, quindi, un volano valido per il conseguimento di concreti obiettivi di innovazione sul piano organizzativo e sul piano tecnologico. La fase di progettazione della formazione in e-learning richiede il coinvolgimento attivo degli uffici interessati, degli uffici che si occupano della formazione - che devono affrontare problematiche nuove e utilizzare nuove metodologie e tecnologie - e degli uffici dei responsabili dei sistemi informativi. L'aggiornamento dei dipendenti degli uffici addetti alla formazione e la loro collaborazione con gli uffici competenti in materia di sistemi informativi sono presupposti indispensabili per il successo del progetto formativo. La fase di erogazione, malgrado diffuse considerazioni ottimistiche sulla flessibilita' dell'e-learning, presenta notevoli problemi organizzativi. Infatti, la modalita' e-learning permette di erogare servizi di formazione senza che il dipendente debba allontanarsi dal proprio luogo di lavoro e senza che vengano imposti vincoli temporali; essa, pero', richiede comunque una ridistribuzione dei carichi di lavoro nel periodo di formazione, in modo da prevedere un congruo numero di ore settimanali da dedicare alle attivita' didattiche programmate, nonché la predisposizione di apposite stazioni di lavoro o di piccoli laboratori locali, destinati alla fruizione dei materiali didattici ed allo svolgimento delle attivita' collaborative. In molti casi, inoltre, il dipendente avra' bisogno di acquisire familiarita' con uno strumento che non usa abitualmente e il percorso formativo dovra' quindi iniziare con l'alfabetizzazione informatica. In presenza di queste circostanze, il dipendente durante il periodo di formazione dovra' essere posto nella condizione di disporre di un adeguato supporto tecnico e di una sistemazione logistica che gli permettano di utilizzare a pieno le potenzialita' offerte dalla modalita' e-learning. Va anche considerato che le infrastrutture tecnologiche (server, reti, stazioni di lavoro) disponibili presso l'amministrazione sono state disegnate in previsione di un normale carico di lavoro degli uffici e sara' quindi necessario verificare che le stesse siano adeguate anche ai fini dell'attivita' formativa. Da questo punto di vista la tecnologia svolge un ruolo determinante e una sua eventuale inadeguatezza potrebbe far fallire anche un progetto ottimo sotto il profilo didattico. Qualora, poi, l'amministrazione scelga di rivolgersi ad un fornitore di servizi tecnologici (ASP - Application Service Provider, oppure LSP - Learning Service Provider), andra' verificata l'adeguatezza dei livelli di servizio forniti e dovra' essere assicurata l'interoperabilita' con gli eventuali sistemi presenti.

4. I ruoli.

Le figure che intervengono in un processo di e-learning sono qui analizzate distinguendo la posizione della P.A. - che rappresenta la domanda di formazione - da quella dei possibili fornitori del percorso formativo, che rappresentano l'offerta.

Dal lato della domanda - come anticipato nella direttiva - essenziale prevedere una figura interna a una o piu' amministrazioni (oppure la riqualificazione di una figura gia'

presente nell'area delle risorse umane) che conosca il contesto ambientale e le problematiche che esso pone, nonché le persone con le quali viene in contatto e sia pertanto in grado di coordinare gli interventi da effettuare, di dialogare con le parti (che rappresentano, come accennato, da un lato la domanda, dall'altro l'offerta), di promuovere, in definitiva, un concreto cambiamento nei processi formativi. L'anzidetta figura dovra' svolgere funzioni di: coordinamento e pianificazione degli interventi, per valutare i fabbisogni formativi e valorizzare le risorse umane; e cio non solo alla luce delle esigenze dell'organizzazione ma anche tenendo in debita considerazione le peculiari caratteristiche, le inclinazioni, le motivazioni delle persone coinvolte; comunicazione tra domanda e offerta, ovvero interfaccia tra l'amministrazione e i fornitori dei servizi di formazione on-line; a questo proposito si richiede il possesso di competenze in materia di e-learning che consentano di cogliere e rappresentare le esigenze dell'organizzazione e di valutare adeguatamente le proposte formulate dalla parte che rappresenta l'offerta; change management, ovvero promozione e sviluppo graduale della cultura dell'e-learning, anche attraverso un'opportuna pianificazione dell'attivita' di formazione (programmando la verifica e l'eventuale aggiornamento delle competenze informatiche, per es. in modalita' blended). Dal lato dell'offerta le funzioni fondamentali di un processo di e-learning sono: la progettazione, la produzione, l'erogazione del servizio. Sotto questo profilo, le competenze necessarie sono molteplici e variamente distribuite, oltre che reperibili nell'ambito delle funzioni e delle fasi in precedenza indicate. Qui di seguito sono elencate le funzioni in cui si concentra una serie di ruoli complessi e che possono essere variamente distribuite - o anche parzialmente sovrapposte - in relazione alla scala territoriale di riferimento, alla complessita' del progetto, alla circostanza che il progetto venga realizzato all'interno dell'amministrazione, ovvero venga fatto ricorso a forme di outsourcing. Si tratta delle funzioni di: project manager, che responsabile dell'organizzazione e della gestione complessiva del progetto, di cui inoltre pubblica i contenuti; gestisce gli accessi al sistema; aggiorna il catalogo dell'offerta formativa; crea le classi virtuali; coordina i tutor e ne raccoglie e integra i report; instructional designer, che definisce le metodologie didattiche ed elabora i contenuti e lo storyboard per la traduzione nel formato multimediale programmato; esperto dei contenuti, che definisce i contenuti e ne cura l'armonizzazione (puo' essere una o piu' persone); team di sviluppo: che un insieme di figure che realizza e implementa i contenuti formativi e comprende: il progettista dell'architettura tecnologica; il content editor, che cura, controlla, approva e aggiorna i contenuti; il multimedia developer, che realizza la versione multimediale dei contenuti. docente/mentor, che cura il processo di erogazione dei contenuti formativi e quello di apprendimento attraverso varie tipologie di attivita', volte tutte a fornire un supporto per quanto attiene, in particolare, all'impatto con il materiale impiegato e la migliore comprensione dello stesso. Nello specifico, questa figura svolge i seguenti compiti: responsabile della gestione e del monitoraggio di una classe virtuale durante l'intero percorso didattico (attraverso sessioni live, sistemi automatici tipo quiz, correzione di progetti ed elaborati); offre un contributo ai fini della comprensione dei contenuti del corso, rispondendo tempestivamente ai quesiti e alle richieste di chiarimento su chat, forum e e-mail; propone gli aggiornamenti dei contenuti del corso in relazione all'andamento effettivo della classe, in quanto, osservando da vicino le esigenze dei discenti e monitorando le attivita' in grado di comprenderne i punti di forza e le eventuali lacune da colmare; valuta i discenti durante il percorso formativo ed al termine dello stesso; tutor di processo/animatore, che segue il percorso formativo del

discente, per il quale diventa un valido punto di riferimento; assiste e supporta il discente e la classe virtuale, monitorando i vari stadi di apprendimento anche tramite il sistema di «tracciamento»; supporta il discente dal punto di vista emotivo e motivazionale; presta attenzione ai feed-back dei discenti e suggerisce eventuali aggiornamenti dei materiali, se necessari; svolge un ruolo di mediatore nell'ambito del gruppo e funge da «animatore» della classe virtuale sollecitando, con opportuni interventi sul forum, i discenti alla discussione; team tecnico: che formato da coloro che gestiscono gli aspetti tecnici (hardware e software di base e LAN) del progetto di e-learning.

5. Principi guida per la qualita' dei progetti di e-learning

Un progetto di e-learning puo' essere di svariate dimensioni: la sua portata un elemento importante ai fini della progettazione dell'intervento formativo da effettuare, che, nell'ambito della P.A., deve comunque tenere conto del profilo dei destinatari, degli obiettivi da raggiungere, della tipologia dei contenuti e del contesto nel quale viene realizzato. Il procedimento di formazione di questo tipo va studiato analizzandone preliminarmente le dimensioni e deve poi essere progettato non solo in funzione del materiale che a tal fine si rende necessario apprestare, ma anche in vista della realizzazione di servizi che siano poi effettivamente utili per l'utente e della creazione di strumenti - riferiti ad uno specifico ambiente di apprendimento o ad una delle piattaforme disponibili in commercio - adeguati a sostenere un processo interattivo e collaborativo tra i vari attori. I fattori che occorre analizzare per progettare l'intervento formativo on-line, e che vanno poi valutati ai fini della determinazione della portata dello stesso, attengono: alla dimensione dell'ente (che possono essere: enti di piccole dimensioni, enti di grandi dimensioni, o raggruppamenti di enti), all'estensione a livello territoriale (potendosi trattare di amministrazioni centrali e di amministrazioni locali), al comparto di appartenenza dell'ente (sanita', scuola, ecc.), al livello degli strumenti tecnologici in atto disponibili presso l'Ente stesso - ai quali fa riferimento anche il citato decreto 17 aprile 2003 concernente i corsi di studio a distanza - alla professionalita' e alle specifiche competenze dei destinatari ai quali l'intervento formativo diretto. Tenuto conto di tutto cioè, opportuno procedere ad un'analisi del fabbisogno di formazione all'interno della singola amministrazione, in termini di: grado di alfabetizzazione informatica, compiti istituzionalmente attribuiti e funzioni svolte, dotazione di infrastrutture (sedi, aule) e apparecchiature informatiche (hardware e software). Le scelte possono dunque articolarsi su una molteplicita' di parametri e dovrebbero essere operate alla luce di numerose e diversificate condizioni obiettive strettamente connesse alla domanda di formazione in termini di vincoli o peculiari esigenze. Va peraltro tenuto presente che qualsiasi intervento richiede comunque la preventiva adozione di iniziative indispensabili ai fini di un proficuo avvio del progetto di formazione, quali: ricognizione (a livello centrale e a livello decentrato) delle strutture/infrastrutture disponibili, in funzione degli interventi di formazione programmati e pianificazione delle spese che necessario effettuare per il raggiungimento dei prefissati obiettivi; interventi di alfabetizzazione informatica, laddove necessari, per dotare l'utenza quanto meno di adeguata competenza nell'impiego degli strumenti informatici. Questo tipo di intervento deve essere progettato in modo da non frapporre alcun ostacolo in sede di accesso al progetto di formazione, ma favorire, al contrario, un primo approccio agli strumenti e alla cultura propri dell'e-learning o una maggiore familiarita' e confidenza con gli stessi se l'utente ha gia' superato le difficolta' che inevitabilmente si presentano

in sede di primo impatto; sotto questo profilo, in molti casi potrebbe trattarsi di interventi formativi in modalita' blended. A questo proposito, va anche considerato che un processo formativo on-line non consiste nella mera diffusione in rete di materiale, ma anche - e soprattutto - nel rendere disponibili, per l'utente e il gruppo di lavoro (la classe virtuale - CV) un complesso di servizi. In un processo di e-learning l'attenzione deve essere incentrata sull'utente, cui attribuire il ruolo di principale attore; in buona sostanza, la formazione dovrebbe essere intesa come un percorso a cui l'utente partecipa attivamente, quindi come un processo interattivo e di reciproca collaborazione tra le parti che al processo stesso intervengono: concezione, questa, ben lontana da quella che vede la formazione muoversi in unica direzione, che va dal docente al discente. Per erogare i servizi secondo le diverse modalita' interattive, il sistema di e-learning utilizza piattaforme/ambienti di apprendimento che consentono la fruizione dei contenuti attraverso vari strumenti - che dovrebbero essere previsti gia' in fase di progettazione secondo le necessita' dell'intervento formativo - quali: comunicazione e interazione tra le persone (docenti, tutor, esperti della materia, altri discenti, supporto tecnico, ecc.), attraverso sessioni live, servizi di posta elettronica (e-mail), forum, bacheca, chat; interattivita' con i materiali: ad esempio con il ricorso ad esercitazioni con feedback o simulazioni su casi di studio; strumenti di valutazione, e autovalutazione, sia del singolo discente che dell'intera classe, che rivestono importanza e peso decisivi nello svolgimento del processo formativo; monitoraggio continuo, per controllare l'efficienza, l'efficacia e, piu' in generale, la qualita' del processo di e-learning.

Tab. 1. Il processo di *e-learning*

FASE	ATTIVITA'
Individuazione dei destinatari della formazione e delle loro esigenze	
Rilevazione dei dati sul personale relativi a natura e competenza del target	
Individuazione del fabbisogno formativo	Analisi dei fabbisogni individuali, dei ruoli e delle esigenze organizzative, alla luce delle norme che attribuiscono nuovi compiti all'amministrazione, tenuto anche conto della programmazione delle assunzioni, della disciplina contrattuale e degli accordi sindacali
Progettazione vincolata alla normativa generale sugli appalti e servizi, al mercato, alle caratteristiche tecniche della formazione, nonché alle dotazioni tecnologiche e alle metodologie da impiegare	Attenzione agli obiettivi dell'azione formativa

	Considerazione delle caratteristiche dell'organizzazione
	Considerazione delle risorse finanziarie
	Considerazione del numero e delle aree professionali del personale
	Analisi della dotazione hardware e software
	Scelta tra le piattaforme tecnologiche e gli ambienti di apprendimento che consentono la fruizione dei contenuti attraverso vari strumenti
	Definizione dei programmi didattici
	Definizione delle metodologie didattiche
	Definizione dei contenuti relativi ai programmi didattici
	Scelta delle modalita' di erogazione (blended, on line in modalita' sincrona, on line in modalita' asincrona, off line)
	Definizione del sistema di verifica e valutazione individuale
	Definizione del sistema di valutazione e di monitoraggio del programma formativo
Erogazione	Erogazione dei corsi secondo le modalita' del piano di formazione
Monitoraggio e valutazione	Valutazione dell'intervento formativo in termini di apprendimento, crescita delle competenze individuali e cambiamento organizzativo
Aggiornamento del piano di formazione	Rimodulazione del piano formativo a seconda delle criticita' rilevate nella fase di monitoraggio

5.1. Progettazione di un'attivita' di e-learning

Le metodologie didattiche.

L'approccio metodologico adottato per un corso erogato in modalita' e-learning dovrebbe sempre impiegare al meglio tutte le specifiche opportunita' che la rete offre, in particolare l'interattivita' e la multimedialita'. Gli interventi di e-learning di qualita' elevata andrebbero realizzati attraverso percorsi di progettazione incentrati sui fabbisogni formativi rilevati in fase di analisi. Il corsista dovra' essere stimolato a giocare un ruolo attivo, a tal fine disponendo, in primo luogo, di materiali multimediali caratterizzati da un'elevata interattivita' (struttura ipertestuale navigabile finemente, presenza di animazioni esplicative, di laboratori virtuali, di test e di apposite linkografie che consentano di integrare nel percorso le risorse disponibili in rete). Inoltre l'attivita' del corsista dovra' inserirsi in un ambiente di «interazione socializzante» (la classe virtuale), che gli consenta un elevato livello di interazioni con il docente, i tutor e i colleghi. In questo contesto, rappresentano aspetti particolarmente qualificanti di un intervento di e-learning: il ruolo attivo dell'utente; l'importanza della classe virtuale, che comporta l'inserimento dell'utente in un apposito ambiente di apprendimento in comune al quale preposto, sotto il profilo organizzativo, un docente/mentor esperto dei contenuti. Dal punto di vista dell'apprendimento, gli obiettivi vengono raggiunti con maggiore facilita' quando gli utenti ne avvertono consapevolmente la necessita', ovvero quando gli stessi percepiscono l'utilita' dell'apprendimento e il divario, in atto esistente, tra cioè che sanno e quanto ancora potrebbero apprendere. E' utile quindi che il percorso formativo proposto sia cosi' strutturato: life-centered (contestualizzato rispetto all'esperienza personale dei corsisti), task-centered (contestualizzato rispetto allo svolgimento di compiti operativi), problem-centered (basato sulla risoluzione di problemi): si tratta, in sostanza, di organizzare l'esperienza formativa in modo che essa sia strettamente e direttamente collegata ai problemi reali e non puramente teorica e astratta. A questo scopo, importante coinvolgere gli utenti proponendo loro attivita' da svolgere, e progetti integrati, con materiali caratterizzati da elevati livelli di interattivita'. Affinché il ruolo attivo e il coinvolgimento siano costanti per tutta la durata del corso puo' essere utile sviluppare alcune ulteriori scelte opzionali quali, ad esempio:
sollecitare il discente a produrre materiali proponendo esercitazioni o progetti da sviluppare in un preciso arco temporale;

pianificare le attivita' da svolgere, fornendo un calendario o un'agenda settimanale che suggerisca il ritmo di studio consigliato ricordando gli appuntamenti presi e gli impegni da rispettare: dalla consegna dei progetti ai momenti di interazione sincrona. Ogni caso richiede certamente un adeguato grado di flessibilita' nella gestione del ritmo di apprendimento dei discenti; l'impiego di un'agenda consente, peraltro, di stimolare le loro motivazioni e di sincronizzare la classe puntando su attivita' basate sulla reciproca collaborazione, nonché di coordinare il lavoro dei vari corsi nel caso in cui l'utente ne stia seguendo piu' di uno in parallelo. Per favorire l'interazione con i materiali possibile offrire ai corsisti alcuni strumenti specifici, quali: navigazione «fine»: cioè navigazione dei materiali con un'interfaccia semplice, che permetta al discente di riconoscere a che punto si trova, che cosa ha gia' visionato, quale il percorso consigliato, ecc.; laboratori virtuali (con possibili simulazioni interattive): si tratta di animazioni che simulano le

fasi piu' significative di un processo. Quando le simulazioni sono interattive il discente puo' intervenire nella dinamica del processo e modificarne alcuni parametri; esercizi interattivi, da svolgere in ambienti di vario tipo, finalizzati all'approfondimento delle modalita' di «traduzione in pratica» degli insegnamenti teorici; possono essere utilizzati per stimolare la curiosita', favorire il recupero e la razionalizzazione delle conoscenze preesistenti, oppure per consolidare l'apprendimento; test di verifica, rafforzamento e autovalutazione: possono essere semplici domande a risposte chiuse, analisi di casi e di siti web, relazioni a tema, progetti piu' articolati (eventualmente da sviluppare in gruppo). E' importante che questi test siano distribuiti lungo tutto il percorso (all'inizio, in itinere, e al termine del percorso formativo) e che siano impostati e monitorati efficacemente (si veda in proposito il punto 5.2); applicazioni: l'obiettivo di questi strumenti di rafforzare e consolidare i contenuti del corso, rendendoli effettivamente applicabili nella pratica.
Puo' trattarsi di: esercizi svolti, casi di studio, esempi concreti, esempi di «inadeguatezza». La scelta del formato di erogazione dipende dall'articolazione dell'applicazione e dal medium piu' adatto per renderla efficace; linkografie/bibliografie: in questo caso i materiali possono essere integrati con apposite selezioni ragionate operate su siti web, che possono facilitare l'interazione in rete dell'utente. E' fondamentale per il successo di questo tipo di apprendimento che il corsista sia inserito all'interno di una classe virtuale, in modo che si senta parte integrante di un gruppo, sia spinto a partecipare alle discussioni proposte dal tutor e a sviluppare propri elaborati con spirito collaborativo. E' anche utile creare un'atmosfera informale, basata su rispetto reciproco, collaborazione, fiducia, sincerita', apertura agli altri, diffuso gradimento. Con lo sviluppo di teorie che vedono come principale stimolo all'apprendimento l'interazione sociale e con il diffondersi della formazione a distanza, nasce - e acquista sempre piu' significato - il concetto di «comunita' di apprendimento», improntata allo scambio reciproco di informazioni su un argomento di comune interesse, da realizzare non piu' in un ben individuato luogo fisico, ma in un determinato arco di tempo, dedicato appunto alle tematiche oggetto della formazione. Si sottolinea, infine, che durante tutto lo svolgimento del percorso didattico dovrebbero essere costantemente reperibili il docente/mentor, in quanto persona esperta per quanto attiene ai contenuti del processo formativo, ed il tutor di processo, la cui professionalita' improntata all'uso delle tecnologie ed alla gestione delle dinamiche didattico-comunicative dell'e-learning.

5.1.2. I contenuti.

I contenuti formativi, tradotti in materiali da inserire nella piattaforma, devono garantire: differenti modalita' di fruizione, multimedialita' e interattivita': ipertesto, audio-video, animazioni, simulazioni e laboratori virtuali, esercitazioni - valutate e non - ecc. La struttura ormai diffusamente accettata quella del Learning Object (LO), «unita' autoconsistenti» e riutilizzabili in varie combinazioni. Un modulo didattico (un argomento) puo' richiedere un'articolazione in parti, a loro volta costituite da piu' unita' e organizzate in un percorso distinto in varie fasi. Nella predisposizione dei contenuti formativi e nella scelta dell'approccio e degli strumenti didattici da impiegare occorre tenere conto della tipologia dei singoli contenuti e dello scopo cui la formazione mira. Di conseguenza, a titolo di esempio, la possibilita' del riutilizzo delle citate «unita' autoconsistenti» dovrebbe tenere in debita considerazione il fenomeno dell'obsolescenza e la circostanza che il materiale didattico richiede una revisione frequente e non puo',

quindi, essere riutilizzato a lungo. Per quanto attiene alla fruizione, dovrebbe essere prevista, di volta in volta, una combinazione di canali di erogazione (on line sincrono, on line asincrono, off line), e la formazione di classi virtuali attraverso cui sviluppare una continua interattivita'. Infine, riveste, particolare importanza la possibilita' di effettuare il cosiddetto «tracciamento» (tracking) del percorso formativo, delle attivita' del singolo utente e della classe virtuale nel suo insieme. In buona sostanza si tratta di registrare tutto il percorso formativo del discente al fine di permettere al tutor di conoscere - in concreto e nelle varie fasi - lo stadio di apprendimento del discente stesso. Si ricorda ancora una volta che l'adozione diffusa dell'e-learning richiede un preventivo programma di formazione sull'uso della piattaforma adottata, per i formatori e per i destinatari ultimi della formazione stessa. La scarsa conoscenza delle modalita' di uso degli strumenti utilizzati puo' compromettere i risultati del progetto. I contenuti multimediali delle lezioni erogate tramite una piattaforma di e-learning possono concretizzarsi in varie forme. I contenuti in streaming audio/video implicano la presenza di uno streaming server e di player appositi per il formato di streaming sulle postazioni dell'utente. L'erogazione in streaming richiede, inoltre, una disponibilita' di banda internet/intranet notevole e variabile in relazione al numero di lezioni organizzate in contemporanea. Questo aspetto, oltre ad incidere sulle decisioni in merito alla convenienza, o meno, di acquisire sistemi propri, ovvero di utilizzare la modalita' ASP (Application Service Provider), influenza anche indirettamente i programmi di formazione. Infatti, se i corsi da effettuare contemporaneamente non sono numerosi preferibile progettare percorsi di formazione a piccoli gruppi per volta, oppure optare per CBT/WBT (Computer Based Training/Web Basic Training) su CD-Rom. Moduli di formazione WBT, anche all'interno di un sistema LMS (Learning Management System), possono utilizzare sistemi alternativi allo streaming per erogare contenuti audio/video; normalmente essi prevedono il download di sequenze filmate pure o «incapsulate» tramite plug-in multimediali (Flash Player). Si tratta comunque di filmati digitali (avi, mpeg) che richiedono codec appositi ed implicano anch'essi notevoli disponibilita' di banda. I sistemi di virtual classroom sono invece rivolti alla formazione sincrona e quindi all'interazione, in tempo reale, tra docente e discenti. Questi sistemi sono propriamente basati su «communication servers» e comportano applicativi e architetture server dedicate. Essi inoltre non implicano ulteriori requisiti per le postazioni client, dal momento che utilizzano prevalentemente tecnologia flash client e gli impegni di banda di trasmissione sono sostanzialmente paragonabili a quelli dei sistemi di streaming live.

5.1.3. Le tecnologie.

Questi ultimi anni sono stati caratterizzati - come accennato - da cambiamenti fondamentali nel campo delle tecnologie, che hanno fortemente influenzato l'architettura dei sistemi formativi (TBL, Technology Based Learning) che sono arrivati ad una fase - genericamente definita di terza generazione - in cui sono stati ottimizzati il riutilizzo e l'efficienza nei processi di manutenzione dei sistemi e dei contenuti di e-learning. Cio' consente la realizzazione di processi virtuosi per valorizzare al massimo l'investimento a suo tempo effettuato. Il disegno delle architetture di sistema giunto, dunque, ad una definizione codificata e ormai largamente condivisa, basata su due livelli, e le componenti tecnologiche di un sistema di e-learning si possono descrivere in termini di moduli del sistema e di infrastruttura di comunicazione. Allo stato, non ha piu' senso identificare un sistema e-learning in una singola piattaforma monolitica e

omni-comprensiva; , per contro, preferibile concepire tale sistema come costituito da piu' componenti e sottocomponenti, software interoperabili grazie all'adozione di standard internazionali, ed ottimizzato per gestire razionalmente le singole attivita' eterogenee che un processo formativo a distanza su internet puo' sottendere. In particolare, una descrizione semplificata dei sotto-moduli presenti in un sistema e-learning completo, comprende:

1) *learning content management system* (LCMS): il modulo dedicato al processo di creazione, gestione e archiviazione dei contenuti didattici e che ne consente «l'assemblaggio» e la condivisione tramite archivi digitali (Digital Repository). Esso eventualmente integra sistemi di authoring per la produzione delle citate «unita' autoconsistenti» e per il loro aggiornamento;

2) *learning management system* (LMS): il modulo dedicato all'erogazione dei corsi e al tracciamento delle attivita' di formazione, nonché alla gestione delle attivita' amministrative (ad esempio: iscrizione dei discenti, gestione di classi, etc.); esso puo' integrare sistemi di testing;

3) classe virtuale (virtual classroom - VC): il modulo che consente l'organizzazione di eventi dal vivo; il docente, ad esempio, comunica in tempo reale in video, in audio e scambiando dati con i discenti collegati al sistema. Il modulo consente anche la registrazione degli eventi e delle interazioni, al fine di riproporle in modalita' asincrona, e l'integrazione con strumenti idonei a porre in comunicazione tra loro, e a fare cooperare, discenti e docenti e i primi tra loro. Detti strumenti possono essere di tipo sincrono (lavagna virtuale, condivisione di applicazioni e documenti, chat, etc.) e asincrono (e-mail, forum, faq, ecc.);

4) sistema di gestione delle competenze: il modulo che supporta la rilevazione delle competenze, la identificazione dei fabbisogni formativi e la proposta dei relativi percorsi formativi (puo' essere incluso nei sistemi 1 o 2 sopra elencati). Le suddette componenti possono essere in tutto o in parte presenti nel sistema di e-learning in relazione alle esigenze del progetto. La struttura modulare e l'esistenza di standard di interoperabilita' ampiamente condivisi consentono, dunque, la costruzione di un sistema completo e-learning - anche mediante l'utilizzo di componenti fornite da differenti costruttori - contraddistinto da caratteristiche peculiari il cui principale punto di forza rappresentato: dalla diffusione dei Learning Objects - detti anche Reusable Learning Objects (RLOs) - che applicano il concetto di riutilizzabilita' ad una delle componenti piu' onerose all'interno di un processo di e-learning:

la produzione di contenuti in auto-istruzione o SW didattico (courseware). La progettazione e la produzione di materiali didattici secondo tale filosofia prevedono una parcellizzazione ed indicizzazione di contenuti a livello ben piu' «granulare» rispetto ai precedenti sistemi, cosi' da consentire anche per la componente courseware la massima riutilizzabilita' e portabilita' fra sistemi ed all'interno di percorsi formativi diversi. dal livello di «granularita» dei contenuti (dimensione dei LO), lasciato libero all'autore, o al produttore, dei contenuti stessi, anche se generalmente preferibile definire ed adottare un'elevata «granularita» dei contenuti, caratteristica che gioca un ruolo determinante ai fini della loro riutilizzabilita'. Inoltre, una elevata «granularita»

favorisce una maggiore tracciabilita' (tracking), consentendo sistemi avanzati che supportano la personalizzazione dinamica nella sequenzializzazione dei contenuti (sequencing); dalla comparsa e rapida affermazione, a livello internazionale, di specifiche e di standard di interoperabilita' basati su tecnologie XML e Web services per il settore e-learning, riconosciuti e condivisibili tra produttori di sistemi e contenuti su scala internazionale. Sta ora rapidamente consolidandosi come standard de facto - data la sua rapida diffusione e impiego - il set di specifiche redatto dall'ente IMS *Global Learning Consortium*, che raggruppa oltre cinquanta operatori del mercato internazionale. Le varie specifiche dell'ente predetto sono state adottate nell'ambito di numerose iniziative nazionali - e di settore - ed hanno consentito di personalizzare differenti profili applicativi, per l'interoperabilita' dei sistemi informativi pubblici e differenti settori specifici (istruzione, medicina, difesa, ecc.). Il livello di interoperabilita' di un sistema di e-learning identificabile sulla base dei seguenti parametri: integrazione del concetto di Learning Object durante tutto il percorso di creazione, archiviazione, gestione, erogazione e tracciamento di contenuti in autoistruzione, cosi' da consentire la massima flessibilita' di riutilizzo dei contenuti e l'adattamento a specifici percorsi e a condizioni di erogazione eterogenee; maggiore uso possibile della tecnologia XML nella descrizione di strutture di dati (ad esempio: contenuti, dati anagrafici, test valutativi, profili e competenze); impostazione architetturale organizzata per componenti modulari gia' espressa o esprimibile secondo formati aperti ed interoperabili. L'attivita' svolta dagli enti di standardizzazione nel settore dell'e-learning particolarmente vasta e gli obiettivi che gli stessi perseguono consistono nel fornire indicazioni di dettaglio sugli standard che i fornitori di soluzioni tecnologiche, servizi e contenuti dovrebbero proporre nelle loro offerte. La tendenza dunque quella di costruire specifiche per ognuna delle componenti e dei servizi presenti in un sistema di e-learning, nonché per il formato dei contenuti. Questa situazione, unita alla circostanza che diverse organizzazioni si stanno occupando di standardizzazione nel settore, ha portato alla nascita, negli ultimi anni, di decine di specifiche per l'interoperabilita' dei vari sistemi e dati coinvolti in un processo di e-learning, che, peraltro, non sono facilmente applicabili integralmente. Si parla, allora, di profili applicativi specifici che enti ed organismi pubblici utilizzano, come sottoinsieme delle regole standard, nel proprio campo di attivita': ne sono un esempio SCORM (*Sharable Courseweare Object Reference Model*) - adottato dal Ministero della difesa e dal Ministero del lavoro USA - e le specifiche eGif elaborate dal Governo inglese. Al riguardo, si preannuncia in questa sede che - in esito all'emanazione delle presenti «Linee guida» - su indicazione del Ministro per l'innovazione e le tecnologie, il Centro nazionale per l'informatica nella pubblica amministrazione elaborera' e proporra' ai Ministri competenti un «profilo applicativo» per la pubblica amministrazione italiana. Per quanto concerne la progettazione di un'infrastruttura di comunicazione per un sistema di e-learning, le considerazioni che seguono partono dal presupposto che le problematiche legate alla conversione da un metodo tradizionale di formazione in aula al metodo di e-learning siano gia' state risolte (conversione dei contenuti, ri-progettazione dei corsi e del programma di formazione, ecc.), al pari di quelle relative alla gestione dei contenuti. Cio' premesso, vengono qui identificate, e formano oggetto di attenzione, tre aree collegate all'infrastruttura verticale: server, rete e postazione di lavoro individuale. Per quanto concerne l'area server va deciso se il caso di dotarsi di un LMS proprio, o se preferibile acquisire il servizio all'esterno (ASP). Nel primo caso sara' necessario dotarsi di una opportuna infrastruttura - sia hardware che software - e

degli skill sistemistici per l'amministrazione e la gestione dell'infrastruttura. Nel secondo caso dovranno essere risolte le problematiche connesse al collegamento con un centro di erogazione servizi remoto, esterno alla rete intranet, in termini di dimensionamento della banda internet in entrata/uscita e gestione delle politiche di routing e sicurezza. La rete e' l'area che solitamente comporta le maggiori necessita' in termini di adeguamento alle esigenze dei servizi di e-learning. Le problematiche da affrontare e risolvere riguardano, per un verso, la gestione delle politiche di sicurezza nell'accesso da parte di applicazioni esterne alla rete intranet, per altro verso l'accesso degli utenti ad una vasta gamma di applicazioni esterne. Un'altra esigenza meritevole di attenzione attiene all'adeguamento della capacita' di banda all'aumento di traffico generato da applicazioni web based e multimediali ed alla gestione del movimento dei dati su una serie di protocolli non «standard» per una rete intranet. La necessita' di supportare applicazioni multimediali nei servizi di e-learning su una rete di trasporto di dati interessa inoltre sia l'infrastruttura di rete geografica che l'infrastruttura di rete locale. Tali applicazioni richiedono comunicazioni simultanee fra gruppi di computer con trasmissione dei pacchetti IP in modalita' multicast, in un processo conosciuto genericamente come «comunicazione multipunto». Devono, inoltre, essere adeguatamente considerati gli aspetti collegati ai requisiti *hardware* e *software* delle postazioni client, che consentono di fruire dei contenuti di e-learning. Sotto questo profilo, relativamente all'*hardware* e' necessario disporre di una stazione di lavoro attrezzata per gestire contenuti multimediali esigenti in termini di potenza di calcolo, memoria e periferiche audio/video. La configurazione *software* dovra' essere compatibile con il sistema di formazione e-learning prescelto in termini di: caratteristiche del software di base, tipo e versione del software di navigazione, presenza dei componenti richiesti per la fruizione dei contenuti multimediali, con la conseguente esigenza di prevedere la gestione di una software distribution degli applicativi mancanti. 5.2. Erogazione di un'attivita' di e-learning. I servizi La fase di erogazione di un'attivita' di e-learning inizia al momento della fruizione dei contenuti da parte dell'utente e puo' avvenire con diverse modalita', che vengono qui di seguito indicate: on-line in modalita' sincrona, attraverso lo strumento della classe virtuale (CV), in cui gli utenti/discenti interagiscono con un docente o tutor della materia: durante la sessione live i discenti possono parlare, utilizzare materiali in vari formati, navigare sul web sotto la guida del tutor, scrivere su una lavagna, fare dei test, formare gruppi di lavoro guidati; on-line in modalita' asincrona, con una fruizione di contenuti interattivi che favoriscono la partecipazione attiva dell'utente singolo, o della classe virtuale, al processo di apprendimento; puo' trattarsi di testi, ipertesti, voce, animazioni, organizzati dai docenti e dagli editor multimediali e fruibili dalla rete; off line, con l'utilizzo di supporti, quali testi cartacei, CD-rom, video, DVD, altri materiali scaricabili, con possibilita' di stampa dei contenuti in formato testo o immagine. E' anche possibile una combinazione tra le precedenti soluzioni. Non bisogna poi dimenticare - ripetesi - che le attivita' di e-learning sono rivolte a destinatari eterogenei, a livello di ruoli, competenze, familiarita' con gli strumenti di rete. Pertanto puo' essere necessaria una adeguata e corretta integrazione tra la formazione a distanza - cosi' come sopra descritta - e la formazione in aula, ovvero la costruzione di un formato di e-learning blended, per il quale l'intervento formativo in aula resta fondamentale, soprattutto quando si tratta di una utenza che ha ancora poca dimestichezza con le pratiche della formazione on line.

5.3. Monitoraggio e valutazione di un'attivita' di e-learning.

Il monitoraggio e la valutazione costituiscono due fattori fondamentali a garanzia del livello di qualita' della formazione nelle varie fasi che la caratterizzano e sotto il profilo dei risultati raggiunti. La citata direttiva 13 dicembre 2001 ha gia' offerto l'opportunita' di sottolineare l'importanza delle attivita' di monitoraggio e valutazione, prevedendo espressamente che «La formazione dovra' essere sviluppata attraverso un sistema di governo, di monitoraggio e controllo che consenta di valutarne l'efficacia e la qualita». Nella stessa direttiva, inoltre, viene evidenziato che le azioni di monitoraggio e di valutazione hanno lo scopo di rilevare la qualita' dei contenuti, il grado di corrispondenza del progetto e delle azioni alle esigenze del personale, nonche' la qualita' sotto il profilo operativo e gestionale: rientrano in questo contesto l'adeguatezza degli strumenti di formazione alle attivita' a cui si riferiscono ed i sistemi di controllo della qualita' durante i percorsi formativi. Nel documento in parola, inoltre, e' dato rilievo all'attivita' di valutazione delle competenze al fine dell'individuazione del fabbisogno formativo e della definizione di politiche e piani di sviluppo, nonche', e soprattutto, all'attivita' di valutazione degli interventi formativi. Sotto questo profilo occorre individuare non soltanto il gradimento dei singoli partecipanti, ma anche il loro livello e la loro capacita' di apprendimento e i risultati da ciascuno raggiunti: l'obiettivo, infatti, e' quello di verificare la portata del cambiamento che si e' verificato nell'amministrazione in esito alle attivita' formative effettuate. Anche le azioni di monitoraggio di un processo formativo di e-learning - che prevede sia la presenza in aula che la formazione a distanza (blended) - si inquadrano nel percorso delineato e comprendono attivita' di valutazione, che possono essere finalizzate alla stima: della gestione delle azioni formative; dei risultati dei processi formativi; delle competenze, cioe' alla corretta individuazione dei fabbisogni formativi e al raggiungimento dei risultati formativi attesi.

5.3.1. Valutazione delle competenze.

Per «competenza» si intende qui l'integrazione di conoscenze, di capacita' e comportamenti organizzativi che la persona e' in grado di porre in atto per realizzare i risultati professionali richiesti dal processo di erogazione di un servizio, sia esso interno o esterno all'organizzazione. La valutazione delle competenze presuppone che siano preliminarmente definiti: i processi fondamentali di servizio che caratterizzano l'organizzazione; i profili professionali di riferimento e il loro posizionamento rispetto ai processi anzidetti; le specifiche professionalita' di ciascun profilo (in relazione alle diverse fasi dei processi) e gli elementi che le caratterizzano; i processi che consentono di giudicare il patrimonio di competenze posseduto dalle persone e di stimarne il livello acquisito. La valutazione delle competenze - che richiede comunque sempre anche l'autovalutazione da parte del destinatario dell'azione formativa - e' compito del dirigente responsabile dell'azione e si realizza attraverso il confronto tra il profilo di competenza atteso e quello posseduto.

5.3.2. Monitoraggio.

Il monitoraggio consiste nella rilevazione sistematica dei dati - di natura organizzativa, gestionale e attinenti alla funzionalita' (anche tecnologica) - legati ai processi di erogazione dell'attivita' formativa. Questa rilevazione e' finalizzata al controllo, all'eventuale modifica e, in ultima analisi, all'ottimizzazione dei processi formativi stessi. Durante l'azione di monitoraggio vengono rilevati, e ponderati, gli indicatori necessari a verificare - prima dell'avvio del progetto (ex ante), durante lo svolgimento (in itinere) e dopo la conclusione dello stesso (ex post) - la corrispondenza tra il programma definito e la sua realizzazione, compresa l'analisi degli eventuali elementi critici o di rischio.

Formano oggetto di attenzione del monitoraggio:

i processi di erogazione della formazione sia in aula che a distanza, ovvero: gli strumenti per il trasferimento dei contenuti (moduli didattici in vari format, loro relativa qualita' e completezza, efficacia didattica e comunicativa);

la tipologia della docenza (sincrona e asincrona);

l'assistenza didattica e motivazionale svolta a distanza. le funzionalita' del sistema organizzativo /gestionale /logistico (ambienti, infrastrutture, sistemi di registrazione, iscrizione e tracking);

le funzionalita' della piattaforma di gestione in relazione al loro impatto sull'erogazione dei percorsi formativi. La raccolta e l'elaborazione dei dati forniti dall'azione di monitoraggio, anche nei percorsi blended, puo' essere gestita integralmente dal sistema: e' essenziale a tal fine provvedere ad una verifica dello spettro dei dati «tracciabili» e delle funzioni di elaborazione predisposte.

5.3.3. Valutazione degli interventi formativi.

L'attivita' di valutazione - intesa come ponderazione e interpretazione di dati ed elementi rilevati durante l'azione formativa e a valle dei processi realizzati - e' finalizzata a evidenziare i risultati raggiunti, in termini di modifiche verificate e riscontrabili. Questa valutazione, che attiene, sia alle persone coinvolte che all'organizzazione nel suo complesso, si basa sulla misurazione dei risultati oggetto di osservazione, che sulla quantificazione del divario riscontrato rispetto agli standard (parametri ed indicatori che ciascuna amministrazione deve rilevare), qualitativi e quantitativi, definiti in fase di progettazione. Degli strumenti di valutazione vanno verificate: l'affidabilita', cioe' la persistenza di osservazione nel tempo e in contesti differenti; la validita' e l'efficacia, che non devono essere soggette a possibili azioni di disturbo da parte di fenomeni esterni; l'utilita', cioe' la capacita' di valutare esattamente l'oggetto al quale sono destinati.

6. Componenti di costo di un progetto di e-learning.

Gli elementi di costo di un progetto complesso possono essere rappresentati con diverse modalita' che, in relazione alla dimensione del progetto stesso, tengono conto:

1. delle fasi in cui esso si articola;
2. delle componenti del sistema e delle risorse umane;
3. dei rapporti con i fornitori. Si indicano, qui di seguito, le componenti di costo definite sulla base delle modalita' di esecuzione del progetto e delle dimensioni prese in considerazione. Per quanto attiene alle fasi in cui si articola, l'e-learning puo' essere descritto come un processo che comprende i seguenti sotto-processi:

a) analisi;
b) disegno;
c) sviluppo;
d) implementazione;
e) valutazione.

Per quanto riguarda le componenti del sistema e le risorse umane, la struttura dei costi sottesa ad un sistema e-learning - come accennato nella direttiva - e' in larga parte commisurata all'insieme dei seguenti fattori:

1. analisi organizzativa;
2. servizi (progettazione, erogazione, gestione e monitoraggio);
3. tecnologie (piattaforme e infrastrutture);
4. contenuti (produzione e manutenzione).

Questi ultimi rappresentano la componente tendenzialmente piu' onerosa, in termini economici, qualitativi o organizzativi. Il motivo di fondo e' legato alla necessita' di disporre di figure professionali specifiche per il processo di generazione dei materiali (almeno per quanto concerne il Project Manager, l'Instructional Designer, l'esperto dei contenuti e il team di sviluppo).

Cio' impone un'attenta valutazione in ordine alle opzioni da operare circa:

1.l'acquisizione di materiali cosiddetti off-the-shelves, ossia a catalogo;

2. la progettazione e la costruzione dei materiali:

    a. da parte della stessa amministrazione;
    b. da parte del fornitore.

La scelta da effettuare e' legata ad un esame comparativo che tiene conto, da un lato, della rispondenza dei contenuti alle esigenze formative dello specifico progetto; dall'altro, dell'impegno economico che viene richiesto. Per le altre componenti, come detto, esistono varie soluzioni disponibili e tra loro integrabili - che possono essere offerte anche da differenti prodotti/fornitori - per progettare e realizzare un sistema e-learning. Per quanto riguarda i rapporti con i fornitori, nell'ambito delle varie piattaforme, uno dei criteri economici piu' significativi da considerare per la scelta di soluzioni e componenti tecnologiche differenti e' rappresentato dalla valutazione del modello di licenze proposto dal fornitore. Quest'ultimo, infatti, potra' fortemente

influenzare, a parita' di funzionalita' tecniche offerte, la scelta in base alla valutazione economica dei differenti sistemi. Esistono diversi modelli di licenze per i singoli componenti, che presentano caratteristiche economiche diverse; al riguardo il progettista dovra' identificare e farsi indicare nel dettaglio, dal fornitore, la tipologia di licenza adottata per ogni specifico componente fornito. I modelli di licenze attualmente utilizzati per i vari componenti e-learning (in particolare, LMS, LCMS e VC) sono:

a) licenze off line, a licenza installata su singolo pc: prevedono un costo a postazione senza interazione/verifica su server centrale e sono particolarmente impiegate per sistemi e tool autore; possono essere a nominativo o a installazione fisica: il secondo tipo e' preferibile in quanto, a parita' di utenze acquisite, consente l'accesso a qualunque utente;
b) licenze a utenti nominali: prevedono un costo a postazione per utente nominale registrato, senza possibilita' di variare i nominativi iscritti; la verifica puo' essere effettuata su base unicamente contrattuale o mediante autenticazione/verifica su server centrale;
c) licenze a utenti non nominali: sono analoghe alle precedenti, ma offrono, inoltre, la possibilita' di riallocazione della stessa licenza ad un altro utente;
d) licenze a utenti concorrenti: prevedono un costo per ogni utente collegato in contemporanea al server centrale; sono molto usate per piattaforme sincrone e stanno comparendo anche in unaversione che presenta opzioni per sistemi LMS asincroni. Per paragonare i costi di licenze a utenti concorrenti a quelli di licenze a utenti nominali (seats) occorre valutare quanti utenti saranno contemporaneamente attivi rispetto a quelli iscritti al servizio;
e) licenze a server (CPU): prevedono un costo a server centrale a volte piu' elevato rispetto a quelli dei modelli precedenti; nel caso di valutazione alternativa a quella di licenze ad utenti non nominali, occorre stimare il numero prevedibile di utenti che il server centrale deve supportare;
f) servizi ASP: prevedono l'erogazione di servizi con un sistema installato presso terzi, con licenze a consumo e possibilita' di quantificazione a corso/mese/utente. Poiche' esistono molte tipologie di servizi ASP e' opportuno considerare se i relativi costi includono quelli di connettivita' e housing/hosting della soluzione e, inoltre, se esistono limiti massimi di corsi e durate temporali minime per la sottoscrizione al servizio.

L'Ente che intende avviare corsi di e-learning per i propri dipendenti, deve tener conto, infine, delle seguenti voci:

costi ripartiti su piu' attivita' formative:
computer e accessori adeguati;
installazione adeguata per connessione rete; disponibilita' di soluzioni hardware (server dedicati, connessioni veloci, consumi di utilizzo);
personale tecnico di servizio; tempo da dedicare al corso per partecipante; acquisti di materiali di supporto;
spese generali per utenze di ufficio (elettricita', telefono, riscaldamento, etc.);
promozione istituzionale, costi diretti per singolo corso: spese di trasferta, per ciascun partecipante, relative alla sua eventuale partecipazione a sessioni di formazione da svolgere in aula;

oneri connessi alla realizzazione di eventuali sessioni di formazione in aula (affitto di locali attrezzati, spese di viaggio e soggiorno sostenute per i docenti, spese per materiali di consumo e per materiali didattici).

7. Considerazioni finali

L'emanazione, da parte del Centro nazionale per l'informatica nella pubblica amministrazione, di queste «Linee guida» - che, come detto, formano parte integrante della direttiva in materia di e-learning delle pubbliche amministrazioni - testimonia l'attenzione rivolta al processo innovativo che sempre piu' in questi anni, sta caratterizzando l'attivita' di formazione, alla luce di un crescente e maggiormente diffuso impiego delle nuove tecnologie informatiche. Questo fenomeno trova adeguata spiegazione se si considerano i peculiari aspetti, di ordine organizzativo e metodologico - oltre che tecnologico - propri della formazione in modalita' e-learning, anche in considerazione del rilevante impatto che essa presenta sull'organizzazione del lavoro nel suo complesso e nei suoi molteplici aspetti. A questa riflessione di base e' improntato il documento, il cui impianto si innesta, in piena sintonia, nel percorso idealmente e concretamente tracciato con la direttiva 13 dicembre 2001, cui ha fatto seguito il programma di interventi sul sistema Paese contenuto nelle «Linee guida» emanate nel giugno 2002 dal Ministro per l'innovazione e le tecnologie, fino ad arrivare, piu' recentemente, al decreto 17 aprile 2003 riguardante le Universita'. Al pari delle iniziative richiamate, anche la presente - che le segue in ordine temporale - e' una tangibile espressione dell'interesse, e dell'impegno, che negli ultimi anni il Governo italiano - come molti altri in ambito europeo - sta dedicando al raggiungimento dell'obiettivo di imprimere una sensibile accelerazione allo sviluppo delle conoscenze con il ricorso a soluzioni virtuali. E cio', nella consapevolezza che esse sono finalizzate all'interoperabilita' dei contenuti e, in ultima analisi, dei servizi resi agli utenti, il cui livello qualitativo e', in larga misura, condizionato dalla progettazione didattica e dall'architettura tecnologica.

D.M. 22 febbraio 2005

Procedure per l'assegnazione dei contributi per apparati per trasmissione o ricezione a larga banda dei dati via Internet.

IL MINISTRO DELLE COMUNICAZIONI

di concerto con

IL MINISTRO DELL'ECONOMIA E DELLE FINANZE

Vista la *legge 30 dicembre 2004, n. 311* (legge finanziaria per l'anno 2005) concernente «Disposizioni per la formazione del bilancio annuale e pluriennale dello Stato» ed in particolare l'art. 1, comma 212;

Ritenuto di dover dare attuazione alle disposizioni contenute nell'art. 1, comma 212 della predetta *legge 30 dicembre 2004, n. 311* concernenti i contributi per agevolare l'accesso alla larga banda ad Internet;

DECRETA:

Art. 1.

Procedure per l'assegnazione dei contributi per apparati per trasmissione o ricezione a larga banda dei dati via Internet.

1. I contributi di cui all'art. 1, comma 212, della *legge 30 dicembre 2004, n. 311*, stabiliti nella misura di € 50 per ciascun accesso, elevata ad € 75 qualora l'accesso alla rete fissa o alla rete mobile UMTS da parte dell'utente ricada nei comuni il cui territorio sia ricompreso nelle aree di cui all'obiettivo 1 del regolamento (CE) n. 1260/1999 del 21 giugno 1999 del Consiglio, e comunque in quelli con popolazione inferiore a diecimila abitanti, sono erogati per il tramite degli operatori di comunicazioni elettroniche con i quali gli utenti abbiano stipulato un contratto di abbonamento annuale al servizio di accesso a larga banda ad Internet. La concessione del contributo disposta entro il limite di spesa indicato al medesimo art. 1, comma 212, della legge.

2. I contributi vengono corrisposti mediante uno sconto di ammontare corrispondente al contributo previsto per ciascun accesso, praticato sull'ammontare dei contratti di abbonamento al servizio di accesso a larga banda ad Internet stipulati a decorrere dal 1° dicembre 2004. Nel caso in cui il contratto di abbonamento al servizio di accesso alla larga banda ad Internet sia stipulato con un operatore di rete mobile UMTS il contributo riconosciuto a condizione che il traffico telefonico fatturato dall'operatore di rete mobile sia per almeno il 30% derivante dalla trasmissione o ricezione a larga banda dei dati via Internet.

3. Il contributo di cui al comma 1 non può essere cumulato, nell'àmbito della stessa offerta commerciale, con il contributo di € 70 di cui all'art. 1, comma 211, della citata

legge 30 dicembre 2004, n. 311, quando erogati, direttamente o indirettamente, da parte dello stesso fornitore nei confronti del medesimo utente.

4. Ai fini dell'erogazione dei contributi, con provvedimento del Ministero, sono stabilite le tipologie e la struttura tecnica dei lotti di autorizzazioni preventive, da rilasciare agli operatori di comunicazioni elettroniche di cui al comma 1 che ne facciano richiesta, ciascuna contenente l'ammontare dello stanziamento relativo al singolo lotto, che stabilito sulla base dei dati di vendita degli accessi a larga banda ad Internet per tipologia di operatore. A tale scopo il Ministero richiede ad un campione rappresentativo di operatori di telecomunicazioni i dati di vendita relativi al mese di novembre. Il provvedimento adottato entro venti giorni dall'entrata in vigore del presente decreto[137]

5. Le tipologie di lotto possono essere modificate in qualsiasi momento dal Ministero, d'ufficio o su istanza degli operatori, debitamente documentata.

Art. 2.

Assegnazione dei lotti di autorizzazioni preventive e rimborso dei contributi erogati

1. A ciascun operatore di comunicazioni elettroniche di cui all'art. 1, comma 1, che risulti assegnatario dei lotti di autorizzazioni preventive ai sensi del presente articolo, sono rimborsati i contributi erogati, in relazione ai contratti di abbonamento al servizio di accesso a larga banda stipulati a decorrere dal 1° dicembre 2004, ai beneficiari propri utenti. I rimborsi sono effettuati nei limiti del fondo assegnato e seguendo l'ordine cronologico dei contratti.

2. I lotti di autorizzazioni preventive sono assegnati ai soggetti di cui al comma 1, che ne abbiano fatto richiesta scritta a mezzo di raccomandata entro dieci giorni dalla data di pubblicazione del provvedimento di cui all'art. 1, comma 4. I lotti, la cui validità massima pari a trenta giorni, sono assegnati a ciascun soggetto entro dieci giorni lavorativi dalla data della comunicazione dell'attivazione del proprio sistema informativo di cui al comma 4 del presente articolo.

3. Per ottenere il rimborso dei contributi e l'eventuale assegnazione di un successivo lotto i soggetti di cui al comma 1 devono inviare al Ministero il documento elettronico contenente gli estremi degli abbonamenti al servizio di accesso a larga banda riferiti al lotto già assegnato.

4. A tal fine i soggetti di cui al comma 1 forniscono al Ministero al momento della presentazione della domanda di cui al comma 2 gli identificativi informatici (indirizzo IP statico e password) di un proprio sistema informativo (server) che operi su Internet con protocollo FTP (File Tranfer Protocol) e consenta l'accesso dall'esterno in sola lettura. Il sistema informativo, realizzato dal soggetto assegnatario del lotto di autorizzazioni preventive e dal medesimo gestito sotto la propria responsabilità, deve

[137] In attuazione di quanto disposto dal presente comma vedi il *D.Dirett. 6 aprile 2005.*

contenere un documento elettronico per ciascun lotto di contributi assegnato con i dati identificativi dei beneficiari che hanno usufruito del contributo, della data dei relativi contratti di fornitura del servizio di accesso a larga banda e dell'operatore che fornisce il servizio stesso.

5. I soggetti di cui al comma 1 comunicano al Ministero, mediante posta elettronica con avviso di ricevimento, la presenza sul proprio sito FTP del file contenente le informazioni sugli utenti che hanno fruito dei contributi relativi al corrente lotto di autorizzazioni preventive assegnato.

6. L'avviso relativo al file di cui al comma 5 inviato dal soggetto assegnatario al termine dell'assegnazione di tutti i contributi ad esso relativi e comunque non oltre il trentesimo giorno dal completamento dell'assegnazione del lotto medesimo. Decorso tale termine non sono più assegnati contributi a valere sul lotto in questione.

7. Il Ministero, entro il decimo giorno lavorativo seguente a quello di segnalazione dell'avviso di cui al comma 5, effettuati i necessari controlli sui dati forniti e sulla consistenza dello stanziamento residuo, rilascia, o segnala di non poter rilasciare, l'autorizzazione ad un lotto successivo, identico al precedente.

8. Entro dieci giorni lavorativi dal rilascio dell'autorizzazione ad un lotto successivo, il Ministero emette un mandato di pagamento, per una quota parte della cifra relativa al rimborso dei contributi riconosciuti, a favore del soggetto assegnatario relativo al lotto precedente. La parte rimanente del rimborso sarà liquidata, insieme alle eventuali compensazioni finanziarie, al termine della gestione dei fondi residui di cui al seguente comma 10. La percentuale di liquidazione del rimborso stabilita con il provvedimento di cui all'art. 1, comma 4.

9. Il Ministero, entro il secondo giorno lavorativo seguente a quello di segnalazione ad un soggetto assegnatario di non poter rilasciare l'autorizzazione ad un lotto di contributi avendo valutato prossimo l'esaurimento dei fondi, rende pubblica la medesima valutazione di esaurimento fondi attraverso le procedure di cui all'art. 3, riservandosi di emettere un provvedimento ai sensi dell'art. 1, comma 5, per la revisione delle tipologie di lotto, in vista dell'assegnazione dei fondi residui.

10. Entro centoventi giorni dalla data di pubblicazione dell'avviso di esaurimento fondi di cui al comma precedente, ciascun soggetto assegnatario deve segnalare, mediante avviso in posta elettronica e file sul sito FTP, i dati relativi ai beneficiari dei lotti al medesimo assegnati, per i quali non sia intervenuta, per qualsiasi motivo, la stipula del contratto e l'attivazione del servizio oppure per i quali sia intervenuto il recesso del contratto. I contributi relativi ai suddetti beneficiari vengono scorporati dal relativo lotto, compensati finanziariamente con il soggetto assegnatario ed entrano a far parte dei fondi residui non assegnati. Gli operatori di rete mobile UMTS assegnatari di lotti di autorizzazioni preventive entro il medesimo termine devono far pervenire all'amministrazione una certificazione, sottoscritta dal legale rappresentante e dal cliente a favore del quale erogato il contributo, che attesti il rispetto del requisito previsto dall'art. 1, comma 2.

Art. 3.

Pubblicità.

1. Il Ministero pubblica sul proprio sito Internet una pagina informativa concernente l'ammontare residuo dello stanziamento tenuto conto di tutti i lotti di autorizzazioni preventive assegnati, fino a quel momento, ai soggetti autorizzati. L'aggiornamento dello stanziamento residuo e l'eventuale avviso di prossimo esaurimento fondi sono effettuati all'assegnazione di ciascun lotto di autorizzazioni preventive ai soggetti di cui all'art. 1, comma 1.

Art. 4.

Revoca del contributo.

1. Qualora risulti che la concessione dei contributi erogati ai sensi del presente decreto stata determinata da dichiarazioni errate o mendaci o false attestazioni il contributo revocato, previa contestazione, in esito a un procedimento in contraddittorio.

2. La revoca dei contributi comporta l'obbligo di riversare all'erario, entro i termini fissati dal provvedimento stesso, l'intero ammontare percepito, rivalutato secondo gli indici ufficiali ISTAT di inflazione in rapporto ai «prezzi al consumo per le famiglie di operai e di impiegati», oltre agli interessi corrispettivi al tasso legale.

3. Ove l'obbligato non ottemperi al versamento entro i termini fissati, il recupero coattivo dei contributi e degli accessori al contributo stesso, rivalutazione e interessi, viene disposto mediante iscrizione al ruolo.

NORMATIVA COMUNITARIA E COMUNICAZIONI ISTITUZIONALI

CONVENZIONE EUROPEA SUI BREVETTI

ARTT. 5-8, DA 51 A 63

Artikel 4a
Konferenz der Minister der Vertragsstaaten

Eine Konferenz der für Angelegenheiten des Patentwesens zuständigen Minister der Vertragsstaaten tritt mindestens alle fünf Jahre zusammen, um über Fragen der Organisation und des europäischen Patentsystems zu beraten.

Kapitel II

Die Europäische Patentorganisation

Artikel 5
Rechtsstellung

(1) Die Organisation besitzt Rechtspersönlichkeit.

(2) Die Organisation besitzt in jedem Vertragsstaat die weitestgehende Rechts- und Geschäftsfähigkeit, die juristischen Personen nach dessen Rechtsvorschriften zuerkannt ist; sie kann insbesondere bewegliches und unbewegliches Vermögen erwerben und veräußern sowie vor Gericht stehen.

(3) Der Präsident des Europäischen Patentamts vertritt die Organisation.

Artikel 6
Sitz

(1) Die Organisation hat ihren Sitz in München.

(2) Das Europäische Patentamt befindet sich in München. Es hat eine Zweigstelle in Den Haag.

Artikel 7
Dienststellen des Europäischen Patentamts

In den Vertragsstaaten und bei zwischenstaatlichen Organisationen auf dem Gebiet des gewerblichen Rechtsschutzes können, soweit erforderlich und vorbehaltlich der Zustimmung des betreffenden Vertragsstaats oder der betreffenden Organisation, durch Beschluss des Verwaltungsrats Dienststellen des Europäischen Patentamts zu Informations- oder Verbindungszwecken geschaffen werden.

Artikel 8
Vorrechte und Immunitäten

Die Organisation, die Mitglieder des Verwaltungsrats, die Bediensteten des Europäischen Patentamts und die sonstigen Personen, die in dem diesem Übereinkommen beigefügten

Article 4a
Conference of ministers of the Contracting States

A conference of ministers of the Contracting States responsible for patent matters shall meet at least every five years to discuss issues pertaining to the Organisation and to the European patent system.

Chapter II

The European Patent Organisation

Article 5
Legal status

(1) The Organisation shall have legal personality.

(2) In each of the Contracting States, the Organisation shall enjoy the most extensive legal capacity accorded to legal persons under the national law of that State; it may in particular acquire or dispose of movable and immovable property and may be a party to legal proceedings.

(3) The President of the European Patent Office shall represent the Organisation.

Article 6
Headquarters

(1) The Organisation shall have its headquarters in Munich.

(2) The European Patent Office shall be located in Munich. It shall have a branch at The Hague.

Article 7
Sub-offices of the European Patent Office

By decision of the Administrative Council, sub-offices of the European Patent Office may be created, if need be, for the purpose of information and liaison, in the Contracting States and with intergovernmental organisations in the field of industrial property, subject to the approval of the Contracting State or organisation concerned.

Article 8
Privileges and immunities

The Protocol on Privileges and Immunities annexed to this Convention shall define the conditions under which the Organisation, the members of the Administrative Council, the

Article 4bis
Conférence des ministres des Etats contractants

Une conférence des ministres des Etats contractants compétents en matière de brevets se réunit au moins tous les cinq ans pour examiner les questions relatives à l'Organisation et au système du brevet européen.

Chapitre II

L'Organisation européenne des brevets

Article 5
Statut juridique

(1) L'Organisation a la personnalité juridique.

(2) Dans chacun des Etats contractants, l'Organisation possède la capacité juridique la plus large reconnue aux personnes morales par la législation nationale ; elle peut notamment acquérir ou aliéner des biens immobiliers et mobiliers et ester en justice.

(3) Le Président de l'Office européen des brevets représente l'Organisation.

Article 6
Siège

(1) L'Organisation a son siège à Munich.

(2) L'Office européen des brevets est situé à Munich. Il a un département à La Haye.

Article 7
Agences de l'Office européen des brevets

Par décision du Conseil d'administration, des agences de l'Office européen des brevets peuvent être créées, en tant que de besoin, dans un but d'information ou de liaison, dans les Etats contractants ou auprès d'organisations intergouvernementales compétentes en matière de propriété industrielle, sous réserve du consentement de l'Etat contractant concerné ou de l'organisation concernée.

Article 8
Privilèges et immunités

Le protocole sur les privilèges et immunités annexé à la présente convention définit les conditions dans lesquelles l'Organisation, les membres du Conseil d'administration, les

d) die Sätze der in den Artikeln 39, 40 und 47 vorgesehenen Zinsen;

e) die Art und Weise der Berechnung der nach Artikel 146 zu leistenden Beiträge;

f) Zusammensetzung und Aufgaben eines Haushalts- und Finanzausschusses, der vom Verwaltungsrat eingesetzt werden soll;

g) die dem Haushaltsplan und dem Jahresabschluss zugrunde zu legenden allgemein anerkannten Rechnungslegungsgrundsätze.

Artikel 51
Gebühren

(1) Das Europäische Patentamt kann Gebühren für die nach diesem Übereinkommen durchgeführten amtlichen Aufgaben und Verfahren erheben.

(2) Fristen für die Entrichtung von Gebühren, die nicht bereits im Übereinkommen bestimmt sind, werden in der Ausführungsordnung festgelegt.

(3) Sieht die Ausführungsordnung vor, dass eine Gebühr zu entrichten ist, so werden dort auch die Rechtsfolgen ihrer nicht rechtzeitigen Entrichtung festgelegt.

(4) Die Gebührenordnung bestimmt insbesondere die Höhe der Gebühren und die Art und Weise, wie sie zu entrichten sind.

ZWEITER TEIL

MATERIELLES PATENTRECHT

Kapitel I

Patentierbarkeit

Artikel 52
Patentierbare Erfindungen

(1) Europäische Patente werden für Erfindungen auf allen Gebieten der Technik erteilt, sofern sie neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind.

(2) Als Erfindungen im Sinne des Absatzes 1 werden insbesondere nicht angesehen:

a) Entdeckungen, wissenschaftliche Theorien und mathematische Methoden;

b) ästhetische Formschöpfungen;

(d) the rates of interest provided for in Articles 39, 40 and 47;

(e) the method of calculating the contributions payable by virtue of Article 146;

(f) the composition of and duties to be assigned to a Budget and Finance Committee which should be set up by the Administrative Council;

(g) the generally accepted accounting principles on which the budget and the annual financial statements shall be based.

Article 51
Fees

(1) The European Patent Office may levy fees for any official task or procedure carried out under this Convention.

(2) Time limits for the payment of fees other than those fixed by this Convention shall be laid down in the Implementing Regulations.

(3) Where the Implementing Regulations provide that a fee shall be paid, they shall also lay down the legal consequences of failure to pay such fee in due time.

(4) The Rules relating to Fees shall determine in particular the amounts of the fees and the ways in which they are to be paid.

PART II

SUBSTANTIVE PATENT LAW

Chapter I

Patentability

Article 52
Patentable inventions

(1) European patents shall be granted for any inventions, in all fields of technology, provided that they are new, involve an inventive step and are susceptible of industrial application.

(2) The following in particular shall not be regarded as inventions within the meaning of paragraph 1:

(a) discoveries, scientific theories and mathematical methods;

(b) aesthetic creations;

d) les taux d'intérêts prévus aux articles 39, 40 et 47 ;

e) les modalités de calcul des contributions à verser au titre de l'article 146 ;

f) la composition et les tâches d'une commission du budget et des finances qui devrait être instituée par le Conseil d'administration ;

g) les principes comptables généralement admis sur lesquels se fondent le budget et les états financiers annuels.

Article 51
Taxes

(1) L'Office européen des brevets peut percevoir des taxes pour toute tâche ou procédure officielle exécutée en vertu de la présente convention.

(2) Les délais de paiement des taxes autres que ceux fixés par la présente convention sont prévus dans le règlement d'exécution.

(3) Lorsque le règlement d'exécution prescrit le paiement d'une taxe, il prévoit également les conséquences juridiques du défaut de paiement dans les délais.

(4) Le règlement relatif aux taxes fixe notamment le montant des taxes et leur mode de perception.

DEUXIEME PARTIE

DROIT DES BREVETS

Chapitre I

Brevetabilité

Article 52
Inventions brevetables

(1) Les brevets européens sont délivrés pour toute invention dans tous les domaines technologiques, à condition qu'elle soit nouvelle, qu'elle implique une activité inventive et qu'elle soit susceptible d'application industrielle.

(2) Ne sont pas considérés comme des inventions au sens du paragraphe 1 notamment :

a) les découvertes, les théories scientifiques et les méthodes mathématiques ;

b) les créations esthétiques ;

c) Pläne, Regeln und Verfahren für gedankliche Tätigkeiten, für Spiele oder für geschäftliche Tätigkeiten sowie Programme für Datenverarbeitungsanlagen;

d) die Wiedergabe von Informationen.

(3) Absatz 2 steht der Patentierbarkeit der dort genannten Gegenstände oder Tätigkeiten nur insoweit entgegen, als sich die europäische Patentanmeldung oder das europäische Patent auf diese Gegenstände oder Tätigkeiten als solche bezieht.

Artikel 53
Ausnahmen von der Patentierbarkeit

Europäische Patente werden nicht erteilt für:

a) Erfindungen, deren gewerbliche Verwertung gegen die öffentliche Ordnung oder die guten Sitten verstoßen würde; ein solcher Verstoß kann nicht allein daraus hergeleitet werden, dass die Verwertung in allen oder einigen Vertragsstaaten durch Gesetz oder Verwaltungsvorschrift verboten ist;

b) Pflanzensorten oder Tierrassen sowie im Wesentlichen biologische Verfahren zur Züchtung von Pflanzen oder Tieren. Dies gilt nicht für mikrobiologische Verfahren und die mithilfe dieser Verfahren gewonnenen Erzeugnisse;

c) Verfahren zur chirurgischen oder therapeutischen Behandlung des menschlichen oder tierischen Körpers und Diagnostizierverfahren, die am menschlichen oder tierischen Körper vorgenommen werden. Dies gilt nicht für Erzeugnisse, insbesondere Stoffe oder Stoffgemische, zur Anwendung in einem dieser Verfahren.

Artikel 54
Neuheit

(1) Eine Erfindung gilt als neu, wenn sie nicht zum Stand der Technik gehört.

(2) Den Stand der Technik bildet alles, was vor dem Anmeldetag der europäischen Patentanmeldung der Öffentlichkeit durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise zugänglich gemacht worden ist.

(3) Als Stand der Technik gilt auch der Inhalt der europäischen Patentanmeldungen in der ursprünglich eingereichten Fassung, deren Anmeldetag vor dem in Absatz 2 genannten

(c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers;

(d) presentations of information.

(3) Paragraph 2 shall exclude the patentability of the subject-matter or activities referred to therein only to the extent to which a European patent application or European patent relates to such subject-matter or activities as such.

Article 53
Exceptions to patentability

European patents shall not be granted in respect of:

(a) inventions the commercial exploitation of which would be contrary to "ordre public" or morality; such exploitation shall not be deemed to be so contrary merely because it is prohibited by law or regulation in some or all of the Contracting States;

(b) plant or animal varieties or essentially biological processes for the production of plants or animals; this provision shall not apply to microbiological processes or the products thereof;

(c) methods for treatment of the human or animal body by surgery or therapy and diagnostic methods practised on the human or animal body; this provision shall not apply to products, in particular substances or compositions, for use in any of these methods.

Article 54
Novelty

(1) An invention shall be considered to be new if it does not form part of the state of the art.

(2) The state of the art shall be held to comprise everything made available to the public by means of a written or oral description, by use, or in any other way, before the date of filing of the European patent application.

(3) Additionally, the content of European patent applications as filed, the dates of filing of which are prior to the date referred to in paragraph 2 and which were published on or after

c) les plans, principes et méthodes dans l'exercice d'activités intellectuelles, en matière de jeu ou dans le domaine des activités économiques, ainsi que les programmes d'ordinateur ;

d) les présentations d'informations.

(3) Le paragraphe 2 n'exclut la brevetabilité des éléments qu'il énumère que dans la mesure où la demande de brevet européen ou le brevet européen concerne l'un de ces éléments, considéré en tant que tel.

Article 53
Exceptions à la brevetabilité

Les brevets européens ne sont pas délivrés pour :

a) les inventions dont l'exploitation commerciale serait contraire à l'ordre public ou aux bonnes moeurs, une telle contradiction ne pouvant être déduite du seul fait que l'exploitation est interdite, dans tous les Etats contractants ou dans plusieurs d'entre eux, par une disposition légale ou réglementaire ;

b) les variétés végétales ou les races animales ainsi que les procédés essentiellement biologiques d'obtention de végétaux ou d'animaux, cette disposition ne s'appliquant pas aux procédés microbiologiques et aux produits obtenus par ces procédés ;

c) les méthodes de traitement chirurgical ou thérapeutique du corps humain ou animal et les méthodes de diagnostic appliquées au corps humain ou animal, cette disposition ne s'appliquant pas aux produits, notamment aux substances ou compositions, pour la mise en oeuvre d'une de ces méthodes.

Article 54
Nouveauté

(1) Une invention est considérée comme nouvelle si elle n'est pas comprise dans l'état de la technique.

(2) L'état de la technique est constitué par tout ce qui a été rendu accessible au public avant la date de dépôt de la demande de brevet européen par une description écrite ou orale, un usage ou tout autre moyen.

(3) Est également considéré comme compris dans l'état de la technique le contenu de demandes de brevet européen telles qu'elles ont été déposées, qui ont une date de dépôt anté-

Tag liegt und die erst an oder nach diesem Tag veröffentlicht worden sind.

(4) Gehören Stoffe oder Stoffgemische zum Stand der Technik, so wird ihre Patentierbarkeit durch die Absätze 2 und 3 nicht ausgeschlossen, sofern sie zur Anwendung in einem in Artikel 53 c) genannten Verfahren bestimmt sind und ihre Anwendung in einem dieser Verfahren nicht zum Stand der Technik gehört.

(5) Ebensowenig wird die Patentierbarkeit der in Absatz 4 genannten Stoffe oder Stoffgemische zur spezifischen Anwendung in einem in Artikel 53 c) genannten Verfahren durch die Absätze 2 und 3 ausgeschlossen, wenn diese Anwendung nicht zum Stand der Technik gehört.

Artikel 55
Unschädliche Offenbarungen

(1) Für die Anwendung des Artikels 54 bleibt eine Offenbarung der Erfindung außer Betracht, wenn sie nicht früher als sechs Monate vor Einreichung der europäischen Patentanmeldung erfolgt ist und unmittelbar oder mittelbar zurückgeht:

a) auf einen offensichtlichen Missbrauch zum Nachteil des Anmelders oder seines Rechtsvorgängers oder

b) auf die Tatsache, dass der Anmelder oder sein Rechtsvorgänger die Erfindung auf amtlichen oder amtlich anerkannten Ausstellungen im Sinn des am 22. November 1928 in Paris unterzeichneten und zuletzt am 30. November 1972 revidierten Übereinkommens über internationale Ausstellungen zur Schau gestellt hat.

(2) Im Fall des Absatzes 1 b) ist Absatz 1 nur anzuwenden, wenn der Anmelder bei Einreichung der europäischen Patentanmeldung angibt, dass die Erfindung tatsächlich zur Schau gestellt worden ist, und innerhalb der Frist und unter den Bedingungen, die in der Ausführungsordnung vorgeschrieben sind, eine entsprechende Bescheinigung einreicht.

Artikel 56
Erfinderische Tätigkeit

Eine Erfindung gilt als auf einer erfinderischen Tätigkeit beruhend, wenn sie sich für den Fachmann nicht in nahe liegender Weise aus dem Stand der Technik ergibt. Gehören zum Stand der Technik auch Unterlagen im Sinn des Artikels 54 Absatz 3, so

that date, shall be considered as comprised in the state of the art.

(4) Paragraphs 2 and 3 shall not exclude the patentability of any substance or composition, comprised in the state of the art, for use in a method referred to in Article 53(c), provided that its use for any such method is not comprised in the state of the art.

(5) Paragraphs 2 and 3 shall also not exclude the patentability of any substance or composition referred to in paragraph 4 for any specific use in a method referred to in Article 53(c), provided that such use is not comprised in the state of the art.

Article 55
Non-prejudicial disclosures

(1) For the application of Article 54, a disclosure of the invention shall not be taken into consideration if it occurred no earlier than six months preceding the filing of the European patent application and if it was due to, or in consequence of:

(a) an evident abuse in relation to the applicant or his legal predecessor, or

(b) the fact that the applicant or his legal predecessor has displayed the invention at an official, or officially recognised, international exhibition falling within the terms of the Convention on international exhibitions signed at Paris on 22 November 1928 and last revised on 30 November 1972.

(2) In the case of paragraph 1(b), paragraph 1 shall apply only if the applicant states, when filing the European patent application, that the invention has been so displayed and files a supporting certificate within the time limit and under the conditions laid down in the Implementing Regulations.

Article 56
Inventive step

An invention shall be considered as involving an inventive step if, having regard to the state of the art, it is not obvious to a person skilled in the art. If the state of the art also includes documents within the meaning of Article 54, paragraph 3, these

rieure à celle mentionnée au paragraphe 2 et qui n'ont été publiées qu'à cette date ou à une date postérieure.

(4) Les paragraphes 2 et 3 n'excluent pas la brevetabilité d'une substance ou composition comprise dans l'état de la technique pour la mise en oeuvre d'une méthode visée à l'article 53 c), à condition que son utilisation pour l'une quelconque de ces méthodes ne soit pas comprise dans l'état de la technique.

(5) Les paragraphes 2 et 3 n'excluent pas non plus la brevetabilité d'une substance ou composition visée au paragraphe 4 pour toute utilisation spécifique dans une méthode visée à l'article 53 c), à condition que cette utilisation ne soit pas comprise dans l'état de la technique.

Article 55
Divulgations non opposables

(1) Pour l'application de l'article 54, une divulgation de l'invention n'est pas prise en considération si elle n'est pas intervenue plus tôt que six mois avant le dépôt de la demande de brevet européen et si elle résulte directement ou indirectement :

a) d'un abus évident à l'égard du demandeur ou de son prédécesseur en droit ou

b) du fait que le demandeur ou son prédécesseur en droit a exposé l'invention dans des expositions officielles ou officiellement reconnues au sens de la Convention concernant les expositions internationales, signée à Paris le 22 novembre 1928 et révisée en dernier lieu le 30 novembre 1972.

(2) Dans le cas visé au paragraphe 1 b), ce dernier n'est applicable que si le demandeur déclare, lors du dépôt de la demande de brevet européen, que l'invention a été réellement exposée et produit une attestation à l'appui de sa déclaration dans le délai et dans les conditions prévus par le règlement d'exécution.

Article 56
Activité inventive

Une invention est considérée comme impliquant une activité inventive si, pour un homme du métier, elle ne découle pas d'une manière évidente de l'état de la technique. Si l'état de la technique comprend également des documents visés à l'article 54,

werden diese bei der Beurteilung der erfinderischen Tätigkeit nicht in Betracht gezogen.

Artikel 57
Gewerbliche Anwendbarkeit

Eine Erfindung gilt als gewerblich anwendbar, wenn ihr Gegenstand auf irgendeinem gewerblichen Gebiet einschließlich der Landwirtschaft hergestellt oder benutzt werden kann.

Kapitel II

Zur Einreichung und Erlangung des europäischen Patents berechtigte Personen – Erfindernennung

Artikel 58
Recht zur Anmeldung europäischer Patente

Jede natürliche oder juristische Person und jede Gesellschaft, die nach dem für sie maßgebenden Recht einer juristischen Person gleichgestellt ist, kann die Erteilung eines europäischen Patents beantragen.

Artikel 59
Mehrere Anmelder

Die europäische Patentanmeldung kann auch von gemeinsamen Anmeldern oder von mehreren Anmeldern, die verschiedene Vertragsstaaten benennen, eingereicht werden.

Artikel 60
Recht auf das europäische Patent

(1) Das Recht auf das europäische Patent steht dem Erfinder oder seinem Rechtsnachfolger zu. Ist der Erfinder ein Arbeitnehmer, so bestimmt sich das Recht auf das europäische Patent nach dem Recht des Staats, in dem der Arbeitnehmer überwiegend beschäftigt ist; ist nicht festzustellen, in welchem Staat der Arbeitnehmer überwiegend beschäftigt ist, so ist das Recht des Staats anzuwenden, in dem der Arbeitgeber den Betrieb unterhält, dem der Arbeitnehmer angehört.

(2) Haben mehrere eine Erfindung unabhängig voneinander gemacht, so steht das Recht auf das europäische Patent demjenigen zu, dessen europäische Patentanmeldung den früheren Anmeldetag hat, sofern diese frühere Anmeldung veröffentlicht worden ist.

(3) Im Verfahren vor dem Europäischen Patentamt gilt der Anmelder als berechtigt, das Recht auf das europäische Patent geltend zu machen.

documents shall not be considered in deciding whether there has been an inventive step.

Article 57
Industrial application

An invention shall be considered as susceptible of industrial application if it can be made or used in any kind of industry, including agriculture.

Chapter II

Persons entitled to apply for and obtain a European patent – Mention of the inventor

Article 58
Entitlement to file a European patent application

A European patent application may be filed by any natural or legal person, or any body equivalent to a legal person by virtue of the law governing it.

Article 59
Multiple applicants

A European patent application may also be filed either by joint applicants or by two or more applicants designating different Contracting States.

Article 60
Right to a European patent

(1) The right to a European patent shall belong to the inventor or his successor in title. If the inventor is an employee, the right to a European patent shall be determined in accordance with the law of the State in which the employee is mainly employed; if the State in which the employee is mainly employed cannot be determined, the law to be applied shall be that of the State in which the employer has the place of business to which the employee is attached.

(2) If two or more persons have made an invention independently of each other, the right to a European patent therefor shall belong to the person whose European patent application has the earliest date of filing, provided that this first application has been published.

(3) In proceedings before the European Patent Office, the applicant shall be deemed to be entitled to exercise the right to a European patent.

paragraphe 3, ils ne sont pas pris en considération pour l'appréciation de l'activité inventive.

Article 57
Application industrielle

Une invention est considérée comme susceptible d'application industrielle si son objet peut être fabriqué ou utilisé dans tout genre d'industrie, y compris l'agriculture.

Chapitre II

Personnes habilitées à demander et à obtenir un brevet européen – Désignation de l'inventeur

Article 58
Habilitation à déposer une demande de brevet européen

Toute personne physique ou morale et toute société assimilée à une personne morale en vertu du droit dont elle relève peut demander un brevet européen.

Article 59
Pluralité de demandeurs

Une demande de brevet européen peut être également déposée soit par des codemandeurs, soit par plusieurs demandeurs qui désignent des Etats contractants différents.

Article 60
Droit au brevet européen

(1) Le droit au brevet européen appartient à l'inventeur ou à son ayant cause. Si l'inventeur est un employé, le droit au brevet européen est défini selon le droit de l'Etat dans lequel l'employé exerce son activité principale ; si l'Etat dans lequel s'exerce l'activité principale ne peut être déterminé, le droit applicable est celui de l'Etat dans lequel se trouve l'établissement de l'employeur auquel l'employé est attaché.

(2) Si plusieurs personnes ont réalisé l'invention indépendamment l'une de l'autre, le droit au brevet européen appartient à celle dont la demande de brevet européen a la date de dépôt la plus ancienne, sous réserve que cette première demande ait été publiée.

(3) Dans la procédure devant l'Office européen des brevets, le demandeur est réputé habilité à exercer le droit au brevet européen.

Artikel 61
Anmeldung europäischer Patente durch Nichtberechtigte

(1) Wird durch rechtskräftige Entscheidung der Anspruch auf Erteilung des europäischen Patents einer Person zugesprochen, die nicht der Anmelder ist, so kann diese Person nach Maßgabe der Ausführungsordnung

a) die europäische Patentanmeldung anstelle des Anmelders als eigene Anmeldung weiterverfolgen,

b) eine neue europäische Patentanmeldung für dieselbe Erfindung einreichen oder

c) beantragen, dass die europäische Patentanmeldung zurückgewiesen wird.

(2) Auf eine nach Absatz 1 b) eingereichte neue europäische Patentanmeldung ist Artikel 76 Absatz 1 entsprechend anzuwenden.

Artikel 62
Recht auf Erfindernennung

Der Erfinder hat gegenüber dem Anmelder oder Inhaber des europäischen Patents das Recht, vor dem Europäischen Patentamt als Erfinder genannt zu werden.

Kapitel III

Wirkungen des europäischen Patents und der europäischen Patentanmeldung

Artikel 63
Laufzeit des europäischen Patents

(1) Die Laufzeit des europäischen Patents beträgt zwanzig Jahre, gerechnet vom Anmeldetag an.

(2) Absatz 1 lässt das Recht eines Vertragsstaats unberührt, unter den gleichen Bedingungen, die für nationale Patente gelten, die Laufzeit eines europäischen Patents zu verlängern oder entsprechenden Schutz zu gewähren, der sich an den Ablauf der Laufzeit des Patents unmittelbar anschließt,

a) um einem Kriegsfall oder einer vergleichbaren Krisenlage dieses Staats Rechnung zu tragen;

b) wenn der Gegenstand des europäischen Patents ein Erzeugnis oder ein Verfahren zur Herstellung oder eine Verwendung eines Erzeugnisses ist, das vor seinem In-Verkehr-Bringen in diesem Staat einem gesetzlich vorgeschriebenen behördlichen Genehmigungsverfahren unterliegt.

Article 61
European patent applications filed by non-entitled persons

(1) If by a final decision it is adjudged that a person other than the applicant is entitled to the grant of the European patent, that person may, in accordance with the Implementing Regulations:

(a) prosecute the European patent application as his own application in place of the applicant;

(b) file a new European patent application in respect of the same invention; or

(c) request that the European patent application be refused.

(2) Article 76, paragraph 1, shall apply mutatis mutandis to a new European patent application filed under paragraph 1(b).

Article 62
Right of the inventor to be mentioned

The inventor shall have the right, vis-à-vis the applicant for or proprietor of a European patent, to be mentioned as such before the European Patent Office.

Chapter III

Effects of the European patent and the European patent application

Article 63
Term of the European patent

(1) The term of the European patent shall be 20 years from the date of filing of the application.

(2) Nothing in the preceding paragraph shall limit the right of a Contracting State to extend the term of a European patent, or to grant corresponding protection which follows immediately on expiry of the term of the patent, under the same conditions as those applying to national patents:

(a) in order to take account of a state of war or similar emergency conditions affecting that State;

(b) if the subject-matter of the European patent is a product or a process for manufacturing a product or a use of a product which has to undergo an administrative authorisation procedure required by law before it can be put on the market in that State.

Article 61
Demande de brevet européen déposée par une personne non habilitée

(1) Si une décision passée en force de chose jugée a reconnu le droit à l'obtention du brevet européen à une personne autre que le demandeur, cette personne peut, conformément au règlement d'exécution :

a) poursuivre, au lieu et place du demandeur, la procédure relative à la demande de brevet européen, en prenant cette demande à son compte,

b) déposer une nouvelle demande de brevet européen pour la même invention, ou

c) demander le rejet de la demande de brevet européen.

(2) L'article 76, paragraphe 1, est applicable à toute nouvelle demande de brevet européen déposée en vertu du paragraphe 1 b).

Article 62
Droit de l'inventeur d'être désigné

L'inventeur a le droit, à l'égard du titulaire de la demande de brevet européen ou du brevet européen, d'être désigné en tant que tel auprès de l'Office européen des brevets.

Chapitre III

Effets du brevet européen et de la demande de brevet européen

Article 63
Durée du brevet européen

(1) La durée du brevet européen est de vingt années à compter de la date de dépôt de la demande.

(2) Le paragraphe 1 ne saurait limiter le droit d'un Etat contractant de prolonger la durée d'un brevet européen ou d'accorder une protection correspondante dès l'expiration de cette durée aux mêmes conditions que celles applicables aux brevets nationaux,

a) pour tenir compte d'un état de guerre ou d'un état de crise comparable affectant ledit Etat ;

b) si l'objet du brevet européen est un produit ou un procédé de fabrication ou une utilisation d'un produit qui, avant sa mise sur le marché dans cet Etat, est soumis à une procédure administrative d'autorisation instituée par la loi.

Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Strasbourg, 28.I.1981

Protocole
Rapport explicatif
English

Préambule

Les Etats membres du Conseil de l'Europe, signataires de la présente Convention,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres, dans le respect notamment de la prééminence du droit ainsi que des droits de l'homme et des libertés fondamentales;

Considérant qu'il est souhaitable d'étendre la protection des droits et des libertés fondamentales de chacun, notamment le droit au respect de la vie privée, eu égard à l'intensification de la circulation à travers les frontières des données à caractère personnel faisant l'objet de traitements automatisés;

Réaffirmant en même temps leur engagement en faveur de la liberté d'information sans considération de frontières;

Reconnaissant la nécessité de concilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples,

Sont convenus de ce qui suit:

Chapitre I – Dispositions générales

Article 1er – Objet et but

Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant («protection des données»).

Article 2 – Définitions

Aux fins de la présente Convention:

a. «données à caractère personnel» signifie: toute information concernant une personne physique identifiée ou identifiable («personne concernée»);
b. «fichier automatisé» signifie: tout ensemble d'informations faisant l'objet d'un traitement automatisé;
c. «traitement automatisé» s'entend des opérations suivantes effectuées en totalité ou en partie à l'aide de procédés automatisés: enregistrement des données,

application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion;

d. «maître du fichier» signifie: la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui est compétent selon la loi nationale, pour décider quelle sera la finalité du fichier automatisé, quelles catégories de données à caractère personnel doivent être enregistrées et quelles opérations leur seront appliquées.

Article 3 – Champ d'application

1. Les Parties s'engagent à appliquer la présente Convention aux fichiers et aux traitements automatisés de données à caractère personnel dans les secteurs public et privé.
2. Tout Etat peut, lors de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou à tout moment ultérieur, faire connaître par déclaration adressée au Secrétaire Général du Conseil de l'Europe:
   a. qu'il n'appliquera pas la présente Convention à certaines catégories de fichiers automatisés de données à caractère personnel dont une liste sera déposée. Il ne devra toutefois pas inclure dans cette liste des catégories de fichiers automatisés assujetties selon son droit interne à des dispositions de protection des données. En conséquence, il devra amender cette liste par une nouvelle déclaration lorsque des catégories supplémentaires de fichiers automatisés de données à caractère personnel seront assujetties à son régime de protection des données;
   b. qu'il appliquera la présente Convention également à des informations afférentes à des groupements, associations, fondations, sociétés, corporations ou à tout autre organisme regroupant directement ou indirectement des personnes physiques et jouissant ou non de la personnalité juridique;
   c. qu'il appliquera la présente Convention également aux fichiers de données à caractère personnel ne faisant pas l'objet de traitements automatisés.
3. Tout Etat qui a étendu le champ d'application de la présente Convention par l'une des déclarations visées aux alinéas 2.b ou c ci-dessus peut, dans ladite déclaration, indiquer que les extensions ne s'appliqueront qu'à certaines catégories de fichiers à caractère personnel dont la liste sera déposée.
4. Toute Partie qui a exclu certaines catégories de fichiers automatisés de données à caractère personnel par la déclaration prévue à l'alinéa 2.a ci-dessus ne peut pas prétendre à l'application de la présente Convention à de telles catégories par une Partie qui ne les a pas exclues.
5. De même, une Partie qui n'a pas procédé à l'une ou à l'autre des extensions prévues aux paragraphes 2.b et c du présent article ne peut se prévaloir de l'application de la présente Convention sur ces points à l'égard d'une Partie qui a procédé à de telles extensions.
6. Les déclarations prévues au paragraphe 2 du présent article prendront effet au moment de l'entrée en vigueur de la Convention à l'égard de l'Etat qui les a formulées, si cet Etat les a faites lors de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, ou trois mois après leur réception par le Secrétaire Général du Conseil de l'Europe si elles ont été formulées à un moment ultérieur. Ces déclarations pourront être retirées en tout ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet trois mois après la date de réception d'une telle notification.

Chapitre II – Principes de base pour la protection des données

Article 4 – Engagements des Parties

1. Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans le

présent chapitre.
2. Ces mesures doivent être prises au plus tard au moment de l'entrée en vigueur de la présente Convention à son égard.

Article 5 – Qualité des données

Les données à caractère personnel faisant l'objet d'un traitement automatisé sont:
a. obtenues et traitées loyalement et licitement;
b. enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;
c. adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;
d. exactes et si nécessaire mises à jour;
e. conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.

Article 6 – Catégories particulières de données

Les données à caractère personnel révélant l'origine raciale, les opinions politiques, les convictions religieuses ou autres convictions, ainsi que les données à caractère personnel relatives à la santé ou à la vie sexuelle, ne peuvent être traitées automatiquement à moins que le droit interne ne prévoie des garanties appropriées. Il en est de même des données à caractère personnel concernant des condamnations pénales.

Article 7 – Sécurité des données

Des mesures de sécurité appropriées sont prises pour la protection des données à caractère personnel enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.

Article 8 – Garanties complémentaires pour la personne concernée

Toute personne doit pouvoir:
a. connaître l'existence d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier;
b. obtenir à des intervalles raisonnables et sans délais ou frais excessifs la confirmation de l'existence ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;
c. obtenir, le cas échéant, la rectification de ces données ou leur effacement lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;
d. disposer d'un recours s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.

Article 9 – Exceptions et restrictions

1. Aucune exception aux dispositions des articles 5, 6 et 8 de la présente Convention n'est admise, sauf dans les limites définies au présent article.
2. Il est possible de déroger aux dispositions des articles 5, 6 et 8 de la présente Convention lorsqu'une telle dérogation, prévue par la loi de la Partie, constitue une mesure nécessaire dans une société démocratique:

a. à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales;
b. à la protection de la personne concernée et des droits et libertés d'autrui.

3. Des restrictions à l'exercice des droits visés aux paragraphes b, c et d de l'article 8 peuvent être prévues par la loi pour les fichiers automatisés de données à caractère personnel utilisés à des fins de statistiques ou de recherches scientifiques, lorsqu'il n'existe manifestement pas de risques d'atteinte à la vie privée des personnes concernées.

Article 10 – Sanctions et recours

Chaque Partie s'engage à établir des sanctions et recours appropriés visant les violations aux dispositions du droit interne donnant effet aux principes de base pour la protection des données énoncés dans le présent chapitre.

Article 11 – Protection plus étendue

Aucune des dispositions du présent chapitre ne sera interprétée comme limitant ou portant atteinte à la faculté pour chaque Partie d'accorder aux personnes concernées une protection plus étendue que celle prévue par la présente Convention.

Chapitre III – Flux transfrontières de données

Article 12 – Flux transfrontières de données à caractère personnel et droit interne

1. Les dispositions suivantes s'appliquent aux transferts à travers les frontières nationales, quel que soit le support utilisé, de données à caractère personnel faisant l'objet d'un traitement automatisé ou rassemblées dans le but de les soumettre à un tel traitement.
2. Une Partie ne peut pas, aux seules fins de la protection de la vie privée, interdire ou soumettre à une autorisation spéciale les flux transfrontières de données à caractère personnel à destination du territoire d'une autre Partie.
3. Toutefois, toute Partie a la faculté de déroger aux dispositions du paragraphe 2:
   a. dans la mesure où sa législation prévoit une réglementation spécifique pour certaines catégories de données à caractère personnel ou de fichiers automatisés de données à caractère personnel, en raison de la nature de ces données ou de ces fichiers, sauf si la réglementation de l'autre Partie apporte une protection équivalente;
   b. lorsque le transfert est effectué à partir de son territoire vers le territoire d'un Etat non contractant par l'intermédiaire du territoire d'une autre Partie, afin d'éviter que de tels transferts n'aboutissent à contourner la législation de la Partie visée au début du présent paragraphe.

Chapitre IV – Entraide

Article 13 – Coopération entre les Parties

1. Les Parties s'engagent à s'accorder mutuellement assistance pour la mise en œuvre de la présente Convention.
2. A cette fin,
   a. chaque Partie désigne une ou plusieurs autorités dont elle communique la dénomination et l'adresse au Secrétaire Général du Conseil de l'Europe;
   b. chaque Partie qui a désigné plusieurs autorités indique dans la communication visée à l'alinéa précédent la compétence de chacune de ces autorités.
3. Une autorité désignée par une Partie, à la demande d'une autorité désignée par une autre Partie:
   a. fournira des informations sur son droit et sur sa pratique administrative en

matière de protection des données;

b. prendra, conformément à son droit interne et aux seules fins de la protection de la vie privée, toutes mesures appropriées pour fournir des informations de fait concernant un traitement automatisé déterminé effectué sur son territoire à l'exception toutefois des données à caractère personnel faisant l'objet de ce traitement.

Article 14 – Assistance aux personnes concernées ayant leur résidence à l'étranger

1. Chaque Partie prête assistance à toute personne ayant sa résidence à l'étranger pour l'exercice des droits prévus par son droit interne donnant effet aux principes énoncés à l'article 8 de la présente Convention.
2. Si une telle personne réside sur le territoire d'une autre Partie, elle doit avoir la faculté de présenter sa demande par l'intermédiaire de l'autorité désignée par cette Partie.
3. La demande d'assistance doit contenir toutes les indications nécessaires concernant notamment:
   a. le nom, l'adresse et tous autres éléments pertinents d'identification concernant le requérant;
   b. le fichier automatisé de données à caractère personnel auquel la demande se réfère ou le maître de ce fichier;
   c. le but de la demande.

Article 15 – Garanties concernant l'assistance fournie par les autorités désignées

1. Une autorité désignée par une Partie qui a reçu des informations d'une autorité désignée par une autre Partie, soit à l'appui d'une demande d'assistance, soit en réponse à une demande d'assistance qu'elle a formulée elle-même, ne pourra faire usage de ces informations à des fins autres que celles spécifiées dans la demande d'assistance.
2. Chaque Partie veillera à ce que les personnes appartenant ou agissant au nom de l'autorité désignée soient liées par des obligations appropriées de secret ou de confidentialité à l'égard de ces informations.
3. En aucun cas, une autorité désignée ne sera autorisée à faire, aux termes de l'article 14, paragraphe 2, une demande d'assistance au nom d'une personne concernée résidant à l'étranger, de sa propre initiative et sans le consentement exprès de cette personne.

Article 16 – Refus des demandes d'assistance

Une autorité désignée, saisie d'une demande d'assistance aux termes des articles 13 ou 14 de la présente Convention, ne peut refuser d'y donner suite que si:

a. la demande est incompatible avec les compétences, dans le domaine de la protection des données, des autorités habilitées à répondre;
b. la demande n'est pas conforme aux dispositions de la présente Convention;
c. l'exécution de la demande serait incompatible avec la souveraineté, la sécurité ou l'ordre public de la Partie qui l'a désignée, ou avec les droits et libertés fondamentales des personnes relevant de la juridiction de cette Partie.

Article 17 – Frais et procédures de l'assistance

1. L'entraide que les Parties s'accordent aux termes de l'article 13, ainsi que l'assistance qu'elles prêtent aux personnes concernées résidant à l'étranger aux termes de l'article 14, ne donnera pas lieu au paiement des frais et droits autres que ceux afférents aux experts et aux interprètes. Ces frais et droits seront à la charge de la Partie qui a désigné l'autorité qui a fait la demande d'assistance.
2. La personne concernée ne peut être tenue de payer, en liaison avec les démarches entreprises pour son compte sur le territoire d'une autre Partie, des frais et droits

autres que ceux exigibles des personnes résidant sur le territoire de cette Partie.
3. Les autres modalités relatives à l'assistance concernant notamment les formes et procédures ainsi que les langues à utiliser seront établies directement entre les Parties concernées.

Chapitre V – Comité consultatif

Article 18 – Composition du comité

1. Un comité consultatif est constitué après l'entrée en vigueur de la présente Convention.
2. Toute Partie désigne un représentant et un suppléant à ce comité. Tout Etat membre du Conseil de l'Europe qui n'est pas Partie à la Convention a le droit de se faire représenter au comité par un observateur.
3. Le comité consultatif peut, par une décision prise à l'unanimité, inviter tout Etat non membre du Conseil de l'Europe qui n'est pas Partie à la Convention à se faire représenter par un observateur à l'une de ses réunions.

Article 19 – Fonctions du comité

Le comité consultatif:

a. peut faire des propositions en vue de faciliter ou d'améliorer l'application de la Convention;
b. peut faire des propositions d'amendement à la présente Convention conformément à l'article 21;
c. formule un avis sur toute proposition d'amendement à la présente Convention qui lui est soumis conformément à l'article 21 , paragraphe 3;
d. peut, à la demande d'une Partie, exprimer un avis sur toute question relative à l'application de la présente Convention.

Article 20 – Procédure

1. Le comité consultatif est convoqué par le Secrétaire Général du Conseil de l'Europe. Il tient sa première réunion dans les douze mois qui suivent l'entrée en vigueur de la présente Convention. Il se réunit par la suite au moins une fois tous les deux ans et, en tout cas, chaque fois qu'un tiers des représentants des Parties demande sa convocation.
2. La majorité des représentants des Parties constitue le quorum nécessaire pour tenir une réunion du comité consultatif.
3. A l'issue de chacune de ses réunions, le comité consultatif soumet au Comité des Ministres du Conseil de l'Europe un rapport sur ses travaux et sur le fonctionnement de la Convention.
4. Sous réserve des dispositions de la présente Convention, le Comité consultatif établit son règlement intérieur.

Chapitre VI – Amendements

Article 21 – Amendements

1. Des amendements à la présente Convention peuvent être proposés par une Partie, par le Comité des Ministres du Conseil de l'Europe ou par le comité consultatif.
2. Toute proposition d'amendement est communiquée par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe et à chaque Etat non membre qui a adhéré ou a été invité à adhérer à la présente Convention conformément aux dispositions de l'article 23.
3. En outre, tout amendement proposé par une Partie ou par le Comité des Ministres est communiqué au comité consultatif qui soumet au Comité des Ministres son avis sur l'amendement proposé.

4. Le Comité des Ministres examine l'amendement proposé et tout avis soumis par le comité consultatif et peut approuver l'amendement.
5. Le texte de tout amendement approuvé par le Comité des Ministres conformément au paragraphe 4 du présent article est transmis aux Parties pour acceptation.
6. Tout amendement approuvé conformément au paragraphe 4 du présent article entrera en vigueur le trentième jour après que toutes les Parties auront informé le Secrétaire Général qu'elles l'ont accepté.

Chapitre VII – Clauses finales

Article 22 – Entrée en vigueur

1. La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe. Elle sera soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation seront déposés près le Secrétaire Général du Conseil de l'Europe.
2. La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats membres du Conseil de l'Europe auront exprimé leur consentement à être liés par la Convention conformément aux dispositions du paragraphe précédent.
3. Pour tout Etat membre qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument de ratification, d'acceptation ou d'approbation.

Article 23 – Adhésion d'Etats non membres

1. Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe pourra inviter tout Etat non membre du Conseil de l'Europe à adhérer à la présente Convention par une décision prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au comité.
2. Pour tout Etat adhérant, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date du dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 24 – Clause territoriale

1. Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.
2. Tout Etat peut, à tout autre moment par la suite, par une déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.
3. Toute déclaration faite en vertu des deux paragraphes précédents pourra être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.

Article 25 – Réserves

Aucune réserve n'est admise aux dispositions de la présente Convention.

Article 26 – Dénonciation

1. Toute Partie peut, à tout moment, dénoncer la présente Convention en adressant une notification au Secrétaire Général du Conseil de l'Europe.
2. La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de six mois après la date de réception de la notification par le Secrétaire Général.

Article 27 – Notifications

Le Secrétaire Général du Conseil de l'Europe notifiera aux Etats membres du Conseil et à tout Etat ayant adhéré à la présente Convention:

a. toute signature;
b. le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion;
c. toute date d'entrée en vigueur de la présente Convention conformément à ses articles 22, 23 et 24;
d. tout autre acte, notification ou communication ayant trait à la présente Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Strasbourg, le 28 janvier 1981, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe et à tout Etat invité à adhérer à la présente Convention.

RISOLUZIONE DEL CONSIGLIO

del 28 gennaio 2002

relativa a un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione

(2002/C 43/02)

IL CONSIGLIO DELL'UNIONE EUROPEA,

IN SEGUITO

alle conclusioni del Consiglio europeo di Stoccolma del 23/24 marzo 2001 secondo cui «il Consiglio svilupperà insieme alla Commissione una strategia globale per la sicurezza delle reti elettroniche, comprensiva di azioni concrete di attuazione»,

RAMMENTANDO I SEGUENTI ATTI:

1. risoluzione del Consiglio del 30 maggio 2001 — Piano d'azione eEUROPE: Sicurezza dell'informazione e delle reti;

2. comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni sulla sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo;

3. comunicazione della Commissione al Consiglio ed al Parlamento europeo — eEurope 2002: Impatto e priorità;

4. piano d'azione eEurope 2002 approvato dal Consiglio europeo di Feira del 19/20 giugno 2000;

5. raccomandazione 95/144/CE del Consiglio, del 7 aprile 1995, su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione [1];

6. raccomandazione del Consiglio, del 25 giugno 2001, sui punti di contatto accessibili 24 ore al giorno ai fini della lotta contro la criminalità ad alta tecnologia [2];

7. comunicazione della Commissione: «Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica»;

8. regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati [3];

9. direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutele delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati [4];

10. direttiva 97/33/CE del Parlamento europeo e del Consiglio, del 30 giugno 1992, sull'interconcessione nel settore delle telecomunicazioni e finalizzata a garantire il servizio universale e l'interoperabilità attraverso l'applicazione dei principi di fornitura di una rete aperta (ONP) [5];

11. 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 [6];

12. direttiva 97/10/CE del Parlamento europeo e del Consiglio, del 26 febbraio 1998, sull'applicazione del regime di forniture di una rete aperta (ONP) alla telefonia vocale e sul servizio universale delle telecomunicazioni in un ambiente concorrenziale [7];

---

[1] GU L 93 del 26.4.1995, pag. 27.

[2] GU C 187 del 3.7.2001, pag. 5.

[3] GU L 8 del 12.1.2001, pag. 1.

[4] GU L 281 del 23.11.1995, pag. 31.

[5] GU L 199 del 26.7.1997, pag. 32.

[6] GU L 24 del 30.1.1998, pag. 1.

[7] GU L 101 dell'1.4.1998, pag. 24.

13. direttiva 1999/93/CE del Parlamento europeo e del Consiglio, del 13 dicembre 1999, relativa ad un quadro comunitario per le firme elettroniche [1];

CONSIDERANDO QUANTO SEGUE:

(1) Le reti e i sistemi di comunicazione sono diventati un fattore chiave dello sviluppo economico e sociale e la loro disponibilità e integrità sono essenziali per infrastrutture fondamentali nonché la maggior parte dei servizi pubblici e privati e l'economia nel suo insieme.

(2) Alla luce del ruolo sempre più importante svolto nell'economia dai servizi elettronici, la sicurezza delle reti e dei sistemi di informazione è diventata sempre più una questione di interesse pubblico.

(3) La sicurezza delle operazioni e dei dati ha assunto un'importanza fondamentale per la fornitura di servizi elettronici, compresi il commercio elettronico e i servizi pubblici on line, e la scarsa fiducia nella sicurezza potrebbe rallentare l'introduzione diffusa di tali servizi.

(4) È necessario che i cittadini, le imprese, le amministrazioni e altre organizzazioni proteggano i propri sistemi di informazione e comunicazione e le banche dati dispiegando se del caso tecnologie efficaci in materia di sicurezza.

(5) Il settore privato, agendo in un contesto di mercato concorrenziale e grazie alla sua capacità di innovazione, offre una varietà di soluzioni adeguate alle vere necessità del mercato.

(6) Data la complessità della sicurezza delle reti e dell'informazione, nell'elaborare interventi in questo campo le autorità pubbliche devono tener conto di una serie di aspetti politici, economici, organizzativi e tecnici e tener presente il carattere decentrato e globale delle reti di comunicazione.

(7) Gli interventi possono essere più efficaci se fanno parte di un approccio europeo, rispettano il buon funzionamento del mercato interno, si basano su una maggiore cooperazione tra gli Stati membri e a livello internazionale e sostengono l'innovazione e la capacità delle imprese europee di essere competitive a livello globale.

(8) Sono già state emanate numerose misure legislative in materia di sicurezza delle reti e dell'informazione, in particolare nell'ambito del quadro normativo dell'UE sulle telecomunicazioni, sul commercio eletttronico e sulla firma elettronica.

(9) Esistono requisiti legali che impongono ai fornitori di servizi di telecomunicazioni di adottare misure tecniche e organizzative adeguate per salvaguardare la sicurezza dei loro servizi. Tali misure garantiscono un livello appropriato di sicurezza in funzione del rischio cui si è di fronte.

(10) La classificazione internazionale ISO-15408 (Criteri comuni) è diventata un sistema riconosciuto per la definizione dei requisiti di sicurezza per computer e prodotti di reti e per la valutazione della conformità di un determinato prodotto a tali requisiti.

(11) La classificazione internazionale ISO-17799 (Codice di buona pratica per la gestione della sicurezza dell'informazione) e analoghe direttive nazionali sono diventate una prassi riconosciuta per la gestione della sicurezza nelle organizzazioni pubbliche e private.

(12) L'infrastruttura Internet dovrebbe assicurare un grado elevato di accesso alle reti e ai servizi e una gestione e un funzionamento in mani salde e sicure, grazie tra l'altro all'adozione di norme aperte e di protocolli sulla sicurezza dell'Internet.

CONSIDERANDO, conformemente alla risoluzione del Consiglio, del 30 maggio 2001, «Piano d'azione eEurope: Sicurezza dell'informazione e delle reti», che la sicurezza delle reti e dell'informazione consiste nel:

— garantire la disponibilità di servizi e di dati,

— impedire interruzioni e intercettazioni non autorizzate delle comunicazioni,

— confermare che i dati trasmessi, ricevuti o archivati sono completi e invariati,

— assicurare la riservatezza dei dati,

— proteggere i sistemi di informazioni e dall'accesso non autorizzato,

— proteggere dagli attacchi in cui siano implicati software «maligni»,

— garantire l'affidabilità dell'autenticazione,

PERTANTO CHIEDE AGLI STATI MEMBRI DI

1. lanciare o rafforzare entro il 2002 campagne di informazione ed istruzione per una maggiore sensibilizzazione in materia di sicurezza dell'informazione e delle reti; orientare tali iniziative specificamente verso le imprese, gli utenti privati e le amministrazioni pubbliche; eleborare tali iniziative di sensibilizzazione in stretta collaborazione con il settore privato, compresi tra l'altro i fornitori di servizi Internet, e incoraggiare le iniziative condotte dal settore privato;

[1] GU L 13 del 19.1.2000, pag. 12.

I

(Atti per i quali la pubblicazione è una condizione di applicabilità)

DECISIONE N. 1151/2003/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

del 16 giugno 2003

che modifica la decisione n. 276/1999/CE che adotta un piano pluriennale d'azione comunitario per promuovere l'uso sicuro di Internet attraverso la lotta alle informazioni di contenuto illegale e nocivo diffuse attraverso le reti globali

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato che istituisce la Comunità europea, in particolare l'articolo 153, paragrafo 2,

vista la proposta della Commissione [1],

visto il parere del Comitato economico e sociale europeo [2],

visto il parere del Comitato delle regioni [3],

deliberando secondo la procedura di cui all'articolo 251 del trattato [4],

considerando quando segue:

(1) La decisione n. 276/1999/CE [5] è stata adottata per un periodo di quattro anni.

(2) Conformemente all'articolo 6, paragrafo 4, della decisione n. 276/1999/CE, la Commissione ha presentato al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni una relazione di valutazione sui risultati ottenuti, dopo due anni, nell'attuazione delle linee d'azione di cui all'allegato I di tale decisione.

(3) I risultati della valutazione sono confluiti nella documentazione di base per un seminario sull'uso più sicuro delle nuove tecnologie online, in occasione del quale esperti di spicco del settore hanno esaminato la probabile evoluzione futura dei temi trattati nel piano d'azione previsto nella decisione n. 276/1999/CE (in prosieguo: «piano d'azione») e hanno formulato raccomandazioni alla Commissione.

(4) Le nuove tecnologie on-line, i nuovi utenti e le nuove tipologie d'uso accentuano i pericoli esistenti o ne creano di nuovi e al contempo aprono un'infinità di nuove opportunità.

(5) Sia a livello nazionale che europeo bisogna garantire il coordinamento negli ambienti più sicuri su Internet. Ci dovrebbe essere un ampio decentramento grazie alla rete di punti focali nazionali e bisognerebbe incoraggiare la partecipazione di tutti i soggetti interessati, in particolare di un numero maggiore di fornitori di contenuti di diversi settori. La Commissione dovrebbe agevolare e sostenere la cooperazione europea e mondiale. È opportuno potenziare la cooperazione tra la Comunità e i paesi candidati e quelli in fase di adesione.

(6) Occorre più tempo per attuare le azioni volte a intensificare la messa in rete, conseguire gli obiettivi del piano d'azione e tener conto delle nuove tecnologie on-line.

(7) Bisogna modificare di conseguenza la dotazione finanziaria che costituisce, per l'autorità di bilancio, il principale punto di riferimento nel quadro della procedura di bilancio annuale.

(8) Occorre prevedere che la Commissione presenti una seconda relazione sui risultati ottenuti, dopo quattro anni, nell'attuazione delle linee d'azione e una relazione finale alla conclusione del piano d'azione.

(9) Occorre modificare l'elenco dei paesi candidati e di quelli in fase di adesione ammessi a partecipare, per includere Malta e la Turchia.

(10) È opportuno prorogare il piano d'azione di due anni, periodo che dovrebbe essere considerato come seconda fase. Ai fini dell'attuazione specifica della seconda fase, bisogna modificare le linee d'azione per tener conto dell'esperienza acquisita e dei risultati della relazione di valutazione.

(11) La decisione n. 276/1999/CE dovrebbe essere modificata di conseguenza,

[1] GU C 203 E del 27.8.2002, pag. 6.
[2] GU C 61 del 14.3.2003, pag. 32.
[3] GU C 73 del 26.3.2003, pag. 34.
[4] Parere del Parlamento europeo dell'11 marzo 2003 (non ancora pubblicato nella Gazzetta ufficiale) e decisione del Consiglio del 26 maggio 2003.
[5] GU L 33 del 6.2.1999, pag. 1.

HANNO ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La decisione n. 276/1999/CE è modificata come segue:

1) il titolo è sostituito dal seguente:

«Decisione n. 276/1999/CE del Parlamento europeo e del Consiglio, del 25 gennaio 1999, che adotta un piano pluriennale d'azione comunitario per promuovere un uso più sicuro di Internet e delle nuove tecnologie on-line attraverso la lotta alle informazioni di contenuto illegale e nocivo, principalmente nel settore della tutela dei bambini e dei minori»;

2) all'articolo 1, il paragrafo 2 è sostituito dal seguente:

«2. Il piano d'azione ha una durata di sei anni, dal 1° gennaio 1999 al 31 dicembre 2004.»;

3) all'articolo 1, il paragrafo 3 è sostituito dal seguente:

«3. La dotazione finanziaria per l'esecuzione del piano d'azione per il periodo dal 1° gennaio 1999 al 31 dicembre 2004 è fissata in 38,3 milioni di EUR.

Gli stanziamenti annuali sono autorizzati dall'autorità di bilancio entro i limiti delle prospettive finanziarie.

Una ripartizione indicativa delle spese figura nell'allegato II.»;

4) all'articolo 3, il primo trattino è sostituito dal seguente:

«— promozione di sistemi di autoregolamentazione da parte degli operatori del settore e di controllo dei contenuti (che si occupino ad esempio di contenuti quali la pornografia infantile o di contenuti che potrebbero comportare danni fisici o mentali o che istighino all'odio basato su differenze di razza, sesso, religione, nazionalità o origine etnica),»;

5) all'articolo 6, il paragrafo 4 è sostituito dal seguente:

«4. Dopo due anni, dopo quattro anni e alla conclusione del piano d'azione, la Commissione presenta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, previo esame da parte del comitato di cui all'articolo 5, una relazione di valutazione sui risultati ottenuti nell'esecuzione del piano d'azione. In base a tali risultati, la Commissione può presentare proposte per correggere l'orientamento del piano d'azione»;

6) all'articolo 7, il paragrafo 1 è sostituito dal seguente:

«1. La partecipazione al presente piano d'azione può essere estesa agli Stati dell'EFTA membri dello Spazio economico europeo (SEE), conformemente alle disposizioni dell'accordo SEE.»;

7) all'articolo 7, il paragrafo 2 è sostituito dal seguente:

«2. La partecipazione al piano d'azione è estesa ai paesi candidati e a quelli in fase di adesione secondo le seguenti modalità:

a) ai paesi dell'Europa centrale e orientale (PECO), conformemente alle condizioni stabilite negli accordi europei, nei protocolli aggiuntivi e nelle decisioni dei rispettivi Consigli di associazione;

b) a Cipro, a Malta e alla Turchia conformemente ad accordi bilaterali da concludere»;

8) l'allegato I è modificato conformemente a quanto indicato nell'allegato I della presente decisione;

9) l'allegato II è sostituito dal testo che figura nell'allegato II della presente decisione.

Articolo 2

Gli Stati membri sono destinatari della presente decisione.

Fatto a Lussemburgo, addì 16 giugno 2003.

Per il Parlamento europeo	*Per il Consiglio*
Il Presidente	*Il Presidente*
P. COX	G. PAPANDREOU

ALLEGATO I

L'allegato I della decisione n. 276/1999/CE è modificato come segue:

1) al punto «Linee d'azione», il quarto trattino del secondo comma è sostituito dal seguente:

«— stimolare la cooperazione e lo scambio di esperienze e delle migliori pratiche a livello europeo e internazionale, specialmente con i paesi candidati e con quelli in fase di adesione,»;

2) al punto «Linee d'azione» sono aggiunti i seguenti terzo e quarto comma:

«Dopo la fase iniziale (1° gennaio 1999 — 31 dicembre 2002), sarà avviata una seconda fase che copre il periodo dal 1° gennaio 2003 al 31 dicembre 2004, nella quale ci si avvarrà del lavoro svolto per raggiungere gli obiettivi fissati nelle quattro linee d'azione della fase iniziale, si apporteranno le modifiche necessarie per tener conto dell'esperienza acquisita e dell'impatto delle nuove tecnologie e della loro convergenza e si garantirà la coerenza con gli altri programmi comunitari.

Più in particolare:

i) La normativa sull'uso più sicuro verrà estesa, soprattutto per migliorare la tutela dei bambini e dei minori, alle nuove tecnologie on-line, compresi i contenuti delle reti mobili e a banda larga, i giochi on-line, il trasferimento di file peer-to-peer, i messaggi di testo e interattivi e tutte le forme di comunicazioni in tempo reale, quali chat room e messaggeria istantanea;

ii) saranno intraprese azioni più incisive per garantire, specialmente nel settore della tutela dei bambini e dei minori, che siano coperte le aree di contenuti illegali e nocivi e comportamenti preoccupanti, con particolare riferimento ai reati ai danni dei bambini, come la pornografia infantile, il traffico di minori, e al razzismo e alla violenza;

iii) sarà incoraggiata una partecipazione più attiva dell'industria dei contenuti e dei media e sarà potenziata la collaborazione con gli organismi pubblici attivi nel settore;

iv) sarà promossa un maggiore messa in rete tra partecipanti ai progetti sulle diverse linee d'azione, in particolare hot-line, classificazione dei contenuti, autoregolamentazione e sensibilizzazione;

v) si cercherà di associare i paesi candidati e quelli in fase di adesione alle attività in corso, condividendo esperienze e know-how, e di moltiplicare i contatti e la collaborazione con attività simili in paesi terzi, specialmente quelli in cui i contenuti illegali sono ospitati o prodotti, e con organizzazioni internazionali.»;

3) al punto 1.1 è aggiunto il seguente sesto comma:

«Nella seconda fase, l'obiettivo sarà quello di completare la copertura della rete negli Stati membri, migliorare ulteriormente l'efficacia operativa della rete esistente, collaborare strettamente con le iniziative di sensibilizzazione sull'uso più sicuro di Internet, in particolare per sensibilizzare maggiormente il pubblico riguardo alle hot-line, fornire assistenza pratica ai paesi candidati e a quelli in fase di adesione che intendono istituire hot-line, adattare gli orientamenti sulle migliori pratiche alle nuove tecnologie e potenziare i legami con hot-line al di fuori dell'Europa.»;

4) al punto 1.2 è aggiunto il seguente quarto comma:

«Nella seconda fase, saranno fornite consulenza e assistenza per garantire la cooperazione a livello comunitario attraverso la messa in rete di strutture appropriate negli Stati membri e tramite una revisione sistematica e un resoconto delle questioni giuridiche e normative pertinenti, per elaborare metodologie comparabili di valutazione delle norme di autoregolamentazione, adattare le pratiche di autoregolamentazione alla nuova tecnologia fornendo informazioni sugli sviluppi di tale tecnologia e le sue modalità d'uso, fornire assistenza pratica ai paesi candidati e a quelli in fase di adesione che desiderano istituire organismi di autoregolamentazione e potenziare i legami con gli organismi di autoregolamentazione al di fuori dell'Europa. Inoltre, si incoraggerà con un maggiore sostegno l'assegnazione di marchi di qualità dei siti.»;

5) al punto 2.1 sono aggiunti i seguenti settimo ed ottavo comma:

«Nella seconda fase, si porrà l'accento sul raffronto tra software e servizi di filtraggio [in termini di prestazioni, facilità d'uso, resistenza alla pirateria informatica (hacking), adattabilità ai mercati europei e alle nuove forme di contenuti digitali]. L'assistenza allo sviluppo di tecnologie di filtraggio sarà fornita nel quadro del programma comunitario di ricerca. La Commissione assicurerà uno stretto collegamento con le attività di filtraggio nel quadro del piano d'azione.

La seconda fase promuoverà l'avvio dell'autoclassificazione da parte dei fornitori di contenuti e l'informazione degli utenti e sui software e i servizi di filtraggio europei.»;

6) al punto 2.2 è aggiunto il seguente terzo comma:

«Nella seconda fase, si sosterrà la collaborazione tra l'industria e le parti interessate, quali fornitori di contenuti, organismi di regolamentazione e autoregolamentazione, società di classificazione dei software e di Internet e associazioni dei consumatori, al fine di promuovere condizioni propizie allo sviluppo e all'applicazione di sistemi di classificazione di facile comprensione e di facile uso per i fornitori di contenuti e per i consumatori, che forniscano ai genitori e agli insegnanti europei le informazioni necessarie per adottare decisioni in sintonia con i loro valori culturali e linguistici e che tengano conto della convergenza delle telecomunicazioni, dei mezzi audiovisivi e delle tecnologie dell'informazione.»;

7) il punto 3.2 è modificato come segue:

a) il quarto comma è sostituito dal testo seguente:

«Scopo del sostegno comunitario è incentivare la sensibilizzazione su vasta scala e fornire un coordinamento complessivo e uno scambio di esperienze in modo da trarre insegnamenti dai risultati dell'azione su base costante (ad esempio aggiornando il materiale distribuito). La Commissione continuerà ad adottare misure intese a promuovere soluzioni per la distribuzione a un gran numero di utenti caratterizzate da un buon rapporto costi-efficacia, segnatamente avvalendosi di organizzazioni che fungano da moltiplicatori e di canali di distribuzione elettronici, così da raggiungere i gruppi destinatari.»;

b) è aggiunto il seguente quinto comma:

«Nella seconda fase, sarà sostenuto lo scambio di migliori pratiche in materia di formazione all'uso dei nuovi media attraverso la creazione di una rete europea finalizzata alla sensibilizzazione sull'uso più sicuro di Internet e delle nuove tecnologie on-line, assistita da:

— un centro di smistamento transnazionale (un portale web) delle pertinenti informazioni e delle risorse di sensibilizzazione e ricerca,

— una ricerca applicata in materia di formazione all'uso dei media che coinvolga tutte le parti interessate (ad esempio settore dell'istruzione, organismi ufficiali e di volontariato per la tutela dei minori, associazioni di genitori, industria, autorità preposte all'applicazione della legge) sull'uso delle nuove tecnologie da parte dei bambini, per individuare gli strumenti educativi e tecnologici atti a proteggerli.

La rete fornirà altresì assistenza ai paesi candidati e a quelli in fase di adesione che intendono avviare azioni di sensibilizzazione e potenzierà i legami con le attività di sensibilizzazione svolte al di fuori dell'Europa.»;

8) al punto 4.2, il secondo, terzo e quarto comma sono sostituiti dal seguente testo:

«La Commissione organizza pertanto seminari e workshop a scadenze regolari per trattare i vari temi del piano d'azione o una combinazione di tali temi. Dovrebbero essere chiamati a partecipare l'industria, i gruppi di utenti, di consumatori, di difesa dei diritti civili e organismi statali incaricati della regolamentazione del settore e dell'applicazione della legge, nonché esperti e ricercatori affermati. La Commissione cercherà di garantire un'ampia partecipazione dei paesi del SEE, dei paesi terzi e delle organizzazioni internazionali.»

ALLEGATO II

RIPARTIZIONE INDICATIVA DELLE SPESE

1.	Creazione di un ambiente più sicuro	20-26 %
2.	Sviluppo di sistemi di filtraggio e classificazione	20-26 %
3.	Incoraggiamento di azioni di sensibilizzazione	42-46 %
4.	Azioni di sostegno	3-5 %
	Totale:	100 %

COMMISSION DES COMMUNAUTÉS EUROPÉENNES

Bruxelles, le 28.7.2003
SEC(2003) 895

DOCUMENT DE TRAVAIL DES SERVICES DE LA COMMISSION

LIGNES DIRECTRICES RELATIVES AUX CRITÈRES ET MODALITÉS DE MISE EN ŒUVRE DES FONDS STRUCTURELS EN FAVEUR DES COMMUNICATIONS ÉLECTRONIQUES

TABLE DES MATIERES

1. FINALITE DU DOCUMENT

Ces lignes directrices ont été élaborées à l'intention des régions désireuses de cofinancer, au travers des fonds structurels, des investissements dans le secteur des communications électroniques. Dans le cadre des fonds structurels, la sélection des projets relevant des programmes régionaux de l'UE est gérée de façon décentralisée et les décisions sont prises en partenariat par les acteurs du programme, c'est-à-dire un ensemble d'entités publiques et privées qui participent à la réalisation des objectifs du programme. Au niveau de l'UE, c'est le Fonds européen de développement régional (FEDER) qui constitue le principal instrument financier de soutien à la cohésion et à la politique régionale de l'UE.

Le présent document fait écho aux séries de lignes directrices qui ont été fournies sous l'égide de la DG REGIO aux gestionnaires et investisseurs des programmes. Son rôle est en particulier d'actualiser et de compléter le document de travail des services de la Commission[1] préparé en 1999 pour l'actuelle période de programmation, de manière à prendre en compte l'évolution récente du secteur concerné.

A la suite de la proposition de la Commission[2] approuvée par le Conseil européen de printemps, les lignes directrices établissent '*les critères et les modalités de mise en oeuvre des fonds structurels en faveur du secteur des communications électroniques, notamment pour le haut débit, en particulier dans les zones rurales et les zones isolées géographiquement et à faible densité de population*'[3]

Les lignes directrices mettent principalement l'accent sur les infrastructures de communications électroniques, tout en maintenant l'importance des mesures liées à la demande et au contenu.

Elles traitent aussi des questions liées à la téléphonie mobile de seconde générationqui sont susceptibles de se poser dans des contextes bien particuliers au cours de la période 2004-2006.

Ces lignes directrices sont présentées à titre indicatif[4]. et complètent les orientations générales pour la révision à mi-parcours des interventions des fonds structurels, prévue

---

1 Commission européenne, Société de l'information et développement régional - Interventions prévues dans le cadre du FEDER pour la période 2000/2006 - Critères pour l'évaluation des programmes, SEC/1999/1217.

2 En 2003, la Communication de la Commision sur les communications électroniques : la voie vers l'économie de la connaissance (COM 2003 65 final) déclare : 'la révision à mi-parcours des programmes des fonds structurels qui aura lieu en 2003 fournit une opportunité pour les Etats membres de mettre davantage l'accent à cette priorité sur la base d'une évaluation des besoins régionaux. Avant le printemps 2003, la Commission fournira aux Etats membres des lignes directrices sur les critères et les modalités de mise en oeuvre des fonds structurels en faveur du secteur des communications électroniques, notamment les infrastructures de haut débit, fixes et sans fil (p7)

3 Conclusions du Conseil européen de Printemps, Corfu, 21 mars 2003

4 Elles s'entendent sans préjudice de toute ligne directrice ou communication que la Commission pourrait adopter en matière d'applicabilité des règles relatives aux aides d'État aux services d'intérêt économique général.

en 2003. Elles tiennent aussi compte de la situation spécifique des nouveaux États membres.

2. CONTEXTE

Depuis 1999, la société de l'information (SI) a connu des changements significatifs, tant en termes de politiques (eEurope) qu'en ce qui concerne le nouveau cadre réglementaire applicable aux réseaux et services de communications électroniques (nouvelle série de directives). Ces changements peuvent avoir un impact significatif sur le soutien des fonds structurels quant au déploiement de la société de l'information dans les régions les plus défavorisées.

- L'évolution des politiques

Le plan d'action eEurope 2002[5], adopté par les chefs d'État et de gouvernement en juin 2000 au Conseil de Feira, a établi que permettre aux régions moins favorisées de participer pleinement à la société de l'information était une priorité pour l'Union. Il recommande également la possibilité d'un soutien financier européen, dans toute l'Union, en faveur des nouveaux services et infrastructures, dès lors que les aides publiques ne faussent pas la concurrence et respectent la neutralité technologique.

En 2002, le Conseil européen de Séville a avalisé le plan d'action eEurope 2005. Celui-ci définit une stratégie visant à doter l'ensemble du territoire européen d'une infrastructure à large bande abondamment disponible, pour les particuliers comme pour les entreprises, à des prix abordables. Il souligne également la nécessité de développer des services et des contenus adéquats, en mettant particulièrement l'accent sur les administrations publiques (gouvernement électronique ou «e-government»), un environnement électronique dynamique pour les affaires (e-business), des services de télésanté (e-health) et des services d'apprentissage électronique (e-learning). Par conséquent, le Conseil européen de printemps en mars 2003 a appelé les Etats membres à mettre en place leurs stratégies nationales en matière de haut débit pour la fin 2003.

- Le cadre réglementaire des communications électroniques

En réponse aux conclusions du Conseil européen spécial tenu à Lisbonne les 23 et 24 mars 2000, et sur la base de sa communication intitulée «Résultats de la consultation publique sur le réexamen 1999 du cadre des communications et lignes directrices pour le nouveau cadre réglementaire» (COM(2000) 239), un ensemble de mesures qui composeront le nouveau cadre réglementaire applicable aux services et réseaux de communication électronique a été adopté au cours de l'année 2002.

---

5 eEurope 2002 - Une société de l'information pour tous - Plan d'action, p. 7

Cadre réglementaire des communications électroniques
Directive 21/2002/CE relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques
Directive 19/2002/CE sur l'accès et l'interconnexion Directive 20/2002/CE sur l'autorisation Directive 22/2002/CE sur le service universel et les droits des utilisateurs Directive 58/2002/CE pour la protection des données à caractère personnel et la protection de la vie privée Directive 77/2002/CE de la Commission sur la concurrence dans les marchés des réseaux et des services de communications électroniques Règlement (CE) n°2887/2000 relatif au dégroupage de l'accès à la boucle locale
Les États membres ont jusqu'au 25 juillet 2003 pour transposer ces textes, à l'exception de la directive sur la protection des données (31 octobre 2003).

Le nouveau cadre réglementaire vise à mettre en place une approche cohérente, fiable et souple de la régulation des réseaux et services de communication électronique permettant de libéraliser les marchés tout en veillant à ce que l'ensemble des utilisateurs bénéficie d'un minimum de services pour un prix raisonnable et à ce que les droits fondamentaux des consommateurs soient protégés.

- La justification de l'intervention des fonds structurels

L'action communautaire au travers des fonds structurels compte parmi ses principaux objectifs le développement et l'ajustement structurel des régions en retard de développement (objectif 1) ainsi que la reconversion économique et sociale des régions (objectif 2)[6]. Les actions financées par les fonds structurels doivent en outre être réalisées dans le respect des autres politiques communautaires, notamment en matière de concurrence.

---

6 Règlement général sur les fonds structurels (n° 1260/1999).

Dans ses lignes directrices pour les programmes de la période 2000-2006[7], la Commission fait de la société de l'information une priorité clé des interventions des fonds structurels et met fortement l'accent sur la demande de services et d'applications.

La société de l'information peut fortement contribuer à renforcer la cohésion économique et sociale, c'est-à-dire à combler le fossé des disparités économiques et sociales en Europe. À l'échelon régional, le succès des stratégies mises en œuvre dépendra toutefois de la capacité des régions à intégrer les technologies de l'information et de la communication mises à leur disposition.

D'importantes mutations dans le secteur des communications électroniques – telles que l'évolution rapide de la technologie, la lente expansion des services à large bande et les changements dans le cadre réglementaire – imposent de repenser le rôle du financement public en tenant compte de son caractère stratégique pour le développement économique. Après des années de libéralisation des marchés, force est aussi de constater que la couverture géographique présente des lacunes évidentes, même dans le cas de technologies déjà au point telles que les réseaux GSM.

Dans les nouveaux États membres, la mise en œuvre de l'acquis dans le domaine de la société de l'information peut avoir une incidence financière considérable étant donné que l'implantation des infrastructures fondamentales en matière de communications électroniques est loin d'être achevée. C'est le cas, notamment, pour le financement des obligations de service universel[8].

Le risque d'un élargissement du «fossé numérique», avec tout ce que cela implique sur le plan économique, comme la délocalisation d'activités, a conduit de nombreux gouvernements à explorer des solutions nouvelles pour encourager le déploiement d'infrastructures à large bande dans les zones les plus défavorisées. Ce sont des régions où le coût de la mise à niveau des infrastructures existantes peut se révéler prohibitif en raison de l'isolement géographique et d'une faible densité de peuplement. Or, dans les zones rurales, l'absence de structures adéquates constitue un obstacle majeur au développement de certaines activités économiques telles que le tourisme, mais aussi une source de disparités sociales.

Le coût des investissements à consentir pour répondre aux besoins de développement actuels et futurs de la société de l'information est souvent difficile à justifier en termes purement commerciaux. Il existe donc un risque que l'absence potentielle de retour financier sur ces investissements remette en cause l'objectif fondamental de l'eEurope 2000, à savoir l'accès pour tous à la société de l'information.

C'est pourquoi les investissements dans le cadre des fonds structurels doivent aller au-delà des considérations commerciales pour prendre en compte des aspects politiques plus

---

7 Commission européenne, Les fonds structurels et leur coordination avec le fonds de cohésion - Orientations pour les programmes de la période 2000-2006, COM 1999 (344)

8 Le nouveau cadre réglementaire (directive 22/2002/CE concernant le service universel et les droits des utilisateurs) prévoit que le service universel est «mis à la disposition de tous les utilisateurs fin[aux], au niveau de qualité spécifié, quelle que soit la localisation géographique de ces derniers et, en fonction des conditions propres à chaque État membre, à un prix abordable.» La portée du service universel est définie comme couvrant, entre autres, l'accès au réseau téléphonique filaire public (communications voix et données) ainsi qu'un accès internet à bande étroite. Elle ne couvre la téléphonie mobile ni l'accès à large bande à l'internet.

larges. Leur rôle est en effet de permettre aux régions les moins favorisées d'être à la pointe du développement de la société de l'information, en accélérant le déploiement de la large bande et en œuvrant pour plus de cohésion territoriale. Cette mission revêt aussi une importance particulière dans la perspective de financements éventuels des services et infrastructures de communications dans les nouveaux États membres, qui soient intégrés à leurs propres plans et programmes de développement.

3. DEMANDE ET CONTENU

L'existence d'infrastructures de communications de haute qualité est une condition fondamentale pour permettre aux citoyens, aux entreprises et aux administrations d'exploiter les possibilités offertes par la société de l'information.

La disponibilité de ces infrastructures peut toutefois se révéler vaine en l'absence de services et applications appropriés mis à la disposition des utilisateurs finaux ou si ces derniers ne disposent pas des connaissances ou des compétences nécessaires pour en faire bon usage. Un contenu relativement faible, une sensibilisation généralement peu développée aux avantages et possibilités qu'offre la société de l'information et une insuffisance de qualifications en matière de technologies de l'information et de la communication (TIC) sont autant d'obstacles fréquemment constatés dans les régions les plus défavorisées.

Si grande que soit l'importance des infrastructures, il faut aussi que les entreprises et les régions aient une perception claire de la demande de nouveaux services qu'engendrera la société de l'information.

Les fonds structurels sont aussi là pour aider les régions à renforcer l'aspect demande de la SI, tout spécialement en ce qui concerne la capacité des entreprises et organes institutionnels à exploiter efficacement les TIC. Plusieurs approches sont possibles pour stimuler la demande:

- - La modernisation du secteur public

  Il convient d'encourager le regroupement de la demande en services à large bande de manière à créer une masse critique d'utilisateurs dans les administrations du secteur public tout en évitant de dépendre d'un opérateur unique.

- La stimulation de la demande dans le secteur privé

  La stimulation de la demande dans des catégories ou «bouquets» de PME permet de développer la sensibilisation aux TIC et d'en encourager l'utilisation.

- Le développement des contenus

  Le financement des contenus, y compris l'«e-gouvernement» et, en particulier, son volet services locaux et régionaux, permet de stimuler la demande de large bande de façon suffisamment ciblée pour développer l'offre.

- Le développement des compétences en matière de technologies numériques

  Doter les populations des compétences nécessaires pour utiliser les connecte à large bande.

Les pouvoirs publics, particulièrement aux échelons régional et local, ont un rôle clé à jouer dans le développement de la société de l'information, (1) en utilisant les applications et les services de la société de l'information dans le processus de modernisation des prestations destinées aux citoyens et aux entreprises, (2) en assurant la promotion de la société de l'information au niveau régional et (3) en suivant l'évolution de la fourniture des réseaux de télécommunications dans la région afin d'éviter l'exclusion et de contribuer au développement équilibré des activités régionales.

S'agissant de ce dernier aspect, l'accessibilité[9] revêt une importance particulière parce qu'elle favorise la demande en suscitant l'intérêt et en donnant aux citoyens, aux entreprises et aux organismes concernés une possibilité de prendre conscience des services génériques et des applications TIC, ainsi que des avantages pratiques liés à leur utilisation. Cela engendrera à son tour la masse critique ou le niveau de demande nécessaires pour renforcer le développement de la société d'information au niveau régional.

Les financements publics consacrés aux initiatives citées doivent respecter les règles établies par le traité en matière d'aides d'État. Selon le cas, ces financements peuvent être jugés compatibles avec ces règles au titre des dispositions applicables, par exemple, aux aides en faveur des petites et moyennes entreprises[10], aux aides à finalité régionale[11] ou aux aides relevant de la clause «de minimis»[12].

4. FINANCEMENT DES INFRASTRUCTURES DE COMMUNICATIONS ELECTRONIQUES: CRITERES REGISSANT L'INTERVENTION DU FEDER

Le plan d'action eEurope 2005 indique que les nouveaux services et infrastructures peuvent bénéficier d'un soutien des fonds structurels dans les régions éligibles, particulièrement lorsqu'il s'agit de zones rurales et isolées. Cette disposition est néanmoins soumise à certains critères qui doivent être pris en compte lors de l'évaluation des investissements dans la société de l'information. Ces critères sont décrits ci-après.

- Nécessité d'un cadre stratégique

  Les aides du FEDER doivent être liées à la stratégie de la région en matière de développement de la société de l'information et déterminés par celle-ci. Plus précisément, les projets d'infrastructure doivent être en relation avec les objectifs de développement économique, c'est-à-dire de croissance économique, de compétitivité régionale et de répartition équilibrée des activités économiques. Les projets isolés ne doivent pas recevoir d'aide, mais être articulés à d'autres actions visant à développer de nouveaux services et applications.

---

9 Plus particulièrement, le FEDER pourrait assister les gouvernements locaux et régionaux dans leurs efforts visant à introduire une administration et des services télématiques en ligne et à fournir à la population un accès facile à ce système. Le FEDER devrait par exemple contribuer à implanter des points d'accès adaptés dans les municipalités ou les communautés locales.

10 Règlement (CE) n° 70/2001 de la Commission du 12 janvier 2001 concernant l'application des articles 87 et 88 du traité CE aux aides d'État en faveur des petites et moyennes entreprises (JO L 10 du 13.1.2001, p. 33).

11 Lignes directrices concernant les aides d'État à finalité régionale, JO C 74 du 10.3.1998, p. 9.

12 Règlement (CE) n° 69/2001 de la Commission du 12 janvier 2001 concernant l'application des articles 87 et 88 du traité CE aux aides de minimis (JO L 10 du 13.1.2001, p. 30).

Dans le cadre de la stratégie, il convient que les projets d'infrastructure s'appuient sur une analyse des possibilités et besoins régionaux identifiés en consultation avec les partenaires socio-économiques dans le respect de critères économiques et institutionnels précis et en tenant compte des infrastructures existantes (c'est-à-dire qu'un inventaire des infrastructures déjà en place doit être dressé avant de planifier un nouvel investissement).

Il appartient en conséquence aux pouvoirs publics, particulièrement au niveau infranational (régions, autorités locales) de proposer des mesures relatives à la société de l'information dans le cadre de programmes nationaux ou régionaux. Ils ont également la responsabilité de veiller à ce que les mesures d'investissement soient en phase avec les objectifs et les besoins régionaux et qu'elles soient cohérentes par rapport à la stratégie globale de développement économique, tout en garantissant leur viabilité économique.

Dans la perspective des futures adaptations à apporter aux programmes des objectifs 1 et 2, la Commission devra être informée du contenu des stratégies, sous la forme d'un cadre simplifié (Annexe I) .

- Ciblage géographique

Les aides du FEDER sont octroyées en tenant compte des particularités régionales, notamment des facteurs géographiques, qui peuvent varier fortement d'une région éligible à l'autre. En principe, les investissements doivent servir aux régions qui, dans des conditions de libre marché, seraient négligées. Il convient de privilégier les zones rurales et éloignées, qui ne disposent pas d'infrastructures adaptées. Des aides du FEDER sont également justifiées dans les régions où les incitations commerciales sont insuffisantes pour pourvoir à l'infrastructure adéquate permettant la mise en place d'applications avancées et de services d'intérêt général.

Bien que les aides régionales soient en principe réservées aux régions éligibles aux objectifs n^{os} 1 ou 2, il est possible de financer des investissements en dehors de ces régions à partir du moment où ceux-ci concernent des régions contiguës (NUTS III) et sont conformes aux règles d'éligibilité fixées dans le règlement (CE) n° 1685/2000[13].

- Neutralité technologique

Les critères de sélection des investissements en matière d'infrastructures de communications électroniques doivent respecter le principe de la «neutralité technologique». Le concours du FEDER ne doit favoriser aucune technologie en particulier ni limiter les choix technologiques des régions.

---

13 «Les dépenses éligibles maximales de l'opération sont calculées au prorata des bénéfices escomptés de l'opération prévue pour la région visée et sont fondées sur une évaluation réalisée par un organisme indépendant de l'autorité de gestion. Les bénéfices sont évalués en tenant compte des objectifs spécifiques de l'assistance et de son impact escompté. L'opération n'est pas éligible au cofinancement si la part des bénéfices est inférieure à 50 %. Pour chaque mesure d'aide, les dépenses éligibles des opérations acceptées au titre du point 2.1 n'excèdent pas 10 % des dépenses totales de la mesure. En outre, les dépenses éligibles de toutes les opérations acceptées au titre du point 2.1 n'excèdent pas 5 % des dépenses totales de l'assistance.»

Lorsqu'un projet prévoit de financer une technologie en particulier - dans le cas de la large bande, par exemple, la technologie DSL, le câble, le satellite, les technologies sans fil, etc. - ou une infrastructure spécialisée, le choix opéré doit être clairement motivé par une analyse coût-bénéfice, compte tenu des autres possibilités existantes pour la fourniture de ce service.

- Accès ouvert

Un concours financier sera octroyé aux projets conformes au nouveau cadre réglementaire sur les réseaux et services de communication et aux règles de concurrence (aides d'État et ententes). Seuls les projets conformes à ces règles seront éligibles à une aide du FEDER, qui devra être assortie d'obligations claires en matière d'accès ouvert.

Le concours du FEDER doit être en principe limité aux infrastructures, c'est-à-dire aux installations (fibres noires, gaines et pylônes,...) et aux équipements ouverts à tous les opérateurs et fournisseurs de services.

Le territoire concerné peut faire l'objet d'un dégroupage de l'accès à la boucle locale. Les conditions de localisation et les exigences techniques applicables aux points d'accès à la nouvelle infrastructure ne doivent pas favoriser les opérateurs dominants sur le plan local ni entraîner de distorsions sur d'autres marchés.

Le cas des projets d'infrastructure réservée

Le financement direct d'installations et d'équipements qui ne sont pas accessibles à tous parce qu'ils sont réservés à un ou plusieurs opérateurs n'est pas un financement d'un projet «d'infrastructure ouverte»; c'est le cas, par exemple, d'installations réservées à un opérateur donné à la suite d'un accord passé avec l'autorité de régulation.

Le financement d'installations ou d'équipements réservés à un utilisateur final donné peut constituer une aide d'État si cet utilisateur est une entreprise. Dans certains cas, ce financement n'est pas considéré comme une aide d'État s'il est nécessaire à la fourniture d'un service d'intérêt économique général (SIEG). Lorsque le financement constitue une aide d'État, il peut être compatible avec le traité en application des règles régissant les aides aux petites et moyennes entreprises et les aides régionales ou de la clause *«de minimis»*.

La fourniture du service doit respecter les principes de transparence, de non-discrimination, de proportionnalité, et de distorsion minimale sur le marché. Si la fourniture du service ne résulte pas d'une procédure ouverte, transparente et non discriminatoire, l'opérateur est tenu de tenir une comptabilité séparée pour le service en question, ce qui permettra de déterminer le montant des compensations publiques ou des redevances applicables pour l'utilisation de ce service, qui sont révisées chaque année.

5. MODALITES DE MISE EN ŒUVRE

Une fois les projets d'infrastructure reconnus comme conformes aux critères susmentionnés, un certain nombre de règles fondamentales de mise en œuvre doivent être respectées. S'agissant du droit de la concurrence, il convient de souligner que le concours

du FEDER ne représente pas une aide d'État au sens de l'article 87, paragraphe 1, mais qu'il doit respecter les mêmes règles et que, le cas échéant, il s'ajoute au financement par les États membres lorsqu'il s'agit de déterminer le montant d'aide compatible.

- Procédure d'appel d'offres

Les contrats doivent être passés par l'intermédiaire d'une procédure d'appel d'offres. De manière générale, celle-ci doit être organisée au niveau approprié (national, régional ou local) sous la supervision de l'autorité compétente, qui doit veiller au respect de la législation applicable et à la cohérence avec les politiques nationales en matière de société de l'information.

Les candidats sont invités à présenter une offre technique et financière. Le contrat sera passé avec l'opérateur qui fournira un service répondant aux caractéristiques voulues et apportant la solution requise au moindre coût.

- Financement

Le concours du FEDER doit se limiter aux ressources nécessaires pour la fourniture de ce service. En principe, il couvre le financement des installations et des équipements ouverts à tous les opérateurs et à tous les fournisseurs de services.

La description des projets doit inclure des informations détaillées suffisantes pour permettre une évaluation adéquate - par les autorités de gestion - de la pertinence par rapport aux objectifs de développement économique et de la compatibilité avec les règles de la concurrence

- Propriété

L'infrastructure subventionnée appartient à une autorité publique, à une entité privée apportant un cofinancement ou à une entité mixte public-privé. Dans tous les cas, il convient de veiller à ce que tous les opérateurs aient accès à l'infrastructure sans discrimination. Le concours communautaire ne doit pas, en principe, renforcer la position dominante d'un opérateur, quel qu'il soit, ni entraîner de distorsion des règles de concurrence

Il conviendra de définir précisément cas par cas les modalités de location de l'infrastructure à des entreprises privées. Dans certains pays, le cadre réglementaire est en cours de modification; ainsi, certaines autorités locales ont le droit, sous certaines conditions, de devenir des opérateurs..

Pour déterminer la conformité avec les cadres réglementaires, il est utile de faire la distinction entre les financements d'infrastructures selon que celles-ci appartiennent à une autorité publique ou à une entreprise privée.

Infrastructure appartenant à une autorité publique

Le financement d'une infrastructure appartenant à une autorité publique ne constitue pas une aide d'État au sens de l'article 87, paragraphe 1. La passation d'un marché de travaux pour la création d'une telle infrastructure doit évidemment respecter la législation communautaire applicable en la matière.

Toutefois, si l'infrastructure est mise à la disposition d'entreprises, il ne peut y avoir de discrimination dans l'accès et il convient de percevoir les redevances appropriées. Ces redevances ne doivent pas couvrir l'ensemble du coût de l'investissement - dans les cas où le marché ne peut fournir de services équivalents - mais elles ne doivent pas permettre aux utilisateurs de l'infrastructure de réaliser des bénéfices supplémentaires au delà d'une rentabilité correcte.

Néanmoins, si un service équivalent à celui fourni par l'infrastructure existe déjà sur le marché, l'infrastructure doit être louée à un prix permettant de couvrir les coûts et d'assurer une rentabilité correcte de l'investissement.

Si un tiers est chargé de la gestion des installations, la concession doit être de durée limitée et résulter d'une procédure ouverte, transparente et non discriminatoire; il est préférable d'opter pour une procédure concurrentielle et de faire payer au détenteur de la concession une compensation répondant aux conditions de marché. De manière générale, cette procédure doit être organisée au niveau approprié (national, régional ou local) sous la supervision de l'autorité compétente, qui doit veiller au respect de la législation applicable et à la cohérence avec les politiques nationales et régionales en matière de société de l'information.

Le gestionnaire de l'infrastructure doit respecter des conditions d'exploitation qui permettent de préserver la nature de l'infrastructure, soit celle d'une infrastructure ouverte sans discrimination à tous les opérateurs fournissant des réseaux et des services de communication électronique.

Infrastructure appartenant à une/des entreprise(s)

En cas de (co)financement d'une infrastructure appartenant à une entreprise, la contribution financière de l'État doit être subordonnée à l'acceptation de conditions d'exploitation qui permettent de préserver sa nature, soit celle d'une infrastructure ouverte sans discrimination à tous les opérateurs fournissant des réseaux et des services de communication électronique.

Il convient de prouver que le montant du financement par l'État constitue le minimum nécessaire pour permettre au projet d'avancer, afin de garantir que l'opérateur qui utilise l'infrastructure ne reçoit pas plus que ce qu'il recevrait pour ses activités dans des conditions de marché normales. C'est pourquoi les financements émanant de l'État doivent être octroyés par l'intermédiaire d'une procédure d'appel d'offres. De manière générale, celle-ci doit être organisée au niveau approprié (national, régional ou local) sous la supervision de l'autorité compétente, qui doit veiller au respect de la législation applicable et à la cohérence avec les politiques nationales en matière de société de l'information. Les candidats sont invités à présenter une offre technique et financière. Il convient de passer le contrat avec l'/les opérateur(s) qui fourni(ssen)t des réseaux de communication électronique répondant aux conditions minimales spécifiées pour ce service (en termes de qualité de service, d'améliorations futures, etc.) au moindre coût.

- Transparence

Les opérateurs d'infrastructures doivent établir un système comptable permettant de calculer et de justifier toute compensation ou toute subvention au regard de la législation communautaire en matière de concurrence. Seul un tel système permet d'établir de

manière transparente et efficace les droits applicables et de répartir entre les différentes parties pertinentes du réseau les différentes composantes du coût.

Le cadre réglementaire relatif aux communications électroniques requiert, en particulier, que les autorités de régulation soit distinctes sur un plan juridique et indépendantes sur un plan fonctionnel des organisations qui sont en charge de la fourniture des réseaux, équipements ou services de communication. Dans le cas où des autorités locales ont des fonctions de régulation, notamment en matière de droits de passage et de permis de construire, les Etats membres devront respecter les principes de transparence et de non-discrimination et faire en sorte que ces droits soient obtenus dans des conditions similaires par des demandeurs qui ne bénéficient pas d'aide.

- Détermination des taux de cofinancement

Il incombe aux régions d'évaluer et de sélectionner les projets. Les taux de concours du FEDER s'appliquent aux projets cofinancés, en fonction de leur rentabilité économique et financière et en application des dispositions prévues par l'article 29, paragraphe 4, du règlement n° 1260/99[14].

Lorsque des projets d'infrastructures de communication sont considérés comme des investissements générateurs de recettes nettes substantielles, les taux cofinancés doivent être justifiés et modulés sur la base d'une analyse coût-bénéfice complète. Il s'agit en général de projets qui génèrent au moins 25 % de bénéfice net par rapport au coût réel de l'investissement, sur la base d'un taux d'actualisation adéquat (soit 6 %).

- Évaluation, suivi et étalonnage

L'appréciation de l'efficacité de l'aide apportée aux régions par les Fonds structurels constitue un aspect essentiel de la responsabilité financière, en termes d'optimisation des ressources et d'estimation des décisions futures en matière d'investissements.

En ce qui concerne l'évaluation préalable des projets en rapport avec la société de l'information, en particulier les projets d'infrastructures de télécommunications, il convient de tenir compte des critères suivants:

---

[14] Règlement (CE) n° 1260/99 sur les Fonds structurels, article 29, paragraphe 4:
«... Lorsque l'intervention concernée implique le financement d'investissements générateurs de recettes, la participation des Fonds à ces investissements est déterminée compte tenu, parmi leurs caractéristiques propres, de l'importance de la marge brute d'autofinancement qui serait normalement attendue pour la catégorie des investissements concernés en fonction des conditions macroéconomiques dans lesquelles les investissements sont à mettre en œuvre, et sans que la participation des Fonds n'entraîne une augmentation de l'effort budgétaire national.
En tout état de cause, la participation des Fonds est soumise aux plafonds suivants:
a) dans le cas d'investissements en infrastructures générateurs de recettes nettes substantielles, l'intervention ne peut dépasser:
i) 40 % du coût total éligible dans les régions couvertes par l'objectif n° 1, auxquels peut être ajoutée une majoration maximale de 10 % dans les États membres couverts par le Fonds de cohésion;
ii) 25 % du coût total éligible dans les zones couvertes par l'objectif n° 2;
iii) ces taux peuvent faire l'objet d'une majoration destinée à des formes de financement autres que des aides directes, sans que cette majoration ne puisse dépasser 10 % du coût total éligible; ...".

- le taux de pénétration des réseaux de communication électronique (en pourcentage du nombre de ménages résidents et, si ces chiffres ne sont pas disponibles, en nombre de lignes pour cent habitants),

- le revenu des réseaux de communication électronique par habitant,

- les opérateurs actifs (services et réseaux) dans la région/zone,

- l'évolution du marché (part de marché et croissance du marché),

- le taux de pénétration, le revenu et la diffusion pour les autres moyens de communication (satellite, techniques sans fil, communications mobile, etc.),

- la fourniture des services à un coût abordable;

Il convient en outre de fournir des informations détaillées sur le projet et sur son promoteur, notamment, le coût total, la rentabilité escomptée de l'investissement en capital, la création d'emplois (directs) estimée, la diversification de l'économie locale dans des activités ayant trait à la connaissance.

Il conviendrait d'utiliser une liste de contrôle des indicateurs pour suivre au fil du temps les réalisations et l'incidence des projets relatifs à la société de l'information soutenus par le FEDER. Il convient de définir des indicateurs régionaux, le cas échéant, en tenant dûment compte des indicateurs du plan d'action *e*Europe 2005. Les objectifs devraient tenir compte des particularités locales.

6. LE CAS DE LA TELEPHONIE MOBILE « DEUXIEME GENERATION »

De manière générale, un investissement dans la téléphonie mobile de la deuxième génération est rentable; un concours du FEDER ne se justifie donc pas du point de vue économique. Bien que la couverture de certaines zones ne soit pas totalement rentable, il convient normalement d'exiger une couverture large d'une portion significative de territoire, notamment grâce à des financements croisés. Toutefois, il est possible qu'un État membre souhaite étendre la couverture à la partie de sa population vivant dans des zones qui ne sont couvertes par aucun réseau («zones blanches») afin de garantir la viabilité économique de ces investissements. Dans ce cas, un concours du FEDER peut être accordé pour les zones blanches si les investissements ne sont pas rentables.

Questions de concurrence

Les investissements qui concernent exclusivement une infrastructure ouverte, c'est-à-dire des installations et des équipements auxquels tous les opérateurs ont accès, sans discrimination, ne posent pas de problèmes particuliers en matière de concurrence. L'itinérance locale doit être garantie aux autres opérateurs à des tarifs équitables si nécessaire pour éviter toute discrimination entre les opérateurs. Il faut pour cela créer, dans le respect des règles de concurrence, un service d'itinérance locale afin de garantir le partage des infrastructures en fonction.

Le financement direct de services ou d'équipements réservés à un ou plusieurs opérateurs n'est pas un financement d'un projet «d'infrastructures»; c'est le cas, par exemple, d'installations réservées à un opérateur donné à la suite d'un accord passé avec l'autorité de régulation. Dans ce cas, une intervention de l'État pourrait être justifiée par le besoin

de fournir un «service d'intérêt économique général» (conformément à l'article 86, paragraphe 2, du traité) dans la mesure où les opérateurs ne se voient pas octroyer d'avantage financier supérieur au coût supplémentaire net du service.

La fourniture du service doit respecter les principes de transparence, de non-discrimination, de proportionnalité, et de distorsion minimale sur le marché. Si la fourniture du service ne résulte pas d'une procédure ouverte, transparente et non discriminatoire, l'opérateur est tenu de tenir une comptabilité séparée pour le service en question, ce qui permettra de déterminer le montant des compensations publiques ou des redevances applicables pour l'utilisation de ce service, qui seront révisées chaque année.

Annexe 1

STRATÉGIE RÉGIONALE DE DÉVELOPPEMENT DE LA SOCIÉTÉ DE L'INFORMATION

(schéma indicatif)

I. Etat des lieux

- Documents stratégiques existants (le cas échéant transmission d'une copie à la DG REGIO)
- Les projets existants : recensement des infrastructures de réseaux (mobile et haut débit), des applications (services) et des usages
- Les besoins en termes de développement économique

II. Les enjeux et les objectifs à moyen et long terme

- Cohérence de la stratégie de la société en matière de la société de l'information avec la stratégie de développement économique de la région ?
- Pertinence des objectifs en matière de la société de l'information et leur contribution aux objectifs du programme
- Principaux enjeux au regard du développement économique

III. Principaux projets à financer

En articulation avec le point I, il convient de fournir les informations nécessaires concernant :

- la nature des actions
- le contenu des projets
- la localisation des investissements
- l'impact financier
- la viabilité économique

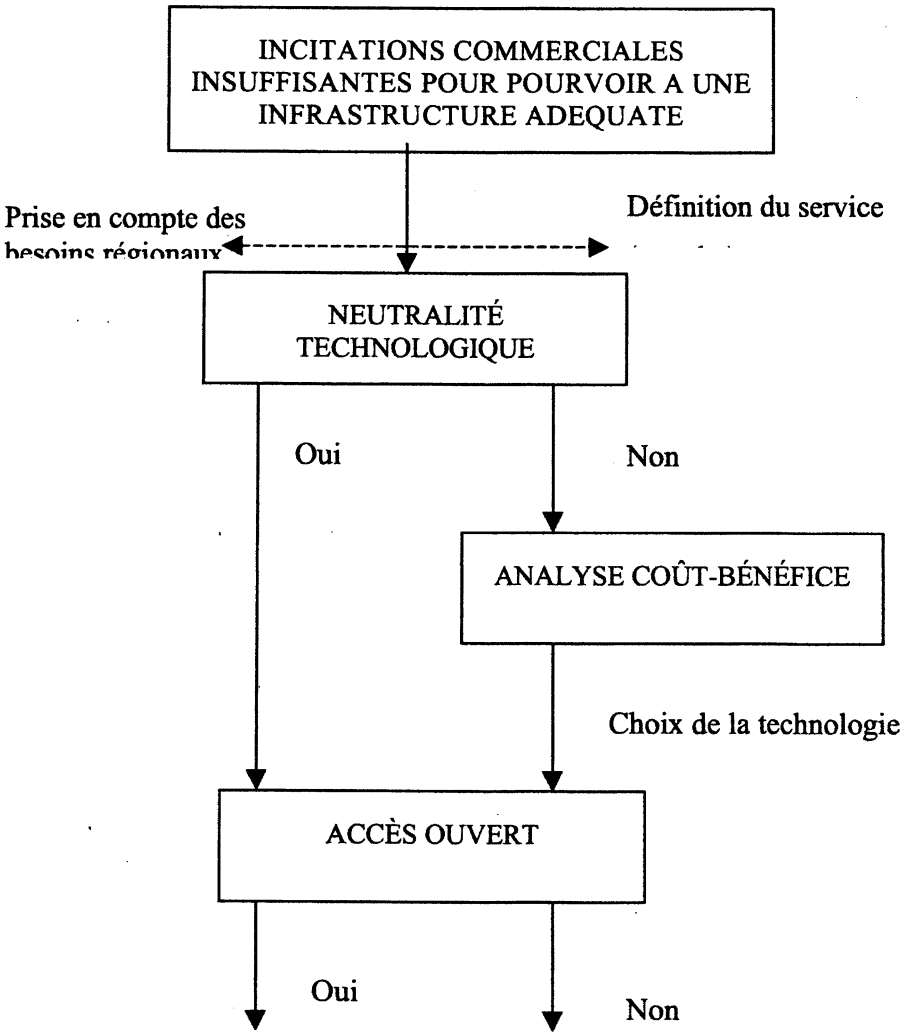
IV. Budget estimé

La région devra fournir une estimation des coûts d'investissement globaux y compris les actions non cofinancées.

Annexes cartographiques : carte téléphonie mobile et carte réseaux à haut débit

Annexe 2

SCHÉMA I : CRITÈRES POUR LE FINANCEMENT D'INFRASTRUCTURES PAR LES FONDS STRUCTURELS



Aide d'État compatible au titre:

- des services d'intérêt économique général (SIEG),
- des aides aux PME
- des aides régionales

Annexe 3

SCHÉMA II : MODALITÉS DE MISE EN ŒUVRE

PROPRIÉTAIRE	PUBLIC	Partenariat public-privé	PRIVÉ
ACTION			
Choix de l'entreprise privée		Appel d'offres	Appel d'offres
Choix du fournisseur d'équipement/de services	Modalités d'application des marchés publics	Appel d'offres	Libre
Choix du gestionnaire d'infrastructure	Concession ou Gestion directe sans contradiction avec le règlement	Sans contradiction avec le règlement	Libre
Accès à l'infrastructure	Ouvert à tous → pas de problème ou Réservé → notification possible	Ouvert à tous → pas de problème ou Réservé → notification possible	Ouvert à tous → pas de problème ou Réservé → notification possible

LEGISLAZIONE IN PREPARAZIONE

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 12.3.2004
COM(2004) 91 definitivo

2004/0023 (COD)

Proposta di

DECISIONE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie online

(presentata dalla Commissione)

{SEC(2004) 148}

RELAZIONE

1. INTRODUZIONE

Internet si è ormai trasformato in un universo domestico. Concepito inizialmente come mezzo di comunicazione ad uso della comunità scientifica, si è sviluppato in strumento utilizzato oggi nelle case, nelle scuole, nelle imprese e nelle pubbliche amministrazioni. Internet è stato la forza trainante che ha caratterizzato la fine del XX e dell'inizio del XXI secolo ma, per molti aspetti, il suo potenziale rimane in gran parte inesplorato.

I contenuti e i comportamenti illegali e nocivi su Internet costituiscono una fonte di preoccupazione permanente per i legislatori, l'industria e gli utenti finali, in particolare i genitori e gli educatori. L'Unione europea è stata la prima, nel 1996, ad avviare un'azione per contrastare i contenuti illegali e nocivi[1].

Il piano d'azione per l'uso sicuro di Internet 1999-2004[2] è un elemento essenziale dell'azione della Commissione in questo campo. Grazie a questa iniziativa è stato possibile istituire una rete europea di *hotline,* stimolare l'autoregolamentazione e i codici di condotta, sostenere lo sviluppo di sistemi di filtraggio e di classificazione dei contenuti e infine promuovere azioni di sensibilizzazione.

Stando ai risultati della valutazione, appena conclusasi, in merito al periodo 1999-2002[3], nei primi quattro anni di funzionamento il piano d'azione ha recato sostanziali benefici ma la complessità delle problematiche e la molteplicità degli attori coinvolti fanno sì che sia necessario intensificare gli sforzi in questo campo.

Si profilano oggi nuove sfide, sia in termini quantitativi che qualitativi.

Dal punto di vista qualitativo, nel concetto di nuove tecnologie rientrano l'aumento costante della potenza di calcolo e della capacità di stoccaggio dei computer; le comunicazioni in banda larga, grazie alle quali è possibile distribuire sulle reti contenuti che, come il video, richiedono grande larghezza di banda; e la maggiore capacità delle reti mobili dell'ultima generazione. La nuova generazione di cellulari sarà in grado di distribuire contenuti "per adulti" e sono allo studio le modalità per limitare l'accesso a tali contenuti in modo che i genitori possano disporre di telefoni con dispositivi di bloccaggio che impediscano ai loro figli di imbattersi inavvertitamente in siti web dal contenuto esplicito e in *chat room* inadatte.

Dal punto di vista quantitativo, le evoluzioni tecnologiche appena menzionate consentono di accrescere il volume e il tipo di contenuti distribuiti.

Il tasso di utilizzo di Internet e delle nuove tecnologie è in aumento. L'accesso di tipo residenziale rappresenta una quota di mercato sempre più importante e i bambini

---

1 Comunicazione sulle informazioni di contenuto illegale e nocivo su Internet (COM(96) 487) e Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione (COM(96) 483).

2 Cfr. nota 22.

3 COM(2003) 653.

che non hanno Internet a casa possono contare su un collegamento a scuola. Il tasso di penetrazione è di oltre il 42% per l'utenza residenziale e superiore al 90% per le imprese e le scuole. Secondo un recente studio di Nielsen/NetRatings, dal mese di aprile 2002 al mese di aprile 2003 il numero di internauti europei che utilizza connessioni rapide (DSL, LAN e modem via cavo) è aumentato del 136%. Taluni paesi hanno registrato un tasso di crescita ancora maggiore, in particolare il Regno Unito (incremento del 235%).

Gli utenti collegati in banda larga trascorrono molto più tempo sulla rete, la utilizzano più spesso e visitano un numero maggiore di siti rispetto agli utenti con connessione telefonica ordinaria, più lenta. In Germania, ad esempio, gli utenti della banda stretta trascorrono in media sette ore e mezzo al mese su Internet mentre gli utenti della banda larga vi trascorrono 21 ore, vale a dire quasi un giorno al mese.

Una recente indagine condotta nell'ambito dei progetti di sensibilizzazione finanziati dall'attuale piano d'azione rivela che in Danimarca, Irlanda, Islanda, Norvegia e Svezia il 97% dei giovani di età compresa tra 9 e 16 anni ha già usato il computer.

Ben quattro bambini su dieci che hanno "chattato" su Internet affermano che le persone così conosciute hanno chiesto di incontrarli di persona. Il 14% dei bambini ha incontrato una persona conosciuta su Internet mentre solo il 4% dei genitori pensa che ciò sia accaduto. Il 44% dei bambini che usano Internet ha visitato un sito pornografico, per caso o volontariamente. Un quarto ha ricevuto materiale pornografico tramite Internet. Il 30% ha consultato siti web contenenti materiale violento mentre solo il 15% dei genitori ritiene che lo abbiano fatto.

Questo aumento della connettività da parte dei bambini avrà su di loro effetti benefici ma comporta anche rischi di "danni collaterali".

La proliferazione di e-mail non richieste, il cosiddetto spam, ha raggiunto un livello tale da rappresentare un grave ostacolo allo sviluppo del commercio elettronico e della società dell'informazione. Gran parte dello spam è costituito di messaggi pubblicitari per siti pornografici, alcuni dei quali chiaramente illegali per ogni tipo di utente. Si ritiene che entro breve oltre il 50% del traffico mondiale di posta elettronica sarà costituito da spam.

2. PROMUOVERE UN USO PIÙ SICURO DI INTERNET E DELLE NUOVE TECNOLOGIE ONLINE

2.1. Il contesto legislativo

I contenuti illegali e i contenuti indesiderati o nocivi richiedono strategie di intervento diverse, anche se, come di frequente nel caso dello spam, i contenuti indesiderati o nocivi possono essere anche illegali.

Queste due categorie di contenuti vanno affrontate in modo diverso.

La definizione di contenuto e comportamento illegale è data dal diritto nazionale e sebbene le caratteristiche comuni siano numerose, vi sono anche significative differenze specifiche tra le leggi dei vari Stati membri (e dei paesi terzi in cui i contenuti possono essere prodotti o ospitati).

Il metodo principale per contrastare i contenuti e i comportamenti illegali consiste nell'intervento delle autorità di polizia per arrestare gli autori del reato e condurli innanzi l'autorità giudiziaria che li processa e li condanna se ritenuti colpevoli. Possono inoltre esistere organismi di regolamentazione incaricati di applicare alcune norme (in materia di protezione dei consumatori, ad esempio) oppure essere applicate soluzioni di tipo civilistico (come nel caso di violazione del diritto d'autore).

Nei nuovi media come Internet questo processo è reso complesso dal fatto che gli elementi costitutivi del reato possono essere distribuiti in paesi diversi e che potrebbe essere difficile esercitare il potere giurisdizionale nei confronti degli imputati principali. È pertanto necessaria una cooperazione internazionale.

Per contenuti indesiderati si intendono quei contenuti che l'utente non chiede di ricevere. I contenuti nocivi sono invece quei contenuti che gli adulti (genitori o insegnanti) ritengono possano nuocere ai minori di cui hanno la responsabilità. Possono vigere disposizioni giuridiche che limitano la distribuzione di contenuti nocivi ai soli adulti (come nel caso della pornografia legale, ad esempio).

Per contrastare i contenuti indesiderati e nocivi si hanno a disposizione diversi strumenti da utilizzare congiuntamente in modo da accrescerne l'efficacia: applicazione delle disposizioni di legge, autoregolamentazione, mezzi tecnici come il filtraggio e azioni di sensibilizzazione.

Per quanto riguarda i contenuti illegali e la regolamentazione della distribuzione dei contenuti nocivi, la responsabilità primaria dei fornitori di contenuti continua ad essere una materia disciplinata principalmente dal diritto nazionale. Inoltre, gli Stati membri hanno sensibilità diverse in materia di esibizione pubblica di nudità e attività sessuali e di esposizione dei minori alla nudità e alla violenza.

Esistono tuttavia strumenti legislativi da cui discendono norme che gli Stati membri sono tenuti a mettere in applicazione.

La direttiva sul commercio elettronico[4] disciplina gli aspetti principali legati alla responsabilità dei prestatori intermediari in caso di semplice trasporto (*mere conduit*), memorizzazione temporanea (*caching*) e accoglienza (*hosting*) dei contenuti.

L'Unione europea è stata la prima ad agire sul fronte giuridico contro le comunicazioni commerciali indesiderate - o spam - adottando la direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche[5], che condurrà, in tutta Europa, ad un divieto dello spam diretto ai privati. La Commissione ha pubblicato una comunicazione[6] al riguardo nella quale individua le azioni da avviare ad integrazione della normative UE per garantire la massima efficacia possibile del divieto di spam.

---

4 Cfr. nota 20.
5 Cfr. nota 19.
6 COM(2004) 28.

La raccomandazione sulla tutela dei minori e della dignità umana[7] contiene raccomandazioni destinate agli Stati membri, all'industria, alle parti interessate e alla Commissione e presenta una serie di indicazioni orientative sulla tutela dei minori. L'applicazione delle disposizioni della raccomandazione è stata oggetto di una prima valutazione nel 2000-2001. La relazione, pubblicata nel 2001[8], indica che, già in quel momento, l'applicazione della raccomandazione era tutto sommato soddisfacente. La Commissione ha adottato una seconda relazione[9] sull'applicazione della raccomandazione basata su un questionario trasmesso agli Stati membri e ai paesi in via di adesione.

La decisione quadro sulla pornografia infantile[10] fissa un insieme di requisiti minimi di cui gli Stati membri devono tener conto nel definire e sanzionare i reati in questo campo.

2.2. Sviluppi futuri

Affidandosi alle tendenze attuali è possibile prevedere il panorama dei nuovi media e i problemi che potrebbero derivarne all'orizzonte 2005 e oltre:

- le nuove tecnologie e le nuove modalità di utilizzo delle tecnologie esistenti evolveranno e forniranno nuove opportunità alla stragrande maggioranza delle imprese e dei cittadini rispettosi della legge;
- i nuovi media assumeranno un ruolo importante nella vita dei minori;
- la criminalità utilizzerà tuttavia i nuovi media per le proprie attività e immaginerà nuove forme di frode nei confronti delle imprese e dei consumatori;
- pur continuando a possedere strutture di produzione e di distribuzione professionali organizzate simili a quelle dei media tradizionali, Internet continuerà a essere caratterizzato da forme di produzione disaggregate che potranno avvalersi delle tecniche di riservatezza e di produzione di *video-on-demand*;
- nel contempo, l'evoluzione tecnologica consentirà di elaborare nuovi strumenti di individuazione e di prevenzione delle azioni criminose e di identificarne gli autori;
- lo sfruttamento sessuale dei minori continuerà sotto forma di pornografia infantile e ricorrendo alle nuove tecnologie per entrare in contatto con vittime potenziali di abusi sessuali.

2.3. Consultazione pubblica

Diverse consultazioni pubbliche tenutesi tra novembre 2002 e settembre 2003 hanno permesso di definire l'entità del problema e di stabilire la necessità di istituire un nuovo programma[11].

---

7 Cfr. nota 21.

8 COM(2001) 106 def.

9 COM(2003) 776.

10 Decisione quadro 2004/68/GAI del Consiglio, del 22 dicembre 2003, relativa alla lotta contro lo sfruttamento sessuale dei bambini e la pornografia infantile (GU L 13 del 20.1.2004, pag. 44).

Tali consultazioni hanno confermato l'importanza dell'iniziativa e la necessità di continuare a garantirne il sostegno a livello comunitario. Si è osservato un consenso in merito al fatto che l'uso sicuro di Internet continua ad destare preoccupazioni e che il problema è reso ancor più acuto dall'emergere di nuove tecnologie e di nuove applicazioni di tali tecnologie. Sono necessarie azioni di diverso tipo a livello locale, regionale, europeo ed internazionale. Le azioni di sensibilizzazione devono in particolare essere dirette agli utenti finali - genitori e minori - e comportare effetti moltiplicatori. L'azione condotta a livello di Unione europea può garantire sempre un valore aggiunto europeo. Le parti interessate hanno sottolineato la necessità di una cooperazione internazionale in questo campo. Tutti hanno concordato sulla necessità di ampliare il campo di applicazione delle azioni del programma, in particolare per affrontare il problema dello spam.

La proposta della Commissione tiene pienamente conto delle opinioni espresse nel quadro delle consultazioni pubbliche. Alcune idee di ampliamento del campo di applicazione del programma, in particolare lo sfruttamento dei minori per fini commerciali, la sicurezza delle reti e dell'informazione e la protezione dei dati, vengono già trattate in alter politiche e in altre iniziative di finanziamento dell'UE. Esse figurano nel messaggio di sensibilizzazione e sono oggetto di adeguati riferimenti.

2.4. Conclusioni

Occorre portare avanti le azioni sia nel campo dei contenuti indesiderati dall'utente finale o potenzialmente nocivi per i minori che nel campo dei contenuti illegali, in particolare la pornografia infantile.

Convenire norme giuridiche vincolanti a livello internazionale è senza dubbio auspicabile ma sarà difficile e richiederà in ogni caso molto tempo. Un eventuale accordo in questo campo non basterebbe del resto a garantire l'applicazione delle norme o la tutela delle persone a rischio.

Sono necessarie misure pratiche per incoraggiare la segnalazione di contenuti illegali agli organismi competenti ad intervenire, per promuovere le migliori pratiche in materia di codici di condotta che corrispondano a canoni di comportamento universalmente riconosciuti e per informare ed educare genitori e minori su come beneficiare dei nuovi media nel modo più sicuro possibile.

Sono indispensabili azioni a livello degli Stati membri che coinvolgano una folta schiera di soggetti: autorità nazionali, regionali e locali; operatori di rete; genitori, insegnanti e amministratori delle scuole ecc. L'UE può favorire l'uso delle migliori pratiche negli Stati membri svolgendo un ruolo orientativo sia all'interno dell'Unione che sul piano internazionale e sostenendo azioni di analisi comparativa (*benchmarking*), di messa in rete e di ricerca applicata a livello europeo.

La cooperazione internazionale è un elemento essenziale di questo approccio e può essere favorita, coordinata, diffusa e applicata mediante le strutture di messa in rete dell'UE.

---

[11] Per ulteriori informazioni al riguardo, si consulti il documento di lavoro dei servizi della Commissione sulla valutazione *ex ante* SEC(...).

3. UN NUOVO PROGRAMMA

3.1. Principi, obiettivi e orientamento

Il nuovo programma sarà improntato ai principi di *continuità* e di *perfezionamento*.

- Continuità: continuare a fare quello che l'Europa sa fare meglio, traendo insegnamento dall'esperienza e basandosi sui risultati delle iniziative già finanziate in modo da garantire la continuità dei loro effetti.

- Perfezionamento: far fronte alle nuove minacce, garantire un valore aggiunto europeo, favorire l'effetto moltiplicatore delle iniziative e ampliarne il raggio d'azione internazionale.

Il nuovo programma dovrebbe conservare lo stesso obiettivo generale, ossia promuovere un uso più sicuro di Internet e delle nuove tecnologie online, in particolare per i minori, e lottare contro i contenuti illegali e i contenuti indesiderati dall'utente finale. Il programma dovrebbe pertanto concentrarsi sugli utenti finali, in particolare genitori, educatori e minori.

Il programma punterà a coinvolgere e riunire i vari soggetti interessati la cui collaborazione è necessaria ma che non sempre possono accomunare i loro sforzi a meno che non vengano istituite le apposite strutture.

Per parti interessate si intendono i fornitori di contenuti, i fornitori di servizi Internet e gli operatori di reti mobili; le autorità di regolamentazione; gli organismi di normalizzazione; gli organi di autoregolamentazione dell'industria; le autorità nazionali, regionali e locali competenti per l'industria, l'istruzione, la tutela dei consumatori, le famiglie, i diritti e il benessere dell'infanzia; e infine le organizzazioni non governative attive nei settori della tutela dei consumatori, della famiglia, dei diritti e del benessere dell'infanzia.

3.2. Azioni

Il programma è articolato in quattro azioni: lotta ai contenuti illegali, contrasto ai contenuti indesiderati e nocivi, promozione di un ambiente più sicuro e sensibilizzazione. Nei quattro casi la cooperazione internazionale è parte integrante dell'azione.

3.2.1. Lotta ai contenuti illegali

Come indicato in precedenza, le pubbliche autorità (polizia, pubblici ministeri e tribunali) sono in prima linea nella lotta ai contenuti illegali. Solo esse possono garantire che gli autori di un reato in questo campo siano perseguiti in giudizio. Le *hotline* sono centri ai quali il pubblico può segnalare contenuti illegali e che successivamente trasmettono tali informazioni all'organo competente (fornitore di servizi Internet, polizia o *hotline* corrispondente) per prenda le misure del caso. Le *hotline* rappresentano il contributo dell'industria e delle organizzazioni non governative a questo processo e permettono di limitare la circolazione dei contenuti illegali. Molte persone, restie a rivolgersi direttamente alla polizia, possono così informare una *hotline* che non riveste carattere ufficiale.

La rete di *hotline* esistente è una struttura unica nel suo genere che non avrebbe potuto essere istituita senza il finanziamento dell'UE. La rete ha notevolmente ampliato il novero dei propri membri ed ha oggi una copertura internazionale.

Le singole *hotline* contribuiscono al funzionamento della rete ma ne traggono anche beneficio. La maggior parte delle segnalazioni che pervengono ad una *hotline* riguarda situazioni in cui il sito *host* o il fornitore di contenuti hanno sede in un paese diverso da quello della *hotline* e al di fuori quindi della giurisdizione dei tribunali del suo paese. Grazie al finanziamento dell'UE la Commissione può garantire che la selezione delle *hotline* si basi su standard europei e che queste contribuiscano efficacemente al funzionamento della rete.

Si propone pertanto di finanziare le attività di coordinamento della rete e le singole *hotline* che la compongono. Occorre al riguardo definire in che modo la perizia tecnica dell'industria possa essere messa al servizio della lotta ai contenuti illegali. La rete andrà estesa affinché copra i nuovi Stati membri e i paesi candidati nonché altri paesi europei in cui vengono prodotti e ospitati contenuti illegali.

Le *hotline* devono agire in stretto coordinamento con le altre azioni, ad esempio quelle in materia di autoregolamentazione e di sensibilizzazione, e potrebbero essere gestite da organismi attivi in tali settori.

La rete di *hotline* deve trattare e trasmettere segnalazioni relative alle principali forme di contenuti illegali che suscitano preoccupazione e non limitarsi alla pornografia infantile. Per far fronte ad altre forme di contenuti illegali quali i contenuti razzisti potrebbero essere necessari meccanismi e competenze diversi.

3.2.2. Contrasto ai contenuti indesiderati e nocivi

Il programma consentirà di finanziare azioni di tipo tecnologico che permetteranno agli utenti di limitare la quantità di contenuti indesiderati e nocivi e – quando li ricevono – di gestirli in modo adeguato, in particolare azioni di valutazione dell'efficacia delle attuali tecnologie di filtraggio, azioni di sostegno allo sviluppo di nuove tecnologie di filtraggio efficaci e finanziamento di misure destinate a facilitare e coordinare lo scambio di informazioni e di buone pratiche in materia di applicazione delle misure anti-spam.

Nel quadro delle altre iniziative per far fronte ai contenuti indesiderati e nocivi saranno approfonditi i lavori di classificazione dei contenuti per tener conto della possibilità di ottenere gli stessi contenuti attraverso meccanismi di fornitura diversi (convergenza) e sarà portata avanti la collaborazione tra specialisti del benessere dell'infanzia ed esperti tecnici in modo da perfezionare gli strumenti di protezione di queste categorie di utenti.

L'attuazione di questa azione avverrà in stretto coordinamento con le azioni di promozione di un ambiente più sicuro (azione di autoregolamentazione) e di sensibilizzazione (informazione del pubblico in merito ai mezzi disponibili per far fronte ai contenuti indesiderati e nocivi).

3.2.3. *Promozione di un ambiente più sicuro*

Opporsi ai contenuti illegali, indesiderati o nocivi è un compito complesso ed esistono sensibili divergenze in merito all'opportunità di tentare di armonizzare le norme nazionali, al contenuto delle norme sostanziali e al modo di affrontare le differenze tra le norme nazionali che probabilmente sussisteranno. Le problematiche in oggetto toccano in particolare la libertà di espressione, la proporzionalità delle misure e la loro fattibilità tecnica.

L'Unione europea ha ribadito il proprio sostegno ad un approccio di autoregolamentazione che garantisca flessibilità e sia in grado di comprendere le esigenze del mezzo di comunicazione in un contesto in cui convergono alta tecnologia, rapidità del cambiamento e dimensione transfrontaliera. Sono ipotizzabili diversi modelli di codici di condotta, ma tutti devono essere improntati alle caratteristiche essenziali di efficacia, equità e trasparenza.

Diverse iniziative sono già state poste in essere, alcune delle quali dotate di caratteristiche innovative che potrebbero servire da esempi di migliori pratiche. Il percorso è tuttavia ancora lungo, sia dal punto di vista dello sviluppo di efficaci approcci di autoregolamentazione nazionali che della costituzione di una piattaforma europea destinata agli operatori del settore.

L'autoregolamentazione non è un processo spontaneo né esclude la necessità di un fondamento giuridico; potrebbe essere necessario un approccio più proattivo al fine di favorire un accordo in merito ad un insieme adeguato di norme comuni e alla loro applicazione.

Il forum per l'uso sicuro di Internet (forum *Safer Internet*), istituito nella seconda fase dell'attuale piano d'azione (2003-2004) come tribuna di discussione tra i rappresentanti dell'industria, le organizzazioni per il benessere dei minori e i responsabili politici, fungerà da piattaforma di scambio di esperienze tra gli organismi nazionali di coregolamentazione e di autoregolamentazione. Servirà inoltre da sede di riflessione sul possibile contributo dell'industria alla lotta contro i contenuti illegali.

3.2.4. *Sensibilizzazione*

Si osserva una forte convergenza di vedute tra responsabili politici e specialisti del settore in merito alla necessità di un'informazione sistematica sull'uso sicuro di Internet – in particolare per quanto riguarda le applicazioni personalizzate, interattive e mobili – che sia collegata con le altre azioni dell'UE dedicate alla formazione sui mezzi di comunicazione e su Internet.

Per ottimizzare l'uso dei fondi disponibili la Commissione dovrebbe concentrarsi su azioni di stimolo che favoriscano l'effetto moltiplicatore e lo scambio in rete delle migliori pratiche.

3.2.5. *Collegamenti con altre iniziative*

Il programma sarà ideato e messo in atto in stretto coordinamento le con altre iniziative in questo campo, in particolare con le azioni derivanti dalla

raccomandazione del Consiglio sulla tutela dei minori e della dignità umana e con il piano d'azione del vertice mondiale della società dell'informazione.

4. BASE GIURIDICA

La base giuridica dell'iniziativa è l'articolo 153, paragrafo 2 del trattato, relativo alla protezione dei consumatori. Si tratta della stessa base giuridica già individuata dal Parlamento europeo e dal Consiglio per il primo piano d'azione per l'uso sicuro di Internet nel 1999[12] e per i due anni di estensione del piano d'azione nel 2003[13]. Tale base giuridica continua ad essere adeguata in quanto, come indicato al punto 3.1, il programma si incentra sugli utenti finali – in particolare genitori, educatori e minori – e promuove l'uso sicuro, da parte loro, di Internet e delle nuove tecnologie online.

---

12 Cfr. nota 22.

13 Decisione n. 1151/2003/CE del Parlamento europeo e del Consiglio del 16 giugno 2003, GU L 162 del 1.7.2003, pag. 1.

(10) Le misure necessarie per l'attuazione della presente decisione devono essere adottate conformemente alla decisione 1999/468, del Consiglio del 28 giugno 1999, recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione23.

(11) È opportuno che la Commissione provveda alla complementarità e alla sinergia tra il programma e le iniziative e i programmi della Comunità ad esso collegati.

(12) La presente decisione istituisce un quadro finanziario per l'intera durata del programma che costituirà il principale riferimento per l'autorità di bilancio, ai sensi del punto 33 dell'accordo interistituzionale del 6 maggio 1999 tra il Parlamento europeo, il Consiglio e la Commissione sulla disciplina di bilancio e sul miglioramento della procedura di bilancio.

(13) Poiché gli scopi dell'intervento prospettato non possono essere realizzati in misura sufficiente dagli Stati membri, a causa del carattere transnazionale delle problematiche in oggetto, e possono dunque, a causa della portata e gli effetti delle azioni previste, essere realizzati meglio a livello comunitario, la Comunità può intervenire, in base al principio di sussidiarietà sancito dall'articolo 5 del trattato. La presente decisione si limita a quanto è necessario per conseguire tali scopi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo,

HANNO ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

[Obiettivo del programma]

1. La presente decisione istituisce un programma comunitario destinato a promuovere un uso più sicuro di Internet e delle nuove tecnologie online, in particolare per i minori, e a lottare contro i contenuti illegali e i contenuti indesiderati dall'utente finale.

   Il programma è denominato *Safer Internet Plus* (di seguito "il programma").

2. Per realizzare l'obiettivo generale enunciato al paragrafo 1, il programma è articolato attorno alle seguenti linee di azione:

   a) lotta ai contenuti illegali;

   b) contrasto ai contenuti indesiderati e nocivi;

   c) promozione di un ambiente più sicuro;

   d) sensibilizzazione.

   Le attività da condurre nell'ambito di tali linee di azione sono descritte nell'allegato I.

   Il programma è attuato secondo le modalità stabilite nell'allegato III.

---

23 GU L 184 del 17.7.1999, pag. 23.

Articolo 2

[Partecipazione]

1. La partecipazione al programma è aperta alle persone giuridiche stabilite negli Stati membri.

   La partecipazione al programma è altresì aperta ai paesi candidati all'adesione conformemente alle disposizioni degli accordi bilaterali da concludere in materia.

2. Possono partecipare al programma, nel rispetto delle disposizioni previste nell'accordo sullo Spazio economico europeo (SEE), le persone giuridiche stabilite negli Stati dell'EFTA membri del SEE.

3. Possono essere ammessi a partecipare al programma, senza sostegno finanziario della Comunità da parte del programma stesso, soggetti giuridici con sede in paesi terzi e organizzazioni internazionali, qualora la loro partecipazione contribuisca concretamente all'attuazione del programma. La decisione di autorizzare tale partecipazione è adottata a norma della procedura di cui all'articolo 4, paragrafo 2.

Articolo 3

[Competenze della Commissione]

1. La Commissione è responsabile dell'attuazione del programma.

2. La Commissione elabora un piano di lavoro sulla base della presente decisione.

3. La Commissione agisce in conformità della procedura di cui all'articolo 4, paragrafo 2 per quanto riguarda:

   a) l'adozione del piano di lavoro e delle sue modifiche;

   b) la determinazione dei criteri e del contenuto degli inviti a presentare proposte, conformemente agli obiettivi enunciati nell'articolo 1;

   c) ogni deroga alle norme stabilite nell'allegato III;

4. La Commissione informa il comitato dei progressi realizzati nell'attuazione del programma.

Articolo 4

[Comitato]

1. La Commissione è assistita da un comitato.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applicano gli articoli 3 e 7 della decisione 1999/468/CE, tenendo conto dell'articolo 8 della stessa.

   Il periodo di cui all'articolo 4, paragrafo 3 della decisione 1999/468/CE è fissato a tre mesi.

3. Il comitato stabilisce il proprio regolamento interno.

Articolo 5

[Sorveglianza e valutazione]

1. Per garantire che il contributo comunitario sia utilizzato in modo efficace, la Commissione si assicura che le azioni intraprese nell'ambito della presente decisione siano oggetto di una valutazione preliminare, di un controllo e di una valutazione conclusiva.

2. La Commissione sorveglia l'esecuzione dei progetti avviati nell'ambito del programma. Al termine di ogni progetto la Commissione ne valuta le modalità di esecuzione e l'impatto per accertare se gli obiettivi prefissati sono stati raggiunti.

3. Entro [due anni dalla data di pubblicazione] della presente decisione la Commissione presenta al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni una relazione di valutazione sull'attuazione delle linee di azione di cui all'articolo 1, paragrafo 2.

   Al termine del periodo di esecuzione del programma la Commissione presenta una relazione finale.

Articolo 6

[Disposizioni finanziarie]

1. Il programma copre un periodo di quattro anni a decorrere dal 1° gennaio 2005.

2. La dotazione finanziaria indicativa per l'esecuzione del programma nel periodo stabilito al paragrafo 1 è di 50 milioni di euro.

   La dotazione relativa al periodo 2005-2006 ammonta a 20,050 milioni di euro mentre quella relativa al periodo 2007-2008 ammonta a 29,950 milioni di euro.

   Gli stanziamenti annuali sono autorizzati dall'autorità di bilancio entro i limiti delle prospettive finanziarie.

3. La ripartizione indicativa delle spese figura nell'allegato II.

Articolo 7

La presente decisione entra in vigore alla data della sua pubblicazione nella *Gazzetta ufficiale dell'Unione europea.*

Fatto a Bruxelles, il [...]

Per il Parlamento europeo
Il Presidente
[...]

Per il Consiglio
Il Presidente
[...]

ALLEGATO I

AZIONI

1. AZIONE 1: LOTTA AI CONTENUTI ILLEGALI

Le *hotline* consentono al pubblico di segnalare contenuti illegali. Queste trasmettono in seguito le informazioni agli organi competenti (fornitore di servizi Internet - ISP, polizia o *hotline* corrispondente) perché prendano le misure del caso. Le *hotline* di diritto civile fungono da complemento a quelle della polizia (quando queste esistono). Il loro ruolo è diverso in quanto non hanno poteri investigativi, né arrestano o perseguono gli autori dei reati. Fungono da centri di competenza che assistono gli ISP per individuare i contenuti che potrebbero risultare illegali.

L'attuale rete di *hotline* è un'organizzazione unica nel suo genere che non avrebbe potuto essere costituita senza un finanziamento UE. Come indicato nella valutazione del programma del 2002, la rete è riuscita ad ampliare il novero dei propri aderenti ed ha raggiunto una dimensione internazionale. Perché le *hotline* possano funzionare al meglio occorre garantire una copertura e una cooperazione su scala europea e ottimizzarne l'efficacia mediante lo scambio di informazioni, migliori pratiche ed esperienze.

Beneficeranno di un finanziamento le *hotline* scelte a seguito di un invito a presentare proposte per fungere da nodi della rete e le attività di coordinamento necessarie per la gestione delle attività della rete europea di *hotline*.

Gli Stati membri e i paesi candidati in cui non operano ancora *hotline* sono tenuti ad istituirne. Queste devono essere integrate in modo rapido ed efficace nella rete europea di *hotline* esistente. Vanno inoltre incoraggiati i collegamenti tra la rete europea e le *hotline* dei paesi terzi, in particolare i paesi europei in cui i contenuti illegali vengono prodotti e ospitati, in modo da definire approcci comuni e garantire il trasferimento del know-how e delle migliori pratiche. Gli strumenti di cooperazione esistenti tra le *hotline* nazionali e le autorità di polizia devono essere perfezionati. Occorre impartire una formazione giuridica e tecnica al personale delle *hotline*. Sarà obbligatoria la partecipazione attiva delle *hotline* alle attività di messa in rete e alle azioni transfrontaliere.

Le *hotline* devono integrarsi nelle iniziative nazionali, essere finanziate dagli Stati membri ed essere finanziariamente sostenibili in modo da poter continuare a funzionare anche oltre la durata del presente programma. Il cofinanziamento è destinato alle *hotline* di diritto civile che integrano le attività delle autorità di polizia senza farne parte e **non** ne beneficeranno pertanto le *hotline* gestite dalla polizia. Le *hotline* devono chiaramente indicare agli utenti le differenze tra le loro attività e quelle della polizia ed informarli del fatto che i contenuti illegali possono essere notificati anche direttamente alla polizia.

Per ottimizzare l'impatto e l'efficacia dei finanziamenti disponibili, la rete di *hotline* deve funzionare nel modo più efficiente possibile. Occorre a tal fine designare un nodo di coordinamento della rete incaricato di facilitare il consenso tra le *hotline* in modo da elaborare orientamenti, metodi di lavoro e pratiche su scala europea compatibili con le disposizioni delle leggi nazionali applicabili alle singole *hotline*.

Il nodo di coordinamento:

- costituirà un'identità e un punto di ingresso unici che forniranno un accesso semplice al competente punto di contatto nazionale;
- promuoverà le attività dell'insieme della rete favorendone la visibilità a livello europeo;
- avrà contatti con gli organismi competenti in modo da completare la copertura della rete negli Stati membri e nei paesi candidati;
- potenzierà l'efficacia operativa della rete;
- elaborerà orientamenti per le migliori pratiche e li adeguerà alle nuove tecnologie;
- organizzerà regolari scambi di informazioni e di esperienze tra le *hotline*;
- fungerà da centro di competenza, di consulenza e di assistenza per le *hotline* che iniziano le loro attività, in particolare nei paesi candidati;
- garantirà i collegamenti con le *hotline* dei paesi terzi;
- manterrà stretti contatti col nodo di coordinamento delle attività di sensibilizzazione (cfr. punto 4) in modo da garantire la coesione e l'efficacia delle attività del programma e sensibilizzare maggiormente il pubblico in merito all'esistenza delle *hotline*;
- parteciperà al forum *Safer Internet* e ad altre manifestazioni pertinenti coordinando gli input/feedback provenienti dalle *hotline*.

Il nodo di coordinamento sorveglierà l'efficacia delle *hotline* e raccoglierà statistiche affidabili e significative sul loro funzionamento (numero e tipo di segnalazioni ricevute, interventi e risultati ecc.).

La rete di *hotline* deve garantire la copertura e lo scambio di segnalazioni in merito alle principali tipologie di contenuti illegali che suscitano preoccupazione e non limitarsi alla sola pornografia infantile. Per affrontare altri contenuti illegali, come quelli di tipo razzista, potrebbero essere necessari meccanismi e competenze diversi che potrebbero rendere necessario il coinvolgimento di altri nodi nazionali competenti in queste problematiche. Considerate le limitate risorse finanziarie e amministrative del programma non tutti questi nodi beneficeranno necessariamente di finanziamenti; questi potrebbero dover essere concentrati per rafforzare il nodo di coordinamento in questi settori.

Possono beneficiare di un finanziamento UE anche le attività di sviluppo di software destinati ad assistere le *hotline* a gestire in modo più efficace il carico di lavoro e le segnalazioni.

2. AZIONE 2: CONTRASTO AI CONTENUTI INDESIDERATI E NOCIVI

Oltre a combattere i contenuti illegali alla fonte, occorre sviluppare strumenti adeguati che consentano agli utenti – adulti responsabili, nel caso dei minori – di

decidere come trattare i contenuti indesiderati e nocivi (responsabilizzazione dell'utente).

Saranno erogati finanziamenti per le azioni destinate ad intensificare l'informazione in merito alle prestazioni e all'efficacia dei software e dei servizi di filtraggio dei contenuti in modo che gli utenti possano avvalersi di questa facoltà.

Parallelamente alla ricerca sulle nuove tecnologie, finanziata dai programmi di ricerca, sarebbe opportuno finanziare progetti incentrati sull'applicazione innovativa delle tecnologie esistenti al fine di ampliare il campo di applicazione dei software e dei servizi di filtraggio ai contenuti veicolati dalle nuove tecnologie o di adattare tali software e servizi di filtraggio alle esigenze specifiche degli utenti europei (ad esempio, aumentando il numero delle lingue riconosciute).

I sistemi di classificazione dei contenuti e i marchi di qualità, unitamente alle tecnologie di filtraggio, autorizzano gli utenti di scegliere i contenuti che desiderano ricevere e forniscono ai genitori e agli educatori europei le informazioni necessarie per decidere secondo i loro valori linguistici e culturali. Possono beneficiare di un finanziamento i progetti intesi ad adattare i sistemi di classificazione e i marchi di qualità in modo che tengano conto della convergenza tra i settori delle telecomunicazioni, dell'audiovisivo e delle tecnologie dell'informazione nonché le iniziative di autoregolamentazione intese ad accrescere l'affidabilità dell'autocertificazione e ad accertare l'accuratezza dei metodi di autovalutazione. Potrebbero essere necessarie nuove attività a sostegno dell'adozione dei sistemi di classificazione e dei marchi di qualità da parte dei fornitori di servizi.

È auspicabile tener conto della sicurezza d'uso delle nuove tecnologie da parte dei minori sin dal momento della loro elaborazione piuttosto che tentare di arginarne le conseguenze una volta ideate. La sicurezza dell'utente finale è un criterio da prendere in considerazione alla stregua delle considerazioni tecniche e commerciali. A tal fine potrebbe essere favorito uno scambio di vedute tra professionisti del benessere dell'infanzia ed esperti tecnici.

Il programma finanzierà pertanto misure di tipo tecnologico che permettano agli utenti di limitare la quantità di contenuti indesiderati e nocivi e di gestire i messaggi spam ricevuti, in particolare:

- valutazione dell'efficacia delle tecnologie di filtraggio disponibili e informazione del pubblico;

- promozione e coordinamento degli scambi di informazioni e di buone pratiche sui mezzi efficaci di applicazione delle misure anti-spam (cfr. comunicazione della Commissione sulle comunicazioni commerciali indesiderate o spam);

- sviluppo di nuove tecnologie di filtraggio efficaci, soprattutto nella seconda fase del programma;

- misure di stimolo all'adozione dei sistemi di classificazione dei contenuti e dei marchi di qualità dei siti web da parte dei fornitori di servizi e misure di adeguamento dei sistemi di classificazione e dei marchi di qualità affinché tengano conto della possibilità di ottenere gli stessi contenuti attraverso sistemi di fornitura diversi (convergenza);

Sarà incoraggiato l'uso di tecnologie che migliorano il livello di riservatezza. Le attività in questo campo si svolgeranno tenendo pienamente conto delle disposizioni della futura decisione quadro del Consiglio sugli attacchi ai sistemi informatici.

Lo sviluppo di nuove tecnologie di filtraggio avverrà tenendo conto dell'evoluzione tecnologica e della necessità, per la Commissione, di adottare un approccio "tecnologicamente neutrale".

L'attuazione di questa azione avverrà in stretto coordinamento con le azioni di promozione di un ambiente più sicuro (autoregolamentazione) e di sensibilizzazione (informazione del pubblico in merito ai mezzi per far fronte ai contenuti indesiderati e nocivi).

3. AZIONE 3: PROMOZIONE DI UN AMBIENTE PIÙ SICURO

La piena operatività di un sistema di autoregolamentazione è un elemento essenziale per limitare il flusso di contenuti nocivi e illegali. L'autoregolamentazione comporta vari elementi: la consultazione e la rappresentatività delle parti interessate; uno o più codici di condotta; organismi nazionali che favoriscano la cooperazione a livello comunitario; valutazione a livello nazionale dei quadri di autoregolamentazione[24]. Nella Comunità sono necessarie ulteriori azioni a sostegno dell'introduzione in Europa di codici di condotta da parte dei siti Internet e delle imprese europee attive nel settore delle nuove tecnologie online.

Il forum *Safer Internet* che sarà istituito nel 2004 nel quadro dell'attuale piano d'azione per l'uso sicuro di Internet diventerà una piattaforma di discussione importante che riunirà rappresentanti dell'industria, autorità di polizia, organizzazioni per la tutela e il benessere dell'infanzia e responsabili politici e consentirà lo scambio di esperienze tra organismi nazionali di coregolamentazione e autoregolamentazione. Fornirà inoltre la possibilità di discutere in che modo l'industria può contribuire a contrastare i contenuti illegali.

Il forum *Safer Internet* rappresenterà sia il punto d'incontro e di discussione per gli esperti del settore che una piattaforma di formazione del consenso e formulazione di conclusioni, raccomandazioni, orientamenti ecc. destinati ai competenti canali nazionali ed europei.

Il forum abbraccerà tutte le linee di azione, faciliterà le discussioni e stimolerà le azioni in materia di contenuti illegali, indesiderati e nocivi. Opererà in sessioni plenarie e in gruppi di lavoro ristretti e costituirà il punto di incontro per i professionisti di diversa provenienza quali enti pubblici, programmi governativi, enti di normalizzazione, industria, altri servizi della Commissione europea, organizzazioni di utenti (ad es. associazioni di genitori e di insegnanti, gruppi di tutela dell'infanzia, organismi di tutela dei consumatori). Il forum permetterà agli

---

[24] Cfr. al riguardo gli orientamenti per l'attuazione, a livello nazionale, di un quadro di autoregolamentazione per la tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione online. Raccomandazione 98/560/CE del Consiglio, del 24 settembre 1998, concernente lo sviluppo della competitività dell'industria dei servizi audiovisivi e d'informazione europei attraverso la promozione di strutture nazionali volte a raggiungere un livello comparabile e efficace di tutela dei minori e della dignità umana GU L 270 del 7.10.1998, pag. 48.

operatori nazionali, in particolare quelli coinvolti nei programmi e nelle iniziative degli Stati membri, di scambiare vedute, informazioni ed esperienze. Esso fungerà da organo di collegamento con altre iniziative della Comunità quale, ad esempio, l'agenzia europea per la sicurezza delle reti e dell'informazione.

Il forum *Safer Internet* avrà i seguenti obiettivi specifici:

1. Stimolare la messa in rete delle competenti strutture degli Stati membri e allacciare contatti con gli organismi di autoregolamentazione non europei.

2. Favorire la formazione del consenso e l'autoregolamentazione in merito a problematiche quali la certificazione di qualità dei siti web, i codici di condotta dei fornitori di servizi, la classificazione dei contenuti intermediali e l'estensione dei sistemi di classificazione e di filtraggio utilizzati per Internet ad altri supporti quali la telefonia mobile e i giochi online.

La Commissione istituirà appositi gruppi di lavoro per trattare problematiche specifiche, con obiettivi chiari e scadenze precise. I risultati dei progetti in corso e dei progetti ultimati cofinanziati dal programma serviranno da input per questo processo. Fungendo da piattaforma di riflessione aperta, il forum contribuirà ad accrescere la sensibilizzazione e la partecipazione dei paesi candidati e dei paesi terzi e servirà da tribuna internazionale in cui trattare un problema d'interesse mondiale. Il forum garantirà pertanto che le principali associazioni attive nel settore, l'industria e i competenti organismi pubblici siano informati e consultati in merito alle iniziative europee ed internazionali per un uso più sicuro di Internet e possano attivamente contribuirvi.

La partecipazione al forum *Safer Internet* sarà aperta alle parti interessate aventi sede in paesi terzi e nei paesi candidati. La cooperazione internazionale sarà rafforzata grazie ad una tavola rotonda collegata al forum che ospiterà un dialogo regolare sulle migliori pratiche, i codici di condotta, l'autoregolamentazione e i marchi di qualità. La Commissione provvederà a trarre il massimo profitto dalle sinergie con altre sedi e iniziative analoghe.

Potrà essere pubblicato un bando di gara per la costituzione della segreteria del forum *Safer Internet*, a cui faranno capo esperti incaricati di suggerire soggetti di studio, preparare i documenti di lavoro, dirigere le discussioni e mettere agli atti le conclusioni.

Potranno inoltre beneficiare di un finanziamento UE progetti di autoregolamentazione finalizzati alla definizione di codici di condotta transfrontalieri. Potranno essere fornite consulenza e assistenza per garantire una cooperazione a livello comunitario mediante la messa in rete dei competenti organismi degli Stati membri e dei paesi candidati e mediante l'esame e la segnalazione sistematici delle rilevanti problematiche giuridiche o regolamentari, per contribuire allo sviluppo di metodi di valutazione e di certificazione dell'autoregolamentazione, per prestare un'assistenza pratica ai paesi che intendono istituire organismi di autoregolamentazione e per ampliare i contatti con gli organismi di autoregolamentazione non europei.

4. AZIONE 4: SENSIBILIZZAZIONE

Le azioni di sensibilizzazione devono vertere su varie categorie di contenuti illegali, indesiderati e nocivi (ad es. contenuti considerati inadatti ai minori, contenuti razzisti e xenofobi, spam) e trattare problematiche inerenti alla tutela dei consumatori, alla protezione dei dati e alla sicurezza delle reti e dell'informazione (virus informatici). Tali azioni devono interessarsi ai contenuti distribuiti sul World Wide Web e alle nuove forme di informazione e comunicazione interattiva rese possibili dalla rapida diffusione di Internet e della telefonia mobile (ad es. servizi *peer-to-peer*, video su banda larga, messaggeria istantanea, *chat room* ecc.).

La Commissione continuerà ad incoraggiare i mezzi redditizi di diffusione dell'informazione ad un gran numero di utenti, in particolare ricorrendo ad organismi "moltiplicatori" e a canali di diffusione elettronica che permettano di raggiungere l'utenza target.

Il programma garantirà un sostegno ad organismi che verranno selezionati a seguito di un invito aperto a presentare proposte. Questi dovranno fungere da nodi di sensibilizzazione in ogni Stato membro e in ogni paese candidato e condurre le azioni e i programmi di sensibilizzazione in stretta collaborazione con le parti interessate a livello nazionale, regionale e locale. Il valore aggiunto europeo dell'iniziativa sarà garantito da un nodo di coordinamento che opererà in stretto coordinamento con gli altri nodi in modo da favorire lo scambio di buone pratiche.

Gli organismi che intendono svolgere queste mansioni devono dimostrare di poter contare sul sostegno delle autorità nazionali. Devono disporre di un mandato chiaro in materia di educazione del pubblico sull'uso sicuro di Internet e dei nuovi media o in materia di formazione sui mezzi d'informazione, e possedere le risorse finanziarie necessarie per dare esecuzione a tale mandato.

I nodi nazionali sono tenuti a:

- concepire una campagna di sensibilizzazione coerente, incisiva e mirata che si avvalga dei media più idonei e tenga conto delle migliori pratiche e dell'esperienza di altri paesi;

- allacciare e mantenere contatti (formali o informali) con i soggetti importanti del settore (enti pubblici, stampa e gruppi editoriali, associazioni di fornitori di servizi Internet) e con le iniziative avviate nei loro paesi per promuovere l'uso sicuro di Internet e dei nuovi media;

- cooperare con le azioni di formazione sui mezzi d'informazione;

- informare gli utenti in merito ai software e ai servizi di filtraggio e alle *hotline* esistenti in Europa;

- cooperare attivamente con gli altri nodi nazionali della rete europea scambiando informazioni sulle migliori pratiche, partecipando alle riunioni, progettando e mettendo in atto un approccio europeo, adattandolo, se necessario, alle preferenze linguistiche e culturali nazionali;

- fungere da centro di competenza e assistenza tecnica per i nodi di sensibilizzazione che cominciano la loro attività (i nuovi nodi potrebbero essere patrocinati da un nodo più esperto).

Per ottenere una cooperazione ed un'efficacia ottimali sarà finanziato un nodo di coordinamento incaricato di fornire supporto logistico e infrastrutturale ai nodi nazionali in modo da garantire buona visibilità a livello europeo e validi meccanismi di comunicazione e di scambio di esperienze affinché gli insegnamenti possano essere messi in pratica in modo continuativo (ad esempio, adattando il materiale di sensibilizzazione).

Il nodo di coordinamento ha il compito di:

- garantire l'efficacia della comunicazione e dello scambio di informazioni e di migliori pratiche all'interno della rete;

- offrire una formazione sull'uso sicuro di Internet e delle nuove tecnologie al personale dei nodi nazionali (formazione dei formatori);

- fornire assistenza tecnica ai paesi candidati che intendono avviare azioni di sensibilizzazione;

- coordinare i servizi di consulenza e assistenza tecnica dei nodi nazionali ai nodi di sensibilizzazione in fase di avvio;

- proporre indicatori e gestire le attività di raccolta, analisi e scambio di dati statistici sulle attività di sensibilizzazione nazionali al fine di valutarne l'impatto;

- fornire l'infrastruttura necessaria per la costituzione di un deposito transnazionale unico e completo (portale web) per le informazioni pertinenti e le risorse di sensibilizzazione e di ricerca con contenuti localizzati (se necessario con siti web secondari), che contenga ritagli di stampa, articoli e bollettini mensili in diverse lingue e che favorisca la visibilità delle attività del forum;

- estendere i collegamenti con le attività di sensibilizzazione non europee;

- partecipare al forum *Safer Internet* e ad altre rilevanti manifestazioni coordinando gli input/feedback provenienti dalla rete di sensibilizzazione.

Secondo le stesse modalità, saranno inoltre condotte ricerche tese a determinare le modalità d'uso dei nuovi media da parte degli utenti, in particolare i minori. A livello UE potrebbero inoltre essere varate nuove azioni, ad esempio per il sostegno a servizi Internet specifici per i minori o l'istituzione di un premio alla migliore iniziativa di sensibilizzazione dell'anno.

ALLEGATO II

RIPARTIZIONE INDICATIVA DELLE SPESE

1)	Lotta ai contenuti illegali	23-28%
2)	Contrasto ai contenuti indesiderati e nocivi	16-23%
3)	Promozione di un ambiente più sicuro	5-9%
4)	Sensibilizzazione	43-50%

ALLEGATO III

STRUMENTI DI ATTUAZIONE DEL PROGRAMMA

1) La Commissione darà attuazione al programma conformemente alle disposizioni tecniche illustrate nell'allegato I.

2) L'esecuzione del programma avverrà per mezzo di azioni indirette comprendenti:

(a) Azioni a costi condivisi

- Progetti pilota e azioni incentrate sulle migliori pratiche. Progetti ad hoc in settori di pertinenza del programma, tra cui progetti di dimostrazione delle migliori pratiche o relativi ad applicazioni innovative di tecnologie esistenti.

- Messa in rete dei vari soggetti del settore per garantire che le azioni abbraccino l'intera Unione e facilitare le attività di coordinamento e di trasferimento delle conoscenze. Le azioni di messa in rete possono essere collegate alle azioni relative alle migliori pratiche.

- Ricerca applicata condotta in modo comparabile su scala europea e dedicata alle modalità di utilizzo dei nuovi media, in particolare da parte dei minori.

- Il finanziamento comunitario non supererà di norma il 50% del costo del progetto. Gli enti pubblici possono beneficiare del rimborso integrale dei costi aggiuntivi.

(b) Misure di accompagnamento

- Le misure di accompagnamento contribuiranno all'attuazione del programma o alla preparazione delle attività future. Non sono considerate ammissibili le attività di commercializzazione dei prodotti, dei processi o dei servizi, le azioni di marketing e di promozione vendite.

  - Analisi comparativa e sondaggi d'opinione destinati ad ottenere dati affidabili sull'uso sicuro di Internet e delle nuove tecnologie online in tutti gli Stati membri, raccolti secondo metodologie comparabili.

  - Valutazione tecnica di tecnologie quali i software di filtraggio, destinate a promuovere l'uso sicuro di Internet e delle nuove tecnologie online. La valutazione verterà anche sulla capacità o meno di tali tecnologie di accrescere il livello di riservatezza.

  - Studi a sostegno del programma e delle sue azioni, in particolare dedicati all'autoregolamentazione e alle attività del forum *Safer Internet*, e preparazione delle attività future.

  - Premiazione delle migliori pratiche.

- Scambio di informazioni, conferenze, seminari, *workshop* e altre riunioni e gestione delle attività di aggregazione.

- Attività di diffusione, informazione e comunicazione.

3) La selezione delle azioni a costi condivisi avverrà sulla base di inviti a presentare proposte pubblicati nel sito Internet della Commissione, conformemente alle disposizioni finanziarie in vigore.

4) Le richieste di contributi comunitari devono essere corredate, ove opportuno, di un piano finanziario contenente tutti gli elementi del finanziamento dei progetti, compresi la richiesta di finanziamento comunitario e l'indicazione di altri finanziamenti richiesti o ottenuti da altre fonti.

5) L'attuazione delle misure di accompagnamento avverrà mediante bandi di gara conformemente alle disposizioni finanziarie in vigore.

SCHEDA FINANZIARIA LEGISLATIVA

Settore(i) politico(i): società dell'informazione

Attività: contenuti e servizi della società dell'informazione

Denominazione dell'azione: Programma comunitario pluriennale inteso a promuovere un uso più sicuro di Internet e delle nuove tecnologie online (*Safer Internet plus*)

1. LINEA(E) DI BILANCIO + DENOMINAZIONE(I)

Linea(e) di bilancio: 09 03 03 (ex B5-821) e 09 01 04 04(ex B5-821A)

2. DATI GLOBALI IN CIFRE

2.1. Dotazione totale dell'azione

50 milioni di euro

2.2. Periodo di applicazione

Dal 1° gennaio 2005 al 31 dicembre 2008

2.3. Stima globale pluriennale delle spese

a) Scadenzario stanziamenti d'impegno/stanziamenti di pagamento (intervento finanziario)

09 03 03 (ex B5-821) in milioni di euro (*al terzo decimale*)

	2005	2006	2007	2008	Totale
Stanziamenti d'impegno	9,500	10,100	14,730	14,730	49,060
Stanziamenti di pagamento[25]					
2005	2,000	-	-	-	2,000
2006	3,700	2,200	-	-	5,900
2007	2,800	3,800	4,600	-	11,200
2008	1,000	2,900	5,700	6,000	15,600
2009 e successivi		1,200	4,430	8,730	14,360
Totale	9,500	10,100	14,730	14,730	49,060

[25] Agli stanziamenti di pagamento per gli anni 2005, 2006 e 2007 vanno aggiunti gli importi relativi all'esecuzione del piano d'azione per l'uso sicuro di Internet (1999–2004).

b) Assistenza tecnica e amministrativa e spese d'appoggio *(cfr. punto 6.1.2.)*

09 01 04 04 (ex B5-821A) in milioni di euro *(al terzo decimale)*

	2005	2006	2007	2008	Totale
Stanziamenti d'impegno/ di pagamento	0,220	0,230	0,240	0,250	0,940

09 03 03 + 09 01 04 04 in milioni di euro *(al terzo decimale)*

Totale parziale a+b	2005	2006	2007	2008	Totale
Stanziamenti d'impegno	9,720	10,330	14,970	14,980	50,000
Stanziamenti di pagamento					
2005	2,220	-	-	-	2,220
2006	3,700	2,430	-	-	6,130
2007	2,800	3,800	4,840	-	11,440
2008	1,000	2,900	5,700	6,250	15,850
2009 e successivi		1,200	4,430	8,730	14,360
Totale	9,720	10,330	14,970	14,980	50,000

c) Incidenza finanziaria globale delle risorse umane e delle altre spese di funzionamento *(cfr. punti 7.2. e 7.3.)*

in milioni di euro *(al terzo decimale)*

	2005	2006	2007	2008	Totale
Stanziamenti d'impegno/ di pagamento	0,950	0,950	0,950	0,950	3,800

TOTALE a+b+c	2005	2006	2007	2008	2009 e succ.	Totale
Stanziamenti d'impegno	10,670	11,270	15,930	15,930		53,800
Stanziamenti di pagamento	3,170	7,080	12,390	16,800	14,360	53,800

2.4. Compatibilità con la programmazione finanziaria e le prospettive finanziarie

X La proposta è compatibile con la programmazione finanziaria in vigore (7,62 milioni di euro nel 2005 e 7,73 milioni di euro nel 2006 provenienti dalla linea di bilancio 09 03 03), dopo i seguenti storni da altre linee di bilancio: 090302 *e*Content (ex linea B5-334), 1 milione di euro nel 2005 e nel 2006; 0902

politica delle comunicazioni elettroniche (ex linea B5-302), 1,1 milioni di euro nel 2005 e 1,6 milioni di euro nel 2006.

☐ La proposta impone una riprogrammazione della corrispondente rubrica delle prospettive finanziarie

☐ Può essere necessario il ricorso alle disposizioni dell'accordo interistituzionale

La proposta iniziale relativa ad un piano d'azione per la promozione dell'uso sicuro di Internet, adottata dalla Commissione nel novembre 1997, prevedeva una dotazione finanziaria di 30 milioni di euro per quattro anni, ma il Parlamento europeo e il Consiglio hanno concesso solo 25 milioni di euro. L'estensione dell'iniziativa per il periodo 2003-2004 ha comportato un aumento della dotazione finanziaria pari a 13,3 milioni di euro, di cui 6,7 milioni per il 2004. L'aumento è stato concesso a seguito di una richiesta della Commissione basata su una stima minimalista di quanto necessario in quel momento. La copertura di alcuni costi del 2004 è stata possibile soltanto cessando il finanziamento dello sviluppo di software e servizi di filtraggio e stornando i relativi importi verso altre voci.

I motivi che spingono a chiedere un sostanziale aumento del finanziamento per il periodo 2005-2008 sono i seguenti:

a) l'ampliamento del campo di applicazione del programma perché verta sull'evoluzione delle tecnologie e sul modo in cui queste vengono utilizzate, in particolare dal punto di vista dello spettacolare aumento del loro uso da parte dei minori; il potenziamento delle attività di sensibilizzazione e il prevedibile aumento del carico di lavoro delle *hotline* dovuto alla quantità di contenuti illegali in circolazione e al numero di segnalazioni effettuate;

b) l'allargamento dell'UE da 15 a 25 Stati membri. Sono necessarie risorse adeguate per costituire, nei dieci nuovi Stati membri, i nodi nazionali che compongono la rete delle *hotline* (azione 1) e la rete di sensibilizzazione (azione 4), e per far fronte alle nuove esigenze dei due coordinatori di rete derivanti dall'aumento del numero di nodi.

c) Il programma verterà non solo su Internet e sulle nuove tecnologie come la telefonia mobile, ma anche sullo spam, ossia l'invio di e-mail commerciali non richieste. L'inserimento dello spam nel campo di applicazione comporterà un aumento della spesa per le azioni 2, 3 e 4.
L'aumento più significativo servirà a coprire i costi delle azioni di coordinamento per lo scambio di informazioni e di buone pratiche sui mezzi efficaci di applicazione delle misure anti-spam e delle azioni di sviluppo delle tecnologie di filtraggio nell'ambito dell'azione 2 "Contrasto ai contenuti indesiderati e nocivi".

2.5. Incidenza finanziaria sulle entrate

X Nessuna incidenza finanziaria (si tratta degli aspetti tecnici dell'attuazione di una misura)

3. CARATTERISTICHE DI BILANCIO

Natura della spesa		Nuova	Partecipazione EFTA	Partecipazione paesi candidati	Rubrica PF
SNO	SD	NO	SÌ	SÌ	N 3

4. BASE GIURIDICA

Articolo 153 del trattato che istituisce la Comunità europea

Decisione .../..../CE del Parlamento europeo e del Consiglio relativa all'adozione di un programma comunitario pluriennale (2005 – 2008) inteso a promuovere un uso più sicuro di Internet e delle tecnologie online (*Safer Internet plus*).

5. DESCRIZIONE E GIUSTIFICAZIONE

5.1. Necessità dell'intervento comunitario

5.1.1. Obiettivi perseguiti

L'obiettivo generale continua ad essere la promozione dell'uso sicuro di Internet, in particolare da parte dei minori, e la lotta contro i contenuti illegali e i contenuti indesiderati dall'utente finale.

Gli obiettivi specifici sono i seguenti:

1) Lottare contro i contenuti illegali consentendo agli utenti di segnalare tali contenuti avvalendosi di una rete di *hotline*.

2) Contrastare i contenuti indesiderati e nocivi: analisi comparativa del software di filtraggio, coordinamento degli scambi di informazioni e di buone pratiche sui mezzi efficaci di applicazione delle norme anti-spam, sviluppo di nuove tecnologie di filtraggio efficaci, adeguamento dei sistemi di classificazione dei contenuti (per tener conto della convergenza).

3) Promuovere un ambiente più sicuro sostenendo le azioni di autoregolamentazione (definizione e attuazione di codici di condotta europei per l'industria) e garantendo una cooperazione a livello comunitario.

4) Sensibilizzare maggiormente il pubblico in merito all'uso sicuro di Internet e delle tecnologie online sostenendo una rete europea di attività di sensibilizzazione.

5.1.2. Disposizioni adottate in relazione alla valutazione ex ante

È stata effettuata un'approfondita valutazione ex ante sulla base di diversi input, tra cui le due valutazioni esterne del piano d'azione 1999-2002[26], la consultazione delle parti interessate del settore e le informazioni raccolte dalla Commissione attraverso le numerose azioni di diverso tipo a cui ha preso parte negli ultimi anni e attraverso i propri contatti con i principali operatori del settore.

---

[26] COM(2003) 591 def. adottato dalla Commissione il 10 ottobre 2003.

Da tali informazioni emerge con chiarezza che i contenuti e i comportamenti illegali e nocivi su Internet continuano ad essere una fonte di forte preoccupazione per i legislatori, l'industria e i genitori. Si prevede che il problema assumerà dimensioni ancora maggiori sia in termini qualitativi (nuove tecnologie, nuove piattaforme) che quantitativi (la quantità e il tipo di contenuti aumenteranno). Questo aumento della connettività da parte dei bambini avrà su di loro effetti benefici ma comporterà anche rischi di "danni collaterali".

La proliferazione delle e-mail commerciali non richieste – il fenomeno dello spam – ha raggiunto proporzioni tali da rappresentare un grave ostacolo allo sviluppo del commercio elettronico e della società dell'informazione.

In materia di contenuti illegali e di regolamentazione della diffusione di contenuti nocivi, la responsabilità primaria dei fornitori di contenuti è una questione ancora essenzialmente disciplinata dal diritto nazionale. Esistono tuttavia strumenti che stabiliscono le regole che gli Stati membri sono tenuti ad attuare in questo campo. La direttiva sul commercio elettronico[27] disciplina la questione della responsabilità del prestatore intermediario per semplice trasporto (*mere conduit*), memorizzazione temporanea (*caching*) e accoglienza dei contenuti (*hosting*). L'Unione europea è stata la prima ad agire sul fronte giuridico contro le comunicazioni commerciali indesiderate adottando la direttiva sulla tutela della vita privata nel settore delle comunicazioni elettroniche[28], che condurrà, in tutta Europa, ad un divieto dello spam destinato ai privati. La raccomandazione sulla tutela dei minori e della dignità umana[29] contiene raccomandazioni destinate agli Stati membri, all'industria, alle parti interessate e alla Commissione e presenta una serie di indicazioni orientative sulla tutela dei minori.

Dalla relazione di valutazione del piano di lavoro per l'uso sicuro di Internet 1999-2002 emerge un consenso, tra le persone e gli organismi consultati, in merito al fatto che il quadro normativo non permette, da solo, di far fronte alla dimensione mondiale del problema. La regolamentazione deve essere integrata da misure pratiche che assistano le autorità di polizia, che consentano agli utenti di proteggersi e di proteggere i minori di chi hanno la responsabilità dai contenuti indesiderati e nocivi, di stimolare l'industria a definire soluzioni di autoregolamentazione e di informare ed educare genitori, insegnanti e minori in merito ai problemi esistenti e al miglior modo di ovviarvi. L'intervento pubblico a livello comunitario, ad integrazione delle iniziative nazionali, regionali e locali, è necessario a causa della dimensione transnazionale del problema e della necessità di una cooperazione internazionale di alto profilo per affrontarlo.

Da tali premesse scaturiscono due conclusioni di tipo operativo:

- vi è consenso circa la necessità di un intervento comunitario complementare alle iniziative condotte dagli Stati membri;

- le linee di azione del programma proposto vertono su aspetti per i quali l'intervento comunitario sarà più appropriato e più efficace.

---

27 Direttiva 2000/31/CE del Parlamento europeo e del Consiglio, dell'8 giugno 2000, relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno (GU L 178 del 17.7.2000, pag. 1).

28 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (GU L 201 del 31.7.2002, pag. 37).

29 Cfr. nota 20.

Nell'elaborare la presente proposta la Commissione ha consultato i servizi responsabili delle varie azioni, ossia le direzioni generali "Educazione e cultura", "Mercato interno" e "Giustizia e Affari interni".

Il programma intende ottimizzare il proprio impatto sul pubblico target ricorrendo alla messa in rete e all'effetto moltiplicatore. L'approccio scelto si basa sui risultati del piano d'azione per l'uso sicuro di Internet 1999-2004 a cui si aggiungono nuovi elementi per tener conto delle nuove sfide. Tali elementi consolidano le azioni, che si rafforzano a vicenda, e ne garantiscono la coerenza senza ridurne la rilevanza per il pubblico target.

È questo l'approccio descritto nella valutazione *ex ante* e successivamente tradotto in obiettivi operativi incentrati su aree di intervento e strumenti di attuazione ben definiti.

5.1.3. Disposizioni adottate a seguito della valutazione ex post

La relazione di valutazione 1999-2002 esprime un giudizio positivo sul piano d'azione sull'uso sicuro di Internet. Gli esperti ritengono che l'iniziativa abbia prodotto risultati significativi nei suoi primi quattro anni di funzionamento ma che la complessità della problematica e la molteplicità delle parti interessate rendano necessarie nuove azioni.

Gli esperti hanno riconosciuto l'impatto positivo del programma attuale, soprattutto nella promozione della messa in rete e nella fornitura di informazioni sui problemi legati all'uso sicuro di Internet e sulle soluzioni per ovviarvi.

Le conclusioni evidenziano in particolare i seguenti elementi.

Le parti interessate concordano sul fatto che gli obiettivi, le priorità e i mezzi di attuazione originali rimangono validi e che le linee di azione sono i meccanismi più idonei per realizzare tali obiettivi.

Sotto il profilo politico l'iniziativa ha avuto il merito fare dell'uso sicuro di Internet un punto fermo dell'ordine del giorno dei lavori delle istituzioni e degli Stati membri dell'UE. Va riconosciuta al riguardo la lungimiranza della Commissione nel richiamare l'attenzione su questi problemi sin dalle prime fasi dello sviluppo di Internet.

Gli esperti hanno formulato una serie di precise raccomandazioni riguardo le linee di azione e le loro modalità di attuazione:

- ampliare il campo d'azione/gli obiettivi al fine di tener conto delle tecnologie della comunicazione nuove ed emergenti, in particolare quelle che possono incidere sull'uso di Internet da parte dei minori (ad es. telefoni mobili 3G);

- adattare la linea di azione relativa alle tecnologie di filtraggio e ai sistemi di classificazione dei contenuti;

- proseguire la costituzione di reti di nodi di sensibilizzazione negli Stati membri;

- proseguire la cooperazione con attori esterni all'Unione europea;

- incoraggiare un maggiore coinvolgimento degli ISP e di altri soggetti del settore;

- focalizzare il programma sugli aspetti in cui può risultare più efficace, ossia a livello europeo/internazionale, mediante messa in rete ed effetti moltiplicatori.

La Commissione ha già anticipato molte di queste conclusioni nelle proprie proposte di prosecuzione del piano d'azione per l'uso sicuro di Internet e le metterà in atto come parte del programma di lavoro 2003-2004. La concezione del programma "*Safer Internet Plus*" terrà pienamente conto di tali conclusioni.

5.2. Azioni previste e modalità dell'intervento di bilancio

Le azioni previste sono quattro:

1) **Lotta ai contenuti illegali**

2) **Contrasto ai contenuti indesiderati e nocivi**

3) **Promozione di un ambiente più sicuro**

4) **Sensibilizzazione**

5.3. Modalità di attuazione

Per ottimizzare l'efficacia rispetto ai costi i contraenti selezionati per gestire le *hotline* e condurre le azioni di sensibilizzazione dovranno beneficiare di un finanziamento per un periodo di tempo superiore (3-4 anni) rispetto alla durata normale prevista dall'attuale piano d'azione per la promozione della sicurezza di Internet (da 18 mesi a 2 anni). Il finanziamento sarà erogato sulla base di un primo contratto, aggiudicato a seguito di una gara di appalto aperta, che avrà di norma una durata di due anni. Successivamente, in esito all'esercizio di valutazione, i progetti di successo potranno essere prorogati e beneficiare di un finanziamento supplementare corrispondente al periodo di proroga.

I meccanismi di erogazione del finanziamento previsti nella proposta ricalcano ampiamente la prassi comunitaria in materia di sovvenzioni e cofinanziamento e si basano su una richiesta finanziaria dettagliata. Tuttavia, in considerazione della limitata portata finanziaria del piano d'azione sulla sicurezza di Internet, dovrebbero poter essere stipulati con le *hotline* e i nodi nazionali di sensibilizzazione contratti più semplici basati su un contributo forfetario al bilancio.

Alcune parti saranno integralmente finanziate dalla Comunità. I finanziamenti saranno erogati a seguito di inviti a presentare proposte e gare di appalto.

La Commissione assumerà la gestione centralizzata del programma. Gli stanziamenti per l'assistenza tecnica e amministrativa e le spese di sostegno sono destinati a coprire i costi di studi, riunioni di esperti, azioni di informazione, conferenze e pubblicazioni direttamente connessi agli obiettivi del programma, oltre ad altre eventuali spese legate all'assistenza tecnica e amministrativa che non implicano compiti delle pubbliche autorità.

6. INCIDENZA FINANZIARIA

6.1. Incidenza finanziaria totale sulla parte B (per l'intero periodo di programmazione)

6.1.1. Intervento finanziario (Stanziamenti d'impegno)

Impegni in milioni di euro *(al terzo decimale)*

Ripartizione	2005	2006	2007	2008	Totale
Lotta ai contenuti illegali	3,150	3,150	3,150	3,150	**12,600**
Contrasto ai contenuti indesiderati e nocivi	0,750	0,750	4,130	4,130	**9,760**
Promozione di un ambiente più sicuro	0,600	1,000	1,000	1,000	**3,600**
Sensibilizzazione	5,000	5,200	6,450	6,450	**23,100**
TOTALE	**9,500**	**10,100**	**14,730**	**14,730**	**49,060**

La ripartizione tra le quattro azioni è indicativa e si basa sulla ripartizione indicata nell'allegato II del progetto di decisione del Parlamento europeo e del Consiglio.

6.1.2 Assistenza tecnica e amministrativa, spese d'appoggio e spese TI (Stanziamenti d'impegno)

Impegni in milioni di euro *(al terzo decimale)*

	2005	2006	2007	2008	Totale
Assistenza tecnica e amministrativa (sito web, servizi editoriali, valutazione dei progetti ecc.)	0,220	0,230	0,240	0,250	**0,940**
Informazione, pubblicazioni, comunicazione					
TOTALE	0,220	0,230	0,240	0,250	**0,940**

Le spese relative alle riunioni del comitato del programma sono imputate alla linea A07031. Le spese per le riunioni delle parti interessate sono imputate alla linea A07030 (cfr. sezione 7).

6.2. Calcolo del costo per ciascuna delle misure previste nella parte B (per l'intero periodo di programmazione)

Impegni in milioni di euro *(al terzo decimale)*

Ripartizione	Tipo di risultati (progetti, fascicoli)	Numero di risultati su 4 anni	Costo unitario medio	Costo totale su 4 anni
Lotta ai contenuti illegali	*Hotline*	25 nodi di rete	0,092 l'anno	9,200
	Attività della rete centrale	1	0,85 l'anno	3,400
	Totale	**26**		**12,600**
Contrasto ai contenuti indesiderati e nocivi	Analisi comparativa e coordinamento delle misure anti-spam, 2 progetti quadriennali, progetti in materia di filtraggio	2 progetti quadriennali 10 progetti di filtraggio	0,4 (l'anno) = 3,2 milioni 6,56 milioni	3,200 6,560
	Totale	**4**		**9,760**
Promozione di un ambiente più sicuro	Azioni di sostegno all'autoregolamentazione, forum *Safer Internet*	10	0,360	3,600
	Totale	**10**		**3,600**
Sensibilizzazione	Nodi di sensibilizzazione	25	0,197	19,700
	Attività della rete centrale	1	0,850	3,400
	Totale	**26**		**23,100**
COSTO TOTALE				**49,060**

Le spese relative ai primi due anni mirano a garantire la continuità e a consolidare le reti di *hotline* e le reti di sensibilizzazione, conservandone lo slancio e assicurandone l'estensione a tutti gli Stati membri e avviando nel contempo nuove azioni in materia di lotta anti-spam e di autoregolamentazione. Nei prossimi anni queste reti saranno chiamate a smaltire un onere di lavoro maggiore, sia in termini qualitativi che quantitativi, ed occorre pertanto garantire loro un sostegno permanente. Gli obiettivi delle due reti sono sostanzialmente diversi: mentre le *hotline* sono centri presso i quali segnalare i contenuti illegali, i nodi di sensibilizzazione sono incaricati di promuovere l'uso sicuro di Internet e nelle nuove reti mobili presso i minori, gli insegnanti e i genitori. Il loro lavoro è fondamentalmente diverso e si prevede che gli Stati membri assegnino questi compiti ad organismi distinti. Lo stesso principio vale per i nodi di coordinamento, i cui compiti dovranno essere svolti da organismi specifici, in grado di promuovere le buone pratiche e di garantire lo scambio di informazioni tra i componenti delle varie reti del loro specifico settore di attività (cfr. allegato I della proposta relativa al programma). Il sostegno ai nodi delle due reti avverrà sulla base del meccanismo di cofinanziamento (sostegno ai "progetti").

Il programma prevede anche che, previo consenso del comitato del programma, possano essere finanziate azioni in paesi terzi. Questa possibilità consentirà – seppure in modo limitato – di garantire un sostegno alle *hotline* dei paesi terzi in cui è ospitata la maggior parte dei contenuti illegali e nocivi.

La seconda linea di azione del programma, relativa al contrasto ai contenuti indesiderati e nocivi, comporterà attività di analisi comparativa dei prodotti di filtraggio e attività di coordinamento e di promozione dello scambio di informazioni e di migliori pratiche sulle tecniche efficaci di applicazione delle misure anti-spam. Nella seconda fase del programma questa linea di azione permetterà di finanziare lo sviluppo di tecnologie di filtraggio e misure di adozione dei sistemi di classificazione dei contenuti e dei marchi di qualità dei siti web.

I risultati target annuali sono stati calcolati sulla base della seguente ripartizione della dotazione finanziaria del programma:

Lotta ai contenuti illegali	23-28%
Contrasto ai contenuti indesiderati e nocivi	16-23%
Promozione di un ambiente più sicuro	5-9%
Sensibilizzazione	43-50%

7. INCIDENZA SUL PERSONALE E SULLE SPESE DI FUNZIONAMENTO

7.1. Incidenza sulle risorse umane

Tipo di posto		Personale da assegnare alla gestione dell'azione su risorse esistenti e/o supplementari		Totale	Descrizione dei compiti inerenti all'azione
		Numero di posti permanenti	Numero di posti temporanei		
Funzionari o agenti temporanei	A B C	4 1 2		4 1 2	Gestione del programma (inviti, programma di lavoro, procedure della Commissione) gestione dei progetti, controllo dei costi
Altre risorse umane			1 END[30]	1	Assistenza tecnica per i progetti
Totale		7	1	8	

Non è previsto personale supplementare - Le esigenze in termini di personale saranno soddisfatte mediante una ridistribuzione interna.

7.2. Incidenza delle spese per risorse umane

Tipo di risorse umane	Importo in euro	Metodo di calcolo
Funzionari Agenti temporanei	756 000 Dai paesi EFTA (cfr. nota)	7 x 108 000
Totale	756 000	

[30] Contributo previsto dei paesi EFTA in materia di personale.

7.3. Altre spese di funzionamento derivanti dall'azione

Linea di bilancio (numero e denominazione)	Importo in euro	Metodo di calcolo (Spese annue)
Dotazione globale (Titolo A7)		
A0701 – Missioni	14 000	20 missioni l'anno all'interno dell'UE x 700
A07040 – Conferenze	100 000	…
A07031 – Comitati obbligatori	40 000	2 riunioni l'anno x 1 partecipante x 25 Stati membri x 800
A07030 – Riunioni non obbligatorie	40 000	2 riunioni l'anno con le parti interessate (20 partecipanti x 1 000 per riunione)
Sistemi d'informazione (A-5001/A-4300)	-	-
Altre spese - Parte A (specificare)	-	-
Totale	**194 000**	

Gli importi corrispondono alle spese totali dell'azione per 12 mesi.

Le esigenze in termini di risorse umane e amministrative saranno coperte con la dotazione assegnata alla DG responsabile della gestione nel quadro della procedura di finanziamento annuale.

8. CONTROLLO E VALUTAZIONE

8.1. Modalità di controllo

Le attività legate all'attuazione e al controllo del programma saranno svolte dai funzionari della Commissione. Il controllo permanente del programma avverrà sulla base delle informazioni ottenute direttamente presso i suoi beneficiari, tenuti a presentare relazioni di attività e relazioni finanziarie intermedie e finali, contenenti anche gli indicatori di rendimento stabiliti nel processo di selezione.

Per garantire la massima qualità nell'esecuzione del programma saranno regolarmente organizzate ispezioni ai progetti e i partecipanti saranno chiamati a riferire periodicamente in merito alle attività svolte.

Tutti i progetti e le azioni comprenderanno meccanismi di autovalutazione o modalità di valutazione ad opera di esperti esterni o fonti interne. Essi conterranno inoltre indicatori di rendimento e indicazioni sulle modalità di proseguimento delle attività.

Per i progetti che consistono in un evento unico, quali seminari e conferenze, si procederà ad un controllo in loco, mentre la valutazione esterna approfondita avverrà sulla base di una campionatura aleatoria e/o di un'analisi dei fattori di rischio.

8.2. Modalità e calendario della valutazione

Al termine del secondo anno di funzionamento del programma verrà realizzata una relazione intermedia. La valutazione ex post incentrata sull'impatto dell'azione avrà luogo al termine del programma.

Ai fini della valutazione sono stati definiti i seguenti indicatori:

Obiettivi generali	**Indicatori**
❑ Promuovere l'uso sicuro di Internet, in particolare da parte dei minori, e lottare contro i contenuti indesiderati dagli utenti finali	- Dati quantitativi/qualitativi sulle azioni, relazioni e altri risultati di tali azioni - Dati quantitativi/qualitativi sulla visione dei partecipanti quanto all'impatto del programma
Obiettivi operativi	**Indicatori**
1. Lotta ai contenuti illegali	- Dati quantitativi/qualitativi sull'efficacia e la visibilità delle *hotline*
2. Contrasto ai contenuti indesiderati e nocivi	- Grado di informazione in merito alle tecnologie disponibili - Numero e campo di applicazione delle iniziative in materia di filtraggio, classificazione dei contenuti e marchi di qualità dei siti a livello europeo
3. Promozione di un ambiente più sicuro	- Numero e campo di applicazione delle iniziative di autoregolamentazione a livello europeo
4. Rafforzamento della cooperazione e della sensibilizzazione	- Livello di conoscenza dell'uso sicuro dei nuovi media da parte dei minori e dei genitori - Portata delle attività di sensibilizzazione, numero di insegnanti/educatori formati al riguardo

9. MISURE ANTIFRODE

Le decisioni di finanziamento e i contratti conclusi tra la Commissione e i beneficiari stabiliscono che la Commissione e la Corte dei conti effettuino controlli presso i locali dei beneficiari di un contributo comunitario e autorizzano queste istituzioni ad esigere pezze giustificative di ogni spesa effettuata a norma di tali contratti, convenzioni e impegni giuridici nei cinque anni successivi alla fine del periodo contrattuale. Ove necessario saranno effettuate verifiche in loco.

I beneficiari sono tenuti a presentare relazioni e rendiconti finanziari. Questi vengono analizzati sotto il profilo del contenuto e dell'ammissibilità della spesa, tenendo conto dello scopo del finanziamento comunitario, così come degli obblighi contrattuali e dei principi di economia e di sana gestione finanziaria.

Le convenzioni finanziarie recano in allegato informazioni di carattere amministrativo e finanziario, intese a precisare le tipologie di spesa ammissibili a norma delle convenzioni stesse. Se del caso, la copertura comunitaria di determinati elementi di costo potrà limitarsi alle voci che risultano reali, individuabili e verificabili nella contabilità del beneficiario, al fine di facilitare l'attività di controllo e di revisione contabile (oltre che di valutazione in sede di selezione) dei progetti destinatari del finanziamento.

In materia di appalti pubblici, come stabilito dagli articoli da 93 a 96 del regolamento finanziario, la Commissione può imporre sanzioni amministrative o pecuniarie nei confronti dei candidati o degli offerenti che rientrano nella casistica di esclusione.

PUBBLICISTICA E
ALTRA DOCUMENTAZIONE UFFICIALE

Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione

VERSO UNA CULTURA DELLA SICUREZZA

OECD OCDE

ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO

ORGANIZZZIONE PER LA COOPERAZIONE E LO SVILIUPPO ECONOMICO

In virtù dell'art.1 della Convenzione firmata il 14 dicembre 1960 ed entrata in vigore il 30 settembre 1961, l'Organizzazione per la Cooperazione e lo Sviluppo Economici (OCSE) ha per obiettivo di favorire le politiche tese a:

- realizzare la maggiore espansione possibile dell'economia e dell'occupazione ed un innalzamento del livello di vita nei Paesi Membri, pur mantenendo la stabilità finanziaria, e di contribuire così allo sviluppo dell'economia mondiale;
- contribuire a una sana espansione economica nei Paesi Membri, e non membri, in via di sviluppo economico;
- contribuire all'espansione del commercio mondiale su una base multilaterale e non discriminatoria, in conformità agli impegni internazionali.

I Membri fondatori dell'OCSE sono: Austria, Belgio, Canada, Danimarca, Francia, Germania, Grecia, Irlanda, Islanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Portogallo, Regno Unito, Spagna, Stati Uniti, Svezia, Svizzera, Turchia. I seguenti paesi sono in seguito diventati Membri per adesione alle date di seguito indicate: Giappone (28 aprile 1964), Finlandia (28 gennaio 1969), Australia (7 giugno 1971), Nuova Zelanda (29 maggio 1973), Messico (18 maggio 1994), Repubblica Ceca (21 dicembre 1995), Ungheria (7 maggio 1996), Polonia (22 novembre 1996) e Corea (12 dicembre 1996). La Commissione delle Comunità Europee partecipa ai lavori dell'OCSE (art.13 della Convenzione dell'OCSE).

Also available in English under the title:

OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security

PREMESSA

Le presenti *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti di informazione: verso una cultura della sicurezza* sono state adottate sotto forma di Raccomandazione del Consiglio in occasione della 1037ª sessione del Consiglio dell'OCSE, il 25 luglio 2002.

INDICE

LE LINEE GUIDA SULLA SICUREZZA DEI SISTEMI E DELLE RETI D'INFORMAZIONE

VERSO UNA CULTURA DELLA SICUREZZA

PREFAZIONE

L'uso dei sistemi e delle reti d'informazione e l'ambiente delle tecnologie dell'informazione nel suo insieme, hanno registrato spettacolari cambiamenti dal 1992, data della prima pubblicazione delle *Linee guida sulla sicurezza dei sistemi e reti d'informazione* dell'OCSE. Tali continui cambiamenti offrono notevoli vantaggi ma richiedono altresì che i governi, le imprese, le altre istituzioni e i singoli utenti che sviluppano, possiedono, forniscono, gestiscono, procedono alla manutenzione e utilizzano i sistemi e le reti d'informazione (parti interessate), dedichino maggiore attenzione alla sicurezza.

Personal computer sempre più potenti, tecnologie convergenti e un'ampia utilizzazione d'Internet hanno sostituito i precedenti sistemi autonomi dalle capacità limitate nell'ambito di reti prevalentemente chiuse. Oggi, le parti interessate sono sempre più interconnesse e le connessioni superano i confini nazionali. Inoltre, Internet è il supporto per infrastrutture vitali quali l'energia, i trasporti e le attività finanziarie e svolge un ruolo centrale nel modo in cui le imprese svolgono le proprie attività, in cui i governi assicurano i servizi ai cittadini e alle imprese e in cui i cittadini comunicano e scambiano informazioni. La natura e la tipologia delle tecnologie che costituiscono l'infrastruttura delle comunicazioni e dell'informazione hanno parimenti registrato una notevole evoluzione. Il numero e la natura dei dispositivi di accesso a tale infrastruttura si sono moltiplicati e differenziati per conglobare i terminali di accesso fissi, senza fili e mobili e gli accessi tramite collegamenti "permanenti" sono in aumento. Ne consegue che la natura, il volume e il carattere sensibile dell'informazione scambiata sono aumentati in modo sostanziale.

Con la loro accresciuta connettività, i sistemi e reti d'informazione sono ormai esposti a un aumento del numero e a una più larga gamma di minacce e vulnerabilità ed emergono quindi nuovi problemi di sicurezza. Per tale motivo, le presenti Linee guida non sono rivolte all'insieme delle parti interessate nell'ambito della nuova società dell'informazione, e suggeriscono la necessità di una maggiore vigilanza e comprensione riguardo alle questioni di sicurezza, e la necessità di sviluppare una "cultura della sicurezza".

I. VERSO UNA CULTURA DELLA SICUREZZA

Le presenti Linee guida rispondono a un contesto in continua evoluzione incitando allo sviluppo di una cultura della sicurezza – sottolineando quindi la necessità di dedicare la massima attenzione alla sicurezza nella fase di sviluppo dei sistemi informativi e delle reti e adottando nuovi approcci e nuovi comportamenti nell'utilizzazione dei sistemi e delle reti d'informazione e nelle interazioni realizzate mediante tali sistemi. Le Linee guida rappresentano una netta svolta rispetto a un'epoca in cui la sicurezza interveniva troppo spesso in modo saltuario nella progettazione e nell'uso delle reti e dei sistemi informativi. Le parti interessate sono sempre più dipendenti dai sistemi d'informazione, dalle reti e dai servizi a loro collegati, i quali devono essere tutti affidabili e sicuri. Solo un approccio che tenga debitamente conto degli interessi di tutte le parti e della natura dei sistemi, reti e servizi connessi, è in grado di offrire un'efficace sicurezza.

Ogni singola parte interessata ha un rilevante ruolo da svolgere per tutelare la sicurezza. Le parti interessate, secondo i loro rispettivi ruoli, devono essere sensibilizzate ai rischi legati alla sicurezza, nonché alle protezioni adeguate e devono assumere le loro responsabilità e prendere misure per migliorare la sicurezza dei sistemi e reti d'informazione.

La diffusione di una cultura della sicurezza richiederà un impulso e una larga partecipazione e dovrebbe portare a conferire una rafforzata priorità alla programmazione e alla gestione della sicurezza e a un'estensione della comprensione della necessità della sicurezza a tutte le parti interessate. Le questioni di sicurezza devono essere un argomento di preoccupazione e di responsabilità a tutti livelli di governo e, delle imprese e per l'insieme delle parti interessate. Le Linee guida offrono un punto di appoggio per instaurare una cultura della sicurezza nell'insieme della società. Le parti interessate potranno così integrare la sicurezza nella progettazione e nell'utilizzazione di tutti i sistemi e di tutte le reti d'informazione. Le Linee guida propongono che tutte le parti interessate adottino e incoraggino una "cultura della sicurezza" per orientare la riflessione, la decisione e l'azione concernenti il funzionamento dei sistemi e delle reti d'informazione.

II. FINALITA'

Lo scopo delle Linee guida è di:

- Estendere all'insieme delle parti interessate una cultura della sicurezza quale mezzo di protezione dei sistemi e delle reti d'informazione.
- Rafforzare la sensibilità rispetto ai rischi per i sistemi e le reti d'informazione, alle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi, nonché alla necessità di adottarli e di attuarli.
- Favorire una maggiore fiducia delle parti nei confronti dei sistemi e delle reti d'informazione e nel modo in cui sono forniti ed utilizzati.
- Creare un assetto generale di riferimento che aiuti le parti interessate a comprendere la natura dei problemi legati alla sicurezza e a rispettare i valori etici nell'elaborazione e nell'attuazione di politiche, pratiche, azioni e procedure coerenti per la sicurezza dei sistemi e reti d'informazione.
- Incoraggiare fra tutte le parti interessate, la cooperazione e la condivisione d'informazioni adeguate all'elaborazione e all'attuazione di politiche, pratiche, azioni e procedure intese alla sicurezza.
- Promuovere la presa in considerazione della sicurezza quale obiettivo rilevante per tutte le parti interessate associate all'elaborazione e all'attuazione di norme.

III. PRINCIPI

I nove principi di seguito presentati sono complementari e devono essere considerati come un insieme. Essi riguardano le parti interessate a tutti i livelli, compreso quello politico e operativo. Secondo quanto indicato dalle Linee guida, le responsabilità delle parti interessate variano secondo il ruolo da loro assunto. Tutte le parti interessate saranno assistite con interventi di sensibilizzazione, d'istruzione, di scambi d'informazione e di formazione per facilitare una migliore comprensione degli argomenti di sicurezza e l'adozione di migliori pratiche in tale settore. Gli sforzi tesi a rafforzare la sicurezza dei sistemi e delle reti d'informazione devono rispettare i valori di una società democratica, in particolare l'esigenza di una libera ed aperta circolazione

dell'informazione e i principi di base del rispetto della vita privata delle singole persone.[1]

1) Sensibilizzazione

Le parti interessate devono essere consapevoli della necessità di tutelare la sicurezza dei sistemi e delle reti d'informazione e delle azioni che possono intraprendere per rafforzare la sicurezza.

La sensibilizzazione sui rischi e sulle protezioni disponibili, è la prima linea di difesa per assicurare la sicurezza dei sistemi e delle reti d'informazione. I sistemi e le reti d'informazione possono essere sottoposti a rischi interni ed esterni. Le parti interessate non solo devono sapere che le falle in materia di sicurezza, possono gravemente incidere sull'integrità dei sistemi e delle reti che controllano ma devono essere anche consapevoli che a causa dell'interconnettività e dell'interdipendenza tra sistemi, essi possono potenzialmente danneggiare le altre parti. Le parti interessate devono riflettere alla configurazione del loro sistema, agli aggiornamenti disponibili per quest'ultimo, allo spazio occupato dal loro sistema nelle reti, alle buone pratiche che possono attuare per rafforzare la sicurezza, nonché ai bisogni delle altre parti interessate.

2) Responsabilità

Le parti interessate sono responsabili della sicurezza dei sistemi e delle reti d'informazione.

Le parti interessate dipendono da sistemi e da reti d'informazione locali e globali interconnessi. Esse devono essere consapevoli della loro responsabilità rispetto alla sicurezza di tali sistemi e reti ed esserne individualmente responsabili in funzione del loro ruolo. Esse devono regolarmente esaminare e valutare le proprie politiche, pratiche, misure e procedure per verificare se siano adeguate al loro ambiente. Coloro che sviluppano, progettano e forniscono prodotti e servizi devono rispondere all'esigenza di sicurezza dei sistemi e delle reti e diffondere informazioni

---

1. In aggiunta alle presenti Linee guida sulla sicurezza, l'OCSE ha elaborato una serie di raccomandazioni integrative concernenti altri aspetti rilevanti della società globale dell'informazione. Esse riguardano la sfera privata (Linee guida sulla tutela della vita privata e i flussi transfrontalieri di dati a carattere personale, OCSE 1980) e la crittografia (Linee guida per la tutela della politica di crittografia, OCSE, 1997). Le presenti Linee guida sulla sicurezza devono essere lette insieme con le Linee guida menzionate più sopra.

adeguate, in particolare tempestivi aggiornamenti affinché gli utenti siano in grado di comprendere meglio le funzioni di sicurezza dei prodotti e dei servizi e le loro responsabilità in materia.

3) Risposta

Le parti interessate devono operare tempestivamente e in uno spirito di cooperazione per prevenire, rilevare e rispondere agli incidenti di sicurezza.

A causa dell'interconnettività dei sistemi e delle reti d'informazione e della tendenza mostrata dai danni a diffondersi, rapidamente ed in modo molto esteso, le parti interessate devono reagire agli incidenti di sicurezza con prontezza e con spirito di cooperazione. Esse devono scambiare, in maniera adeguata, le informazioni di cui dispongono sulle minacce e vulnerabilità e devono creare procedure per una rapida ed efficace cooperazione volta a prevenire e a rilevare gli incidenti di sicurezza e a rispondervi. Ciò potrebbe comportare scambi d'informazioni e una cooperazione transfrontaliera, ove autorizzato.

4) Etica

Le parti interessate devono rispettare i legittimi interessi delle altre parti.

I sistemi e le reti d'informazione sono presenti ovunque nelle nostre società e, le parti interessate debbano essere consapevoli del fatto che la loro azione o inazione può causare danni ad altrui. Un comportamento etico è quindi indispensabile e le parti interessate devono adoperarsi per elaborare e adottare pratiche esemplari e incoraggiare comportamenti che tengano conto degli imperativi di sicurezza e che rispettino gli interessi legittimi delle altre parti interessate.

5) Democrazia

La sicurezza dei sistemi e delle reti d'informazione deve essere compatibile con i valori fondamentali di una società democratica.

La sicurezza deve essere assicurata nel rispetto dei valori riconosciuti dalle società democratiche e, in particolare la libertà di scambiare pensieri e idee, della circolazione dell'informazione, la riservatezza dell'informazione e delle comunicazioni, la riservatezza delle informazioni a carattere personale, l'apertura e la trasparenza.

6) Valutazione dei rischi

Le parti interessate devono procedere a valutazioni dei rischi.

La valutazione dei rischi consente d'individuare le minacce e le vulnerabilità e deve essere sufficientemente estesa per coprire l'insieme dei principali fattori interni ed esterni quali la tecnologia, i fattori fisici e umani, le politiche e i servizi forniti da terzi che hanno implicazioni sulla sicurezza. La valutazione dei rischi consentirà di determinare il livello accettabile di rischio e, faciliterà l'istituzione di misure di controllo adeguate per gestire il rischio di pregiudizio per i sistemi e le reti d'informazione secondo la natura e il valore dell'informazione da proteggere. La valutazione dei rischi deve tenere conto dei pregiudizi sugli interessi altrui o causati ad altrui, resi possibili dalla sempre più estesa interconnessione dei sistemi informativi.

7) Concezione e applicazione della sicurezza

Le parti interessate devono integrare la sicurezza quale elemento essenziale dei sistemi e delle reti d'informazione.

I sistemi, le reti e le politiche devono essere adeguatamente concepiti, applicati e coordinati per massimizzare la sicurezza. Uno degli assi più importanti, ma non esclusivo, di tale sforzo si concentra sulla concezione e sull'adozione di misure di protezione e delle soluzioni adeguate per prevenire o limitare i possibili pregiudizi legati alle vulnerabilità e alle minacce identificate. Le misure di protezione e le soluzioni devono essere allo stesso tempo, tecniche e non tecniche e commisurate al valore dell'informazione nei sistemi e reti d'informazione dell'organizzazione. La sicurezza deve essere un elemento fondamentale dell'insieme dei prodotti, servizi, sistemi e reti e deve far parte integrante della concezione e dell'architettura dei sistemi. Per l'utente finale, la concezione e l'attuazione della sicurezza servono essenzialmente a selezionare e configurare prodotti e servizi per i propri sistemi.

8) Gestione della sicurezza

Le parti interessate devono adottare un approccio globale della gestione della sicurezza.

La gestione della sicurezza deve essere basata sulla valutazione dei rischi ed essere dinamica e globale, per coprire tutti i livelli di attività delle parti interessate e tutti gli aspetti dei loro interventi. Essa deve altresì anticipare e includere le risposte alle minacce emergenti, la prevenzione, la rilevazione e la soluzione agli incidenti, la riattivazione dei sistemi, la

manutenzione permanente, il controllo et l'audit. Le politiche di sicurezza dei sistemi e delle reti d'informazione, le pratiche, le azioni e le procedure in materia di sicurezza devono essere coordinate ed integrate per creare un coerente sistema di sicurezza.

9) Rivalutazione

Le parti interessate devono esaminare e rivalutare la sicurezza dei sistemi e delle reti di informazione e introdurre adeguate modifiche nelle loro politiche, pratiche, azioni e le procedure di sicurezza.

Nuove o mutevoli vulnerabilità e minacce sono costantemente scoperte. Tutte le parti interessate devono permanentemente riesaminare, rivalutare e modificare tutti gli aspetti della sicurezza per affrontare tali rischi evolutivi.

RACCOMANDAZIONE DEL CONSIGLIO CONCERNENTE LE LINEE GUIDA SULLA SICUREZZA DEI SISTEMI E DELLE RETI D'INFORMAZIONE

VERSO UNA CULTURA DELLA SICUREZZA

Il CONSIGLIO,

Vista la Convenzione relativa all'Organizzazione per la Cooperazione e lo Sviluppo Economico del 14 dicembre 1960 e in particolare, visti i suoi articoli 1 b), 1 c), 3 a) et 5 b) ;

Vista la Raccomandazione del Consiglio concernente le Linee guida sulla protezione della vita privata e su i flussi transfrontalieri di dati di carattere personale, del 23 settembre 1980 [C(80)58(Final)] ;

Vista la Dichiarazione su i flussi transfrontalieri di dati adottata dai governi dei Paesi membri dell'OCSE, dell'11 aprile 1985 [C(85)139, Allegato] ;

Vista la Raccomandazione del Consiglio relativa alle Linee guida sulla politica di crittografia, del 27 marzo 1997 [C(97)62/FINAL] ;

Vista la Dichiarazione ministeriale relativa alla protezione della vita privata sulla rete mondiale, del 7-9 dicembre 1998 [C(98)177/FINAL, Allegato] ;

Vista la Dichiarazione ministeriale sull'autenticazione per il commercio elettronico, del 7-9 dicembre 1998 [C(98)177/FINAL, Allegato] ;

Riconoscendo che i sistemi e le reti d'informazione sono sempre più adoperati e acquisiscono una crescente valenza per i governi, le imprese, le altre organizzazioni e i singoli utenti;

Riconoscendo che il crescente ruolo svolto dai sistemi e dalle reti d'informazione nella stabilità e l'efficienza delle economie nazionali e degli scambi internazionali, e nella vita sociale, culturale e politica, e l'accentuarsi della dipendenza nei loro confronti impongono particolari sforzi per proteggere e favorire la fiducia nei loro confronti;

Riconoscendo che i sistemi e le reti d'informazione e il loro espandersi al livello mondiale conducono a nuovi e ad accresciuti rischi;

Riconoscendo che i dati e le informazioni conservati o trasmessi per il tramite di reti d'informazione, sono esposti a minacce dovute ai vari mezzi che consentono di accedere senza permesso, all'utilizzazione, all'illecita appropriazione, all'alterazione, alla trasmissione di codici malevoli, al rifiuto di servizio o alla distruzione, e richiedono adeguate misure di protezione;

Riconoscendo la necessità di un'ulteriore sensibilizzazione su i rischi che incidono su i sistemi e sulle reti d'informazione e sulle politiche, pratiche, azioni e procedure disponibili per affrontare tali rischi e di incoraggiare adeguati comportamenti in quanto costituiscono una tappa essenziale nello sviluppo di una cultura della sicurezza ;

Riconoscendo la necessità di rivedere le politiche, le pratiche, azioni e procedure attuali per adoperarsi affinché rispondano adeguatamente alle sfide in continuo mutamento, poste dalle minacce alle quali sono esposti i sistemi e le reti d'informazione ;

Riconoscendo il comune interesse a incoraggiare la sicurezza dei sistemi e delle reti d'informazione mediante una cultura della sicurezza che incoraggi un coordinamento e una cooperazione internazionale adeguati, per rispondere alle sfide poste dai pregiudizi che le falle di sicurezza possono causare alle economie nazionali, agli scambi internazionali, nonché alla partecipazione alla vita sociale, culturale e politica.

Riconoscendo inoltre che le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza*, allegate alla presente Raccomandazione, sono di applicazione volontaria e non incidono sui diritti sovrani degli Stati ;

E riconoscendo che lo scopo delle presenti Linee guida, non è quello di suggerire che esiste una qualsiasi e unica soluzione in materia di sicurezza, né tantomeno d'indicare quali politiche, pratiche, azioni e procedure particolari siano adeguate ad una data situazione, quanto di fornire un assetto più generale di principi che sia in grado di favorire una migliore comprensione sul modo in cui le parti interessate, possono allo stesso tempo usufruire dello sviluppo di una cultura della sicurezza e contribuirvi;

PRECONIZZA l'attuazione delle presenti *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza* dai governi, dalle imprese, dalle altre organizzazioni e dai singoli utenti che sviluppano, possiedono, forniscono, gestiscono, procedono alla manutenzione e utilizzano sistemi e reti d'informazione;

RACCOMANDA ai Paesi Membri :

Di elaborare nuove politiche, pratiche, azioni e procedure o di modificare quelle esistenti per rispecchiare e prendere in conto le *Linee guida sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza,* adottando e favorendo una cultura della sicurezza, conformemente alle predette Linee guida;

Di avviare azioni di consultazione, di coordinamento e di cooperazione, a livello nazionale e internazionale, per l'applicazione delle Linee guida;

Di diffondere le Linee guida nell'insieme dei settori, pubblico e privato, in particolare presso i governi, le imprese, le altre organizzazioni e i singoli utenti, per diffondere una cultura della sicurezza, e incoraggiare tutte le parti interessate a adottare un comportamento responsabile e a adottare le necessarie misure secondo il ruolo che svolgono ;

Di mettere le Linee guida alla disposizione dei Paesi non membri il più rapidamente possibile e in maniera adeguata ;

Di procedere ogni cinque anni al riesame delle Linee guida al fine di promuovere una cooperazione internazionale sulle questioni connesse alla sicurezza dei sistemi e delle reti d'informazione ;

INCARICA il Comitato della politica dell'informazione, dell'informatica e delle comunicazioni dell'OCSE di fornire il suo sostegno all'applicazione delle Linee guida.

La presente Raccomandazione sostituisce la Raccomandazione del Consiglio sulle Linee guida per la sicurezza dei sistemi d'informazione del 26 novembre 1992 [C(92)188/FINAL].

ITER DELLA PROCEDURA

Le Linee guida sulla sicurezza sono state ultimate nel 1992 e quindi riesaminate nel 1997. Il presente esame è stato avviato nel 2001 dal Gruppo di lavoro sulla sicurezza dell'informazione e la vita privata (GLSIFP), nell'ambito di un mandato attribuito dal Comitato della Politica dell'informazione, dell'informatica e delle comunicazioni (PIIC) e accelerato a seguito della tragedia dell'11 settembre.

La stesura è stata avviata da un Gruppo di esperti del GLSIFP riunitosi a Washington, DC, il 10 e 11 dicembre 2001, a Sydney il 12-13 febbraio 2002 e a Parigi il 4-6 marzo 2002. Il GLSIFP si è riunito il 5-6 marzo 2002, il 22-23 aprile 2002 e il 25-26 giugno 2002.

Le presenti *Linee guida dell'OCSE sulla sicurezza dei sistemi e delle reti d'informazione: verso una cultura della sicurezza* sono state adottate sotto forma di Raccomandazione del Consiglio dell'OCSE nella sua 1037ª sessione, il 25 luglio 2002.

SISTEMA STATISTICO NAZIONALE
ISTITUTO NAZIONALE DI STATISTICA

RAPPORTO ANNUALE

(ESTRATTO)

La situazione del Paese nel 2003

ISTAT

3.3.4 L'uso delle tecnologie dell'informazione e della comunicazione delle imprese

Accesso al Web: Italia sotto la media Ue ...

In tutti i paesi europei[8] Internet è di gran lunga la rete di comunicazione elettronica più diffusa tra le imprese residenti, seguita a distanza dalle reti Intranet (Tavola 3.15). Nel 2003 l'accesso al Web è, nell'Unione europea, disponibile ormai alla quasi totalità delle imprese di medie e di grandi dimensioni, con percentuali di diffusione quasi ovunque superiori al 90 per cento. Leggermente più contenute, ma comunque in sensibile crescita rispetto al 2002, sono le quote di diffusione relative alle piccole imprese (con 10-49 addetti), che vanno da un minimo del 66 per cento in Portogallo ad un massimo del 97 per cento in Finlandia. In tre paesi nordici (Danimarca, Finlandia, e Svezia) più del 95 per cento delle imprese residenti dispone di un accesso al Web. Su percentuali più contenute, ma comunque superiori al 90 per cento, si attestano la Germania (95 per cento) e il Belgio (91 per cento), seguite dagli altri paesi tra cui l'Italia con l'83 per cento.

... e agli ultimi posti nell'Ue15 per diffusione di Intranet

Minore è la diffusione delle reti Intranet, che raggiunge quote superiori al 40 per cento solo in Lussemburgo (44 per cento delle imprese residenti), in Svezia (43 per cento delle imprese residenti) e in Belgio (41 per cento delle imprese residenti), mentre negli altri paesi le quote si attestano tra il 22 e il 34 per cento delle imprese residenti. L'Italia risulta essere tra i paesi con minore diffusione di reti Intranet, ma tra le imprese di grandi dimensioni (250 addetti e oltre) i valori sono allineati a quelli del resto d'Europa.

Ancora nel 2002 il commercio elettronico, sia per acquisti che per vendite via Internet, continua ad essere un fenomeno assai meno consolidato dell'accesso al Web, anche se in molti paesi gli acquisti via Internet sono praticati da circa il 20 per cento delle imprese con almeno dieci addetti.

... e commercio elettronico

Il quadro che emerge in merito alla diffusione del commercio elettronico mostra un gruppo di paesi che stacca nettamente gli altri; fra questi ultimi l'Italia, dove gli acquisti via Internet sono ancora una pratica poco utilizzata dalle imprese. In particolare sono ai primi posti in questa attività la Svezia (22 per cento delle imprese residenti con acquisti via Internet), l'Irlanda (21 per cento) e i Paesi Bassi (20 per cento) che, con altri paesi (Danimarca, Austria, Belgio, Regno Unito), formano il gruppo leader in Europa per la diffusione degli acquisti via Internet. Negli altri paesi tale modalità non raggiunge mai incidenze superiori al 15 per cento e per alcuni non arriva al 10 per cento. L'Italia, insieme a Spagna e Portogallo, si colloca in quest'ultimo gruppo, con valori nettamente inferiori a quelli del gruppo leader per tutte le classi dimensionali.

In generale nei paesi dell'Unione europea la pratica delle vendite via Internet è meno diffusa di quella degli acquisti. Solo alcuni paesi (Paesi Bassi, Finlandia, Danimarca, Belgio, Norvegia e Irlanda) registrano una diffusione di imprese con vendite via Internet relativamente elevata e compresa tra il 17 per cento e il 12 per cento). Gli altri paesi, fra cui l'Italia, denotano una situazione in cui le imprese con vendite via Internet sono ancora in numero marginale, con percentuali comprese fra l'1 per cento e il 9 per cento.

Nell'ambito del quadro che emerge dalla rilevazione armonizzata europea sull'uso delle tecnologie dell'informazione e comunicazione (Ict) nelle imprese, l'Italia occupa una posizione intermedia sia nell'accesso al Web sia nell'uso delle reti Internet, soprattutto se il confronto viene effettuato a parità di classe dimensionale. Al contrario il nostro Paese è ancora in ritardo nell'utilizzo della re-

[8] I dati si riferiscono alla terza indagine comunitaria dell'Eurostat con i paesi membri svolta nel 2003 sull'uso delle tecnologie Ict nelle imprese con oltre 10 addetti in alcuni settori del manifatturiero e dei servizi.

Tavola 3.15 - Imprese con almeno 10 addetti che utilizzano Ict e che effettuano commercio elettronico (a) per paese, tipo di utilizzo e classe di addetti - Anno 2003
(valori percentuali sul totale imprese)

CLASSI DI ADDETTI	Italia	Austria	Belgio	Danimarca	Finlandia	Germania	Irlanda	Lussemburgo	Norvegia	Paesi Bassi	Portogallo	Regno Unito	Spagna	Svezia
UTILIZZO DI INTERNET														
10-49	25	28	35	25	27	18	28	42	24	24	25	20	25	37
50-249	53	56	64	46	57	40	47	54	48	48	52	47	45	65
250 e oltre	77	81	85	80	77	65	81	64	77	74	70	70	70	90
Totale	**28**	**34**	**41**	**30**	**34**	**22**	**34**	**44**	**29**	**28**	**30**	**26**	**29**	**43**
DISPONIBILITÀ DI ACCESSO AL WEB														
10-49	81	87	90	96	97	94	83	83	87	84	66	77	79	94
50-249	96	98	98	99	100	98	96	93	96	94	87	94	93	100
250 e oltre	98	100	98	99	100	98	99	99	99	97	97	99	99	100
Totale	**83**	**89**	**91**	**97**	**97**	**95**	**86**	**85**	**88**	**86**	**70**	**80**	**82**	**95**
ACQUISTI ON LINE VIA INTERNET (b)														
10-49	4	18	18	19	13	10	19	13	....	18	7	17	2	21
50-249	3	17	22	20	15	9	27	11	....	26	11	24	2	23
250 e oltre	4	27	22	24	13	8	31	23	....	31	13	32	3	31
Totale	**3**	**19**	**19**	**19**	**14**	**10**	**21**	**13**	**....**	**20**	**8**	**18**	**2**	**22**
ACQUISTI ON LINE VIA ALTRE RETI (b)														
10-49	1	2	4	5	2	0	3	5	3	....	0	13	0	2
50-249	1	7	8	8	7	1	5	12	8	....	3	21	1	3
250 e oltre	5	18	14	20	14	4	9	13	13	....	6	38	4	19
Totale	**1**	**3**	**4**	**6**	**4**	**1**	**4**	**6**	**4**	**....**	**1**	**15**	**1**	**3**
VENDITE ON LINE VIA INTERNET (b)														
10-49	2	9	13	13	13	7	10	8	12	15	2	8	1	8
50-249	2	9	12	13	17	8	14	11	12	22	3	10	1	12
250 e oltre	6	17	18	15	15	7	18	19	11	31	6	19	3	20
Totale	**2**	**9**	**13**	**13**	**14**	**8**	**11**	**9**	**12**	**17**	**2**	**9**	**1**	**9**
VENDITE ON LINE VIA ALTRE RETI (b)														
10-49	1	2	4	4	3	1	3	5	2	....	0	10	0	3
50-249	4	9	12	13	14	5	9	10	7	....	2	24	3	9
250 e oltre	10	20	24	24	24	11	14	14	13	....	9	34	11	25
Totale	**1**	**4**	**6**	**6**	**6**	**2**	**4**	**6**	**3**	**....**	**1**	**13**	**1**	**4**

Fonte: Eurostat
(a) I settori di attività economica coperti sono: D, F, G, H, I, K, O.
(b) I dati sono riferiti all'anno 2002.

te Internet a fini di commercio elettronico. Nondimeno segnali positivi emergono in termini di dinamica interna al nostro sistema produttivo, poiché la diffusione delle Ict tra le imprese cresce nel 2003 rispetto all'anno precedente, migliorando contemporaneamente le modalità di utilizzo.

Tre imprese italiane su cinque sono informatizzate

Nel 2003 il 61 per cento delle imprese italiane era informatizzato, registrando rispetto all'anno precedente una crescita del 4,5 per cento, dovuta in gran parte alla variazione positiva del 4,8 per cento delle imprese con meno di 10 addetti, essendo le altre già informatizzate con quote superiori al 90 per cento[9] (Tavola 3.16). Dunque si vanno riducendo le differenze tra imprese delle varie dimensioni, come anche quelle tra macrosettori di attività economica. In particolare nei servizi si è registrato un significativo incremento della quota delle imprese informatizzate nei comparti meno avanzati.

Tavola 3.16 - Imprese informatizzate per tipologia di tecnologie dell'informazione e della comunicazione e classe di addetti - Anno 2003 (a) *(valori percentuali sul totale delle imprese informatizzate e variazioni percentuali rispetto all'anno precedente)*

CLASSI DI ADDETTI	Totale		Tipologia					
			Con e-mail		Con Internet		Con sito Web	
	2003	Var. %	2003	Var. %	2003	Var. %	2003	Var. %
			INDUSTRIA					
1-9 (b)	61,0	6,1	56,3	7,1	67,8	*n.a.*	22,5	2,7
10-49	95,0	1,3	78,4	1,0	84,1	4,7	49,7	4,7
50-99	99,8	0,4	94,8	0,6	96,7	1,1	76,0	1,3
100-249	99,8	0,0	98,2	0,9	98,2	1,0	83,3	4,8
250 e oltre	100,0	0,1	99,1	0,1	99,8	0,6	87,9	5,2
Totale industria	**66,7**	**5,0**	**62,1**	**4,9**	**72,1**	**n.a.**	**29,9**	**2,8**
			SERVIZI					
1-9 (b)	58,7	4,6	59,8	12,1	71,4	*n.a.*	18,4	6,8
10-49	92,5	0,3	79,8	1,8	85,3	4,9	48,2	3,3
50-99	98,5	0,1	93,6	7,6	94,8	4,4	65,4	6,1
100-249	98,6	1,7	94,9	4,6	97,3	5,4	70,0	4,8
250 e oltre	99,5	-0,2	96,4	0,9	96,5	1,2	81,6	11,8
Totale servizi	**59,6**	**4,5**	**60,7**	**11,5**	**72,1**	**n.a.**	**19,8**	**6,3**
			TOTALE					
1-9 (b)	59,0	4,8	59,2	11,3	70,9	*n.a.*	19,1	5,9
10-49	93,9	0,8	79,0	1,3	84,6	4,8	49,1	4,1
50-99	99,3	0,3	94,4	3,1	96,0	2,3	72,1	2,9
100-249	99,3	0,7	96,9	2,1	97,8	2,5	78,3	4,6
250 e oltre	99,8	0,0	98,0	0,3	98,3	0,8	85,2	7,5
Totale	**60,8**	**4,5**	**61,0**	**10,1**	**72,1**	**n.a.**	**21,7**	**5,1**

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese con almeno 10 addetti. Anni 2001-2002 e 2002-2003 e solo per la classe di addetti 1-9: Indagine sui risultati economici delle piccole e medie imprese
(a) Nel campo di osservazione sono considerate le sezioni D, E, G, H, I, K.
(b) I dati sono riferiti al 30 giugno di ciascun anno.

Aumenta l'utilizzo del pc e Internet tra gli addetti

Nel 2003 il 94,6 per cento delle imprese italiane con nove addetti e oltre aveva almeno un personal computer (pc), ma solo il 43,8 per cento degli addetti utilizzava il pc almeno una volta alla settimana per svolgere il proprio lavoro e poco più della metà di questi utilizzava computer connessi ad Internet (24,3 per cento) (Tavola 3.17). Tuttavia questi indicatori di intensità dell'uso dei pc sono migliorati notevolmente rispetto agli anni precedenti. In particolare il confronto con il 2002 mostra variazioni percentuali

[9] Per le imprese con 1-9 addetti i dati sono tratti dall'elaborazione del modulo Multiscopo associato alla rilevazione sui conti economici delle imprese attive nei settori dell'industria e dei servizi e, per le imprese con almeno 10 addetti, dalla rilevazione sull'utilizzo delle Ict da parte delle imprese, condotta dall'Istat secondo criteri armonizzati a livello Ue.

Tavola 3.17 - Addetti che usano personal computer connessi o meno a Internet per classe di addetti - Anno 2003 (a) *(valori percentuali sul totale addetti e variazione percentuale rispetto all'anno precedente)*

CLASSI DI ADDETTI	Addetti che usano pc		Addetti che usano pc connessi a Internet	
	2003	Var. %	2003	Var. %
	INDUSTRIA			
10-49	26,9	1,5	15,6	15,3
50-99	36,6	8,2	20,1	20,6
100-249	42,0	7,0	21,2	23,5
250 e oltre	49,4	3,5	21,9	-1,7
Totale industria	**37,8**	**4,2**	**19,1**	**10,0**
	SERVIZI			
10-49	47,9	4,2	31,0	23,5
50-99	49,1	5,4	31,0	18,2
100-249	52,6	8,3	33,6	21,3
250 e oltre	53,3	2,9	29,5	17,3
Totale servizi	**51,0**	**4,3**	**30,6**	**19,9**
Totale	**43,8**	**4,7**	**24,3**	**16,2**

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese con almeno 10 addetti. Anni 2001-2002 e 2002-2003

(a) Nel campo di osservazione sono considerate le sezioni D, E, G, H, I, K e la divisione 92.

consistenti, sia nell'industria sia nei servizi, della quota di addetti che usano il pc almeno una volta a settimana (+4,7 per cento) e della quota di addetti che usano pc connessi ad Internet (+16,2 per cento). Gli incrementi più consistenti si registrano nella fascia di imprese con 50-249 addetti e soprattutto tra le imprese dei servizi. Meno consistenti sono gli incrementi registrati dai due indicatori tra le grandi imprese (con 250 addetti e oltre), cosicché si restringono i differenziali tra classi dimensionali.

Imprese informatizzate: tre su cinque hanno l'e-mail, una su cinque ha un sito Web

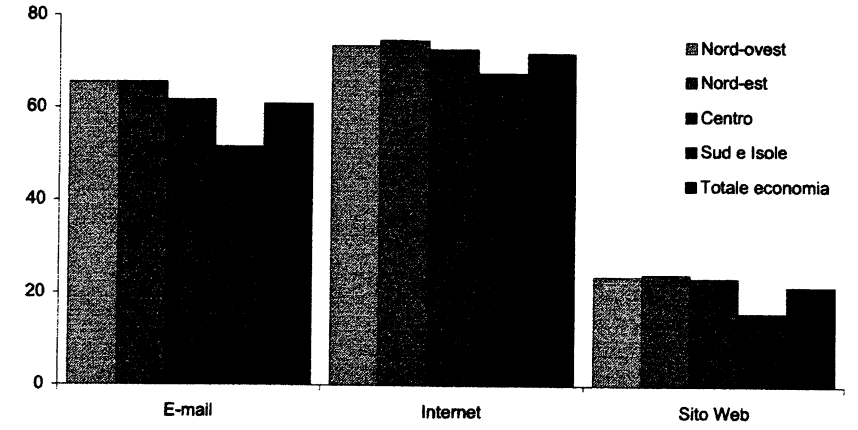
In aumento anche l'utilizzo di Internet nelle imprese informatizzate, soprattutto nei servizi e tra le imprese dell'industria con 10-49 addetti. Consistenti sono stati nel 2003 gli aumenti della diffusione di e-mail e siti Web: tre imprese informatizzate su cinque sono ormai dotate di posta elettronica (+10 per cento rispetto al 2002) e quasi il 22 per cento ha un sito Web (+5,1 per cento rispetto al 2002). I maggiori incrementi si sono registrati nel settore dei servizi e nella fascia di addetti 1-9, con l'eccezione delle variazioni in aumento avvenute nell'adozione di siti Web che ha interessato più intensamente le grandi imprese con oltre i 249 addetti del settore dei servizi (+11,8 per cento) (Tavola 3.16). Restano peraltro consistenti le differenze tra aree geografiche del Paese, in particolare, con riferimento al grado di diffusione della disponibilità di posta elettronica, di accesso a Internet e di dotazione di sito Web. Nondimeno le differenze vanno diminuendo grazie a tassi di variazioni superiori nel Mezzogiorno rispetto a quelli delle altre ripartizioni (Figura 3.17).

Boom della connessione veloce a Internet

Le imprese informatizzate con Internet stanno di anno in anno sostituendo l'utilizzo del modem (dal 39,5 per cento del 2002 al 36,5 per cento del 2003) a favore di una connessione più veloce a larga banda, in particolare xDSL, che ha raggiunto nel 2003 il 36,7 per cento, registrando un incremento del 103 per cento rispetto all'anno precedente. In generale la connessione Isdn è comunque ancora quella più utilizzata anche se la sua quota relativa è scesa dal 54,6 per cento del 2002 al 45,2 per cento del 2003. Tuttavia le modalità di connessione veloce sono già preferite all'Isdn dalla maggioranza delle imprese con almeno 50 addetti, sia dell'industria sia dei servizi (Tavola 3.18).

Solo una piccola parte delle imprese informatizzate italiane effettua transa-

Figura 3.17 - Imprese informatizzate per tipologia di Ict utilizzata e per ripartizione geografica - Anno 2003 *(valori percentuali)*



Fonte: Istat, Rilevazione sulle tecnologie dell'informazione della comunicazione nelle imprese con almeno 10 addetti

Tavola 3.18 - Tipologie di connessione a Internet per classe di addetti - Anno 2003 *(valori percentuali sul totale imprese informatizzate connesse a Internet e variazione percentuale rispetto all'anno precedente)*

CLASSI DI ADDETTI	Tipologie di connessione a Internet					
	Modem analogico		Isdn		xdsl	
	2003	Var. %	2003	Var. %	2003	Var. %
			INDUSTRIA			
10-49	41,9	-3,4	48,8	-19,8	26,3	157,1
50-99	22,4	-27,6	42,0	-35,8	53,6	133,6
100-249	19,2	-29,6	35,3	-32,4	62,5	72,3
250 e oltre	24,2	-12,0	26,3	-31,6	62,6	64,4
Totale industria	**38,8**	**-5,7**	**47,1**	**-22,0**	**31,1**	**135,4**
			SERVIZI			
10-49	34,1	-9,4	43,5	-24,7	42,1	81,0
50-99	30,4	-13,7	36,6	-31,7	57,7	79,0
100-249	28,0	-19,4	34,1	-23,4	59,1	72,8
250 e oltre	25,7	-18,1	35,7	-19,6	55,7	31,5
Totale servizi	**33,4**	**-10,2**	**42,6**	**-25,1**	**44,1**	**78,7**
Totale economia	**36,5**	**-7,6**	**45,2**	**-23,3**	**36,7**	**103,3**

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese con almeno 10 addetti. Anni 2001-2002 e 2002-2003

(a) Nel campo di osservazione sono considerate le sezioni D, E, G, H, I, K. e la divisione 92.

E-commerce: aumentano gli acquisti, diminuiscono le vendite

zioni commerciali utilizzando reti elettroniche (Internet, Edi). Nel 2002 gli acquisti on line sono stati effettuati da poco meno dell'8 per cento di esse, mentre le vendite on line sono state effettuate da circa il 4 per cento (Tavola 3.19). Le quote relative tendono ad aumentare in misura consistente con il crescere delle dimensioni di impresa, raggiungendo i valori massimi del 23 per cento circa, sia per gli acquisti sia per le vendite, nelle unità con 250 addetti e oltre. I fenomeni descritti sono largamente comuni alle imprese informatizzate sia dell'industria sia dei servizi.

Nell'ultimo anno per il quale sono disponibili i dati, anche nella diffusione del commercio elettronico si sono avuti aumenti significativi nel numero delle imprese, mentre sono diminuiti i valori scambiati.

Tavola 3.19 - Imprese che effettuano acquisti o vendite on line (a) per classe di addetti - Anno 2002 *(valori percentuali sul totale delle imprese informatizzate e variazione percentuale rispetto all'anno precedente)*

CLASSI DI ADDETTI	Acquisti on line		Vendite on line	
	2002	Var. %	2002	Var. %
	INDUSTRIA			
1-9	5,4	16,0	3,9	-2,7
10-49	6,6	13,2	2,5	-25,9
50-99	14,0	19,2	5,3	-5,4
100-249	18,7	50,2	14,5	10,2
250 e oltre	25,1	-1,3	28,5	7,6
Totale industria	***6,0***	***15,6***	***3,8***	***-6,0***
	SERVIZI			
1-9	8,1	20,8	3,7	-4,8
10-49	13,1	28,9	6,6	13,3
50-99	14,9	31,8	6,7	3,5
100-249	20,0	55,7	9,6	7,9
250 e oltre	21,3	45,8	15,8	104,2
Totale servizi	***8,3***	***21,4***	***3,9***	***-3,6***
	TOTALE ECONOMIA			
1-9	7,7	20,4	3,7	-4,5
10-49	9,5	22,6	4,2	-3,2
50-99	14,4	23,7	5,8	-1,9
100-249	19,2	52,4	12,6	9,1
250 e oltre	23,5	11,5	23,0	22,1
Totale	**7,9**	**20,6**	**3,8**	**-4,1**

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese con almeno 10 addetti. Anni 2001-2002 e 2002-2003; modulo Multiscopo dell'Indagine sui risultati economici delle piccole e medie imprese

(a) Nel campo di osservazione sono considerate le sezioni D, E, G, H, I, K.

Nel 2002 il numero delle imprese che ha effettuato acquisti on line è aumentato del 20,6 per cento rispetto all'anno precedente, mentre il numero di quelle con vendite on line ha subito una flessione del 4,1 per cento (Tavola 3.20). In termini di valori scambiati on line dalle imprese con almeno dieci addetti si sono verificate consistenti diminuzioni, pari a poco meno del 32 per cento per gli acquisti elettronici e al 23 per cento circa per le vendite.

Tavola 3.20 - Valori scambiati on line dalle imprese con oltre 10 addetti (a) per classe di addetti e ripartizione geografica - Anno 2002 *(incidenza percentuale sul valore degli acquisti o delle vendite totali e variazione percentuale rispetto all'anno precedente)*

CLASSI DI ADDETTI E RIPARTIZIONI GEOGRAFICHE	Acquisti on line		Vendite on line	
	2002	Var. %	2002	Var. %
	CLASSI DI ADDETTI			
10-49	1,2	14,5	0,3	-58,3
50-99	0,6	-53,6	0,7	-36,2
100-249	2,4	2,3	3,2	41,1
250 e oltre	4,3	-41,0	3,1	-27,5
	RIPARTIZIONI GEOGRAFICHE			
Nord-ovest	3,8	-3,3	2,6	-10,4
Nord-est	1,8	19,7	2,0	55,3
Centro	1,7	-73,2	1,0	-69,7
Sud e Isole	1,2	-44,0	1,0	-31,3
Industria	**1,9**	**-60,2**	**2,6**	**-33,7**
Servizi	**3,3**	**36,5**	**1,2**	**42,9**
Totale	**2,6**	**-31,8**	**2,0**	**-22,7**

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese con almeno 10 addetti. Anni 2001-2002 e 2002-2003

(a) Nel campo di osservazione sono considerate le sezioni D, E, G, H, I, K e la divisione 92.

I servizi richiesti tramite Internet alle pubbliche amministrazioni

Internet ha offerto la possibilità di migliorare i canali di relazione delle imprese con la Pubblica amministrazione grazie al miglioramento dei tempi, delle modalità di trasferimento dei dati e dei livelli di interazione.

I servizi richiesti dalle imprese vanno dalla semplice fornitura di informazioni on line all'accesso a pratiche amministrative, alla partecipazione a gare di appalto on line (e-procurement) *fino ai pagamenti on line.*

Secondo i dati della rilevazione sull'utilizzo delle Ict nelle imprese nel 2003 i servizi on line delle amministrazione pubbliche più richiesti dalle aziende sono quelli informativi (Tavola 3.21). L'82,6 per cento delle imprese con connessione ad Internet richiede tali servizi con un picco superiore al 90 per cento per le imprese con 100 addetti ed oltre e con una maggiore incidenza nelle imprese residenti nel Sud e Isole (84,7 per cento).

Ma la domanda di servizi pubblici on line si manifesta anche con l'accesso a pratiche amministrative (24,9 per cento delle imprese), con l'effettuazione di pagamenti on line (16 per cento) e nella partecipazione al servizio di e-procurement *(10,4 per cento). Nel complesso questi servizi, che richiedono un maggiore sforzo in termini di interazione e sicurezza, sono ancora molto meno diffusi della semplice erogazione di informazioni.*

Le imprese con 250 addetti ed oltre sono quelle che più diffusamente utilizzano i servizi pubblici on line, mentre a livello territoriale sono le imprese del Mezzogiorno ad utilizzarle, in particolare nel caso delle operazioni di e-procurement.

Rispetto all'anno precedente, nel 2003 le imprese mostrano una crescita notevole della domanda di informazioni on line, con picchi per le imprese con 10-49 addetti e per quelle del Mezzogiorno. L'accesso alle pratiche amministrative registra variazioni più elevate per le grandi imprese (250 addetti ed oltre) e per quelle residenti nelle regioni del Centro.

Per le operazioni di e-procurement *e i servizi di pagamento on line sono le imprese medio-grandi e quelle del Mezzogiorno a mostrare le dinamiche migliori.*

*Nel complesso si stanno affermando servizi avanzati quali l'*e-procurement *e i pagamenti on line e nel processo di crescita le imprese del Mezzogiorno acquistano sempre maggiore importanza, trovando in Internet un canale di contatto con la Pubblica amministrazione più interessante di quelli tradizionali.*

Tavola 3.21 - Servizi on line delle pubbliche amministrazioni richiesti dalle imprese - Anni 2002 e 2003
(valori e scarti percentuali)

	Ottenere informazioni		Partecipare a operazioni di e-procurement (gare telematiche, negozi elettronici, market place)		Accedere a pratiche amministrative (concess., autorizzaz., licenze, brevetti ecc.)		Effettuare pagamenti on line nei confronti dell'amministrazione	
	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)
SETTORI								
Industria e costruzioni	82,2	7,5	11,1	3,3	23,8	3,8	15,5	0,1
Servizi	83,3	8,5	9,4	5,5	26,5	4,8	16,8	3,7
Totale	82,6	8,0	10,4	4,2	24,9	4,3	16,0	1,6
CLASSI DI ADDETTI								
10-49	81,5	8,6	9,9	3,9	23,6	4,0	15,5	1,4
50-99	88,5	5,1	12,6	7,7	29,6	5,6	18,9	3,9
100-249	91,4	3,7	14,1	4,0	34,8	3,0	19,2	0,1
250 e oltre	91,9	5,6	17,9	5,6	43,0	12,1	20,7	4,3
RIPARTIZIONI GEOGRAFICHE								
Nord-ovest	83,6	7,3	8,2	2,5	24,4	3,7	16,6	1,2
Nord-est	80,0	6,8	9,3	4,5	25,9	4,8	15,6	1,7
Centro	83,0	8,4	10,6	2,9	25,6	6,1	14,9	1,2
Mezzogiorno	84,7	11,5	16,5	8,7	23,3	2,0	16,5	3,2

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese. Anni 2002 e 2003
(a) Percentuale di imprese con connessione a Internet nel 2003.
(b) Variazione delle quote fra 2002 e 2003 calcolata rispetto a settori omogenei. Non sono inclusi i settori delle costruzioni, istruzione, sanità e dello smaltimento, altre attività spettacolo, agenzie di stampa, biblioteche, musei, archivi, attività sportive, altre attività ricreative e dei servizi.

Le attività tra imprese e banche tramite Internet

Il successo di Internet nei rapporti tra banche e imprese è dovuto principalmente all'opportunità di svolgere le tradizionali operazioni bancarie direttamente dai computer dell'impresa connessi a Internet, grazie all'affermazione di affidabili sistemi di sicurezza informatica.

Oggi le opportunità offerte dall'integrazione delle reti informatiche banche-imprese su Internet superano lo schema tradizionale di corporate banking *interbancario, che, già preesistente a Internet, concentrava in sé le interazioni telematiche. Le nuove funzionalità offerte da Internet consentono un'integrazione più articolata fra i sistemi di rete delle imprese e delle banche, rendendo disponibile un ventaglio più ampio di servizi finanziari sia informativi che dispositivi.*

L'indagine sulle tecnologie dell'informazione e della comunicazione nelle imprese ha contribuito all'osservazione delle imprese connesse a Internet che utilizzano i canali telematici per interagire con le banche secondo la tipologia di servizio adottato (Tavola 3.22).

I risultati riferiti al 2003 mostrano la notevole diffusione dei servizi informativi on line, adottati dal 75,2 per cento delle imprese con connessione a Internet, in special modo da quelle di medie dimensioni. I servizi di incasso e pagamento riscuotono nel complesso un successo assai ampio, poiché il 61,1 per cento delle imprese con connessione a Internet li ha utilizzati nel 2003. La loro diffusione è più marcata nel settore dell'industria, nelle imprese di medie dimensioni e nelle regioni settentrionali. Inoltre crescono notevolmente nel 2003 rispetto al 2002. Gli scambi di flussi elettronici per operazioni bancarie e commerciali, la tipologia di servizio più simile al tradizionale corporate banking *interbancario, sono generalmente meno diffusi, ma con punte di utilizzo tra le imprese con più di 249 addetti*

Gli altri servizi bancari, quali la richiesta di finanziamenti on line e il trading on line, *sono assai poco diffusi, né si rilevano segnali di dinamicità rispetto al 2002.*

Dal quadro complessivo emerge il successo crescente di Internet per i rapporti tra banche e imprese, centrato sull'asse portante dei servizi informativi e dei servizi di incasso e pagamento che sono sempre più diffusi e che hanno messo in secondo piano l'incidenza del corporate banking *interbancario, mentre fanno ancora fatica ad affermarsi la richiesta di finanziamenti on line e il* trading on line.

Tavola 3.22 - Imprese con almeno 10 addetti che utilizzano i servizi bancari via Internet per tipo di servizio, macrosettore e classe di addetti - Anni 2002 e 2003 *(valori e scarti percentuali)*

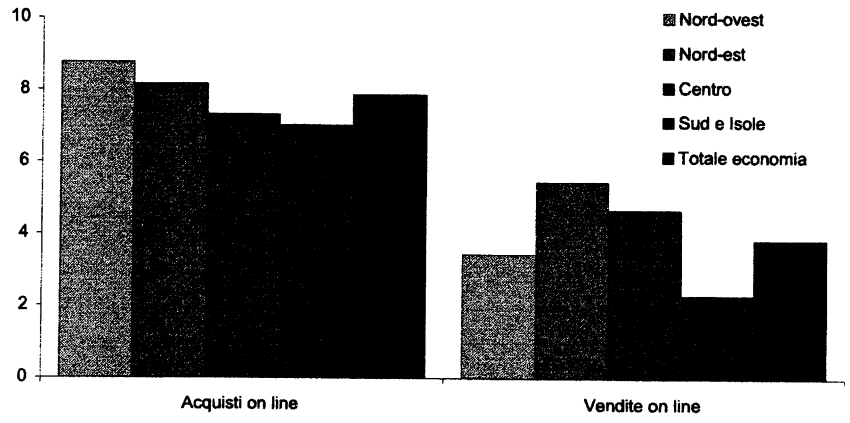
	Servizi informativi sul conto corrente		Servizi di incasso e pagamento		Scambi di flussi elettronici per operazioni bancarie e commerciali		Finanziamenti		Investimenti finanziari	
	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)	Incidenza (a)	Scarto (b)
SETTORI										
Industria e costruzioni	76,0	6,1	62,0	4,1	42,8	0,1	5,0	0,8	3,4	-0,6
Servizi	73,9	7,2	59,7	7,5	37,7	1,8	5,3	0,2	3,6	-0,1
Totale	75,2	6,5	61,1	5,5	40,7	0,7	5,1	0,5	3,5	-0,4
CLASSI DI ADDETTI										
10-49	74,4	5,9	60,1	4,6	39,1	-0,2	5,0	0,5	3,4	-0,3
50-99	81,3	10,1	68,7	10,4	50,6	6,5	5,4	0,4	3,4	-1,4
100-249	80,0	10,0	67,0	10,7	51,6	5,8	5,6	0,1	3,9	0,2
250 e oltre	76,0	12,5	61,9	13,6	53,7	7,5	6,9	2,0	3,6	-0,2
RIPARTIZIONI GEOGRAFICHE										
Nord-ovest	74,8	6,1	60,9	6,0	43,9	0,3	3,8	-0,4	3,3	-0,4
Nord-est	78,4	6,2	67,7	5,8	43,6	1,0	5,7	1,3	2,9	-0,4
Centro	76,3	7,3	57,8	4,3	38,2	0,3	6,2	1,1	4,0	0,8
Sud e Isole	69,3	8,1	54,2	6,4	32,4	3,0	5,8	0,3	4,0	-1,9

Fonte: Istat, Rilevazione sulle tecnologie dell'informazione e della comunicazione nelle imprese

(a) Percentuale di imprese con connessione a Internet nel 2003.

(b) Variazione delle quote fra 2002 e 2003 calcolata rispetto a settori omogenei. Non sono inclusi i settori delle costruzioni, istruzione, sanità e dello smaltimento, altre attività spettacolo, agenzie di stampa, biblioteche, musei, archivi, attività sportive, altre attività ricreative e dei servizi.

Figura 3.18 - Imprese che effettuano acquisti o vendite on line per ripartizione geografica - Anno 2002 *(valori percentuali sul totale imprese informatizzate)*



Fonte: Istat, Rilevazione sulle tecnologie dell'informazione della comunicazione nelle imprese con almeno 10 addetti

Queste complessive variazioni sono il risultato di performance piuttosto differenziate tra imprese dell'industria e quelle dei servizi, nonché tra le imprese di varie classi dimensionali. In particolare, tra il 2001 e il 2002 la dinamica delle imprese con commercio elettronico è stata più favorevole nei settori del terziario, sia per una maggior crescita dal lato degli acquisti sia per una minor diminuzione dal lato delle vendite. Inoltre il numero delle imprese che effettuano scambi on line è aumentato maggiormente tra quelle di dimensioni medio-grandi dal lato degli acquisti e tra quelle di grandi dimensioni dal lato delle vendite. Anche in termini di valore il settore dei servizi contribuisce positivamente alla dinamica dei valori scambiati on line, sia dal lato degli acquisti che da quello delle vendite, mentre al settore industriale va imputata la complessiva diminuzione dei valori scambiati nel 2002 rispetto all'anno precedente.

Nord-est in testa nelle vendite on line

Le differenze territoriali relative alla diffusione degli acquisti on line non sono rilevanti a livello di ripartizioni geografiche: la quota di imprese con acquisti on line decresce dal Nord al Sud e Isole ma lo scarto si mantiene limitato a 1,5 punti percentuali. Più rilevanti le differenze relative alla diffusione delle vendite on line: nel Mezzogiorno solo il 2,3 per cento delle imprese informatizzate ricorre alle vendite on line mentre nel Nord-est l'analoga quota è pari al 5,4 per cento, cosicché lo scarto tra le due aree è di 2,1 punti percentuali a favore della prima (Figura 3.18). Relativamente più consistenti sono le differenze in termini di valori scambiati nel Nord-ovest rispetto alle altre ripartizioni e in particolare al Mezzogiorno: l'incidenza degli acquisti on line è del 3,8 per cento nel Nord-ovest mentre nel Sud e Isole è dell'1,2 per cento; analoga differenza si riscontra riguardo all'incidenza delle vendite on line. Quanto infine alle variazioni dei valori scambiati per via elettronica tra il 2001 e il 2002 si registrano dinamiche differenti tra il Nord-est, che è l'unica ripartizione con consistenti incrementi dal lato sia delle vendite sia degli acquisti, e le altre ripartizioni che sono invece caratterizzate da variazioni negative dei valori scambiati.

In conclusione, il check-up periodico che l'Istat effettua sulla diffusione e l'uso delle tecnologie Ict presso le imprese italiane mostra un recupero del ritardo segnalato nelle precedenti edizioni del Rapporto, con livelli che si collocano ormai in prossimità della media Ue15. Segnali incoraggianti provengono dalle dinamiche di diffusione delle infrastrutture e dei computer e di propagazione delle modalità d'uso. Tuttavia, ancora una volta, la frammentazione del nostro sistema produttivo e la prevalenza delle microimprese sono di ostacolo alla generalizzazione dell'innovazione nelle tecnologie e nei modi di operare, soprattutto in tema di commercio elettronico e nello sviluppo di "mercati virtuali".

REGULATORY REFORM AS A TOOL FOR BRIDGING THE DIGITAL DIVIDE

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

FOREWORD

This document has been prepared under the supervision of the Information Computer and Communications Policy Division, of the Directorate for Science, Technology and Industry, and is published under the responsibility of the Secretary-General of the OECD. This work was funded by the Japan International Co-operation Agency.

TABLE OF CONTENTS

Boxes

REGULATORY REFORM AS A TOOL FOR BRIDGING THE DIGITAL DIVIDE

Abstract

The digital divide touches all regions and economies of the world and threatens to slow progress towards the goal of an all-inclusive information society. Policy makers are faced with the divide's daunting complexity but have a range of policy tools that have proven effective in expanding access throughout the world. Of these tools, regulatory reform has had perhaps the largest impact in both developed and developing economies alike.

The severity of the digital divide in OECD countries is much less than in other parts of the world, due partially to higher income levels, but also as a result of important regulatory reforms initiated over the past several decades. These reforms have paved the way for competitive markets to develop and flourish with minimal intervention.

Regulatory reform can play a key role in non-OECD economies. Policy makers in developing economies should consider the regulatory reforms that have proven the most successful in the OECD, namely liberalizing telecommunication markets, creating a separate telecommunications regulator, opening spectrum for new wireless technologies and promoting the development of human ICT capacity.

As regulatory reforms take effect, telecommunication markets become more efficient and social and economic welfare are enhanced for all stakeholders in an economy via positive externalities. Telecommunications infrastructure can play a key role in economic development, which can create a virtuous cycle where incomes improve and access increases. Telecommunication technologies have also played an important role in enhancing total factor productivity in OECD economies and in employment growth.

As recent events have shown, telecommunication networks can also play a key public safety role in an economy, especially as a tool for disaster warning and recovery efforts. Economies with under-developed telecommunication markets and networks may face higher risks in the face of future catastrophes than economies with extensive networks and public safety systems in place. As a result, this paper includes a section on the need to examine the role of regulatory reform of emergency telecommunication services as a cost-effective and essential way to ensure the optimum contribution of ICTs to disaster warning and recovery.

This paper examines one narrow aspect of the digital divide, the effects of regulatory reform on telecommunication networks. While regulatory reform is only one part of the global digital divide problem, it can play a key role in helping telecommunication markets bridge some of the gaps on their own. It is therefore imperative that policy makers consider regulatory reform as a necessary but not sufficient step towards overcoming the digital divide.

Introduction

The digital divide is an important problem that policy makers face and it is much more complex than simply building out telecommunication networks and infrastructure. The divide is the result of a wide range of social factors, including but not limited to income, education and literacy. Telecommunication infrastructure alone will not guarantee that users will be able to access and take advantage of services on the network.

In many developing economies, low literacy rates decrease the utility of a number of Internet services available to users. The lack of software and instructions in minority languages also presents a huge barrier to ICT adoption in many parts of the world. However, one of the main hindrances to ICT adoption is simply income. For many, the cost of owning a mobile handset or even making a phone call is prohibitive. Therefore, policy discussions of digital divide policy must consider social, technical and economic factors.

Because of the digital divide's complex nature, researchers often must evaluate narrow aspects of the divide and make corresponding policy suggestions. This is not to imply that other aspects of the digital divide are not important or that the digital divide can be solved with individual, narrow remedies. Rather it reflects the need for a multi-disciplinary approach to ensuring equal access to ICTs.

This paper will focus on one element that can help improve access to telecommunications in all the world's economies, regulatory reform[1]. While an economy's regulatory regime is only one aspect of the overall digital divide, proper implementation of key policies can effectively help expand networks, reduce prices, improve quality of service and increase user access. Telecommunication markets in many economies have grown and flourished under private sector control as long as certain regulatory elements were in place. This paper will examine the elements that have been the most successful throughout the OECD and look at ways in which they can be applied and adopted in developing economies as a way to expand access to telecommunications[2].

The paper will begin with a brief introduction to the digital divide, followed by key regulatory reforms that have laid the foundation for successful markets in the OECD. The paper will then highlight several non-OECD economies where regulatory reform has been successful and briefly examine how human capital investments can have long-term benefits for ICT adoption. Finally, the paper will conclude with an overview of the regulatory aspects of emergency warning and recovery.

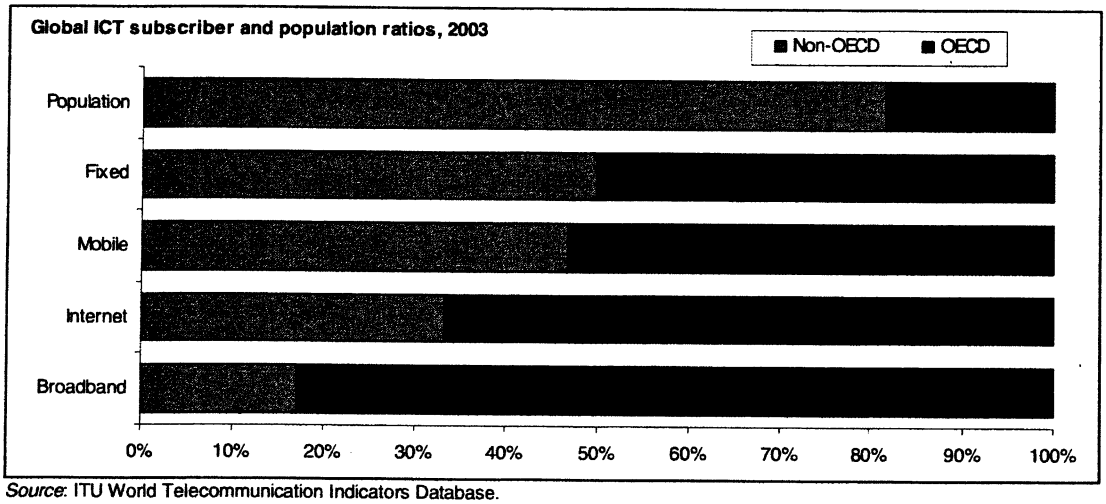
The scope of the digital divide

Telecommunication markets and regulatory policies in OECD countries have been particularly successful at extending access to rural and remote regions. While the digital divides in developing economies are often much more pronounced than those faced in the OECD, the fundamental problem remains the same: extending access to all in a society and all geographic areas. Elements from OECD country experiences can be extracted and applied in developing economies as a first step towards improving access. Policy makers in developing economies should consider the policy tools which have shown the most success throughout the OECD[3], namely liberalizing telecommunication markets, developing a sound regulatory framework and fostering of effective competition among telecommunication providers[4].

As mentioned earlier, the digital divide is a multifaceted problem, forcing policy makers to develop a multi-level approach to bridging it. Some of the problems include a dearth of physical infrastructure and telecommunication investment, difficult topography, low population densities, a lack of both general and ICT-specific skills, regulatory uncertainty and a lack of efficient market structures, institutions and competition. The situation has become much more pronounced for many developing economies, as

settlement payments from international voice calls have fallen, decreasing the availability of hard currency for network investments. Technologies such as Voice over IP (VoIP) offer benefits to users, but also reduce revenues for traditional fixed-line operators who may be responsible for providing access.

Figure 1. Figure 1. Global ICT subscriber and population ratios (OECD and Non-OECD)



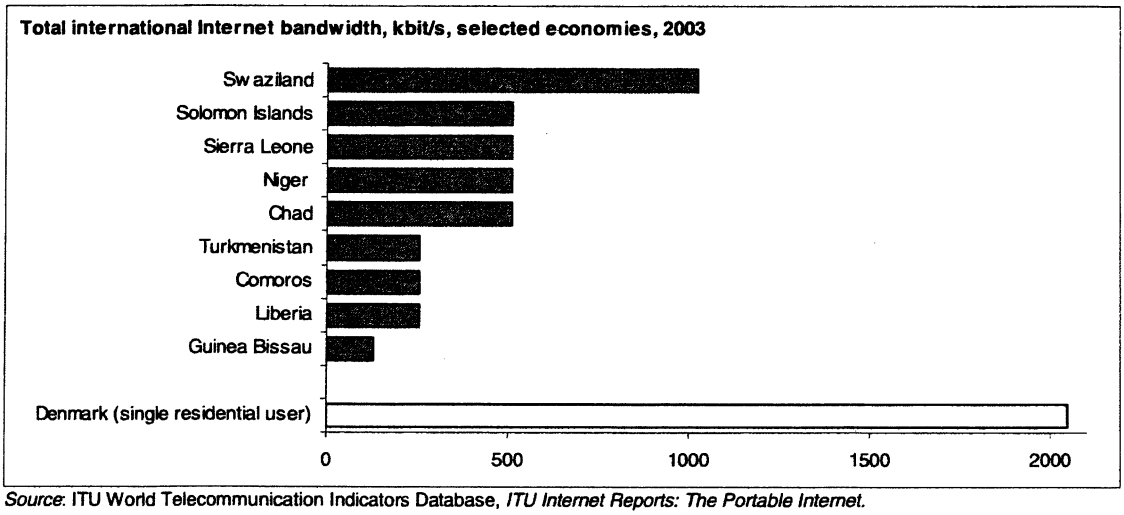
Source: ITU World Telecommunication Indicators Database.

Policy makers have been concerned about access inequalities since the introduction of telephone service more than 100 years ago. In the 1990's, the focus started shifting from providing access to voice services over fixed lines to dial-up Internet access. In 1995, 1998 and 2000, the United States Department of Commerce released its *Falling through the Net* reports that examined unequal access between rural and urban areas, race, education level, gender and age. In 2000, the OECD released *Understanding the Digital Divide*, which examined the unequal distribution of access throughout OECD countries. These reports, and many others from the same period, focused on Internet access at speeds of 14.4 to 56 kbit/s. Only a few years later, those previously characterised as "haves" as dial-up users would be considered "have nots" for the emerging broadband divide.

The digital divide has narrowed according to several measures of access around the world, although the divide varies significantly by technology (see Figure 1). OECD member countries account for only 18% of the world population but a majority of the world's fixed, mobile, Internet and broadband subscribers. Non-OECD countries have made significant gains in fixed telephony, accounting for just fewer than 50% of the world's fixed lines. The penetration of mobile telephony is also expanding quickly outside the OECD, in part due to calling-party-pays billing and pre-paid mobile minutes. Non-OECD countries make up 46% of the world's total mobile subscribers.

The gains made throughout non-OECD countries in Internet and broadband are impressive but there remains much room for increased growth. Internet subscribers in non-OECD countries accounted for only one-third of the world's Internet subscriber base in 2003. The subset of broadband subscribers shows an even greater disparity. Only 17% of the world's broadband subscribers were from outside the OECD in 2003. The significant progress among non-OECD countries in fixed and mobile telephony has taken time so as new technologies emerge, especially in OECD countries, there may be more pronounced gaps between OECD and non-OECD countries.

Figure 2. Figure 2. Total international Internet bandwidth in developing economies



Source: ITU World Telecommunication Indicators Database, *ITU Internet Reports: The Portable Internet.*

The digital divide has been most pronounced in the lowest income areas of the world. Often, the lack of basic network infrastructure significantly hampers the adoption of new end-user technologies. Internet technologies, which often require an expensive outside connection from the country to the world, have been particularly slow to reach users in low-income economies. As an example, the total population of Liberia must share an international Internet connection of just 256 kit/s, the equivalent of just one baseline residential broadband connection in the OECD. Other developing economies face similar bandwidth constraints. A single 100 Mbit/s broadband user in a leading broadband country such as Japan has access to as much international connectivity as the 45 countries with the lowest international connectivity combined[5]. Figure 2 compares the total international Internet bandwidth available in several developing economies with broadband speeds available to a single residential user in another leading broadband country, Denmark.

The problem is particularly acute in many developing economies with low Internet connectivity and little local content available to domestic users. International bandwidth demands will remain high until Internet content and services are available on servers in domestic markets. The rollout of new Internet exchanges in developing economies has helped keep some data exchange local and lowered the international bandwidth costs. In Egypt for example, investments in Internet exchange points have typically had a return on investment of six months[6]. Operators have reported that the maintenance costs are negligible compared to the dramatic cost savings of keeping Internet data exchange local.

Local content and services – especially in local languages – will be a key to increasing demand. There is a symbiotic relationship between the development of content and the development of connectivity in many OECD countries. The experiences in developing economies should be similar, with increases in connectivity facilitating the development of local content.

In addition to more international exchanges, high-speed, international infrastructure is becoming more accessible in developing economies. A recent example is the new SAT3/WASC/SAFE submarine fibre cable extending from Spain and Portugal, down the west coast of Africa, around the Cape and over to the west coast of India. Costal countries in Africa can tap into the fibre, while landlocked countries can establish connections via costal countries. International Internet connectivity via satellite and terrestrial wireless services is also falling in price.

The digital divide is not simply about a lack of cabled or wireless telecommunication infrastructure to users. The actual network interfaces such as mobile handsets, PCs and PDA-type devices are often too expensive for individual users in many developing economies. However, secondary markets for handsets and computers are helping supply much-needed terminals to users in developing economies at affordable prices. Used handsets in the developed economies, for example, are often turned in and may eventually make their way to users in developing economies, providing inexpensive, mobile connectivity for users with low monthly incomes (see Box 1).

Box 1. Used handsets fuelling mobile growth in Cambodia

Cambodia's fixed-line penetration has grown from 0.04 to 0.22 lines per 100 inhabitants in the ten years leading up to 2003. Cambodia's low fixed-line penetration rate was more of a concern in 1993 than in 2003, due to the rapid take-up of mobile telephony. In 2003, Cambodia had 750 000 mobile subscribers compared to 30 000 subscribers on the fixed-line network – a ratio of 25 mobile phone subscribers per fixed line.

Much of Cambodia's rapid take-up of mobile phones has been due to the availability of second-hand mobile handsets and pre-paid mobile phone plans. Users can purchase mobile handsets for roughly USD 10 to use with a pre-paid GSM SIM card. With Cambodia's gross national income per capita at USD 310 in 2003, the initial handset cost is roughly three per cent of annual income. Mobile tariffs are relatively inexpensive with users often spending USD 5 per month on calls.

Internet access penetration rates in Cambodia are very low due to the low number of PCs (12 000 in the country), a sporadic electrical supply, expensive access charges and a lack of Khmer-language content. While PC-based Internet access has been slow to expand, Internet access provided over a mobile phone may offer the best method for delivering data services, especially as next generation handsets start reaching secondary markets.

Source: Ministry of Posts and Communications of Cambodia

Much of the digital divide effort is focused on extending telecommunication infrastructure and supplying terminals to users. However, illiteracy and a lack of IT skills are major components of the digital divide and must be considered and addressed alongside efforts to expand the physical network.

The combination of low literacy levels and low bandwidth presents policy makers in developing economies with a bandwidth paradox. Users in developing economies often do not have literacy or ICT skills sufficient to take advantage of low-bandwidth, text communication. Illiterate ICT users require audio and video technologies to take advantage of ICTs, helping to partially explain the rapid take-up of mobile telephony in developing economies. However, users in developing economies have such limited access to bandwidth that usually their only choices for communication are text-based. The result is an entire segment of the population underserved by text-based communication technologies.

Policy makers, telecommunication operators and aid agencies must be keenly aware of complex social situations in the planning and implementation of digital divide projects. Efforts to simply supply a village with Internet access, without considering social consequences can lead to failure of the project (see Box 2).

Box 2. Peruvian Community Access Struggles

Projects to bring ICTs to rural and underserved populations can have limited success if certain social issues within the community are not sufficiently addressed. In 2000, IDRC Canada and Red Cientifica Peruana established an Internet telecentre in the Peruvian Amazon in Marakiri Bajo as a way to preserve the indigenous culture and improve access to education, markets and politics. Marakiri Bajo had no running water or electricity and the telecentre was established using a generator and satellite communication links. One of the key components of the project was a video conferencing system that allowed people to access courses from educational institutions across Peru.

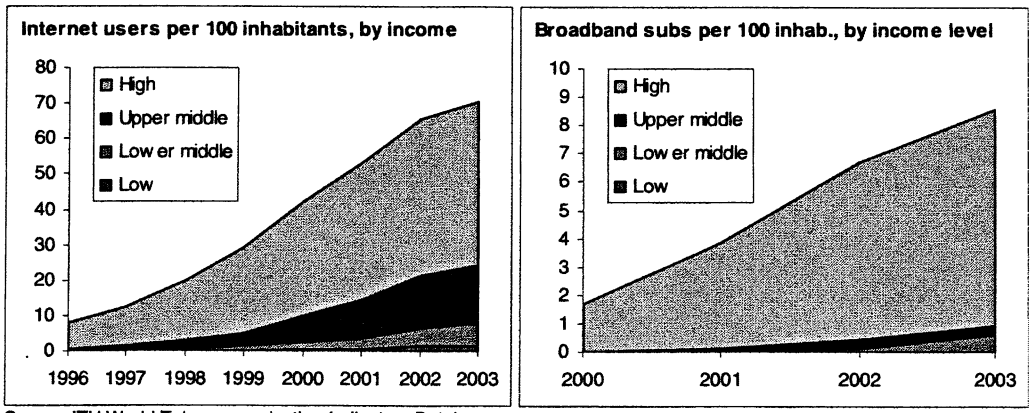
While the telecentre was intended to service the whole community of both indigenous Ashaninka and newer inhabitants, the "mesticos", it was operated and used dominantly by the Ashaninka. The result was non-Ashaninka and people in surrounding communities were reported to feel excluded from the centre and the services it offered. In August of 2001, the telecentre burned down and the circumstances around the fire were unclear. The surviving equipment was eventually put to use to power a local radio station instead of another telecentre.

Source : Bjorn Soren Gigler, Including the Excluded – Can ICTs empower poor communities? Towards an alternative evaluation framework based on the capability approach.

Digital progress

While the digital divide is a very significant problem in developing economies, recent data show that people around the world have much better access to ICTs than they did even 10 years ago, with the largest improvements in middle-income countries. This has been possible with advances in technology and regulatory reform. However, just as the connectivity for a certain technology (e.g. dial-up Internet access) improves across income levels, a new technology (e.g. broadband) appears – leaving users in developing economies continually "playing catch-up" (see Figure 3).

Figure 3. Figure 3. Internet users and broadband subscribers per 100 inhabitants worldwide



Source: ITU World Telecommunication Indicators Database.

The cycle of technological development is likely to continue along the same path: adoption and commercialization of new ICT technologies in higher-income economies, slower penetration into lower-income markets, and the subsequent development of new technologies. In such a rapidly changing market, the "technologies of the day" are less important than the overall efficiency of the market and the regulatory environment. In a well functioning market, only technologies that are economically viable and efficient

will survive. Therefore, the role of policy makers should be to create an efficient and agile market that is capable of quickly integrating new technologies and keeping prices low for consumers via competition.

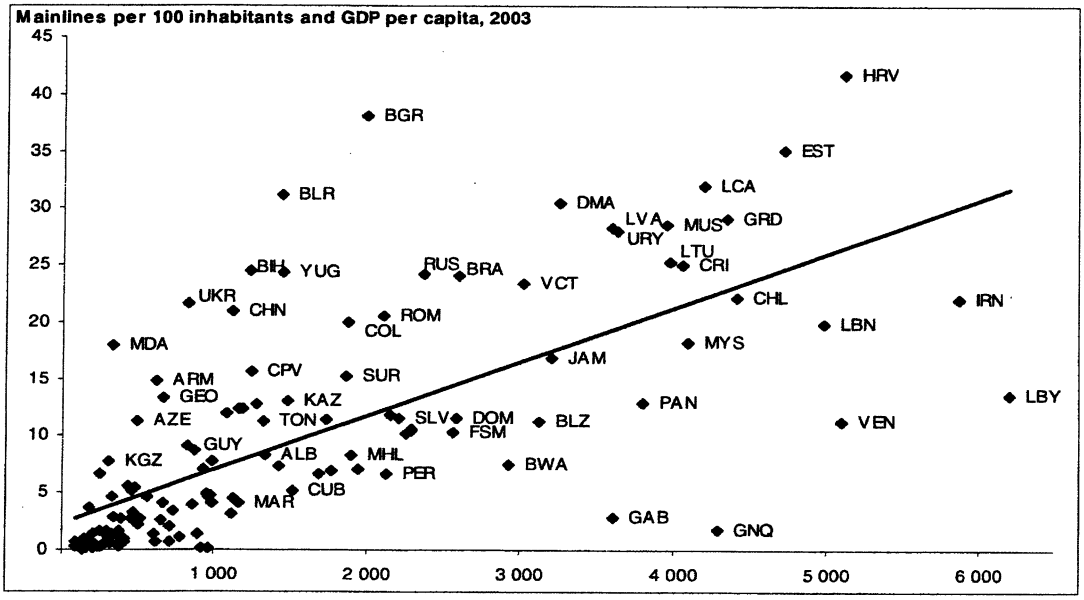
Over the past 20 years, the OECD has been urging governments to liberalize the telecommunication sectors in their countries. These policies have included setting up a regulatory framework, creating an independent and separate regulator, developing a strong foundation for regulatory action, encouraging competition throughout the sector and privatising telecommunication operators. These policies were often initially met with scepticism. However, over a period of two decades they have proven to be, on the whole, very effective.

In 2003, the 30 OECD countries accounted for 50% of the world's fixed-line subscribers, 53% of mobile subscribers, 67% of Internet subscribers, and 83% of the world's broadband subscribers. High income levels have certainly played a role in telecommunication penetration rates throughout the OECD, but sound policy, efficient markets and effective regulation have also been important components in the success.

While telecommunication liberalization is in the advanced stages throughout the OECD, policy makers in some non-OECD economies have also successfully applied the same market principles in their own economies with similar success. This paper will re-examine some of the basic policy instruments, with a focus on how policy makers outside the OECD are implementing them.

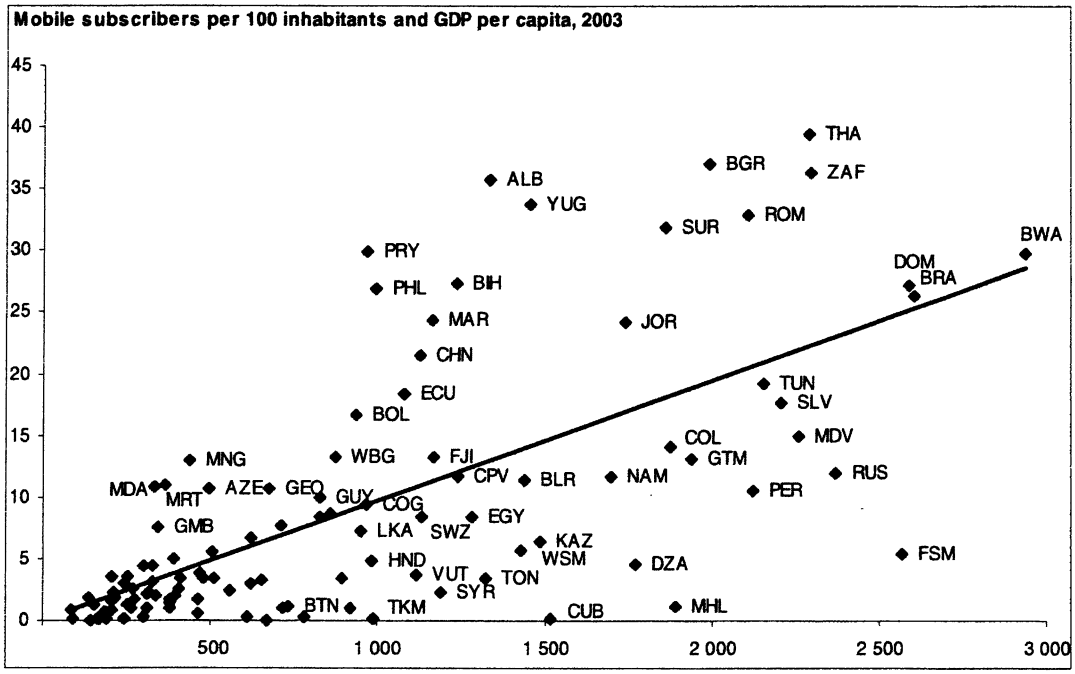
Before looking into specific policies, it is worth noting which countries have the highest telecommunication penetration rates at certain income levels. This allows policy makers to examine policy and market conditions that may have played a role in a country's ICT success. Penetration rates are only one measure of an ICT market, but it can be helpful to compare the adoption of communication technologies among countries at similar income levels. Policy makers have long noted the relationship between ICT access and GDP. Scatter plots of penetration rates over GDP can offer an effective way to see how countries compare with similar-income counterparts (see Figures 4, 5 and 6).

Figure 4. Figure 4. Fixed-line penetration and GDP per capita



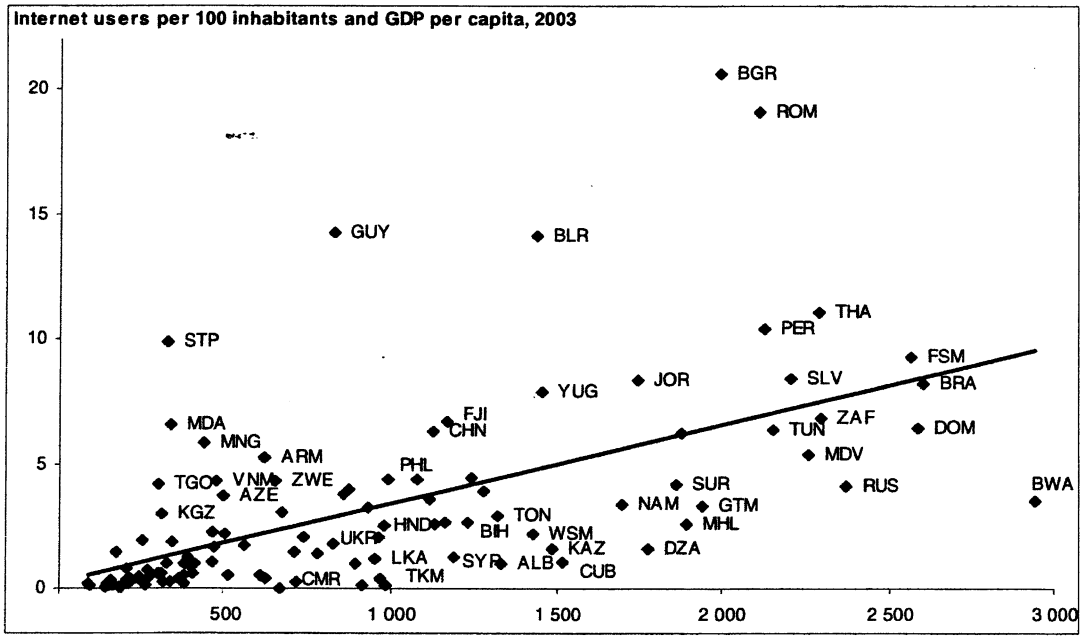
Source: ITU World Telecommunication Indicators Database.

Figure 5. Figure 5. Mobile penetration and GDP per capita



Source: ITU World Telecommunication Indicators Database.

Figure 6. Figure 6. Internet users per 100 inhabitants and GDP per capita



Source: ITU World Telecommunication Indicators Database.

Figures 4, 5 and 6 show scatter plots of various ICT subscriptions per 100 inhabitants by income level. A simple linear trend line is included for basic comparison but should not be considered a robust measure of the relationship between GDP and penetration rates. Economies are represented by their ISO 3-digit codes.

Figure 4 shows mainline penetration and GDP throughout the world in 2003. There is substantial variation among penetration rates at similar income levels with several economies having much higher penetration rates than their incomes alone would predict. The former Soviet Republics such as Armenia, Belarus, Estonia, Georgia, Latvia, Lithuania, Moldova, Ukraine and the Russian Federation all have higher penetration rates than other countries at similar income levels. At lower income levels, other examples include Cape Verde, China, Colombia, Romania, Brazil, Dominica, Mauritius, Sri Lanka, Grenada and Suriname. At higher income levels, non-OECD economies with relatively higher penetration levels include Bulgaria, St. Lucia, Bosnia and Herzegovina, St. Kitts and Nevis, Malta, Chinese Taipei, and Cyprus.

Figure 5 examines the relationship between the number of mobile subscribers per 100 inhabitants and GDP. The figure again includes a fitted trend line. Some economies in the chart have mobile penetration rates significantly higher than their levels of GDP would suggest. Examples include Paraguay, Albania, Bulgaria, Morocco, Thailand, South Africa, Romania, the Philippines, China, Ecuador, Bolivia and Mongolia. At higher income levels, economies with relatively higher penetration rates include Jamaica, Estonia, Lithuania, Seychelles, Malta, Slovenia, Chinese Taipei, and Hong Kong (China).

Figure 6 shows the relationship between GDP and Internet access. Several economies with relatively low income levels have impressive penetration levels. These include Bulgaria, Romania, Belarus, Guyana, São Tomé and Principe and Moldova. At higher income levels, economies such as Jamaica, Chile, Barbados, Latvia, Estonia, Slovenia, Chinese Taipei, Malaysia, Singapore and Hong Kong (China) have higher penetration rates than other economies at similar income levels.

The economies listed above have high ICT penetration rates for a variety of reasons, often particular to each economy. However, there are other elements of their success that are common among economies and OECD members as well. These typically include regulatory reform elements, such as market liberalization, effective competition, and the presence of a separate regulator.

Telecommunication market liberalization

The level of competition in the market is often a good indicator of telecommunication penetration rates. Economies with higher levels of competition usually benefit from lower prices and higher penetration levels. The contrast between penetration rates in monopoly and competitive markets, even within the same country can be pronounced (see Box 3).

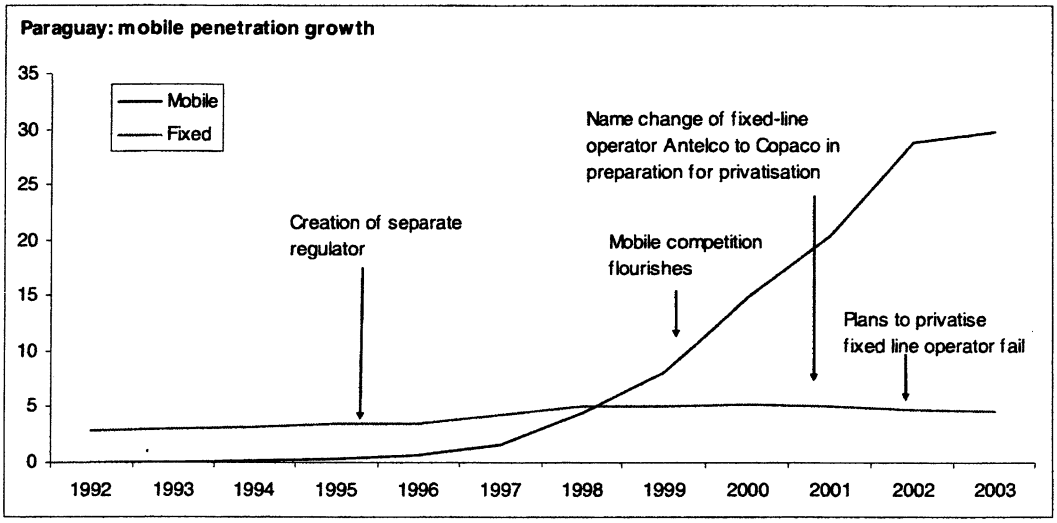
Liberalized markets in the same region and at similar income levels typically have penetration rates higher than those with non-liberalized markets. For example, the Latin American countries of Belize and Brazil have similar income levels but fixed-line penetrations vary considerably. In Belize, the incumbent operator maintains a monopoly on fixed-line provision and the penetration rate is low at only 11.3 lines per 100 inhabitants. In Brazil, the fixed-line market is considered fully competitive and the penetration rate is more than double that of Belize, at 24.1 subscribers per 100 inhabitants.

Mobile markets show similar trends. Competitive mobile markets typically show higher penetration rates than those which have not been liberalized. Jordan and Oman are good examples. Jordan's GDP per capita in 2003 was roughly USD 1800, less than one fourth of Oman's GDP per capita of USD 8 100. However, Jordan's mobile penetration rate of 22.9 in 2002 was higher than Oman at 18.3 (see Figure 7).

Box 3. Comparison of a competitive mobile and monopoly fixed-line network in Paraguay

The government in Paraguay started liberalizing the telecommunications market in 1996 with the creation of a separate regulator, Conatel. Mobile licenses were awarded and competition in the mobile market thrived, helping push mobile penetration rates towards 30 subscribers per 100 inhabitants in 2003. By contrast, the government-owned fixed-line operator still has a monopoly on the provision of fixed services. Plans to privatise the incumbent operator, Copaco (formerly Antelco), were initially delayed, and finally abandoned in June 2002. As a result, Paraguay's mobile market thrives while the fixed-line market languishes.

The efficiency of Paraguay's mobile market can be seen in regional comparisons. Paraguay's mobile penetration rate of 29.9 mobile subscribers per 100 inhabitants is just slightly under the regional average of 34.4 for the Americas. The fixed-line situation is very different. Paraguay's fixed-line penetration rate of 4.61 is much lower than the regional average of 34.5 fixed lines per 100 inhabitants.

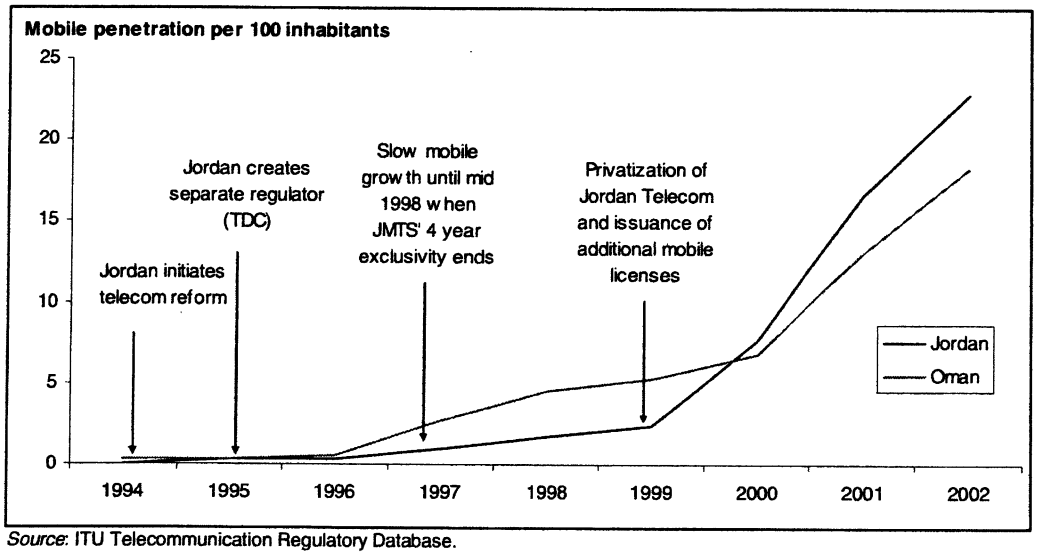


Source: ITU Telecommunication Regulatory Database

Much of Jordan's success in the mobile market can be attributed to the regulatory reforms started in 1994. Jordan lagged behind Oman in mobile penetration until competition was introduced into the mobile market in 1999. Oman's mobile growth has still been considerable, given the mobile operator's monopoly position. However, the liberalized market in Jordan eclipses Oman's growth, despite differences in income levels between the two.

Finally, markets with effective Internet competition often have higher penetration rates than their incomes alone would suggest. This can be seen in countries such as Latvia and Estonia, where penetration rates are as high as those found in many of the world's richest economies. Latvia's Internet penetration rate of 40.6 Internet users per 100 inhabitants in 2003 was higher than Chinese Taipei, France, Switzerland, Italy and Belgium despite the country having a GDP per capita of USD 3600 per year. Both Latvia and Estonia have very efficient ISP markets with a large number of licenses awarded to Internet service providers (ISPs). In 2004, Latvia had 195 ISP licenses, while Estonia had 112.

Figure 7. Figure 7. Mobile growth in Jordan and Oman



Source: ITU Telecommunication Regulatory Database.

The examples of Paraguay, Brazil, Jordan, Estonia and Latvia highlight the key role competition plays in increasing access. In the markets with competition, penetration rates increased faster than in similar markets with monopoly market structures.

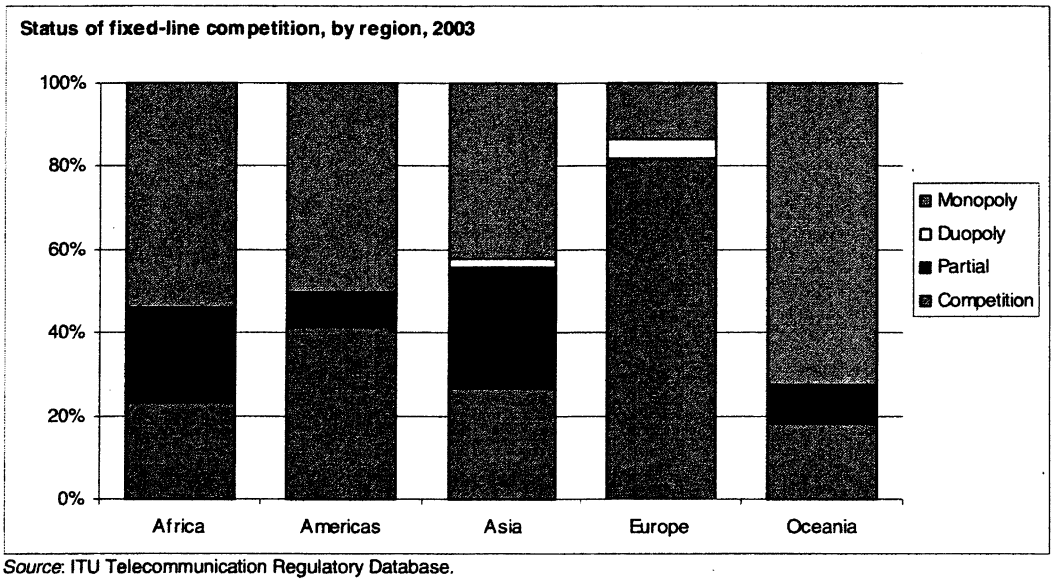
Regional statistics on the status of telecommunication markets highlight certain areas where competition has taken a greater hold than others. Figures 8 and 9 show the regional breakdown of market structure in mobile and fixed lines in 2003. At the end of 2003, slightly more than 80% of European economies had full competition in the fixed-line market. Monopoly providers operated in around 14% of economies. In Africa a majority of economies (54%) have markets with fixed-line monopolies. Only 23% of economies in Africa are fully competitive. In Asia, nearly 42% of economies still have monopoly fixed-line provision, in contrast with 55% with either partial or full competition.

Competition in the mobile sector is higher than fixed lines in all regions except for Europe. The level of full mobile competition in Africa, at 54%, is similar to the percentages for both Europe and the Americas. Competition in Africa's mobile sector helps account for Africa's robust growth in mobile services and increasing penetration levels.

On a global level, mobile markets have been traditionally more competitive than fixed-line markets. While fixed-line networks are characterized by an element of natural monopoly relating to the access network, mobile markets typically have multiple providers, each with a different frequency band assigned by the regulator. This typically allows for much more robust competition in the mobile market than fixed-lines.

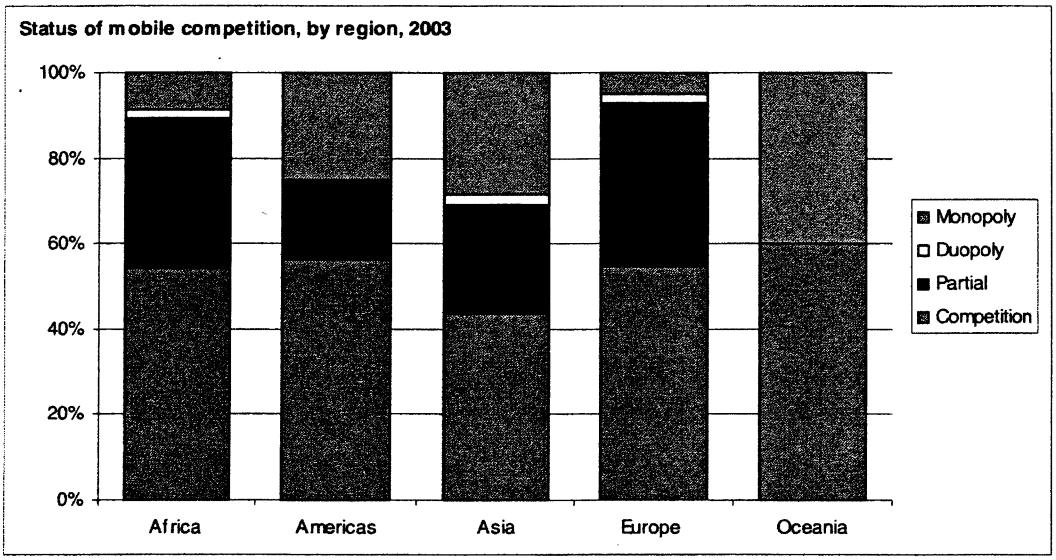
Competition in mobile markets is responsible for an innovation that has arguably played a vital role in reducing the digital divide throughout the world, pre-paid telephony. Since users in developing economies often have little or no access to credit, the introduction of pre-paid services in markets around the world has allowed users without credit to have mobile service. Pre-paid accounts now comprise 36% of all mobile accounts in the world[7].

Figure 8. Figure 8. Status of fixed-line competition



Source: ITU Telecommunication Regulatory Database.

Figure 9. Figure 9. Status of mobile competition



Source: ITU Telecommunication Regulatory Database.

Regulatory independence

As telecommunication markets evolve, so does the need for a strong, effective regulatory regime. Effective regulation is important to ensure that markets function properly and services are delivered to

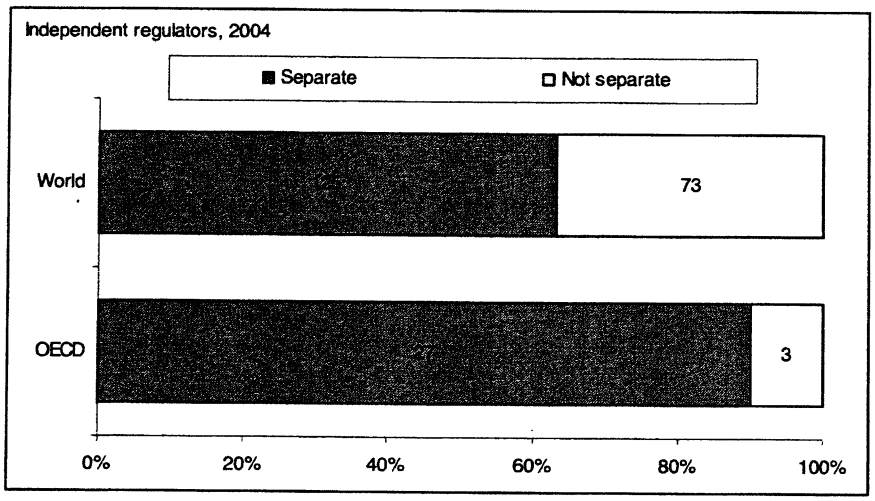
consumers and businesses efficiently and fairly. Evidence shows that one of the key elements of regulatory success is the existence of an independent and separate regulator, outside the influence of both government policy and private-sector interests.

The evolution of telecommunication regulation in developing economies is closely following earlier experiences in the OECD. In most countries of the world, telecommunication services were initially provided by the government. As the technologies improved and penetration rates increased, the limitations of monopoly provision became more pronounced.

In many countries, the first step was to separate the duties of service provision and regulation and put them into separate entities. This process is essential to promote impartiality and create a truly separate regulator who is not beholden to outside interests. The second step was to separate policy from regulatory functions ensuring that the regulator had sufficient authority to implement policy effectively.

In 2004, 90% of OECD countries had an independent regulator in comparison to 58% worldwide (see Figure 10). The role of the regulator varies from country to country, but common policy tools include privatising state-owned operators, licensing new entrants, determining interconnection policy, ensuring non-discriminatory access, setting price controls in non-competitive market segments, developing and enforcing competition regulation, and mandating universal service requirements.

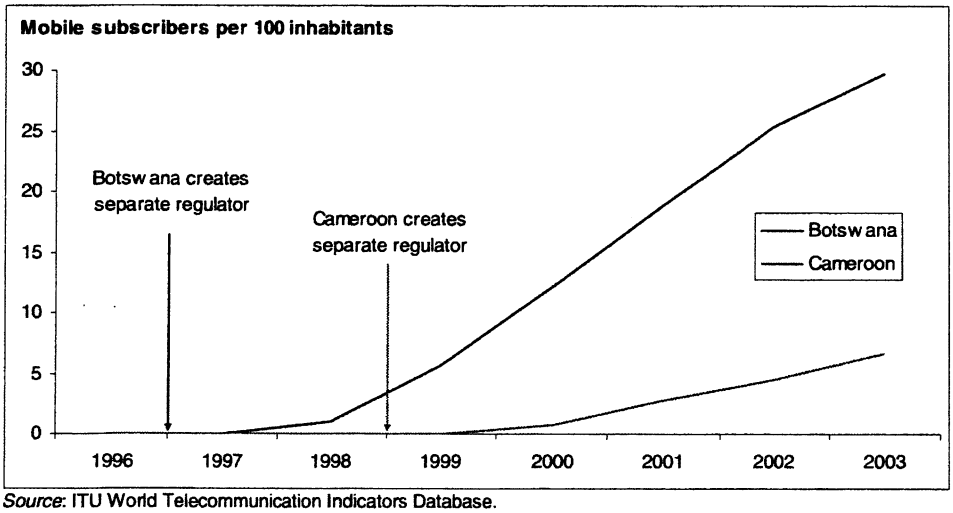
Figure 10. Figure10. The status of independent regulation in the OECD and worldwide



Source: ITU World Telecommunication Indicators Database.

Certain regions with traditionally low penetration rates have benefited from the introduction of separate regulator to oversee the development of the telecommunication market. In Africa, roughly two-thirds of economies have regulators who are separate from the government. In several African markets the introduction of a separate regulator has been immediately followed by rapid growth in mobile penetration. The examples of Cameroon and Botswana are given in Figure 11.

Figure 11. Figure 11. Growth in Africa and the creation of separate regulators



Source: ITU World Telecommunication Indicators Database.

The introduction of a separate regulator is an important first step when liberalizing a telecommunication market. However, the existence of separate regulator, in itself, does not guarantee the success of a market.

Several other elements must be in place to ensure the success of the regulatory body. First, the existing legal framework for telecommunications must be created. This usually entails the creation of a telecommunication law that facilitates the opening of the market and sets out the powers of the regulatory body. Second, the law must give the regulator the authority, autonomy, and means to effectively apply regulations in a market. These characteristics are important, especially in markets where incumbent operators have extensive political and financial power. At the same time, the regulator must have the authority to enact policies that will be vital to the development of the telecommunications market. These include, but are not limited to, mandating interconnection, unbundling the local loop and imposing open access requirements.

Regulatory reform is a process that takes time to achieve results, especially regulatory and administrative capacity building. Investment in capacity building in all countries involves initial costs but deliver high future returns.

Spectrum policy and wireless connectivity

Wi-Fi (IEEE 802.11)[8] adoption has been very high throughout the OECD as users install wireless home systems, operators roll out commercial networks and equipment manufacturers build Wi-Fi connectivity into their products. The rapid adoption of Wi-Fi has pushed prices down and allowed entrepreneurs in developing economies to use off-the-shelf equipment to quickly roll out wireless networks.

These new wireless networks usually operate in license-exempt spectrum bands. Policy makers can help spur innovation in these wireless networks by making certain frequency bands license-exempt. On a global scale, the World Radio Conference in 2003 allocated spectrum in the 5 GHz band for license-exempt use. However, the most common and least-expensive Wi-Fi equipment operates in the 2.4 GHz

band which has not been harmonized for use worldwide. Spectrum policy makers in developing economies should thus examine ways to allow the rollout of Wi-Fi based systems.

New and evolving technologies such as WiMAX (IEEE 802.16)[9] will also require new spectrum from regulators. Difficulties in obtaining spectrum for new wireless technologies will hamper the market in providing innovative solutions to the digital divide. Regulators in developing economies should examine existing spectrum allocations and work to accommodate new wireless technologies.

Success stories

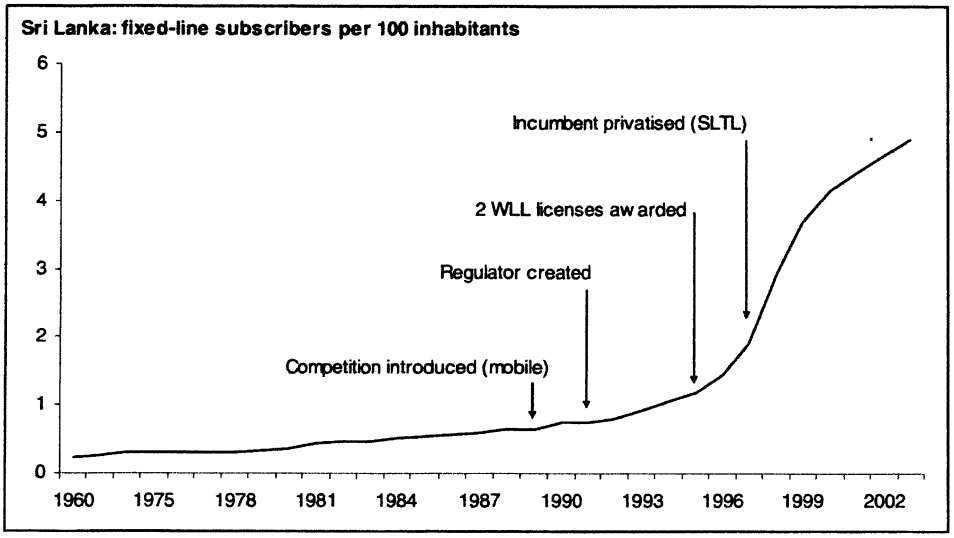
Asia has recently received considerable attention from telecommunication policy makers as Asian economies top the rankings in broadband penetration, broadband speeds, mobile penetration and mobile Internet use. Asian economies, those belonging to the OECD such as the Republic of Korea and Japan, and non-OECD economies such as Chinese Taipei and Hong Kong, China have received the most attention due to their top tier rankings. However, several developing economies in Asia have made significant progress in bridging the digital divide and building out networks. This section examines regulatory developments in three Asian countries: Sri Lanka, India and China.

The introduction of competition to markets has a profound effect on penetration rates, even when the competition comes via a different technology. Evolving wireless technologies such as WiMAX may dramatically increase the reach of backbone networks in developing economies, but other wireless technologies have already been implemented and have made a difference in competitive markets around the world.

The Telecommunications Regulatory Commission of Sri Lanka introduced competition to the fixed-line market in 1996, with the awarding of wireless local loop (WLL) licenses to Suntel and Lanka Bell. The licenses allowed each company to set up wireless last-kilometre connections to end users, and started a period of strong competition for fixed-line services. The awarding of licenses was part of a new regulatory framework put into place in 1991 with the creation of the separate regulator. The new regulatory framework and subsequent competition for fixed lines has led to rapid growth in Sri Lanka's access opportunities (see Figure 12).

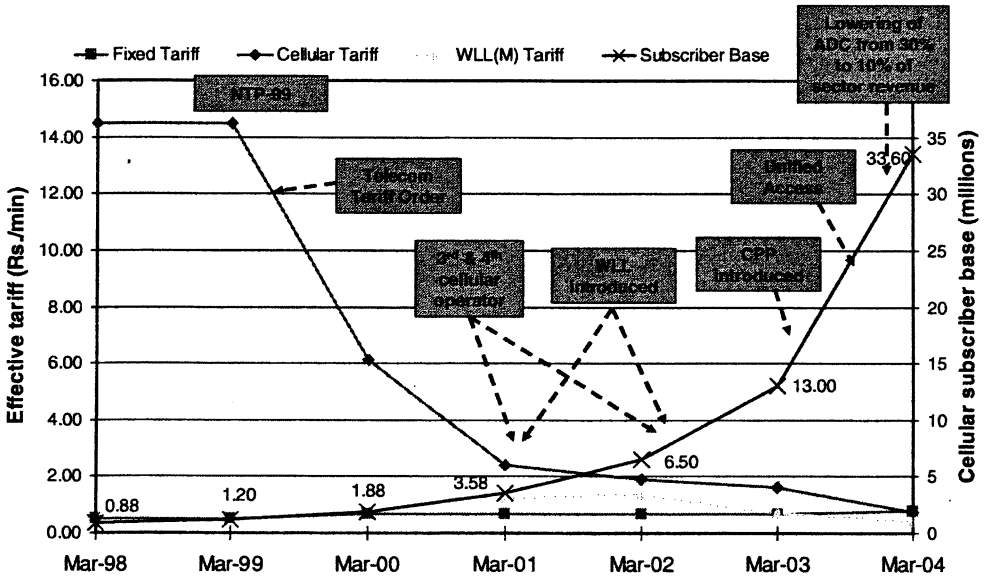
Sri Lanka's fixed-line market benefited from the competition provided by a wireless technology, highlighting the importance of inter-modal competition in telecommunication markets. As inter-modal competition continues to grow, so will the importance of technologically-neutral regulation.

Figure 12. Figure 12. Competition in Sri Lanka via wireless local loop



Sources: ITU World Telecommunication Indicators Database and http://www.comunica.org/samarajiva.html.

Figure 13. Figure 13. The effect of India's successful regulatory reforms on mobile penetration and price



Source: Telecom Regulatory Authority of India.

In India, the Telecom Regulatory Authority of India (TRAI) has completely restructured its regulatory framework to promote technological neutrality and take advantage of inter-modal competition. The decision was made, in part, due to the astounding success of several unregulated services (e.g. SMS, VoIP) that compete directly with regulated services. As a result, TRAI has been in the process of moving towards

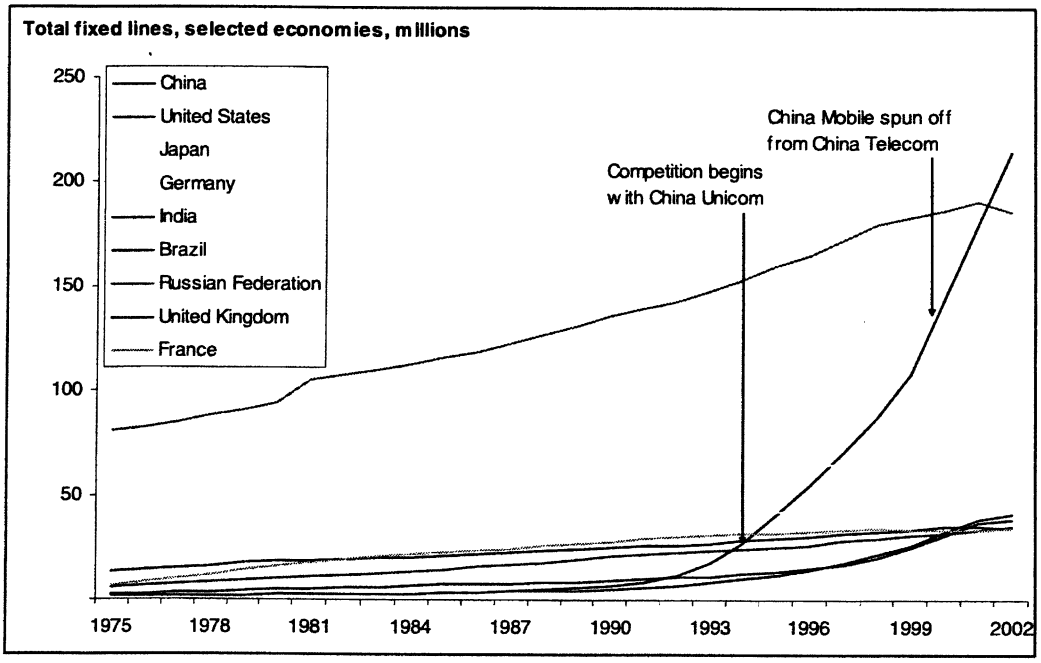
a unified licensing regime that would replace separate licensing based on technology, service or geographic area. Any licensee with one wired or wireless connection will be able to provide any service including: telephony, Internet access, broadband, television and other value-added services.

Also as part of the new regulatory framework, TRAI introduced new competition by issuing additional mobile licenses in 2001 and 2002 and awarding WLL licenses in 2002. In another important step, India moved from receiving-party-pays (RPP) to a calling-party-pays (CPP) structure in an effort to spur mobile take-up. India's reforms have been very successful, with a marked increase in mobile subscribers and a fall in mobile tariffs (see Figure 13). The reforms introduced by TRAI in India may eventually have an impact on the global telecommunication market, given India's large population and potential market size.

While India's large telecommunication market continues to grow, China now has the largest mobile and fixed-line markets in the world. In July 2004, there were 299 million fixed-line subscribers and 310 million mobile subscribers. Internet subscribers reached 87 million with a penetration rate of 6.7 subscribers per 100 inhabitants. Chinese broadband infrastructure is also growing at the rate of nearly 1 million new subscribers per month, with 18.8 million subscribers in July 2004.

Much of China's recent growth is a result of effective competition in the Chinese mobile and fixed-line markets. The Chinese government introduced competition into the market in 1994, with the creation of China Unicom. Neither the incumbent, China Telecom, nor China Unicom has been privatised but competition flourishes. The result of this competition has been a dramatic increase in both mobile and fixed access (See Figure 14).

Figure 14. Figure 14. China's regulatory reform and infrastructure growth



Source: : ITU World Telecommunication Indicators Database.

Human capacity building

Much of the research on telecommunication markets has focused on what policy makers can do to improve the amount of physical telecommunication capital in an economy. However, physical infrastructure is only one component of an efficient and vibrant telecommunications market, with human capital also playing a vital role.

Telecommunication markets are complex and require a wide range of skills from users who access the network, engineers who maintain it, and policy makers who regulate. As physical telecommunication infrastructure develops so must the capacity of users, network technicians and policy makers. High-capacity IP networks are of limited use in economies where users lack basic ICT knowledge. Up-to-date networks may fail in an economy that lacks competent technicians and engineers. Economies must also produce people with the skills to build and maintain networks, run telecommunication businesses as well as develop and enforce regulations.

Policy makers in several governments have focused on building an inclusive information society by targeting youth in schools. Programs that connect and educate students create a generation of savvy computer users who form the foundation of a vibrant telecommunication market.

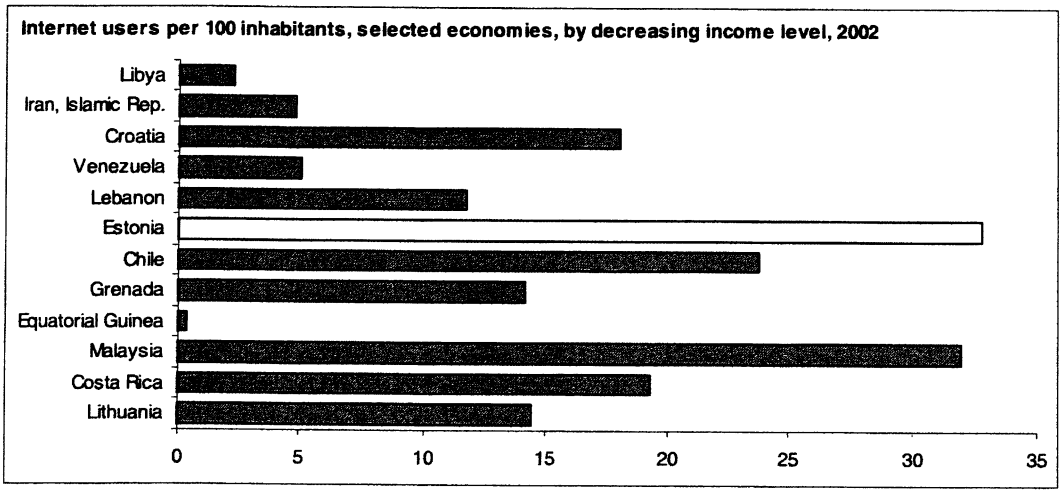
OECD countries have emphasized ICT skills in their efforts to connect all schools to the Internet, train students in ICTs and provide programs for non-students to obtain computer literacy. These efforts have paid off handsomely in countries such as Korea where a strong government push to supply ICT training to those affected by the 1997 financial crisis has helped fuel PC and broadband adoption. Policy makers in non-OECD countries have created similar plans and have boosted penetration rates. One such economy is Estonia where government initiatives aimed at promoting a computer-literate generation have been successful.

Estonian policy makers have been successful developing a broad base of ICT skills throughout the country. The government's flagship program, Tiger Leap, has successfully integrated information and communication technologies into classroom instruction, resulting in a new generation of students with computer skills who demand faster Internet connections, better content and more extensive telecommunication network coverage. In Estonia, introducing students to computers early in their studies has also helped move more students towards technical careers later.

The results have been strong impressive with Estonians achieving penetrations equal or higher than other richer countries in Europe. In June 2004, TNS Emor Internet usage surveys show that 52% of Estonians between the ages of 6 and 74 use the Internet. The same study finds that the most active Internet users are people between the ages of 12 and 24, 90% of whom use the Internet. The percentages are also high for primary school students where two-thirds of students between the ages 6 and 9 are Internet users[10].

In addition to teaching ICT skills early to students, Estonia's policy makers have made promoting ICT use a priority. One example is new street signs giving the direction and distance to the nearest public Internet access point. The signs are marked with "@ Internet", an arrow and the distance to the nearest of 700 public Internet access points across the country. The government has also taken a pro-active approach to integrating computers and telecommunications into government activities. The Estonian government has paperless "e-cabinet" meetings where government cabinet members can examine documents and cast votes via computer. Estonia's projects have largely been a success, with mobile, fixed and Internet penetration rates as high as other leading European economies (see Figure 15).

Figure 15. **Figure 15. Estonia's high Internet penetration rate among similar-income economies**



Source: ITU World Telecommunication Indicators Database.

Regulatory aspects of disaster warning and recovery

Recent natural disasters have highlighted the importance of developed, and well-functioning telecommunication markets – as well as the importance of ensuring that users around the world have access to potentially life-saving emergency telecommunication services. A number of these services fall under the authority of the regulator as components of universal service requirements. Therefore, it is important to examine how the regulatory environment may need to evolve to ensure the best emergency services are available to the largest percentage of the population as possible.

On December 26, 2004, the world's largest earthquake in forty years unleashed a powerful tsunami on nations around the Indian Ocean's rim, causing cataclysmic damage. Estimates have calculated the initial loss of life at over 150,000 people, most of whom had no advanced warning of the approaching wave. Rescue workers, aid agencies and government officials mobilized quickly to respond to the crisis while engineers worked at re-establishing communication links with affected areas. SMS messages and mobile communications proved resilient in the aftermath of the devastation.

In the weeks following the disaster, the key priorities were providing clean water, food and shelter to those affected and minimizing the threat of disease. However, many of the discussions in the press after the disaster reflected on how communication networks could be used as an advance warning tool to mitigate the effects of future natural disasters. Indeed, as telecommunication networks expand, particularly mobile networks, so does the government's ability to quickly spread key information in times of crisis or danger.

Broadcast networks, such as radio and television, have typically been among the most cost-effective and efficient at sending mass messages quickly. However, as the number of mobile subscribers in an economy surpasses a certain penetration threshold, mobile phones offer a much more effective and constant method for locating users and passing along vital information. There are several benefits of spreading information via text messages to mobile phones. First, users typically carry their phones with them at all times and can be reached when away from a television or radio. Second, the low-data intensity of text messaging allows for messages to make it through even when circuits can not handle a simple voice call[11].

The telecommunication networks in the affected areas were used not only by the rescuers to pass information but also as a tool to locate people stranded in the aftermath of the tsunami. Sri Lankan network operators were able to identify 10,252 internationally roaming mobile phones on their networks at the time the waves hit land. After the Sri Lankan operators sent each roaming phone a text message asking users to contact emergency response, nearly 23% responded. As mobile network operators quickly re-established service to affected areas with the use of portable electric generators, any mobile phones appearing on the network could be quickly traced and emergency crews dispatched. The Swedish government asked its country's mobile operators to send text messages to all Swedish-registered phones in Thailand requesting users either call their families or contact the Swedish Embassy. Danish operators were able to provide information about all mobile phone communications between Denmark and Indonesia, Thailand and Sri Lanka just before and after the tsunami[12].

Finally, the Internet also played a key role in rescue and recovery operators after the tragedy as pictures of victims and missing people appeared on websites for families and relatives to search. Certainly the economies with extensive networks to begin with were, in one aspect, better prepared to deal with emergency response than other, less-developed telecommunication markets. Indeed, one of the most potent lessons from the tragedy has been how people from all countries of the world benefit in times of crisis from developed telecommunication networks in affected economies.

Emergency services in an economy are often handled by a number of government, public and private entities. Various agencies specialize in different aspects of disaster warning and recovery but coordination during a disaster has sometimes proven difficult. Telecommunication regulators are often involved with emergency communications during a disaster since there is often a requirement that emergency telephone services are provided as part of universal service requirements for fixed-line providers.

Existing emergency regulations have worked well in economies with high fixed-line penetration rates. However, most economies struggling with the digital divide lack the type of developed fixed-line infrastructure necessary to sufficiently cover the population, severely hampering the effectiveness of fixed-line emergency services. Since mobile phones greatly outnumber fixed lines in many developing economies, regulators should examine how existing policies may need to be reconsidered to take advantage of mobile telephony.

This section will briefly examine several emergency telecommunication services that are currently available, their benefits and possible ways they could be adapted to take advantage of new communication technologies. The list is only a small sample of the many emergency preparedness systems available around the world. These examples do not necessarily represent best practices but rather offer a glimpse into how telecommunication networks are currently being used to provide emergency services in several countries.

As mentioned earlier, the tsunami has helped highlight how telecommunication networks could be used as an important emergency broadcast system. Systems currently exist in Hong Kong (China), the United Kingdom and the United States that can notify users of danger in their area via either a mobile phone or a fixed line.

One of the proposals to come out of the discussions after the tsunami is an emergency SMS service that could send a bulk message to all mobile subscribers near cell towers in an affected area. The SMS messages could be targeted geographically, by cell tower, and sent quickly by the mobile providers. The efficiency of such a system would likely be highly correlated to the mobile penetration rate in a given area, highlighting the importance of expanded mobile access. Hong Kong, China's use of such a system during the SARS pandemic is probably the largest experience to date.

Hong Kong, China: SARS information by SMS

The government of Hong Kong, China used such a system in April 2003, broadcasting 6 million SMS messages in an effort to quell a rumour that the city would be quarantined during the SARS pandemic[13]. A rumour was purportedly started by a teenager who built a mock website stating Hong Kong was an "infected city". Once the rumour started to cause panic in the city, the government quickly launched a blanket SMS that transmitted a message from the Director of Heath announcing that there were no plans to declare Hong Kong an infected area.

Hong Kong, China's use of the SMS broadcast was largely seen as a success. However, the experience highlighted some areas for improvement for future mass SMS warnings. Network congestion prevented some of the messages from arriving and many of the messages arrived up to six hours later.

United Kingdom: City Alert Texting System (C.A.T.S.)[14]

Mobile users in the United Kingdom can register the postal codes where they live and work with an emergency news texting service (C.A.T.S.) and receive detailed emergency messages when problems arise in any of their registered postal codes. The system can send warnings about critical events such as severe weather, chemical fires, terrorist alerts, traffic accidents and road delays. Users are given simple directions to follow in the text message to keep them out of danger. Subscribers are charged GBP 1.50 per postal code registered, which includes unlimited alerts for one year. C.A.T.S. services are currently available in several cities throughout the United Kingdom.

One drawback of the C.A.T.S system is the inability to pass information based on the physical location of the phone. Subscribers to the service input the zip codes where they spend most of their time but would not be notified, for example, if they happened to be near a dangerous situation in a zip code they had not registered.

SMS alert systems show great promise for early warning but there are several problems that must be resolved for them to be effective. For example, the authenticity of early-warning systems that rely on SMS must be verifiable by users. If they are not, malicious SPAM messages could start dangerous rumours and degrade the trustworthiness of such a system. Several challenges to building an early SMS warning system are given in Table 1 below.

Table 1. Table 1. Challenges to building an SMS early warning system

1.	**Authenticity:** Users must have a way to verify the authenticity of messages they receive. This involves developing methods to verify the source as well as educating the public on how to recognize "spoofed" messages.
2.	**Local languages:** Delivering timely, emergency information may require operators to send messages in several languages from the same cell tower. This would require a method for determining which language would be the most appropriate for a given subscriber.
3.	**Voice messages in areas with low literacy areas** SMS messages would be largely ineffective in areas characterised by low levels of literacy. In these areas a recorded voice message may be more appropriate for a mass broadcast. Mobile operators could send SMS messages to all subscribers who had ever sent an SMS from their phone (indicating a level of literacy) and voice messages to all other subscribers. Maximizing the number of SMS messages sent would help keep traffic levels lower on the network during the crisis.
4.	**Prioritizing emergency calls** Fixed-line networks can give priority to calls destined to emergency response numbers and a similar system

on mobile networks could help keep lines available for emergency personnel during peak-usage times around a disaster.

United States: Emergency fixed-line notifications

A number of communities throughout the United States have set up emergency fixed-line telephone notification systems to quickly contact residents in the case of a natural disaster or other emergency situation. These services have been particularly popular in areas of the mountain west, which are prone to wildfires that can spread quickly and shift suddenly, threatening entire communities[15]. In the case that a wildfire is approaching a community, an automated system can quickly call all residents in the affected area with a recorded message, telling them to take certain precautions or evacuate the area. The system usually makes a series of calls, first warning users to prepare and then a later call to leave the premises when they are in imminent danger.

Residential phone numbers are mapped to individual street addresses so calls can be made on a street-by-street basis or over an entire city or town at once. These systems have been successful at passing along important messages to residences but are limited to fixed-line telephones.

Fixed-line emergency notification systems typically work well in areas with high fixed-line penetrations. The success is partially due to the ability to "geo-code" a phone number to a stationary address (e.g. a house). Emergency personnel can then simply designate certain areas of a city or town, and with a simple database query, can have a computer send out bulk phone messages to affected homes.

A similar system could work for mobile users, although location information would need to be gathered by different means, either by a global positioning system (GPS) or via information gleaned from cell towers in communication with a mobile phone. Mobile phone manufacturers have begun including GPS capabilities into mobile phones, in part due to emergency service regulations mandated by governments. Rollout of these devices has been slow, due in part to satellite reception problems inherent in GPS systems. GPS position reporting from a mobile phone will only work when the phone has an unobstructed view of a good portion of the sky, typically outdoors. Phones that are indoors or in dense urban areas with high buildings will be unable to report their position accurately. Even outdoors, GPS systems require an initial "warm-up" period of up to one minute while the phone analyzes satellite signals to obtain its bearings.

Mobile operators can also determine the precise location of a mobile phone via triangulation of radio frequency (RF) communications with mobile towers in the near vicinity. One drawback is these systems are computationally prohibitive for operators with a large number of users on the network at any given time.

Policy makers and operators may be more inclined to look into a system which could leverage the both GPS position reporting and cell tower communication to broadcast targeted emergency communications in over a very small area. Otherwise, the most cost effective and efficient method for broadcasting an emergency message would be to simply send an SMS to all users serviced by a given tower.

The examples above looked at ways emergency communication systems can pass information on to a large number of people quickly. Other emergency systems have a much narrower focus, protecting an individual. Services in Ireland and the UK focus on the safety two vulnerable groups of people in particular, those whose work takes them to dangerous places alone and children.

Ireland: Mobile phone network protects lone workers[16]

The mobile operator O2 in Ireland has introduced a system to help lone workers who may enter dangerous or risky areas as part of their jobs, specifically social workers, community nurses and postal staff. With the system, the mobile user first records a message giving the details of the visit before leave. Once the mobile user completes the visit, he or she is required to confirm that the visit has ended safely by tapping a code into their phone.

If the mobile user does not log off, the system will send two phone calls, at five minute intervals, to check for a response from the mobile user. If the second call remains unanswered, emergency crews can quickly be dispatched to the area of the phone using details included in the pre-recorded message.

The system also includes a panic button users can press that immediately sends out a distress signal to an emergency response centre. Economies with high mobile phone penetration rates have also been able to take advantage of the technologies to locate missing children or individuals.

United Kingdom: Childwatch[17]

The Childwatch system in the United Kingdom is a registry of mobile phone numbers of people who associate with a particular child. The list could include friends, teachers, neighbours and family. If a child goes missing, an emergency message is quickly relayed to the entire list of mobile subscribers who associate with the child, asking if they know where the child is and where he or she was last seen. Often one of the contacts knows the whereabouts of the child and the chain of emergency procedures can stop. If no one on the contact list knows the child's whereabouts the police and other relevant agencies can then take swift action. The system has been credited with improving the chances of locating abducted children by decreasing the amount of time required to verify the abduction. It has also reduced the number of "false alarm" child alerts.

Telecommunication networks provide important early-warning functions during disasters but also play a vital role in coordinating and passing along information about survivors and victims to family and friends after a disaster. These systems can be used to arrange reunions or to identify victims, particularly internationally. The "I Am Alive" system was developed after the Kobe earthquake in Japan and provides a repository for survivor and victim's information after a disaster.

Japan: "I Am Alive" (IAA) system[18]

An earthquake in Kobe, Japan in January 1995 caused massive damage and claimed the lives of over 5000 people. The "I Am Alive" Alliance evolved in the aftermath of the earthquake as a way to gather and organize information about survivors and victims. IAA systems allow various organizations to accumulate and store information in a common database by use of automated data exchange. Information can be submitted to the IAA system by Internet, mobile phone or fax and then searched online.

The emergency systems mentioned above are only a few of many such systems around the world but highlight the availability of technologies that can notify users during emergencies and keep them out of harm's way. Regulators may be faced with significant challenges when working to incorporate new technologies into existing emergency system requirements. Open discussion of the difficult regulatory issues will be necessary to find solutions and ensure the economy moves closer to an optimum contribution of ICTs to disaster warning and recovery.

Conclusion

Telecommunication networks and services play an important role in modern economies as an enabling technology in traditional economic sectors and in new economic activities such as electronic commerce. Telecommunication technologies have also played an important role in enhancing total factor productivity in OECD economies and in employment growth[19]. As recent events have shown, telecommunication networks can also play a key public safety role in an economy, especially as a tool for disaster warning and recovery efforts. Economies with under-developed telecommunication markets and networks may face higher risks in the face of future catastrophes than economies with extensive networks and public safety systems in place. While the benefits of e-learning, e-health and e-commerce cannot be overlooked, the public safety aspect of telecommunication networks has recently intensified the focus on the need to ensure good ICT access to all the world's inhabitants.

This paper has looked at one narrow aspect of the digital divide, the effects of regulatory reform on telecommunication networks. While regulatory reform is only one part of the global digital divide problem, it can play a key role in helping telecommunication markets bridge some of the gaps on their own. It is therefore imperative that policy makers consider regulatory reform as a necessary but not sufficient step towards overcoming the digital divide.

The severity of the digital divide in OECD countries is much less than other parts of the world, in part to higher incomes but also as a result of important regulatory reforms initiated over the past 30 years. These reforms have paved the way for markets to develop and supply telecommunication services with the least amount of intervention. There still remain problems with the digital divide in the OECD, especially in rural and remote areas. However, operators in the OECD have expanded networks quickly and the scope of the problem should be well diminished in the next two years.

The situation outside of the OECD is more pronounced, with large parts of the population without basic ICT access in many economies and regions. Certain technologies, such as the mobile phone, have helped bridge the communication divide but the rapid pace at which telecommunication technologies are evolving has left many economies in a constant state of "catch-up". Regulatory reform can thus play a key role in many of these economies as a way to ensure the telecommunication market is given the best chance of succeeding on its own without intervention. Policy makers in non-OECD economies should consider the policies that have been the most successful in the OECD, namely liberalizing markets, creating a separate regulator, opening spectrum for new wireless technologies and developing human capital in regards to ICTs.

Policy makers throughout the world should be concerned about the digital divide, not simply because of the services ICTs provide to users but because of the externalities that accompany developed networks and ICT-savvy users. Telecommunications infrastructure can play a key role in economic development, which can create a virtuous cycle where incomes improve and access increases[20]. Developing economies have increasingly been able to attract IT and service outsourcing from developed economies and these gains rely on a high-quality telecommunications infrastructure and a population with ICT skills[21]. Examples include India and Sri Lanka's call centres and the outsourcing of computer programming to Eastern Europe.

As mentioned earlier, an economy's regulatory regime is only one facet of a very complex problem that includes affordability, education and other social circumstances. Policy makers must take all into account when devising an overall digital divide strategy since many of the factors are interconnected. While the social situation in each economy varies drastically, the key principles behind regulatory reform have been tried and tested with success in countries and regions around the world.

NOTES

1 The OECD report, *Providing Low-Cost Information Technology Access to Rural Communities in Developing Countries: What works? What pays?* (2004) takes a broader approach to the digital divide in the rural areas of developing economies, offering detailed experiences and evaluation of several business plans for telecommunication service provision.

2 The OECD report, *The development of broadband access in rural and remote areas* (2004), highlights new technologies and policies that have helped extend access to rural areas within the OECD. Solutions for the digital divide in rural areas of the OECD can also be applied in rural areas of developing economies. http://www.oecd.org/dataoecd/38/40/31718094.pdf

3 For more information on the success of regulatory reform throughout the OECD, see The OECD Reports on Regulatory Reform Series, http://www.oecd.org/topic/0,2686,en_2649_37421_1_1_1_1_37421,00.html

4 The World Bank has a large number of publications on the effects of telecommunication competition in developing economies. For more information readers should consult InfoDev's Telecommunications Regulation Handbook, edited by Hank Intven, 2000. In addition, the World Bank publication, Implementing Reforms in the Telecommunications Sector, Lessons from Experience, Edited by Bjorn Wellenius and Peter A. Stern, offers examples from around the world.

5 ITU World Telecommunication Indicators Database.

6 Amr M. Aboualam, EgyNet, National and Pan-African IXP Special Workshop, ITU TELECOM Africa, May 6, 2004.

7 ITU World Telecommunication Indicators Database.

8 Wi-Fi is short for wireless fidelity. It is a term developed by the Wi-Fi Alliance to describe wireless local area network (WLAN) products that are based on the Institute of Electrical and Electronics Engineers' (IEEE) 802.11 standards. Wi-Fi is typically used as a means to connect computers wirelessly to the Internet over a range of up to 100 metres. (http://www.wi-fi.org/).

9 WiMAX is a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL. WiMAX should provide fixed, nomadic, portable and, eventually, mobile wireless broadband connectivity without the need for direct line-of-sight with a base station. WiMAX should be able to extend a wireless Internet connection within a typical cell radius deployment of three to 10 kilometres. At these distances, WiMAX equipment should allow up to 40 Mbit/s of connectivity, roughly the equivalent of 700 dial-up Internet connections. (http://www.wimaxforum.org/about/faq/).

10 Information from the Estonian Ministry of Foreign Affairs at: http://www.vm.ee/estonia/kat_175/pea_175/2972.html

11 See the BBC story, "Text messages aid disaster recovery" at: http://news.bbc.co.uk/2/hi/technology/4149977.stm

12 Story from the Boston Globe, December 29, 2004, "Internet, cellphones are aiding the search", at: http://www.boston.com/news/world/asia/articles/2004/12/30/internet_cellphones_are_aiding_the_search/

[13] For more information, see "Text messaging used to allay SARS fears", April 3, 2003 at: http://www.guardian.co.uk/online/news/0,12597,928906,00.html

[14] For more information see: http://www.cityalert.co.uk/static/aboutcats.htm

[15] Services mentioned were from http://www.intrado.com/

[16] For more information see: http://www.techcentral.ie/techcentral/pcwork/wireless_mobile/guardian_to_protect_vulnerable_workers.xml

[17] Information about the services is available at: http://www.cityalert.co.uk/static/aboutcats.htm

[18] The IAA Alliance website is available in Japanese with main pages translated into English at: http://www.iaa-alliance.net/en/about/

[19] The *OECD Communication Outlook 2005* highlights how the telecommunications industry, over the past decade, has played an increasingly important role in economy-wide productivity growth and technological diffusion. The industry's infrastructure and services provide a fundamental underpinning for information economies.

[20] The OECD Report, *The New Economy: Beyond the Hype* (2001), concluded that ICTs have a large potential to contribute to more rapid growth and productivity gains. The OECD revisited the same topic in 2003 with *ICT and Economic Growth: Evidence from OECD Countries, Industries and Firms* (2003) and found that the assumptions and conclusions drawn in 2001 still hold.

[21] Rapid developments in ICT provide increasing opportunities for international sourcing. In particular, "knowledge work" such as data entry and information processing (IT services), research and consultancy services can be carried out remotely via the Internet and through multimedia conferencing. The *OECD Information Technology Outlook 2004* highlights the drivers and impediments to outsourcing of business services, the dynamics of business process restructuring, and the skills dimension of international sourcing

Comitato tecnico nazionale
sulla sicurezza informatica e
delle telecomunicazioni nelle
pubbliche amministrazioni

Proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni per la pubblica amministrazione

MARZO 2004

Ministero per l'Innovazione e le Tecnologie

Ministro delle Comunicazioni

1. Premesse e linee ispiratrici

1.1 Introduzione

I fattori di crescita ed evoluzione dell'ICT, con particolare riguardo allo sviluppo di reti di interconnessione tra i sistemi informativi, e la sua diffusione in uno spettro di applicazioni sempre più vasto impongono una rigorosa attenzione agli aspetti legati alla sicurezza. Questo fattore vale per tutto lo scenario delle applicazioni informatiche e di telecomunicazioni, in particolare per la PA. Infatti, la diffusione dell'utilizzo delle reti presenta ormai coefficienti di crescita esponenziali e le applicazioni su reti aperte sono divenute una realtà non più esclusiva del mondo imprenditoriale, bensì una necessità gestionale e di colloquio delle Pubbliche Amministrazioni, tra loro, con le imprese, con i cittadini.
Internet sta divenendo sempre più il sistema di scambio di informazioni, di accesso alle grandi banche dati, di esecuzione di transazioni e disposizioni finanziarie, di sviluppo di attività professionali e, parallelamente si sta evidenziando la sua attuale fragilità. A fianco di eventi distruttivi motivati da vandalismo, azioni di cyber terrorismo, puro esibizionismo cibernetico, si verificano molti attacchi rivolti a carpire informazioni, per scopi di concorrenza commerciale piuttosto che per attuare frodi informatiche. Non vanno dimenticate le troppo abusate forme di attacco a sistemi informatici e di comunicazione, che sono finalizzate principalmente a compromettere il corretto funzionamento di un sistema o a carpire informazioni commerciali o informazioni relative alle abitudini di vita di un utente, quali spyware, cookies, sniffing, tracking, hijacking, sino a raggiungere intollerabili azioni invasive delle caselle di posta elettronica come lo spamming.
In questo scenario la sicurezza informatica deve essere un elemento fondamentale nel processo di avvicinamento, tramite la tecnologia, del cittadino e delle istituzioni private (i "clienti" dell'e-government) alla PA. Infatti, aldilà della disponibilità di servizi, è necessario fornire al "cittadino" precise garanzie in relazione al rispetto delle principali proprietà di sicurezza dei servizi stessi, al fine di assecondare quelle attività di coinvolgimento e di collaborazione tra "cittadino" e PA, che sono alla base di ogni processo di e-government.

Queste considerazioni impongono la ricerca delle necessarie garanzie. La prima è quella di poter dialogare con servizi della P.A. che offrano:
- un elevato grado di sicurezza, in termini di riservatezza, integrità disponibilità e autenticità;
- il trattamento dei dati personali e la gestione delle transazioni fatte secondo i dettami delle direttive europee e della normativa sulla protezione dei dati personali;
- una chiara informazione sulle modalità da seguire per richiedere controlli ed azioni correttive e rivolgere reclami.

La seconda garanzia è quella di una visione unitaria della sicurezza in rete che può derivare solo da una stretta cooperazione tra le istituzioni, le imprese e i maggiori protagonisti della high tech e dei servizi ICT al fine di disporre:
- di standard semplici e sicuri;
- dello sviluppo e della diffusione di tecnologie che contribuiscano a migliorare la sicurezza dei prodotti e dei servizi;
- di norme di base, chiare ed omogenee tra loro, corredate dalle necessarie ed applicate sanzioni amministrative e penali;

- di una azione di autoregolamentazione fondata su convinti e rispettati codici deontologici;
- di infrastrutture che possano assecondare il processo di "messa in sicurezza" delle risorse e delle attività, in ambito nazionale, della società dell'informazione.

Si ponga infine attenzione al fatto che il tema della sicurezza nell'e-government accomuna tutta la PA, centrale e locale. Al proposito si ricorda che il Comitato tecnico della commissione permanente per l'Innovazione e le Tecnologie, nel documento "L'e-government per un federalismo efficiente" dell'aprile 2003, identifica le regole per l'uso sicuro dei servizi di e-government:

1. assicurazione dell'integrità e la riservatezza delle informazioni che transitano in rete;
2. affidabilità e certificazione delle fonti di erogazione dei servizi;
3. consultazione esclusiva delle informazioni di carattere personale da parte del legittimo proprietario dei dati;
4. minor numero possibile di informazioni di carattere personale richieste all'utente nell'interazione con i sistemi di e-government e utilizzo di queste informazioni esclusivamente per verificare il diritto ad accedere ai servizi;
5. concessione dell'abilitazione all'accesso ai servizi solo in funzione di specificità dell'utente (cittadinanza, appartenenza a categorie professionali, ecc.) attestate dagli organismi competenti.

1.2 Le iniziative del Governo

L'istituzione del Ministro per l'Innovazione e le Tecnologie ed i piani di finanziamento di numerosi progetti di e-government da questo approvati, destinati a far crescere il livello di efficienza degli Enti locali, dalle Regioni, alle Province, ai Comuni grandi, medi e piccoli, sino alle Comunità montane, confermano l'intenso impegno delle PPAA nella razionalizzazione dei processi amministrativi e nella volontà di avviare un dialogo più snello ed efficace con i cittadini. Affinché si compia con pieno successo l'opera di realizzazione dell'impianto di e-government é indispensabile consolidare l'azione governativa anche sugli aspetti della sicurezza ICT.
Si consideri anche il fatto che aspetti tecnologici fondamentali per la realizzazione dell'e-government, quali la larga banda e l'open source, non hanno possibilità di diffusione se non accompagnati da una adeguata infrastruttura di sicurezza.

Il Ministro dell'Innovazione e delle Tecnologie si è già fatto promotore di importanti iniziative atte ad avviare un vero e proprio sistema di sicurezza per l'e-government:

- la direttiva sulla sicurezza ICT, emanata con direttiva del Presidente del Consiglio dei Ministri 16 gennaio 2002, contiene i requisiti minimi per il raggiungimento dei quali tutte le amministrazioni devono attrezzarsi dopo aver effettuato una autovalutazione sul proprio livello di sicurezza ICT;
- il Comitato Tecnico Nazionale sulla Sicurezza ICT, (nel seguito Comitato), istituito con Decreto Interministeriale del Ministro delle Comunicazioni e del Ministro per l'Innovazione e le Tecnologie nel luglio 2002, che ha il compito di raggiungere gli obiettivi di sicurezza attraverso le seguenti fasi funzionali:
  - esame della situazione della P.A. rispetto ai temi della sicurezza;
  - elaborazione e diffusione di linee guida;

- stesura di progetti di attuazione dei principi fissati;
- realizzazione e controllo dell'avanzamento dei progetti;
- fornitura di consulenza e supporto alla realizzazione.

• l'approvazione del decreto per l'istituzione di uno schema nazionale per la certificazione di sicurezza secondo gli standard ITSEC e Common Criteria di prodotti e sistemi ICT che non trattino informazioni relative al segreto di stato, avvenuta in data 29 ottobre 2003.

1.3 Il Comitato

Senza voler riportare l'intero contenuto del Decreto istitutivo del Comitato, è però il caso di ricordare le funzioni previste nel Decreto all'articolo 2, "Funzioni del Comitato":

1. Il Comitato, al fine del raggiungimento di un livello di sicurezza nelle informazioni conforme a criteri standard internazionali e per garantire integrità e affidabilità dell'informazione, formula le proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni (ICT) per la pubblica amministrazione, in particolare ai fini della redazione:
   a) del Piano nazionale della sicurezza delle tecnologie dell'informazione e comunicazione della pubblica amministrazione, di cui verifica annualmente lo stato di avanzamento, identificando le eventuali misure correttive;
   b) della predisposizione del modello organizzativo nazionale di sicurezza ICT per la pubblica amministrazione, del quale verifica la relativa attivazione e applicazione.
2. Il Comitato formula, inoltre, proposte in materia di regolamentazione della certificazione e valutazione della sicurezza, nonché ai fini della predisposizione di criteri di certificazione e delle linee guida per la certificazione di sicurezza ICT per la pubblica amministrazione, sulla base delle normative nazionali, comunitarie e internazionali di riferimento.
3. Il Comitato elabora linee guida per la predisposizione delle intese con il Dipartimento della funzione pubblica in ordine alla formazione dei dipendEnti pubblici in tema di sicurezza ICT."

Il presente documento contiene le proposte di cui al punto 1. sopra citato. Si sottolinea anche che, su proposta del Comitato, sono stati già stanziati i fondi dal Comitato dei Ministri per la Società dell'informazione nella riunione del 18 marzo 2003 per le due seguenti iniziative:
- un progetto di "CERT per la Pubblica Amministrazione";
- un "Centro di formazione e sensibilizzazione del personale della PA",

e che il Comitato intende anche promuovere alcune altre iniziative concrete, di supporto all'attuazione del Piano, così come richiesto nel Decreto; in particolare:
- la produzione di linee guida sulla sicurezza informatica, redatte con il contributo non solo dei responsabili informatici della PA, ma anche con quello delle associazioni rappresentative delle imprese e dei cittadini;
- la promozione di incontri periodici con la PA, con provider internet, con realtà rilevanti di banche, finanza, assicurazioni, commercio e industria, al fine di armonizzare il sistema sicurezza ICT italiano, sfruttando le più riuscite esperienze e capacità di tutte le realtà nazionali;
- la determinazione di alcuni obiettivi operativi relativi ad aspetti urgenti e sentiti dagli utenti ICT, come l'abuso di spamming e dei cookie.

1.4 Le proposte del Comitato per il Piano Nazionale e il modello organizzativo

Nella prima parte di questo documento, "Proposte per un sistema di governo della sicurezza ICT nella PA", vengono presentate una serie di indicazioni relative alla costituzione di una infrastruttura organizzativa, che possa farsi carico a livello nazionale di coordinare un processo di "messa in sicurezza" delle PPAA, unitamente ad una serie di indicazioni in merito alle iniziative di tipo legislativo che dovrebbero essere intraprese nel settore.
La seconda parte di questo documento, "Linee guida per l'attuazione della sicurezza ICT nella PA", contiene l'indicazione di una serie di attività da intraprendere con estrema urgenza per avviare il suddetto processo.
Il Comitato ritiene, nella situazione contingente del livello di sicurezza rilevato da un primo ciclo di incontri con i responsabili dei sistemi informativi della PAC, che le indicazioni contenute nel presente documento, siano le più urgenti. L'evolversi della situazione attuale dovrà ovviamente riflettersi in adeguamenti e revisioni successive del documento stesso.

1.5 Premesse finali

Il Comitato ha preventivamente definito i seguenti punti, relativamente al Piano Nazionale che verrà realizzato sulla base delle proposte:
1. area di competenza del Piano:
- amministrazioni dello Stato;
- aziende ed amministrazioni autonome dello Stato;
- Enti pubblici non economici nazionali;
2. requisiti attuativi del Piano:
- la verifica del rispetto del Piano sarà effettuata attraverso un monitoraggio.

I tempi e i modi di realizzazione del Piano e del modello organizzativo sono stati volutamente lasciati indefiniti, ritenendo il Comitato che siano oggetti specifici delle fasi realizzative.
Il Piano e il modello organizzativo acquisteranno natura normativa con decreto legislativo su iniziativa del Ministro Stanca, di concerto con il Ministro Gasparri in base all'art. 10 della legge 29-07-2003 n° 229.

1.6 Cenni sulla regolamentazione normativa ed amministrativa in tema di sicurezza ICT nei sistemi informatici pubblici

1.6.1 Premessa

La formulazione delle proposte concernenti le strategie in materia di sicurezza informatica e delle telecomunicazioni di cui all'art.2 del Decreto Interministeriale del 24 luglio 2002 rende necessario, ad avviso del Comitato, esaminare anche gli aspetti giuridico-normativi del problema. Per far ciò appare necessario tracciare una ricostruzione del quadro normativo ed amministrativo relativo alla sicurezza informatica che, allo stato, come rilevato dalla dottrina specialistica, presenta indubbi caratteri di frammentarietà e di scarsa coerenza sistematica. I capitoli che seguono cercano quindi di ricostruire, in modo necessariamente sintetico, le linee del trend normativo sviluppatosi nel corso dei decenni precedenti in modo da offrire un panorama, il più possibile completo, della situazione

concernente la materia e di consentire ai "decision makers" di valutare la situazione stessa e, eventualmente, di intervenire sul piano politico-normativo allo scopo di dettare le prescrizioni che apparissero necessarie per regolamentare la materia in modo esaustivo e coerente nell'ambito pubblico.
L'importanza della predisposizione di sistemi efficienti di sicurezza informatica relativamente al settore pubblico è stata ben sottolineata nella Direttiva del Ministro per l'innovazione e le tecnologie del 16 gennaio 2002 allorché è stato affermato che le informazioni gestite dai sistemi informativi pubblici costituiscono una risorsa di valore strategico per il governo del Paese e che questo patrimonio deve essere efficacemente protetto e tutelato al fine di prevenire possibili alterazioni sul significato intrinseco delle informazioni stesse[1].

1.6.2 Le prime iniziative normative

Come già accennato, la situazione normativa e regolamentare per quanto riguarda la sicurezza informatica nell'ambito pubblico presenta un aspetto non unitario essendo le varie prescrizioni, in generale, contenute in provvedimenti sparsi e non collegati tra di loro non esistendo, sino al 2001, un preciso indirizzo politico al riguardo ed un centro amministrativo di riferimento. Le stesse lodevoli iniziative in materia dell'AIPA, data la scarsa incidenza dell'azione della stessa sulle burocrazie ministeriali, poco sollecite tradizionalmente a recepire in modo organico ed integrabile l'innovazione tecnologica, non sembrano aver avuto esiti concreti.

Un primo tentativo di mettere ordine nel settore dell'informatica pubblica è stato probabilmente quello compiuto dal Ministro per la Funzione pubblica dell'epoca con la Circolare n.51223 del 21 maggio 1990 avente come titolo "Indirizzi di normalizzazione delle tecnologie dell'informazione nella pubblica amministrazione" un paragrafo della quale era dedicato ai criteri generali per la sicurezza fisica delle installazioni e per la sicurezza logica delle applicazioni. Va ricordato anche il D.lgs.n. 39 del 12 febbraio 1993 con il quale, tra l'altro, venne creata l'AIPA che, secondo il testo dell'art.7, c.1.lett.a) aveva anche il compito di dettare i "criteri tecnici" riguardanti la sicurezza del sistemi[2].

---

[1] Dalle audizioni svolte dal Comitato è emerso che le Amministrazioni hanno ,in genere, adottato misure di sicurezza, soprattutto per quanto riguardava la protezione dei dati personali. Tuttavia, come fatto presente da alcune Amministrazioni, ed in particolare dai rappresentanti della Presidenza del Consiglio dei Ministri, nell'appunto del 12/12/2002 le cui puntualizzazioni appaiono, per così dire, emblematiche della situazione, le misure adottate .."non comprendono ,....,gran parte della base minima citata nel documento allegato 2 della G.U del 22/3/02 ..." Inoltre nel documento citato si afferma, senza mezzi termini, che "per soddisfare adeguatamente a quanto richiesto nel tempo di un anno è comunque prevedibile che si incontrino grosse difficoltà da parte dell'Amministrazione, essendo necessario un grosso sforzo organizzativo ed economico per istituire un'organizzazione di qualità per la sicurezza ..."
In tema di sicurezza informatica e di "stato dell'arte" in materia va citata una ricerca sulla sicurezza informatica negli Enti Locali del luglio 2002 (peraltro effettuata su un campione ristretto di Comuni), dall'ANCITEL secondo cui "solo il 12% dei Comuni intervistati ha adottato sistemi di difesa derivati da una valutazione complessiva dei rischi e di una vera applicazione delle policy di sicurezza, integrando le tecniche di firewalling con quelle di intrusion detection ed antivirus centralizzato. Di contro "il 48% dichiara di utilizzare almeno una delle due tecniche sopraccitate, dimostrando un certo grado di attenzione al problema... Il restante 40% del campione indagato, conferma la preoccupante e diffusa tendenza a trattare operativamente le problematiche della sicurezza informatica con una poco chiara visione progettuale e, conseguentemente, si assemblano sistemi di sicurezza destrutturati ..."

[2] Nel campo della sicurezza informatica pubblica va ricordata la figura dell'Autorità Nazionale della Sicurezza, posta alle dipendenze della Presidenza del Consiglio dei Ministri, che si serve per la sua attività di controllo e di omologazione dell'Ufficio Centrale per la Sicurezza. Il suo campo di attività riguarda la protezione delle informazioni coperte dal segreto di stato, trattate in sistemi di elaborazione automatica e/o elettronica di dati e delle notizie di cui è vietata la divulgazione previste dall'art.12 della legge n.801 del 24 ottobre 1977. Nell'ambito delle sue competenze l'ANS ha emanato varie direttive con DPCM., l'ultima è stata quella dell'11 aprile 2002.

Vanno ricordati,tra gli altri, anche: il D.lgs. n.212 del 12/7/1991 relativo alle modalità di accesso delle amm/ni pubbliche al sistema informativo dell'anagrafe tributaria, art.1; il DPR 27 /6/1992 n.352c, art.6; il c.d.Accordo Schengen (artt:114 e 118), ratificato dall'Italia con legge n.388 del 30 settembre 1993; il DPCM del 5/5/1994, relativo alle modalità tecniche e ripartizione delle spese connesse alla realizzazione di collegamenti, ecc., art.7 ed 8; il D.P.R 23/12/1997 n.522, relativo ai compiti del Centro Tecnico per l'assistenza ai soggetti che utilizzano la RUPA, art. 2; il D.P.R. 10/11/1997 n.513, Regolamento recante criteri e modalità per l'archiviazione e la trasmissione di documenti con sistemi informatici e telematici, art.3, comma 3; il DPCM del 20/11/1997, Principi e modalità di attuazione della rete G-net, pr. 2; il D.P.R. n.428 del 20/10/1998, Regolamento per la tenuta del protocollo amministrativo con procedura informatica, ecc., art.3, comma 1 lett.a) e c); il DPCM 27/10/1999 n.437, Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica, ecc., art 8; il DPCM del 31/10/2000, Regole tecniche per il protocollo informatico, ecc., art. 4.1 comma lett. c); il DPCM del 30/5/2002, Direttiva per la conoscenza e l'uso del domicilio internet "gov.it", ecc., pr. 26. Esistono infine vari decreti ministeriali relativi a specifici settori che qui non si elencano per brevità nonché varie circolari dell'AIPA in materia.

1.6.3 Sicurezza informatica e protezione dei dati personali

L'esame della normativa relativa alla sicurezza informatica fa emergere una particolare circostanza e cioè una prevalenza negli anni tra il 1996 ed il 2000 di prescrizioni dettagliate in tema di misure di sicurezza dirette alla protezione dei dati personali[3].

Il trend normativo ha inizio con l'art.15 della legge n.675 del 23 dicembre 1996 (Tutela delle persone e di alti soggetti rispetto al trattamento dei dati personali) intitolato "Sicurezza dei dati" il cui comma 2 prevedeva la successiva emanazione di apposite "misure minime di sicurezza", poi effettivamente emanate con il DPR 28 luglio 1999 n.318 (successivamente, insieme ad altri provvedimenti citati in questo scritto -vedi, ad es, il D.lgs. 171/98, abrogato dal D.lgs. 30/6/2003 n.196, su cui amplius)[4]

Va osservato che con la legge n. 675/10 1996 venne introdotta la necessità del "documento programmatico per la sicurezza" (art.6) per quanto riguardava il trattamento dei dati di cui agli artt.22 e 24 della legge n.675/96.

Per inciso si rileva che il secondo comma del citato art.6 stabiliva che l'efficacia delle misure di sicurezza indicate nel documento programmatico avrebbe dovuto essere oggetto di controllo periodico da eseguirsi almeno annualmente.
Qualche innovazione in materia è stata introdotta con il D.lgs. n.196/2003 agli artt. da 31 a 36 e con il disciplinare tecnico di cui allegato B relativo alle misure minime di sicurezza,

[3] Motivi socio politici inerenti anche ad un forte pressing effettuato da vari interessati sui "decision makers" dell'epoca, sembrano fornire una plausibile spiegazione in ordine alla indubbia prevalenza dell'azione politico-legislativa in tema di protezione della privacy rispetto alle esigenze, pur estremamente importanti, relative all'adozione, in modo coerente ed unitario, di iniziative decise in tema di sicurezza informatica nei sistemi pubblici. Con la creazione della figura del Ministro per l'innovazione e le tecnologie il problema della sicurezza informatica pubblica ha assunto carattere prioritario, rientrando tra gli obbiettivi governativi.

[4] Vari provvedimenti normativi emessi nel periodo 1996/2000, allorché accennano alla sicurezza informatica, richiamano espressamente l'art.15 della legge 675/1996. Vedi, ad es., l'art.2 del D.lgs. 13/5/1998 n.171, l'art.3, c.4 del DPR 10/11/1997 n.313, l'art.11 del D.M. 31/7/1998, ecc.

estendendosi -tra l'altro- la redazione del documento programmatico, prima previsto soltanto in relazione al trattamento dei dati sensibili e giudiziari, a tutti i trattamenti di dati personali[5].

1.6.4 Le linee guida in tema di sicurezza informatica

Una decisa azione governativa diretta a sviluppare l'informatizzazione delle strutture della P.A. ed a regolamentare anche la sicurezza dei sistemi informatici pubblici si è verificata, come già detto, con la creazione della figura del Ministro per la Innovazione e le Tecnologie che già con il documento dal titolo" Linee Guida del Governo per lo sviluppo della società dell'informazione", al pr. 1/21 aveva annunciato la redazione del Piano Nazionale per la sicurezza ICT e la privacy, seguito poi dalla fondamentale Direttiva del 16/01/2002, relativa alla sicurezza informatica e delle telecomunicazioni nelle PA., elaborata di concerto con il Ministro delle Comunicazioni alla quale erano allegati due documenti di orientamento (Valutazione del livello di sicurezza e Base Minima di sicurezza). L'azione è stata completata nella prima fase con la creazione, mediante il Decreto Interministeriale del 24/7/2002, del Comitato Tecnico Nazionale della sicurezza informatica e delle telecomunicazioni nelle P.A.[6].

Per completezza di esposizione vanno qui ricordate le prescrizioni in tema di sicurezza informatica elaborate a cura dell'AIPA e cioè le" Linee Guida in tema di sicurezza informatica" pubblicate nel periodico Quaderni dell'AIPA, n.2, ottobre 1999, e soprattutto, la Raccomandazione n.1/2000 avente come titolo" Norme provvisorie in materia di sicurezza dei siti Internet delle Amministrazioni Centrali e degli Enti Pubblici"[7].

1.6.5 Spunti per eventuali iniziative normative in materia di sicurezza informatica

Probabilmente, data la eterogeneità delle fonti normative e regolamentari relative alla materia, sarebbe opportuno, anche alla luce della legge 29/7/2003 n.229, (Interventi in materia di qualità della regolamentazione normativa e della codificazione-Legge di semplificazione 2001) e particolarmente dell'art.10 (Riassetto in materia di società dell'informazione) comma 1, e comma 2, lett.d) ricorrere allo strumento del decreto legislativo su iniziativa del Ministro per l'Innovazione e le Tecnologie, di concerto con quello delle Comunicazioni allo scopo di approntare un testo che coordini e regoli compiutamente la materia. L'opportunità di siffatta iniziativa appare chiara, ad avviso del Comitato, ove si consideri la necessità di coordinare l'attività di svariate entità pubbliche, stabilendo prescrizioni di natura cogente, in modo da assicurate coerenza ed uniformità di indirizzo, pur facendo salve le particolari esigenze di alcuni soggetti pubblici. Passando ad altro argomento e tenendo presenti anche le dichiarazioni del Ministro per

---

[5] Qualche perplessità tuttavia suscita il confronto tra il testo dell'art.34 del D.lgs. n.196/2003 ed il par.19 dell'allegato B, intitolato "Documento programmatico sulla sicurezza" il quale, invece, prevede la redazione del citato documento soltanto nel caso dei dati sensibili e giudiziari, ripristinandosi in tal modo il testo dell'art.6 dell'abrogato DPR n.318/1999. Inoltre né l'art.34 né il pr.19 dell'allegato B contengono la prescrizione del secondo comma del citato art.6 del DPR n.318 circa l'obbligo del controllo periodico, Quid iuris?

[6] Vedi in materia anche il paragrafo relativo alla sicurezza nella Direttiva del Ministro per l'innovazione , intitolata Linee Guida in materia di digitalizzazione dell'Amministrazione, del 20/12/2002. Dal canto suo il Ministro delle Comunicazioni con il Decreto del 14/1/2003, emesso di concerto con il Ministro della Giustizia, ha creato un Osservatorio per la sicurezza delle reti e la tutela delle telecomunicazioni.

[7] Accenni alla materia sono contenuti in vari documenti dell'AIPA, vedi, ad es, "Lo Studio di fattibilità relativo alla RUPA" del gennaio 1996, la Relazione Annuale 2001, vol II, e il Piano Triennale 2002-2005 relativo alla informatica nella P.A.. Dal canto suo il Ministero della Giustizia ha commissionato al Politecnico di Torino uno studio dal titolo " Linee Guida per lo sviluppo di piani di sicurezza dei sistemi informatici del Ministero della Giustizia " consegnato il 12/11/2002. In argomento vedi anche i decreti dello stesso Ministro del 24/5/2001 2 del 27(3/2002)

l'Innovazione e le Tecnologie relativamente allo sviluppo della posta elettronica, interna ed esterna, nell'ambito pubblico, appare opportuno disciplinare la materia, particolarmente per quanto riguarda la condotta degli operatori e degli utenti e le conseguenze legali di eventuali abusi, servendosi dello strumento regolamentare previsto dalla legge 10/1/2003 (Disposizioni ordinamentali in materia di Pubbliche Amministrazioni) con particolare riferimento all'art.27, comma 8, lett. E) che prevede appunto l'estensione della posta elettronica nell'ambito delle P.A. e dei rapporti tra P.A. e privati.
Altra area di intervento potrebbe essere quella dell'*outsourcing* nel campo pubblico, strumento che è previsto in generale per il settore pubblico da alcune disposizioni normative (vedi, tra l'altro, l'art.2 del D.lgs.12/2/1993 n.39, l'art.3, comma 2 del DPR 28/10/1994 n.478, e, da ultimo, i pr.25 e 26 - allegato B- del D.lgs. 30/6/2003 n.196.) e la cui estensione è stata sottolineata sia dalle indagini effettuate dall'AIPA (vedi il Piano Triennale 2003/2005) sia dalle audizioni svolte dallo stesso Comitato il quale, da tempo- sia detto per inciso-, ha manifestato le sue perplessità in ordine al ricorso a tale strumento per quanto riguarda particolarmente la sicurezza informatica. La necessità, in ogni caso, di un controllo penetrante da parte dell'Ente committente e di correlativi e particolari requisiti da parte del fornitore del servizio, in specie per quanto riguarda la serietà delle garanzie offerte - in particolare quanto all'affidabilità e professionalità del personale incaricato- postula che la "cabina di regia" in tema di sicurezza informatica resti saldamente nelle mani dell'Amministrazione. Ad avviso del Comitato, data la situazione di eterogeneità delle condotte da parte delle Amministrazioni pubbliche nella gestione della materia, sarebbe probabilmente opportuno un intervento normativo specifico.
Sempre nell'ambito di un auspicato intervento normativo in tema di sicurezza informatica andrebbe anche presa in considerazione la possibilità, peraltro largamente ammessa da alcune legislazioni estere (in particolare in USA) di ricorrere, almeno in relazione a particolari sistemi informatici c.d.critici, all'opera del *Tiger Teams o Red Teams* allo scopo di testare dall'esterno la validità delle misure adottate e la impenetrabilità del sistema informatico evidenziando le eventuali "falle" delle reti e suggerendo, al bisogno, gli eventuali rimedi. Va da sé che le aziende alle quali dovesse essere affidato tale delicato incarico dovrebbero rispondere a criteri assoluti di affidabilità e per i componenti delle equipes dovrebbe essere previsto uno speciale NOS[8].

1.7 Cenni sulle iniziative internazionali in tema di sicurezza informatica.

In correlazione con il tema trattato e per offrire un succinto panorama delle iniziative recenti e attuali nel settore internazionale concernente le strategie dirette ad assicurare la protezione delle reti informatiche, verrà qui di seguito tracciato un breve panorama di tali iniziative. Come è noto, da tempo le maggiori organizzazioni internazionali si sono date carico del problema relativo alla sicurezza informatica e le azioni intraprese sono di recente divenute più incisive: ciò sia a seguito dell'attentato di New York dell'11 settembre 2001 e delle sue conseguenze, sia a causa dell'uso della rete per motivi di lotta politica e specificatamente di aggressione terroristica, sia infine a seguito dei gravi attacchi condotti verso le reti ed i sistemi di informazione mediante le tecniche cd. DoS e DdoS nei confronti della rete Internet a cui si sono aggiunte le diffusioni di Worms e Virus.

[8] Particolare attenzione occorrerebbe dedicare, ad avviso del Comitato, ai problemi tecnici e giuridici delle reti Wireless.

La prima, e forse più importante iniziativa si deve all'OCSE che già nel 1992 emanò una Raccomandazione del Consiglio (16.11.1992) concernente le Linee Direttrici relative alla sicurezza dei sistemi di informazione, poi rivista e modificata recentissimamente in data 27 luglio 2002.

Nell'ambito dell'Unione Europea è da ricordare che il Consiglio approvò già nel 1992 una Decisione nel settore della sicurezza dei sistemi di informazione. Successivamente il 26 gennaio 2001 la Commissione inviò al Consiglio e al Parlamento una importante Comunicazione dal titolo "Creare una società dell'informazione sicura, migliorando la sicurezza delle infrastrutture dell'informazione mediante la lotta alla criminalità informatica".
A fronte di tale comunicazione il Parlamento emise il 6 settembre 2001 una "Raccomandazione relativa alla strategia per creare una società dell'informazione sicura".
Peraltro la stessa Commissione il 16 gennaio 2001 aveva inviato al Consiglio un'altra importante Comunicazione dal titolo "Sicurezza delle reti e sicurezza dell'informazione. Proposta per un approccio strategico europeo".
In essa richiamava tra l'altro il lavoro svolto dagli organismi pubblici e privati di intervento in caso di emergenza informatica (CERT) e da organismi simili, rilevando tuttavia che i CERT operavano in modo diverso a seconda degli Stati membri, per cui la cooperazione appariva difficile. In ogni caso - ricordava la Commissione - il coordinamento a livello internazionale avveniva tramite il CERT/CC, un organismo parzialmente finanziato dal Governo USA, per cui i CERT europei apparivano tributari della politica di divulgazione delle informazioni del CERT/CC e di altri organismi. Infine la Commissione suggeriva agli Stati membri l'opportunità di potenziare risorse e competenze dei CERT nazionali esistenti nell'ambito dell'UE e suggeriva, inoltre, di creare una rete dei CERT per lo scambio di informazioni, rete che avrebbe dovuto essere collegata ad organismi dello stesso tipo, attivi in tutto il mondo, come ad esempio il sistema di segnalazione degli incidenti proposto dal G8.

In esito a tale comunicazione il Parlamento europeo ha emanato il 22 ottobre 2002 una Risoluzione nella quale, dopo aver affermato che i CERT presenti nei vari Stati membri operavano in modo eterogeneo il che rendeva la cooperazione inutilmente complessa, e dopo aver citato il moltiplicarsi a livello internazionale di iniziative pubbliche e private per assicurare la affidabilità delle reti, quali ad esempio la rete per lo scambio di informazioni sulla sicurezza istituito nell'ambito del G8, nonché le reti di EUROPOL ed INTERPOL, in relazione agli aspetti istituzionali concordava con la Commissione sulla necessità di istituire quanto prima una "Task force" sulla sicurezza delle reti con determinati specifici obiettivi[9].

[9] Altri testi importanti in materia di sicurezza informatica sono la Risoluzione del Consiglio UE del 18/02/2003 avente come titolo "Per una cultura della sicurezza delle reti e dell'informazione", nella quale, tra l'altro, si invitano gli Stati membri a promuovere la sicurezza quale componente essenziale del governo pubblico e privato, in particolare incoraggiando l'assegnazione delle responsabilità, e la Posizione Comune n. 39-2003, definita dal Consiglio il 26/05/2003 in vista della Decisione del Parlamento Europeo e del Consiglio circa l'adozione di un piano pluriennale (2003-2005) per il monitoraggio del piano di azione eEurope, la diffusione delle buone prassi ed il miglioramento della sicurezza delle reti e dell'informazione (MODINIS).
Occorre ricordare anche il programma USA per la sicurezza, recentemente sottoscritto dal Presidente Bush e avente come titolo "National Strategy to Secure Cyberspace", il quale prevede – tra l'altro – la costituzione di una National Security Response System, una struttura pubblico/privata coordinata dal Department of Homeland Security di recente istituzione, sistema che, nel settore della sicurezza, ha i seguenti compiti, relativamente alle vulnerabilità, agli allarmi ed agli attacchi informatici, e cioè: Analysis, Warning, Incident Management, Response/Recovery.

A seguito di tali iniziative e decisioni, la Commissione UE nel febbraio di quest'anno elaborò uno schema di proposta relativa alla costituzione di una Rete europea e di una Agenzia avente per oggetto la "Information Security" che avrebbe dovuto operare come punto di riferimento e di affidabilità in vista della sua indipendenza, della qualità dei suoi pareri e dei risultati conseguiti, delle informazioni fornite, della trasparenza delle sue procedure e dei suoi moduli operativi nonché della sua diligenza nei compiti affidatigli. L'Agenzia avrebbe espletato i suoi compiti in stretto collegamento con gli Stati membri ed avrebbe dovuto essere aperta ai contatti con l'industria e con i gruppi interessati. Obiettivo principale dell'Agenzia, secondo il documento originario, sarebbe stato quello di facilitare l'applicazione delle iniziative e misure comunitarie relative alla sicurezza delle reti e dell'informazione ed aiutare ad ottenere la interoperabilità delle funzioni di sicurezza nella rete nei sistemi di informazione, contribuendo in tal modo al funzionamento del Mercato Interno e stimolando in ultima analisi le capacità della Commissione e degli Stati membri in tema di sicurezza delle reti e dell'informazione.

I compiti dell'Agenzia erano molteplici così come indicato nell'art. 2 della proposta originaria. Secondo gli intendimenti della Commissione, l'Agenzia avrebbe dovuto essere strutturata nel modo seguente:
a) Management Board;
b) Executive Director e relativo staff;
c) Advisory Board;
d) Working Groups (eventuali).

In relazione alla istituzione dell'Agenzia in questione il Consiglio il 5/6/2003 convenne un orientamento generale che conteneva tre modifiche rispetto al testo proposto dalla Commissione[10], e chiese al Comitato dei Rappresentanti permanenti di esaminare il parere del Parlamento Europeo (prima lettura) non appena disponibile per consentirgli di adottare una posizione comune in una delle successive sessioni. Il testo dell'Orientamento generale è stato approvato nell'ottobre scorso ma con due astensioni, una della delegazione tedesca ed una di quella inglese. A sua volta il Comitato economico e sociale emise il 18/06/2003 un parere favorevole ma con osservazioni in merito alla proposta della Commissione.

Il 20 novembre u.s. il Parlamento Europeo ha esaminato la proposta più volte citata approvandola ma con non trascurabili modifiche rispetto al documento originario della Commissione. Secondo la Risoluzione il compito dell'Agenzia deve essere quello di contribuire a mantenere un alto ed effettivo livello di " network and information security" nell'ambito della Comunità e di sviluppare una cultura della sicurezza informatica e delle reti a beneficio dei cittadini, dei consumatori e delle organizzazioni del settore pubblico e privato dell'Unione Europea, contribuendo in tal modo ad un corretto funzionamento del Mercato Interno.

[10] Le modifiche principali erano: a) limitazione dell'attività dell'Agenzia ad un ruolo di consultazione e soppressione delle disposizioni riguardanti il comitato consultivo; b) modificazione della composizione del Consiglio d'amministrazione con l'inclusione di un rappresentante per ciascuno Stato, di tre rappresentanti nominati dalla Commissione e di altri tre rappresentanti, privi del diritto di voto, ciascuno dei quali in rappresentanza dell'industria, della tecnologia dell'informazione e della comunicazione, dei gruppi di consumatori e degli esperti universitari in materia di sicurezza delle reti e dell'informazione.
Non può tacersi,come gia detto nel testo, che appare quantomeno strano che si sia trascurata del tutto la componente giuridica, giacché la funzione consultiva non può prescindere dalla conoscenza delle implicazioni giuridiche e normative della sicurezza informatica.

I molteplici compiti dell'Agenzia sono indicati dettagliatamente nell'art.3 della Risoluzione: il principale è quello di raccogliere le informazioni appropriate per analizzare i rischi correnti ed emergenti, in particolare a livello europeo, che potrebbero compromettere l'affidabilità delle reti di comunicazioni elettroniche ovvero l'autenticità, l'integrità e la riservatezza delle informazioni ricevute e trasmesse attraverso tali reti e fornire il risultato delle analisi agli Stati Membri della Comunità.

La struttura dell'Agenzia è così definita:

1) **Management Board**, composto da un rappresentante per ciascuno degli Stati Membri, tre rappresentanti nominati dalla Commissione,tre rappresentanti nominati dal Consiglio su nominativi proposti dalla Commissione, senza diritto di voto, ciascuno dei quali rappresenta uno dei seguenti gruppi: industria ITC, gruppi di consumatori, esperti accademici nel settore della sicurezza informatica e delle reti;

2) **Executive Director**, indipendente nelle sue funzioni, nominato dal Management Board per un periodo di cinque anni sulla base di una lista di candidati, meritevoli e dotati di documentate esperienze amministrative e manageriali proposti dalla Commissione a seguito di una "open competition" annunciata sulla GUCE;

3) **Permanent Group Stakeholders**, nominati dall'E.D. e che rappresentino importanti stakeholders, quali industrie ICT, gruppi di consumatori, esperti accademici nell'ambito della sicurezza delle reti e dell'informazione, avente funzione di consulenza per l'E.D. dal quale è presieduto.

È auspicabile che l'Agenzia dia risalto agli aspetti relativi alla componente giuridica, in quanto le funzioni da svolgere richiedono necessariamente il supporto di giuristi specializzati in materia di sicurezza informatica.

Per concludere, il problema relativo alla sicurezza informatica è certamente serio e non può essere risolto soltanto a livello nazionale, data la transnazionalità degli attacchi, per cui, superate le obiezioni di tipo giuridico e per evitare "situazioni di galleggiamento" della Agenzia in ambito comunitario, occorrono iniziative giuridiche e politico-legislative che diano vita ad organizzazioni corrispondenti nei Paesi membri, organizzazioni la cui esistenza appare il presupposto indispensabile per una azione comune e per un effettivo coordinamento operativo.

Proposte concernenti le strategie
in materia di sicurezza informatica
e delle telecomunicazioni (ITC)
per la pubblica amministrazione

Parte prima
proposte per un sistema di governo della sicurezza ict nella PA

2. Parte prima - Proposte per un sistema di governo della sicurezza ICT nella PA

2.1 Modello organizzativo

La gestione della sicurezza nella P.A. deve essere eseguita attraverso un opportuno processo che preveda lo sviluppo di politiche di sicurezza sia a livello di Amministrazione (l'intera P.A. o, se necessario, specifiche Pubbliche Amministrazioni o parti di esse) sia a livello di sistemi ICT. Nell'ambito di tali politiche uno degli aspetti più rilevanti è costituito dalla individuazione dei ruoli ai quali assegnare la responsabilità di svolgere le principali funzioni che le politiche stesse considerano necessarie ai fini di una corretta gestione della sicurezza. Alcuni di tali ruoli sono di tipo centralizzato e prevedono l'istituzione di appositi organismi attraverso i quali assicurare la fornitura di servizi di sicurezza utili per tutte le Pubbliche Amministrazioni, servizi che sarebbe antieconomico realizzare in ciascuna di esse. Altri ruoli sono invece da collocare all'interno delle singole Amministrazioni e sono stati in gran parte già definiti nell'allegato 2 della direttiva [1].
Un primo ruolo centralizzato è evidentemente quello attribuito con il decreto 24/7/2002 del Ministro delle Comunicazioni e del Ministro per l'Innovazione e le Tecnologie al Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni. Si tratta di un ruolo di coordinamento, indirizzamento e monitoraggio nella gestione della sicurezza ICT da parte delle Pubbliche Amministrazioni, come risulta dall'elenco dei compiti, riportato nell'introduzione, assegnato al Comitato.

Attualmente il Comitato non dispone tuttavia di risorse: pertanto non può offrire alla P.A. una serie di servizi operativi dei quali si percepisce invece una forte necessità.
Per tale motivo si ritiene che sia da considerare la sua confluenza in un apposito organismo dotato di mezzi atti a consentirne piena operatività, cui è stato assegnato il nome di Centro Nazionale per la Sicurezza Informatica (CNSI), e le cui funzioni verranno descritte nel paragrafo che segue.
Successivamente verranno trattati ulteriori organismi preposti alla fornitura centralizzata di servizi operativi e, a seguire, i ruoli da prevedere nell'ambito delle singole Amministrazioni al fine di completare la definizione del modello organizzativo.

2.1.1 Il Centro Nazionale per la Sicurezza Informatica (CNSI)

Nell'ambito di questa sezione si definisce quale potrebbe essere la struttura organizzativa del CNSI e le funzionalità che dovrebbe svolgere. Tale organismo, nelle intenzioni del Comitato, deve possedere autonomia organizzativa e contabile nelle forme di una agenzia o alto commissario.

Il CNSI è realizzato sulla base dei seguenti presupposti:
- Molte organizzazioni o loro responsabili che decidono di adottare soluzioni ICT spesso trascurano il problema sicurezza. Quindi non si preoccupano di proteggere i propri sistemi, che divengono così facili obiettivi di attacchi informatici. D'altro lato le tecnologie per la sicurezza sono difficili da comprendere e gestire correttamente.

Questo significa che vi è la necessità di incentivare azioni mirate a promuovere la sicurezza informatica nonché programmi di formazione per il corretto uso delle tecnologie.

- Laddove esistano contromisure efficaci per far fronte a problemi di sicurezza, la situazione può cambiare drasticamente nel caso di forme di attacco innovative o mutanti. In questi casi per individuare la soluzione ad un attacco informatico può essere necessaria la consultazione di esperti in diversi settori e la disponibilità di sofisticati laboratori di ricerca. Sono poche le organizzazioni che possono disporre di queste risorse.
- La soluzione di problemi derivanti dall'insicurezza dei sistemi può richiedere la collaborazione di più entità non necessariamente residenti nella stessa nazione; è quindi indispensabile per poter far fronte ad ogni problema di questo tipo contattare ed interallacciare rapporti con diverse organizzazioni di diversi paesi. Questa azione può essere svolta solo da opportuni organismi che abbiano ricevuto un riconoscimento nazionale ed internazionale che consenta loro lo svolgimento delle suddette "indagini".

Tutto ciò significa che il CNSI deve predisporre efficaci piani di consapevolezza, deve poter disporre di risorse e competenze per far fronte ad attacchi informatici sviluppando "intelligence" e soprattutto deve essere inserito in un contesto internazionale. Tale organismo, per poter svolgere efficacemente i propri compiti deve inoltre godere di particolari prerogative.

Il Centro Nazionale per la Sicurezza Informatica deve infatti essere autonomo ed indipendente da ogni fornitore di prodotti e servizi di sicurezza informatica; deve possedere, direttamente o indirettamente, le competenze necessarie per generare le informazioni di cui necessita e saper valutare criticamente quelle ottenute da altre fonti; deve inoltre essere messo in grado di emanare, nell'ambito delle proprie competenze, direttive a tutte le Pubbliche Amministrazioni. Accanto a queste prerogative il CNSI ha degli obblighi verso i propri utenti: a fronte di una richiesta d'intervento da parte di un utente deve essere in grado di garantire, in ogni situazione, tempi di risposta estremamente contenuti, e deve essere in grado di generare e distribuire informazioni di qualità molto elevata.

2.1.2 Le funzionalità del Centro Nazionale per la Sicurezza Informatica

Gli obiettivi principali del Centro Nazionale per la Sicurezza Informatica devono essere:

- accrescere il livello medio di protezione dei sistemi informatici degli utenti Internet Italiani con particolare riferimento agli utenti della Pubblica Amministrazione;
- predisporre le misure adeguate per far fronte ad eventuali attacchi informatici a sistemi della PA;
- predisporre le misure adeguate per ripristinare in tempi brevi i sistemi compromessi.

Si riporta di seguito un elenco dettagliato delle attività che devono essere intraprese dal CNSI. Per una migliore chiarezza espositiva si suddividono in tre categorie in base al loro principale scopo: prevenzione, rilevamento e risposta.

Prevenzione

Promuovere programmi per accrescere la consapevolezza del problema sicurezza informatica tra gli utenti della rete Internet. Come già accennato precedentemente diversi prodotti e metodologie sono disponibili per far fronte al problema della sicurezza informatica; la grande maggioranza degli utenti della rete ne ignorano, però, i fondamenti essenziali o addirittura ignorano il problema.

Studiare, valutare e promuovere l'uso di "best practice" nel settore della sicurezza informatica. La maggior parte delle tecnologie e metodologie di sicurezza sono relativamente moderne e tra gli utenti non esiste sufficiente esperienza nell'uso di questi strumenti. È necessario quindi un piano per la diffusione di informazioni sull'uso e l'applicazione degli stessi. Tale informazione deve coprire diversi settori che vanno dai processi aziendali legati alla sicurezza, agli schemi per la classificazione delle informazioni, ai meccanismi di identificazione/autenticazione, PKI, firewall, intrusion detection system, sand-box, ecc. ecc..
Promuovere attività di ricerca e la cooperazione tra i centri di ricerca. La ricerca è l'unico strumento che può essere utilizzato per aumentare il livello di sicurezza degli attuale prodotti ICT e per creare e diffondere il livello di conoscenza necessario per far fronte o prevenire nuove forme di intrusione informatica. È quindi necessario promuovere la creazione di centri di ricerca nel settore della sicurezza informatica e costituire uno stretto legame tra il CNSI e questi centri.

Raccogliere e distribuire informazioni aggiornate sulle intrusioni e relative contromisure. È necessario rendere disponibili tutte le informazioni legate a nuove forme di intrusione al fine di consentire agli utenti di poterle riconoscere. A tal fine è indispensabile costruire un data base pubblico contente questo tipo di informazioni. Nella diffusione di tali informazioni è inoltre da privilegiare un approccio "push", essere cioè propositivi e tempestivi nella diffusione di informazioni aggiornate.

Promuovere corsi di formazione per i dipendenti della Pubblica Amministrazione . La formazione è il primo passo da compiere per far crescere negli utilizzatori delle tecnologie la consapevolezza del problema sicurezza. Nell'ambito della Pubblica Amministrazione il problema è particolarmente sentito ed è quindi necessario predisporre un massiccio programma di formazione per tutti gli utilizzatori.

Promuovere il ricorso agli standard di sicurezza. La certificazione dell'IT security in accordo agli standard riconosciuti a livello internazionale rappresenta un mezzo importante per costruire la fiducia e la confidenza sia nei confronti di un'organizzazione che tra le varie parti coinvolte. In sostanza, due standard ISO/IEC sono applicabili per la certificazione. Lo standard ISO 15408, noto anche come Common Criteria for Information Technology Security, che fornisce le principali direttive per la valutazione e certificazione di prodotti e sistemi informatici. Lo standard ISO 17799, che invece fornisce importanti indicazioni sulle misure organizzative da intraprendere, in un'azienda, per poter far fronte al problema della sicurezza informatica.

Rilevamento
Controllare le attività svolte sulla rete. Al fine di individuare situazioni anomale correlate ad attacchi in corso è necessario controllare costantemente la rete. Esistono tecnologie che potrebbero essere utilizzate per supportare questo tipo di attività, che denominiamo monitoraggio attivo. Il monitoraggio attivo è molto importante poiché consente di "catturare" sul nascere un tentativo di intrusione o un attacco in corso. Questo tipo di monitoraggio consente inoltre di raccogliere dati attendibili sulle intrusioni informatiche che possono essere proficuamente utilizzati per previsioni e trend nel settore.

Collezionare ed analizzare tutte le segnalazioni provenienti dagli utenti finali. Un altro modo per monitorare la rete, che possiamo chiamare monitoraggio passivo, è quello di raccogliere le segnalazioni di intrusioni inoltrate da utenti finali e, dopo averle analizzate, utilizzarle per gli scopi di cui al punto precedente. Questo approccio richiede però che l'utente finale possieda una notevole padronanza delle tecnologie, requisito soddisfatto solo in minima parte dagli utenti della rete.

Risposta

Fornire supporto agli utenti vittime di un'intrusione. Individuata o ricevuta la segnalazione di un'intrusione è necessario fornire il necessario supporto, in termini di competenze tecniche, alla vittima. Gli obiettivi di questa fase devono essere: ridurre l'impatto dell'attacco sul sistema vittima, tentare di risalire all'intrusore e consentire il ripristino dei sistemi compromessi nel minor tempo possibile.

Contattare uno o più centri di ricerca. Al fine di individuare la tecnica utilizzata e le contromisure da adottare, i dati relativi all'intrusione devono essere inviati ad esperti del settore che dalla loro analisi potranno risalire alle cause ed alle origini. Una volta individuate le cause sarà estremamente facile individuare le contromisure per evitare l'attacco. Questa fase si rende ovviamente necessaria solo per intrusioni di cui non si conoscono gli effetti e le contromisure.

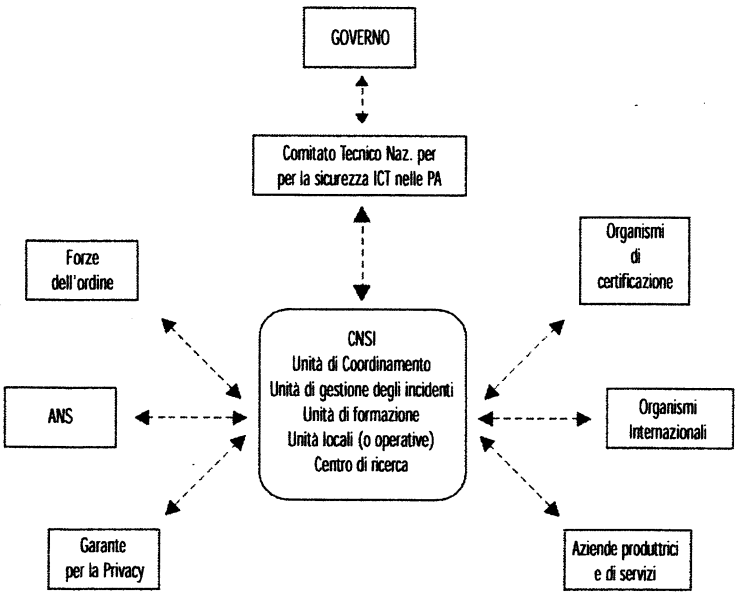
Allertare tutti i responsabili di sistemi che possono essere oggetto di un attacco simile. Un altro modo per ridurre gli effetti di un attacco informatico è quello di limitare il numero di sistemi compromessi. Questo effetto può essere ottenuto allertando in tempo debito tutte le potenziali vittime di un attacco e fornendo loro le istruzioni per come far fronte allo stesso.
Diffondere l'informazione a livello internazionale. Nel caso in cui ci si trovi di fronte ad una nova forma di attacco informatico è necessario allertare l'intera comunità Internet; è quindi necessario che il CNSI sia in collegamento con organismi equivalenti in tutto il mondo.

2.1.3 La struttura del Centro Nazionale per la Sicurezza Informatica

Al fine di assicurare la massima tempestività nella diffusione delle informazioni, di garantire un assoluto livello di qualità e omogeneità della stessa e di poter aver una visione unica e complessiva sulla situazione di sistemi della P.A. è importante che il CNSI sia, logicamente parlando, un'unica entità che opera su scala nazionale. Fisicamente si può ipotizzare che lo stesso sia composto da diverse unità dislocate sul territorio nazionale; è però importante che le stesse facciano riferimento ad un unico centro di raccordo. Inoltre si ritiene che debba trattarsi di un organismo civile che non mancherà però di avere i necessari rapporti con le forze dell'ordine, l'Autorità Giudiziaria, l'Autorità Nazionale per la Sicurezza ed ogni altra istituzione che a livello nazionale si occupa del problema. Il modello proposto individua nell'ambito del CNSI cinque componenti fondamentali che devono cooperare affinché il CNSI possa raggiungere i propri obiettivi.
Riportiamo una breve descrizione di queste componenti e rinviamo ai paragrafi successivi una descrizione più dettagliata degli stessi. Talune componenti potrebbero essere realizzate presso singole P.A., ove esistano già le necessarie competenze. In altri casi il CNSI potrà attivare convenzioni con Enti esterni pubblici o privati per la fornitura parziale o totale dei servizi di una componente.

1. Unità di coordinamento: il compito principale del centro di coordinamento è quello di raccordare tutte le attività intraprese dalle varie unità che operano all'interno della struttura, di raccogliere, elaborare e distribuire informazioni, di coordinare le attività delle varie unità operative e fornire alle stesse il necessario supporto.
2. Unità di gestione degli incidenti informatici: si tratta di un'unità preposta al rilevamento delle intrusioni informatiche sui sistemi della Pubblica Amministrazione ed alla loro gestione. Questa unità svolge anche il ruolo di centro early warning e information sharing, come sarà chiarito nella sezione successiva.
3. Unità di formazione: compito di questa Unità è la predisposizione e l'erogazione di corsi di formazione per i dipendenti della P.A. in tema di sicurezza ICT.
4. Unità Locali (o Operative): si tratta di organismi tecnici preposti alla gestione operativa della sicurezza informatica, che svolgono il loro operato presso le Pubbliche Amministrazioni dove operano di concerto con il CNSI e quindi svolgono anche una funzione di raccordo tra il CNSI e le varie sedi della Pubblica Amministrazione. Ogni istituzione di rilievo della P.A. deve prevedere una di queste unità operativa.
5. Centro di ricerca Il principale scopo di questo centro di ricerca è quello di creare il corpo di conoscenze e di esperienze necessarie per risolvere casi di minacce o attacchi informatici particolarmente complessi, prevedere nuove forme di attacco informatico e virus. Un ulteriore compito svolto da questo centro è la formazione del personale del CNSI con alti contenuti scientifici e tecnologici nel settore della sicurezza informatica.
6. Una rete di rapporti e collaborazioni con istituzioni ed Enti che a livello nazionale ed internazionale si occupano della problematica. Riportiamo brevemente in Figura 1 un possibile schema di interrelazioni che il CNSI dovrà sviluppare. Queste relazioni si dovranno concretizzare attraverso la definizione e la realizzazione di tavoli di lavoro comuni, osservatori su tematiche di comune interesse, studi e ricerche comuni, ecc. ecc.

Figura 1: Schema delle interrelazioni del CNSI



2.1.3.1 L'Unità di Coordinamento

È la componente del CNSI incaricata di attivare e dirigere tutte le attività del Centro, promuovere specifiche attività di ricerca nel settore, svolgere le funzioni di raccolta e smistamento delle informazioni e fornire supporto consulenziale a tutte le Pubbliche Amministrazioni, specie quando vengono richieste rapide implementazioni di progetti o misure preventive urgenti. Questa componente del CNSI deve anche farsi carico di intrattenere rapporti con equivalenti organismi che operano a livello internazionale nello stesso settore.

I principali obiettivi che l'unità di coordinamento dovrebbe perseguire sono:

- aumentare il livello di consapevolezza del problema "sicurezza informatica" in tutta la PA;
- predisporre azioni al fine di migliorare le capacità di prevenzione degli incidenti informatici nella PA;
- adoperarsi affinché il CNSI diventi, nel panorama nazionale, un punto di riferimento nonché un centro di eccellenza nelle diverse tematiche che caratterizzano la sicurezza informatica (Metodologiche, Legali, Tecniche);
- costruire rapporti tra il CNSI e tutte le istituzioni, che nel panorama nazionale si interessano al problema;
- fungere da unità di crisi in caso di gravi problemi riguardanti il mondo dell'IT;
- adoperarsi affinché, attraverso il CNSI, il livello di esposizione al rischio informatico delle singole amministrazioni, diminuisca sensibilimente.

Accanto alle necessarie competenze di management l'Unità di coordinamento dovrà anche possedere quelle di ordine tecnologico per i seguenti motivi:

- accrescere la credibilità dell'istituzione verso il mondo esterno;
- consentire all'unità di coordinamento di disporre di una fonte di informazioni garantita in situazioni critiche.
- svolgere al meglio le funzioni di rappresentanza nei rapporti internazionali.

Il team di supporto tecnico deve sempre mantenere un alto livello di competenze tecnologiche, in particolar modo riguardo ai prodotti commerciali, specialmente quelli diffusamente utilizzati nei settori pubblici e deve essere in grado di operare negli ambiti qui sotto riportati.

- selezione dei prodotti ICT in base alle proprietà di sicurezza;
- formazione, informazione e consiglio sulle tecnologie dell'IT security;
- assistenza attiva durante gli incidenti informatici più critici;
- penetration testing;
- analisi di software;
- altri tipi di supporto tecnico nel campo dell'IT security.

2.1.3.2 Le Unità di gestione degli incidenti e di formazione

Queste unità vengono diffusamente descritte nel seguito del documento.

2.1.3.3 Le Unità Locali (o Operative)

Ogni pubblica amministrazione, sia centrale che locale, è direttamente responsabile per la realizzazione di un livello sufficiente di sicurezza nei confronti dei propri sistemi informatici. Ciò significa che ogni Amministrazione deve essere in grado di identificare e di valutare le conseguenze della sua dipendenza dall'IT e di occuparsi dei rischi implicati da tale dipendenza. Più precisamente ogni amministrazione deve provvedere alla elaborazione di

una propria politica di sicurezza che includa, tra l'altro, un piano di Business Continuity. La struttura organizzativa delle unità locali è definita successivamente, nell'ambito del paragrafo che tratta i ruoli nelle singole Amministrazioni.
In questo quadro al CNSI è attribuita la responsabilità di fornire a tutte le Amministrazioni, attraverso le unità locali, le competenze necessarie per svolgere le attività sopra descritte e fornire un supporto operativo nella fase di monitoraggio dei sistemi e gestione degli incidenti. Sarà quindi indispensabile garantire lo scambio reciproco di informazioni tra il CNSI e queste Amministrazioni ai fini di consentire ad entrambi di mantenere adeguatamente aggiornato il proprio livello di informazione.

2.1.3.4 Centro di ricerca

Nell'organigramma del CNSI il centro di ricerca svolge il ruolo di fonte di notizie e competenze per il centro di coordinamento del CNSI e per l'Unità di Gestione degli Incidenti. Il centro di ricerca potrà assistere le altre entità espletando studi o ricerche, per acquisire informazioni esaustive e per assicurare la formazione del personale specialistico. Come già anticipato il Centro di Ricerca non è necessariamente un organo del CNSI ma può essere costituito da una o più entità esterne con il quale il centro di coordinamento decide di stabilire dei rapporti di collaborazione. Anche in questo caso visto il ruolo di indipendenza che il CNSI deve mantenere rispetto al mercato, è auspicabile che i centri individuati non siano Enti appartenenti ad organizzazioni commerciali.

2.1.4 Rapporti con le altre istituzioni

Di fondamentale importanza per il CNSI è possedere la massima visibilità su ciò che accade sia in ambito nazionale che internazionale nel settore della sicurezza informatica: a tal scopo è necessario che il CNSI intrattenga regolari rapporti con Enti nazionali ed internazionali che perseguano obiettivi equivalenti, come di seguito riportati.

2.1.4.1 Forze dell'ordine

Nel nostro paese tutte le forze dell'ordine (Polizia, Finanza e Carabinieri) posseggono unità specializzate per la lotta contro il crimine informatico nelle diverse forme in cui si presenta. È indispensabile per il CNSI stabilire dei rapporti di collaborazione e di reciproco scambio di informazioni con ciascuna di queste unità.

2.1.4.2 Autorità Nazionale per la Sicurezza

È estremamente importate che il CNSI sia raccordato con l'Autorità Nazionale per la Sicurezza e che tra i due Enti si instauri un rapporto di reciprocità improntato allo scambio di informazioni e alla produzione di documenti e linee guida comuni.

2.1.4.3 Organismi di Certificazione

Come descritto nel seguito del documento, le certificazioni di sicurezza possono essere eseguite sia a livello dell'organizzazione sia a livello dei sistemi ICT. In quest'ultimo caso la struttura nell'ambito della quale le certificazioni vengono eseguite viene denominata Schema Nazionale di Certificazione ed è coordinata da un Organismo di Certificazione governativo. Nel quadro della sicurezza informatica del paese lo Schema Nazionale svolge quindi un ruolo molto critico. È quindi estremamente importante che lo stesso, tramite l'Organismo di Certificazione, stabilisca con il CNSI un rapporto di stretta collaborazione per un reciproco travaso di competenze e di informazione.

2.1.4.4 Altri Enti privati

Nella lotta all'insicurezza informatica è estremamente importante che i settori pubblici e privati che operano nel settore siano in grado di condividere le conoscenze e fornire supporto reciproco per far fronte alle "emergenze informatiche". È quindi auspicabile che nell'ambito del settore privato nascano delle iniziative analoghe al CNSI con le quali interallacciare stretti rapporti di collaborazione. A tale riguardo vale forse la pena rifarsi all'esperienza USA dove il 22 maggio 1998 attraverso la direttiva presidenziale USA PDD-63, è stata data la spinta decisiva per la nascita di Information Sharing and Analisys Center (ISAC), all'interno di ognuno dei settori ritenuti critici per la sicurezza della nazione. Brevemente ricordiamo che gli ISAC sono associazioni di aziende private preposte alla diffusione di dati relativi agli attacchi ed alle vulnerabilità informatiche. Il sistema ISAC raccoglie questi dati dai propri membri e da altre fonti esterne e li diffonde ai propri membri dopo averli opportunamente analizzati ed integrati in un'immagine coerente che rispecchi lo stato attuale della minaccia informatica.

2.1.4.5 Cooperazione internazionale

La società dell'informazione non conosce confine; proprio per questo motivo e per proteggerla da attacchi di diverso tipo, deve essere prevista una struttura di difesa che operi e che si basi sulla cooperazione internazionale. È quindi importante che il CNSI instauri contatti stabili con la nascente Agenzia Europea per la Sicurezza Informatica (ENISA), l'Agenzia statunitense per la Sicurezza Informatica, il NISCC inglese (National Infrastructure Security Coordination Centre), il SEMA (Swedish Emergency Management Agency) svedese, il BSI (Bundesamt fur Sicherheit in der Informationstechhnik) tedesco, il "Secrétrariat Général de la Défense Nazionale", francese.
Il nostro Paese inoltre dovrebbe assumere un ruolo attivo nei processi che si occupano della definizione di standard comuni per la sicurezza, nei processi che si occupano di trattamento delle informazioni e nella definizione delle infrastrutture IT.
L'Italia dovrebbe anche sostenere attivamente gli accordi e le regole internazionali riguardo la rilevazione di attività non autorizzate all'interno de sistemi informativi e nel settore informatico in generale. Tali rilevazioni possono, sotto ben definiti vincoli di privacy e di segretezza, avvenire anche all'interno dei confini nazionali.

2.1.5 L'Unità di gestione degli attacchi informatici

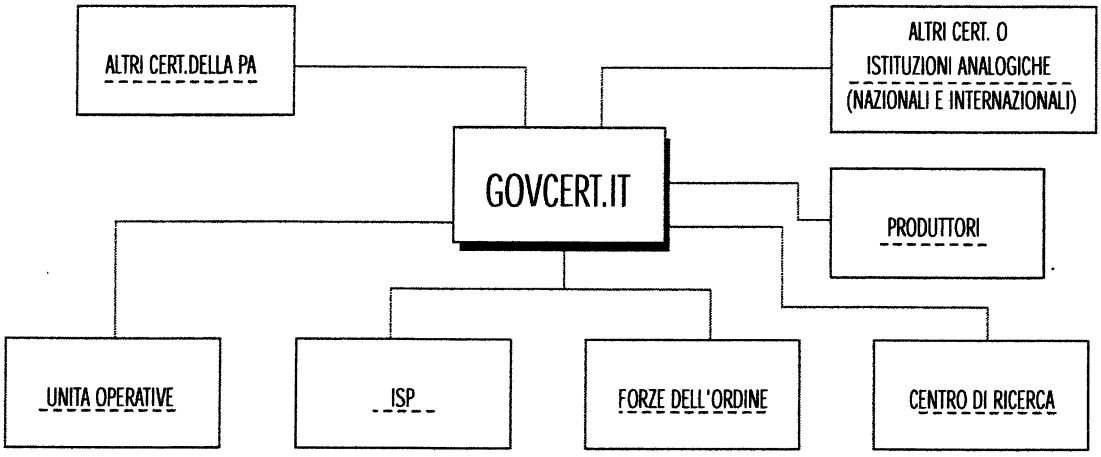
Nell'ambito della sicurezza informatica una particolare attenzione è sicuramente rivolta agli attacchi informatici, definiti come una serie di attività svolte intenzionalmente da un "avversario" per ottenere un accesso non autorizzato ad un sistema informatico. Nell'ambito del CNSI si è quindi pensato di predisporre un'apposita unità preposta a gestire i diversi aspetti legati alla prevenzione, al rilevamento ed alla gestione degli attacchi informatici. Vista la complessità sia in termini di articolazione che di funzionalità che questa unità deve possedere si riportano qui di seguito, seppur sommariamente le funzionalità che devono essere svolte da questa unità:

- Information sharing: inteso come la possibilità di condividere informazioni ed esperienze relative ad attacchi o più in generale vulnerabilità informatiche con entità equivalenti che operano sul territorio nazionale o in ambito internazionale;
- Early Warning: inteso come capacità di avvisare tempestivamente i responsabili delle infrastrutture informatiche, sulla presenza di nuove vulnerabilità e nuovi pericoli;

- Rilevamento e gestione delle intrusioni: l'unità deve intervenire direttamente a risolvere situazioni di incidente informatico in tutte quelle pubbliche amministrazioni che non dispongono di una propria struttura per lo svolgimento di questa funzione, o può operare in supporto ad altre strutture equivalenti nella soluzione di intrusioni informatiche;
- Distribuzione di informazioni per la prevenzione degli incidenti informatici;
- Raccolta ed elaborazione delle informazioni relative agli incidenti informatici.

Per svolgere queste funzioni l'unità si avvale di un Computer Emergency Response Team che opera a livello di pubblica amministrazione e che al fine di evitare equivoci potrà denominarsi GOVCERT.IT. Al fine di acquisire una reale efficacia è importante che il GOVCERT.IT operi in stretta collaborazione con le entità che si indicano in Figura 2.

Figura 2: Struttura dell'Unità per la gestione degli attacchi informatici



Di seguito si descrivono queste entità ed il ruolo che le stesse svolgono nell'ambito dell'unità di gestione degli attacchi informatici.

2.1.5.1 GOVCERT.IT

Si tratta dell'organismo su cui è imperniata l'intera Unità. Lo scopo principale di GOVCERT.IT deve essere quello di gestire gli attacchi IT non solo a livello dell'Amministrazione centrale, ma, eventualmente e in conformità con adeguati accordi, anche a livello di Amministrazioni locali. Non solo attraverso il monitoraggio attivo il GOVCERT.IT sarà in grado di intercettare preventivamente i tentativi di intrusione e quindi ridurre drasticamente l'impatto degli stessi. Il GOVCERT.IT deve diventare, per tutta la P.A., il punto di riferimento per quanto riguarda le informazioni che riguardano gli attacchi informatici: tecniche di intrusione, vulnerabilità, minacce e patch. Il team deve svolgere i seguenti compiti:

- ricevere i reports degli attacchi;
- distribuire alarms e warnings in relazione ad attacchi informatici;

- mantenere le statistiche sugli attacchi informatici;
- dare supporto e informazioni riguardo a contromisure per prevenire gli attacchi informatici;
- fornire informazioni su rischi, vulnerabilità e minacce;
- svolgere su richiesta e previo nulla osta del Centro di coordinamento, attività di penetration testing sui sistemi dell'Amministrazione;
- fornire supporto alle P.A. qualora le stesse siano oggetto di un attacco informatico ovvero un virus. Tale supporto si esplica nel fornire indicazioni alle persone che presidiano i sistemi informatici delle suddette P.A. sulle azioni più appropriate da eseguire per ridurre gli effetti dell'intrusione e quelle da intraprendere per ripristinare i sistemi compromessi dall'attacco;
- diffondere le informazioni di sicurezza preventiva inerenti i sistemi in possesso delle P.A.;
- cooperare con organi nazionali e internazionali nella prevenzione delle intrusioni informatiche;
- cooperare con le forze dell'ordine nella prevenzione e gestione delle intrusioni informatiche;
- stimolare la nascita di organismi equivalenti in ambito pubblico e privato;
- monitorare la rete della P.A. centrale al fine di intercettare eventuali attacchi informatici (7 x24);
- promuovere l'effettuazione di esercitazioni.

È estremamente importante che GOVCERT.IT sia formato da personale altamente qualificato che gli consenta di guadagnare credibilità e reputazione nell'ambito della comunità Internet e di conseguenza quella visibilità che è necessaria per poter consentire ad un CERT di operare con il massimo rendimento.
Nel nostro continente in particolare i Governi di Francia, Germania, Inghilterra, Olanda, Svezia e Finlandia hanno già provveduto a costituire un CERT per la Pubblica Amministrazione centrale.

La collocazione operativa dell'Unità è presso il CNIPA, al fine di avvalersi delle capacità tecniche ivi residenti. È prevedibile un impegno di circa 15 persone. Sono anche da prevedere eventuali servizi erogati da fornitori esterni opportunamente selezionati. Si può stimare come previsione dei costi per un biennio di attività la cifra di 2,5 mln di euro.

2.1.5.2 Altri CERT della PA

Come già anticipato è necessario prevedere che alcune Pubbliche Amministrazioni decidano di costituire in propria autonomia l'Unità di risposta alle intrusioni informatiche. Ad oggi, ad esempio risulta che il Ministero della Difesa abbia già da tempo attivato, nell'ambito dello Stato Maggiore della Difesa, un CERT denominato CERT.DIFESA.IT, che opera su tutti gli Enti di competenza del Ministero della Difesa. Sicuramente altre amministrazioni vorranno seguire l'esempio del Ministero della Difesa mentre altre decideranno di affidarsi al GOVCERT.IT.

Nell'ambito del Piano Nazionale della sicurezza informatica è però fondamentale che siano stabiliti degli stretti contatti tra questi organismi e che sia creato uno spirito di collaborazione e scambio di informazione. In particolare sarà necessario prevedere momenti di incontro periodici per lo scambio di informazioni, iniziative comuni quali la

predisposizione di alert, linee guida ecc. ecc. È importante che tutti gli altri CERT della P.A. possano avvalersi delle risorse messe a disposizione da GOVCERT.IT per la soluzione dei problemi più incombenti.

2.1.5.3 Altri CERT o organi equivalenti

Attualmente esistono più di 120 CERT al mondo, di cui 79 in Europa. Questi CERT si sono federati al fine di facilitare lo scambio di informazioni e l'aiuto reciproco, in due grosse organizzazioni il FIRST (Forum of Incident Response and Security Teams), che opera a livello mondiale e il TF-CSIRT (Task Force- Computer Security Incident Response Team) una task force costituita presso la Trans-European Academic Network (TERENA), che accorpa la stragrande maggioranza dei CERT Europei. È estremamente importante che GOVCERT.IT aderisca e partecipi attivamente a queste istituzioni al fine di allargare sempre più il proprio bagaglio di conoscenze ed esperienze. Ovviamente stretti rapporti dovranno anche essere allacciati con i due CERT che attualmente operano a livello nazionale: il CERT-IT e il GARR-CERT.

2.1.5.4 Unità Locali (o Operative)

Si è già parlato delle unità locali nel paragrafo 2.1.3.3. e si è sottolineato che queste unità devono possedere anche competenze tecniche. Le unità locali con l'ausilio del GOVCERT.IT forniscono supporto alle proprie amministrazioni e le aiutano a risolvere situazioni critiche, provvedendo anche a mantenerle aggiornate sui problemi di sicurezza informatica. Le unità locali possono essere coinvolte nella preparazione e diffusione di programmi di formazione per il personale tecnico delle amministrazioni e di sessioni di divulgazione per gli utenti finali. Nel caso in cui un'unità locale non riuscisse a risolvere un problema posto da un'amministrazione farà riferimento al GOVCERT.IT o al CNSI.

2.1.5.5 Internet Service Provider

Gli ISP sono una componente importante dell'intera organizzazione e sono attualmente gli unici organismi in grado di raggiungere ogni utente Internet, in particolare ogni Pubblica Amministrazione, e consentire attività di monitoraggio attivo. Essi possono facilmente raggiungere ogni utente ad essi connesso per inviargli messaggi informativi o di allerta, oppure possono ricevere segnalazioni dagli stessi da trasmettere agli organi competenti della struttura. Gli ISP sono anche i punti dove è possibile inserire sistemi di monitoraggio di una serie di parametri quantitativi del traffico di rete che consentono di intercettare sul nascere eventi anomali. Un ISP che riceve la notifica di un'intrusione o un tentativo di intrusione può risolvere il caso, se possiede le necessarie competenze, oppure rivolgersi all'unità operativa del CNSI.

2.1.5.6 Produttori

Con il termine "Produttori" ci si riferisce a tutti gli operatori che realizzano prodotti software, in particolare sistemi operativi e prodotti di sicurezza, con particolare riferimento ai produttori di antivirus. È estremamente importante avere dei contatti diretti con queste aziende poiché tipicamente sono proprio i sistemi operativi o più in generale i prodotti software che contengono dei buchi di sicurezza, e quindi quando queste debolezze sono rilevate è necessario rifarsi immediatamente al relativo costruttore perché lo stesso individui le patch correttive da applicare. Nel caso di virus è invece molto importante potersi rifare ai costruttori di antivirus perché preparino nel minor tempo possibile il relativo antidoto.

2.1.5.7 Centri di Ricerca

Per la soluzione di particolari problemi o casi di intrusione il centro di coordinamento deve potersi avvalere dell'apporto di uno o più centri di ricerca specializzati nei diversi settori della sicurezza informatica. Il principale scopo di questi centri di ricerca è quello di creare, attraverso attività di ricerca, il corpo di conoscenze e di skill necessari per risolvere casi particolarmente complessi, prevedere nuove forme di attacco informatico e virus.

2.1.5.8 La gestione degli Incidenti

Dopo aver descritto le principali componenti e le relative attività degli organismi che compongono l'unità di gestione degli attacchi informatici del CNSI se ne delineano qui le modalità operative nella gestione di un incidente, ferme restando le altre funzionalità.

La gestione di un incidente avviene solitamente attraverso le seguenti fasi:
- l'unità operativa dell'Amministrazione che subisce l'intrusione contatta il GOVCERT.IT via email o web server segnalando l'intrusione e gli effetti da questa provocati; nel caso in cui per l'Amministrazione in questione sia stato attivato un servizio di monitoraggio attivo sarà il GOVCERT.IT che attiverà automaticamente la procedura di gestione degli incidenti avvertendo l'unità operativa di riferimento;
- ricevuta la segnalazione il CERT provvede a registrare l'incidente e a studiare le caratteristiche dell'attacco; individuate le quali si può risalire alle cause che hanno consentito l'attacco e quindi alla loro rimozione; in questa fase il GOVCERT.IT può avvalersi della sua rete di collaborazioni; in prima istanza può interpellare la comunità dei CERT ed il proprio centro di ricerca;
- se ci si trova di fronte ad una nuova forma di virus o di attacco informatico si allerta attraverso i propri canali di comunicazione (in particolare gli ISP) l'intera comunità Internazionale e si attivano i costruttori di antivirus o i produttori del prodotto compromesso per individuare delle patch risolutive o l'antivirus;
- si contatta poi il provider dal cui dominio proveniva l'intrusione per tentare di raccogliere informazioni sul possibile intrusore e contemporaneamente si coinvolgono le forze dell'ordine; nel caso in cui l'intrusione provenga dall'estero si contatta il CERT di riferimento;
- individuate le contromisure, si ricontatta l'unità operativa del sito colpito e gli si forniscono le informazioni necessarie per ripristinare la situazione rimuovendo le cause che hanno consentito l'intrusione;
- l'incidente viene chiuso.

Per molte delle suddette comunicazioni è ovviamente opportuno disporre di un canale di comunicazione cifrato, ma questi dettagli sono al di fuori della portata di questo documento.

Con questo modo di procedere si raggiungono almeno tre scopi:
- chi riporta l'incidente riceve l'assistenza necessaria per risolvere i propri problemi;
- in caso di nuove forme di attacco è possibile allertare in tempo debito la comunità internazionale;
- i dati raccolti possono essere utilizzati per scopi statistici e fornire informazioni essenziali per l'identificazione di attacchi contro il paese e i suoi interessi nazionali.

2.1.5.9 Early Warning e Information Sharing

Per sistema di Early Warning si intende una struttura che sia in grado di diffondere capillarmente e in tempo utile informazioni il più possibile accurate su nuove minacce o precauzioni da prendere per proteggere i propri sistemi informatici da nuove forme di attacco. Tutta la comunità internazionale è protesa alla realizzazione di sistemi di early warning che sono ritenuti uno strumento estremamente importate per ridurre drasticamente gli effetti di un'intrusione informatica. Le informazioni che devono essere distribuite sono disponibili da diverse fonti ma generalmente in forma non direttamente accessibile ad un utente medio.

Queste informazioni sono:
- Warning e Alert: sono documenti che descrivono imminenti minacce o vulnerabilità di sistemi informatici; sono rilasciati dalle più svariate fonti e nelle più svariate modalità.
- Servizi di helpdesk: necessari per supportare gli utenti nella comprensione dei documenti sopra menzionati o per ripristinare il sistema in caso di incidente informatico.

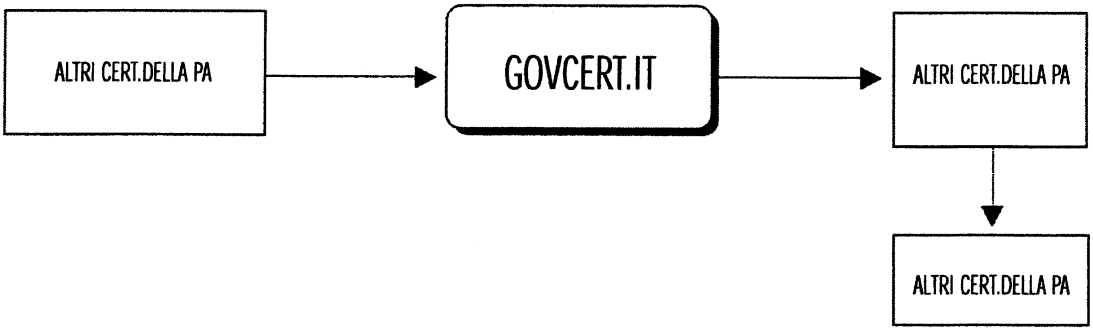
Come già detto queste informazioni sono in gran parte disponibili sulla rete; non tutti gli attori però ne vengono in possesso nello stesso istante. Per rendere il processo di diffusione di queste informazioni il più rapido possibile è quindi necessario prevedere delle forme di condivisione delle informazioni (Information Sharing) tra tutti gli Enti che possono accedere ad esse. In una prima fase è necessario definire delle iniziative di Information Sharing a livello nazionale e in un secondo tempo estendere le stesse a livello internazionale. Per la realizzazione di tali iniziative è consigliabile ispirarsi alle diverse iniziative in vari stati.

Le più significative sono:
- la comunità dei CERT/CSIRT svolge questa attività da lungo tempo, le informazioni diffuse in questo caso però oltre a non essere sufficientemente tempestive, sono molto specialistiche e quindi dirette solo agli addetti ai lavori;
- negli USA sotto la spinta governativa sono stati avviati gli ISAC, già precedentemente descritti. Attualmente sono in corso negli USA iniziative per consentire lo scambio di informazioni tra i diversi ISAC ed è allo studio la realizzazione di una rete per collegare tra loro CERT, ISAC e centri di studio e ricerca, questa rete è stata per ora denominata Cyber Warning & Information Network (CWIN);
- in UK l'istituzione governativa NISCC (Nationl Infrastructure Security Coordination Centre) fornisce informazioni sulla sicurezza informatica a tutti le istituzioni governative e attraverso il sito web a tutti i cittadini;
- simili attività sono svolte in Francia dal CERT-A, nei Paesi Bassi dal CERRT-RO, in Germania dal CERT-BUND e in Finlandia dal CERT-FI.

Tutte queste iniziative sottolineano l'importanza dell'argomento e riteniamo che lo stesso debba essere affrontato anche nel nostro paese. In particolare il CNSI dovrebbe farsi promotore per la costruzione di una simile struttura che dovrebbe essere costruita intorno al GOVCERT.IT. Come già anticipato una simile struttura deve essere basata su una fitta rete di comunicazione con tutti gli attori che operano su Internet al fine di consentire:
- un'intercettazione immediata delle informazioni dal momento del loro rilascio;
- una diffusione capillare della stessa.

È quindi fondamentale che nell'ambito di questa struttura il CNSI stringa accordi di partnership con tutte le entità che sono in grado di fornire informazioni utili allo scopo. È inoltre auspicabile che anche in ambito privato si provveda alla costituzione di strutture che facilitino lo scambio di informazioni tra le varie realtà e con le quali sarebbe più facile stipulare accordi. In prospettiva la struttura di early warning del CNSI potrebbe essere la seguente:

Figura 3: Struttura del sistema di Early Warning del CNSI



2.1.6 L'Unità di formazione

Un'adeguata gestione della sicurezza ICT all'interno della P.A. non può prescindere dalla necessità che tutti i soggetti coinvolti in tale gestione siano in grado di svolgere con la sensibilità e la competenza richieste i compiti associati al ruolo che ricoprono (per quanto riguarda l'affidabilità, che è ovviamente altrettanto importante, sono state svolte varie considerazioni nel paragrafo relativo alla gestione del personale).

Ciò vale ad esempio per i dirigenti, che devono possedere un'adeguata sensibilità per le problematiche di sicurezza ed essere consapevoli dei danni, spesso cospicui, che possono derivare dalla mancata protezione del patrimonio informativo trattato dai sistemi ICT dell'Amministrazione. In assenza di tale sensibilità e consapevolezza, infatti, con l'attuale crescita dei fenomeni di cybercrime, si dovrebbero più attentamente rilasciare le autorizzazioni, da parte delle Direzioni, per gli investimenti nel campo della sicurezza.
Discorso analogo può farsi per i soggetti che ricoprono ruoli di responsabilità nella gestione tecnica della sicurezza ICT (ad esempio il Responsabile della sicurezza ICT, il Responsabile dei sistemi informativi automatizzati ed i suoi assistenti, l'Addetto alle verifiche di sicurezza ICT ed i suoi assistenti): tali soggetti, infatti, devono mantenere costantemente aggiornate conoscenze tecniche altamente specialistiche al fine di consentire la prevenzione degli incidenti di sicurezza o almeno la minimizzazione dei relativi danni.
La carrellata sui soggetti per i quali è richiesta un'adeguata sensibilizzazione e formazione non sarebbe completa se non si considerassero gli utenti finali dei sistemi ICT dell'Amministrazione, per i quali è estremamente importante il possesso di conoscenze che garantiscano la corretta utilizzazione dei servizi di sicurezza disponibili sui sistemi ICT utilizzati (ad esempio scelta idonea delle password e oculata gestione delle stesse, collaborazione nell'aggiornamento del sw, nella misura stabilita dal Responsabile dei sistemi informativi automatizzati, ecc.) e la padronanza delle norme e procedure di sicurez-

za riferibili agli utenti (ad esempio sollecita segnalazione di anomalie ai responsabili della gestione tecnica della sicurezza ICT, esecuzione periodica di back-up ove tale servizio non sia disponibile in forma centralizzata, eventuali divieti di stabilire connessioni della rete dell'Amministrazione con l'esterno utilizzando collegamenti modem, ecc.).

Inevitabilmente, nei casi in cui tra il personale di un'Amministrazione non siano presenti soggetti in possesso delle competenze necessarie per qualcuno dei ruoli sopra descritti, non rimane altra scelta che affidarsi inizialmente a risorse esterne (outsourcing). È però del tutto evidente che la P.A. dovrebbe tendere a non delegare ad altri una materia così delicata come la sicurezza ICT e dovrebbe conseguentemente arrivare a disporre di professionalità tali da consentirle di ricoprire con risorse interne i vari ruoli sopra descritti. Ciò potrà realizzarsi solo se la P.A. si doterà permanentemente di un'Unità di formazione nel campo della sicurezza ICT che riesca a raggiungere con corsi, diversificati in base al ruolo ricoperto, il maggior numero possibile di dipendenti della P.A. Sarà anche importante che dopo la prima erogazione dei corsi vengano previsti frequenti aggiornamenti per evitare che le conoscenze trasferite con la prima erogazione diventino rapidamente superate.

Per tale motivo si è deciso di inserire nell'ambito del CNSI un'unità appositamente dedicata alla formazione. I principali obiettivi che questa unità si propone sono:
- creare la necessaria consapevolezza in ordine alle minacce, vulnerabilità e rischi che potenzialmente possono gravare sul patrimonio informativo della P.A.;
- generare la conoscenza di base per comprendere i fabbisogni di sicurezza e relativi accorgimenti di prevenzione/protezione in termini organizzativi, operativi, tecnologici e giuridico-normativi;
- promuovere l'utilizzo di adeguate metodologie e strumenti relativamente alla gestione dei processi fondamentali della sicurezza;
- monitorare e valutare il grado di fruizione dei corsi ed il livello di apprendimento dei partecipanti individuando le azioni di miglioramento;
- istituire l'eventuale attività di "tutoraggio" on-line per supportare approfondimenti su temi specifici.

I compiti e le competenze di questa unità sono:
- predisporre i contenuti dei programmi di formazione;
- predisporre i tempi ed i modi per l'erogazione dei suddetti corsi;
- indirizzare e coordinare i docenti e le attività formative;
- promuovere i contatti con i media al fine di pubblicizzare adeguatamente l'iniziativa formativa sulla sicurezza del patrimonio informativo della P.A.;
- partecipare alle sessioni dei corsi sia come osservatore sia come portatore di competenze e know how;
- valutare l'andamento dei corsi evidenziando eventuali disallineamenti con gli obiettivi definiti, provvedendo ad un pronto reindirizzamento delle attività ed eventualmente dei contenuti dei corsi.

La collocazione operativa dell'Unità è presso l'Istituto Superiore di Comunicazioni (Ministero delle Comunicazioni).
Si può stimare come previsione dei costi per un biennio di attività la cifra di 2,5 mln di euro.

2.2 Ruoli delle singole amministrazioni: le unità locali.

Le unità locali sono di fatto il front-end del CNSI. È attraverso queste unità che le informazioni e le iniziative elaborate dal CNSI sono trasmesse alle singole amministrazioni, e che i problemi di queste ultime, in materia di sicurezza informatica, possono essere portati all'attenzione del CNSI. Per lo svolgimento di queste funzionalità è fondamentale che le singole amministrazioni si dotino di un'adeguata infrastruttura, sinora genericamente indicata come unità locale. Nell'ambito di un'unità locale accanto ai ruoli già definiti nell'allegato 2 della direttiva[1] [1] ne vanno aggiunti altri che rendano possibile una capillare attuazione della politica di sicurezza ed un'altrettanto capillare verifica circa l'attuazione stessa.
Prima di descrivere tali ruoli è opportuno precisare che, sebbene sia auspicabile la loro ricopertura da parte di personale della PA, può ritenersi ammissibile il coinvolgimento di risorse esterne (outsourcing) ove non esistano o sia troppo costoso formare le competenze necessarie. Tale giudizio potrebbe però mutare una volta che fosse diventato pienamente operativo l'organismo responsabile della formazione e sensibilizzazione dei dipendenti della P.A. nell'area della sicurezza ICT, che in effetti trova come importante motivazione per la sua costituzione anche il risparmio economico per la P.A. relativamente alle voci di spesa connesse con le esternalizzazioni dei servizi di sicurezza. In ogni caso è comunque estremamente importante che nei casi di outsourcing siano ben definite contrattualmente le responsabilità e gli impegni che il fornitore del servizio deve assumersi, in sintonia con quanto previsto in [4].
Di seguito vengono riportati per comodità alcuni dei ruoli già definiti nell'allegato 2 della direttiva [1] per ogni singola Amministrazione. Più precisamente vengono presi in considerazione quei ruoli per i quali si ritiene necessario integrare i compiti già associati ad essi nella direttiva [1] con ulteriori compiti che tengono conto di quanto previsto nel presente documento. Successivamente verranno invece descritti i ruoli aggiuntivi che si ritiene opportuno introdurre.

Comitato per la Sicurezza ICT
È l'organo cui viene demandata, in base alla direttiva [1] la politica della sicurezza delle infrastrutture tecnologiche e del patrimonio informativo gestito prevalentemente con soluzioni automatizzate. Ne fanno parte a titolo di esempio:
- il responsabile/coordinatore generale per la legge 626
- il responsabile/coordinatore generale per la legge 675
- il responsabile della segreteria NATO/UEO o di analoga articolazione per il segreto di Stato
- il responsabile dei sistemi informativi ex d.lgs. 39/93
- il responsabile della sicurezza ICT (da nominare ove non previsto)
- il responsabile della sicurezza delle infrastrutture e del controllo degli accessi
- il responsabile dell'ufficio legislativo
- il responsabile della programmazione e pianificazione finanziaria

Alla luce di quanto esposto nei precedenti paragrafi, al Comitato per la Sicurezza ICT dovrebbero in particolare essere assegnati i seguenti compiti principali:

[1] Per i riferimenti tra parentesi quadre ved. paragrafo 2.3.8

- definire, ove necessario, una politica di sicurezza ICT dell'Amministrazione per gestire in modo specifico la protezione di particolari informazioni/servizi dell'Amministrazione, fornendo indicazioni di maggior dettaglio rispetto a quelle generali contenute nella politica di sicurezza della P.A.; a tal fine dovrà essere applicata una opportuna metodologia di analisi e gestione dei rischi;
- richiedere, se necessario, assistenza al Comitato Tecnico Nazionale per la sicurezza informatica e delle telecomunicazioni nelle Pubbliche Amministrazioni relativamente alla definizione della politica di sicurezza ICT dell'Amministrazione;
- trasmettere al responsabile della sicurezza ICT le indicazioni della politica di sicurezza ICT della P.A. e della eventuale politica di sicurezza ICT dell'Amministrazione ai fini del loro recepimento all'interno dell'Amministrazione;
- nominare l'Addetto alle verifiche di sicurezza ICT, ruolo più avanti definito;
- gestire l'aggiornamento della politica di sicurezza ICT dell'Amministrazione tenendo anche conto delle indicazioni del Responsabile della sicurezza ICT, dell'Addetto alle verifiche di sicurezza ICT, del Responsabile dei sistemi informativi automatizzati e dei Proprietari dei dati e delle applicazioni.

Responsabile della sicurezza ICT

In base alla direttiva [1] è il soggetto cui compete la definizione delle soluzioni tecniche, in attuazione delle direttive impartite direttamente dal Ministro o su indicazione del Comitato per la sicurezza ICT. La definizione delle soluzioni tecniche deve essere eseguita dal Responsabile della sicurezza ICT sviluppando opportune politiche di sicurezza dei sistemi ICT che trattano le informazioni e applicazioni utilizzate nell'ambito dell'Amministrazione. Tale sviluppo deve essere eseguito partendo dalle indicazioni contenute nella politica di sicurezza della P.A. e nella eventuale politica di sicurezza dell'Amministrazione e si deve avvalere di una metodologia di analisi e gestione dei rischi, come descritto nel seguito. Il Responsabile della sicurezza ICT ha il compito di fornire al Responsabile dei sistemi informativi automatizzati le definizioni relative alle soluzioni tecniche al fine della loro realizzazione e del monitoraggio del loro corretto funzionamento.

Responsabile dei sistemi informativi automatizzati

È il referente istituito dal decreto legislativo 39/93, cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza, la committenza delle attività da affidare all'esterno. Il Responsabile dei sistemi informativi automatizzati può nominare suoi Assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'amministrazione.

Gestore esterno

È il fornitore di servizi che opera sotto il controllo del responsabile dei sistemi informativi. Fintanto che non sarà completata l'attuazione di un adeguato piano di formazione e sensibilizzazione del personale della P.A. in tema di sicurezza ICT attraverso l'istituzione dell'apposito organismo i soggetti che ricopriranno questo ruolo potranno anche svolgere servizi critici dal punto di vista della sicurezza (ad esempio quelli connessi con i ruoli, successivamente descritti, di Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT). In tali casi è estremamente importante che l'Amministrazione si cauteli adeguatamente esplicitando chiaramente nei contratti gli obblighi e le responsabilità che il Gestore esterno deve assumersi nel

fornire il servizio e mantenendo il più possibile un controllo sugli aspetti di maggiore criticità che caratterizzano il servizio stesso.

Proprietario dei dati e delle applicazioni
È ciascun direttore generale per la sfera di informazioni di diretta competenza o trattamento. Ai fini di una corretta gestione della sicurezza ICT è necessario che i Proprietari dei dati e delle applicazioni interagiscano strettamente con il Comitato per la Sicurezza ICT sia in una fase iniziale, ai fini dell'eventuale predisposizione di una politica di sicurezza ICT dell'Amministrazione, sia successivamente, per garantire un tempestivo aggiornamento della politica stessa reso necessario da significative variazioni relative ai dati e alle applicazioni gestite.

Gli ulteriori ruoli, non esplicitamente definiti nella direttiva [1], che si ritiene necessario considerare sono descritti nel seguito.

Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT
A tale importante ruolo compete principalmente il compito di provvedere alla prima installazione e configurazione delle misure di sicurezza sui sistemi ICT dell'amministrazione e al costante aggiornamento hw/sw di tali sistemi al fine di eliminare o ridurre tempestivamente le vulnerabilità note che per tali sistemi vengono scoperte. I soggetti che ricoprono questo ruolo potranno ricevere indicazioni circa l'aggiornamento dei sistemi ICT dal Responsabile della sicurezza ICT, dal Responsabile dei sistemi informativi automatizzati e direttamente dall'organismo GOVCERT.IT, una volta che sia stato istituito e che risulti operativo.

Addetto alle verifiche di sicurezza ICT
Secondo quanto specificato nella direttiva [1], svolge un'attività di controllo saltuaria che si sviluppa attraverso un vero e proprio audit. Tale audit deve mirare a verificare la completa e corretta realizzazione delle soluzioni tecniche ed il recepimento di tutte le indicazioni contenute nella politica di sicurezza della PA, nella eventuale politica di sicurezza dell'Amministrazione e nelle Politiche di sicurezza dei sistemi ICT. Ove necessario l'Addetto alle verifiche di sicurezza ICT potrà avvalersi di tecniche di penetration testing al fine di verificare la resistenza dei sistemi ICT dell'Amministrazione ad eventuali attacchi. In base al principio della separazione dei compiti enunciato nella direttiva [1], l'Addetto alle verifiche di sicurezza ICT non può essere chi ha il compito di installare, configurare e aggiornare le soluzioni tecniche definite dal Responsabile della sicurezza ICT (Assistente del Responsabile dei sistemi informativi automatizzati nel campo della sicurezza ICT). Nei casi in cui sia richiesto un livello di sicurezza più elevato alle verifiche periodiche eseguite dai soggetti che ricoprono questo ruolo dovrà essere aggiunta l'effettuazione di vere e proprie certificazioni della sicurezza ICT.
L'Addetto alle verifiche di sicurezza ICT può nominare suoi Assistenti in numero proporzionato alla complessità dei servizi informatici gestiti dall'amministrazione.

Assistente dell'Addetto alle verifiche di sicurezza ICT
A tale importante ruolo compete principalmente il compito di eseguire sui sistemi ICT dell'Amministrazione il piano di auditing sviluppato dall'Addetto alle verifiche si sicurezza ICT.

2.3 Il "processo della sicurezza ICT" nella PA

L'adozione e la gestione delle più appropriate misure di sicurezza ICT nell'ambito di un'organizzazione richiede alla stessa la rivisitazione e l'adeguamento di una serie di processi e funzioni dando vita a quello che viene solitamente definito come il processo della sicurezza ICT. Queste misure correttive sono generalmente introdotte in maniera graduale e sono definite in un documento noto come politica di sicurezza[12]. La definizione di questo documento è quindi un requisito irrinunciabile per la predisposizione e la buona riuscita di un processo di "messa in sicurezza" di un'organizzazione. A tale proposito vale la pena ricordare che nell'ambito di un'organizzazione una politica di sicurezza può essere sviluppata a diversi livelli:

- a livello dell'intera organizzazione (nel caso in esame la P.A.), in questo caso il documento raccoglierà tutte le prescrizioni che si ritiene debbano valere in qualsiasi parte dell'organizzazione stessa; può essere utile precisare che, pur essendo d'alto livello, questo documento non deve necessariamente limitarsi a contenere prescrizioni molto generali. È infatti anche possibile includere in tale politica eventuali specifiche tecniche dettagliate che si desideri siano soddisfatte da tutti i sistemi ICT dell'organizzazione;
- a livello di singole componenti, nel caso di un'organizzazione molto complessa (come la PA), può essere conveniente sviluppare ulteriori politiche di sicurezza valide per una singola Amministrazione o per parti di essa. In genere tale convenienza sussiste quando è possibile individuare un dominio sufficientemente ampio entro il quale si debbano adottare modalità di gestione e protezione omogenee che non siano già previste nella politica di sicurezza dell'intera organizzazione;
- Nelle politiche di sicurezza fin qui citate, che si possono considerare di tipo organizzativo, non sono trattate in modo completo le modalità secondo le quali i singoli sistemi ICT devono gestire e proteggere le informazioni da essi trattate. A tale scopo devono infatti essere sviluppate ulteriori politiche di sicurezza valide per sistemi ICT specifici o per classi di essi. Nelle politiche di sicurezza di tipo organizzativo, tuttavia, vengono generalmente fornite indicazioni circa le modalità secondo le quali si ritiene che le politiche dei sistemi ICT debbano essere sviluppate.

Di seguito sono riportate alcune indicazioni in merito ai processi, che nell'ambito della P.A. devono essere coinvolti dal processo di sicurezza, e un primo insieme di prescrizioni, le più rilevanti ad un elevato livello di generalità, che si ritiene debbano essere inserite nella politica di sicurezza di una Amministrazione al fine di garantire una efficace protezione del patrimonio informativo da essa gestito. Ovviamente tale elenco non è da ritenersi esaustivo ma vuole semplicemente essere una base comune di riferimento per tutte le amministrazioni. In particolare si ritiene che la maggior parte delle indicazioni contenute in questa sezione debba essere considerata nella stesura di un documento di politica di primo livello cioè il cui dominio di applicazione è l'intera Pubblica Amministrazione. A tale proposito si rammenta che per P.A. si intendono i destinatari della direttiva [1] e quindi:

[12] Per politica di sicurezza si intende l'insieme delle leggi, regole e pratiche (di tipo tecnico, o di tipo procedurale o attinenti alla sicurezza fisica e del personale) che regolano la gestione e protezione dei beni (principalmente le informazioni) all'interno del dominio di validità della politica stessa.

- le Amministrazioni dello Stato
- le aziende ed Amministrazioni autonome dello Stato
- gli Enti pubblici non economici nazionali.

Nel seguito del presente documento, per semplicità espositiva si è scelto di indicare con il termine generico "Amministrazione" un'organizzazione pubblica che sia di uno dei tipi sopra elencati.

2.3.1 Adozione di una metodologia di analisi del rischio

Ogni Amministrazione che intenda provvedere allo sviluppo di adeguate politiche di sicurezza dovrà necessariamente rifarsi ad una metodologia di analisi del rischio inteso come quel processo necessario per identificare i rischi di sicurezza e determinarne la loro portata. In altri termini l'analisi del rischio è quel processo che definisce le esigenze di sicurezza ICT di un'organizzazione e concorda su quali siano le più appropriate misure di controllo.

A tal fine ogni Amministrazione potrà avvalersi di una metodologia di analisi e gestione dei rischi che segua l'approccio descritto in [1]. Tale approccio si basa sulla considerazione che un'analisi accurata di tutti i sistemi ICT richiederebbe tempi e costi molto elevati che spesso non risulterebbero giustificati dall'entità dei rischi associati ai sistemi stessi. Conseguentemente l'approccio prevede che su tutti i sistemi ICT (o classi di essi) venga preliminarmente eseguita un'analisi dei rischi ad alto livello che consenta di stimare approssimativamente il livello di rischio. Successivamente si procede nel modo seguente:

1) per tutti i sistemi ICT che l'analisi preliminare ha riconosciuto "a basso rischio" viene adottata una protezione di base tra quelle comunemente riconosciute valide per la tipologia dei sistemi stessi (si veda a tal proposito il paragrafo denominato "Adozione di standard per la sicurezza")
2) per tutti i sistemi ICT ad elevata criticità viene eseguita un'analisi dei rischi accurata basata su metodologie strutturate (un esempio di tale metodologia è fornito in [3], e nella seconda parte di questo documento sono riportate delle linee guida per l'individuazione di una corretta metodologia di analisi dei rischi).

2.3.2 Adozione di un piano di Business Continuity

Naturalmente tutti gli sforzi devono essere compiuti affinché gli incidenti informatici non abbiano a verificarsi, adottando le opportune contromisure sia livello tecnico sui sistemi ICT sia a livello organizzativo. Nei casi, tuttavia, in cui l'incidente finisce ugualmente per verificarsi è estremamente importante che sia stato sviluppato e che sia pienamente operativo un piano che garantisca il più possibile la continuità dei servizi offerti dai sistemi ICT colpiti dall'incidente. A tale scopo è necessario che sia sviluppato per l'intera P.A. un piano di Business Continuity. Lo scopo di questo piano è quello di individuare tutte le misure (tecnologiche e organizzative) atte a garantire la continuità dei processi dell'organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni. Nella seconda parte di questo documento sono riportate delle linee guida su come debba essere affrontato questo problema nell'ambito della Pubblica Amministrazione.

2.3.3 Stesura di capitolati per l'acquisizione di sistemi/prodotti ICT dotati di funzionalità di sicurezza

Una volta selezionate, con l'ausilio di una metodologia di analisi e gestione dei rischi, le funzionalità di sicurezza di cui deve essere dotato un sistema/prodotto ICT di cui necessita la P.A. diventa molto importante formularne le specifiche in modo accurato e non soggetto a molteplici interpretazioni da parte dei fornitori. A tal fine il riferimento a precise specifiche tecniche quali gli standard effettivi o de facto costituisce la soluzione più consigliabile. A tal proposito ricordiamo che per quanto riguarda l'individuazione di funzionalità di sicurezza idonee a contrastare le minacce ipotizzabili per il sistema valide indicazioni possono essere trovate in [8] e, soprattutto, in [12]. A tal riguardo si può fare ad esempio riferimento al paragrafo 2.5 che riporta i meccanismi di sicurezza che sono stati oggetto di standardizzazione da parte di ISO/IEC/JTC1/SC27. Qualora si sia interessati a contrastare minacce tipiche per una prefissata tipologia di prodotto, un ausilio particolarmente valido è costituito dai cosiddetti Protection Profile, sviluppati utilizzando lo standard ISO/IEC IS 15408 (Common Criteria) per la valutazione della sicurezza di sistemi e prodotti ICT.

2.3.4 Gestione del personale

Il personale addetto all'utilizzo dei sistemi ICT che tratta informazioni e applicazioni rilevanti dal punto di vista della sicurezza ICT e, soprattutto, il personale che ricopre i ruoli di gestione della sicurezza ICT sopra descritti deve essere attentamente selezionato sulla base di criteri di affidabilità e competenza, in modo da rendere il più possibile basso il rischio che tale personale possa compiere, intenzionalmente o accidentalmente, azioni che compromettano la protezione delle informazioni e applicazioni dell'Amministrazione. È anche necessario che il personale suddetto sia messo in condizione di svolgere al meglio i suoi compiti, dotandolo delle risorse e del supporto necessari e consentendogli la fruizione di un adeguato piano di formazione e sensibilizzazione nell'area della sicurezza ICT. Inoltre dovrà essere garantita un'alta motivazione del personale, preferibilmente istituendo ruoli specifici per la sicurezza ICT che prevedano un trattamento adeguato alle responsabilità assunte. Queste ultime, d'altro canto, dovranno essere ben esplicitate e formalizzate negli incarichi conferiti, così come previsto in [3], [4], [5] e [6].

2.3.5 Sicurezza nell'accesso di terze parti ai sistemi ICT della P.A.

È evidente che non avrebbe senso gestire adeguatamente il personale della P.A. che utilizza i sistemi ICT se non ci si preoccupasse anche dell'accesso ai sistemi stessi che la P.A. deve consentire a soggetti esterni per offrire alcuni servizi. In parte il tema è stato già trattato nell'ambito delle considerazioni svolte relativamente al ruolo "Gestore esterno" previsto nella direttiva [1]. Considerazioni del tutto analoghe possono essere qui ripetute, conformemente a quanto previsto in [3] e [4], per qualsiasi accesso di terze parti ai sistemi ICT della P.A.. Ad esempio per gli accessi che, diversamente da quelli del Gestore esterno, sono necessari per la fornitura di un servizio da parte della P.A. piuttosto che da parte del soggetto esterno. Occorrerà infatti, soprattutto nei casi in cui sia inevitabile concedere privilegi di accesso particolarmente elevati, far assumere formalmente alla terza parte impegni e responsabilità che la obblighino a comportamenti corretti sotto il profilo della sicurezza ICT. In tali casi, inoltre, la massima attenzione dovrà essere posta nell'equipaggiare i sistemi ICT della P.A. con funzionalità di sicurezza (controllo d'accesso, monitoraggio delle azioni degli utenti, ecc.) che offrano le più ampie garanzie.

2.3.6 Outsourcing

Come già evidenziato precedentemente è facile che nel settore della sicurezza ICT, a causa di carenza di competenze interne, un'Amministrazione sia costretta ad affidare la gestione della propria sicurezza ICT a risorse esterne (outsourcing). In questi casi va ribadita la necessità di un controllo molto rigoroso da parte dell'Ente committente e l'esplicita richiesta di particolari requisiti da parte del fornitore del servizio, in specie per quanto riguarda la serietà delle garanzie offerte, con particolare riguardo all'affidabilità e professionalità del personale incaricato.
Va comunque fatto salvo il principio che la "cabina di regia" in tema di sicurezza informatica resti saldamente nelle mani dell'Amministrazione.

2.3.7 Il ricorso alle certificazioni di sicurezza nella PA

Definiamo in questa sezione una serie di indicazioni che è opportuno seguire relativamente all'uso delle certificazioni di sicurezza nell'ambito di una Pubblica Amministrazione.

2.3.7.1 Le certificazione della sicurezza ICT

I due principali tipi di certificazione della sicurezza ICT oggi utilizzati sono stati entrambi oggetto di standardizzazione ISO/IEC, sebbene per uno dei due, come vedremo, il relativo processo non si può considerare completo. Più precisamente nel 1999 è stata adottata in tutte le sue tre parti dall'ISO/IEC la raccolta di criteri denominata Common Criteria che consente la valutazione e certificazione della sicurezza di prodotti e sistemi ICT. Tale adozione si è formalmente realizzata attraverso l'emanazione dello standard ISO/IEC IS 15408. L'anno successivo, questo stesso organismo internazionale ha fatto propria solo la prima parte di un altro standard di certificazione della sicurezza ICT che è stato sviluppato in Gran Bretagna, il ben noto BS7799 che nella versione ISO/IEC ha assunto la denominazione IS 17799-1.
La seconda parte dello standard, quella che contiene le indicazioni più precise ai fini della certificazione, è invece al momento disponibile solo come standard della British Standards Institution. Lo standard ISO/IEC IS 15408 (Common Criteria) e la coppia di standard ISO/IEC IS 17799-1 e BS7799-2, sebbene abbiano in comune la sicurezza ICT, hanno lo scopo di certificare cose ben diverse. Nel caso dei Common Criteria (in seguito denominati brevemente CC), infatti, oggetto della certificazione è, come già anticipato, un sistema o un prodotto ICT[13], nel caso invece del BS7799 ciò che viene certificato è il processo utilizzato da un'organizzazione, sia essa una società privata o una struttura pubblica, per gestire al suo interno la sicurezza ICT (tale processo, come è noto, viene indicato nello standard con l'acronimo ISMS che sta per "Information Security Management System"). In altri termini, la certificazione BS7799 può essere considerata una certificazione aziendale, del tipo quindi della ben nota certificazione ISO 9000, ma specializzata nel campo della sicurezza ICT[14].

---

[13] Un sistema ICT, secondo la terminologia utilizzata nei CC, è un'installazione informatica utilizzata per scopi ben specificati e in un ambiente operativo completamente definito. Un prodotto ICT, invece, è un dispositivo hardware o un pacchetto software progettato per l'uso e l'installazione in una grande varietà di sistemi.

[14] La precisazione circa l'oggetto della certificazione è opportuna poichè, alcune caratteristiche dello standard britannico BS7799-2 potrebbero generare confusione e far ritenere che la relativa certificazione possa rendere quasi superflua la certificazione Common Criteria. Infatti, tra i requisiti che un'organizzazione deve soddisfare per poter ottenere una certificazione BS7799, ve ne sono anche alcuni che rappresentano requisiti funzionali per i sistemi/prodotti ICT dell'organizzazione. Ai fini della certificazione BS7799, tuttavia, è sufficiente verificare che i suddetti requisiti funzionali siano stati selezionati sulla base di una corretta analisi e gestione dei rischi e verificare a campionamento che le corrispondenti funzioni di sicurezza siano presenti sui sistemi ICT ove risultano necessarie. *(Segue)*

2.3.7.2 I servizi di certificazione in Italia

Le valutazioni e certificazioni della sicurezza di sistemi/prodotti ICT sono state effettuate in Italia a partire dal 1995 limitatamente al settore della sicurezza nazionale. Più precisamente, fino alla primavera del 2002 sono stati obbligatoriamente sottoposti a certificazione secondo i criteri europei ITSEC tutti i sistemi/prodotti ICT utilizzati in ambito militare per trattare informazioni classificate concernenti la sicurezza interna ed esterna dello stato. Con il DPCM dell'11 aprile 2002, pubblicato sulla Gazzetta Ufficiale n. 131 del 6 giugno 2002, è stata resa obbligatoria la certificazione anche per i sistemi/prodotti ICT che trattano informazioni classificate al di fuori del contesto militare e si è prevista la possibilità di utilizzare i CC in alternativa ai criteri ITSEC. La struttura utilizzata per le suddette valutazioni e certificazioni include un Organismo di certificazione, le cui funzioni sono svolte dall'Autorità Nazionale per la Sicurezza - Ufficio Centrale per la Sicurezza (ANS-UCSi), e da un certo numero di Centri di Valutazione (Ce.Va.). Attualmente sono accreditati quattro Ce.Va., uno solo dei quali appartenente alla P.A., ossia quello gestito dall'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione del Ministero delle Comunicazioni (ISCTI).
Recentemente é stato istituito un nuovo Schema Nazionale utilizzabile per valutare e certificare, secondo i CC o i criteri ITSEC, i sistemi/prodotti ICT che non trattino informazioni classificate. In tale Schema è previsto che il ruolo di Organismo di certificazione sia svolto dall'ISCTI.

Per quanto riguarda invece le certificazioni di sicurezza relative allo standard BS7799 due organismi sono stati accreditati in Italia dal Sincert per operare in accordo alla parte due dello standard britannico, la quale come già detto, non è stata fino ad oggi recepita dall'organismo internazionale ISO/IEC.

2.3.7.3 Indicazioni relative all'utilizzo delle certificazioni nell'ambito della P.A.

Per quanto riguarda la coppia di standard ISO/IEC IS 17799-1 e BS7799-2, i principi ispiratori sono stati già recepiti negli allegati 1 e 2 della direttiva [1]. Tuttavia alcune delle verifiche previste negli standard sono state affidate alle singole Amministrazioni, mentre ovviamente in una certificazione sono svolte da un organismo accreditato. Tale scelta iniziale ha evidentemente il limite di non garantire che chi esegue le verifiche abbia tutte le competenze allo scopo necessarie e che il principio di separazione dei compiti di realizzazione e di verifica della sicurezza indicato nella direttiva [1] sia soddisfatto. Sulla base delle informazioni derivabili dal questionario di autovalutazione descritto nell'allegato 1 della direttiva [1], nonché di ulteriori informazioni disponibili sulle singole Amministrazioni, il Comitato potrà raccomandare, nei casi in cui risultino situazioni di elevata criticità per le quali si debbano richiedere elevate garanzie circa il processo di gestione della sicurezza ICT, che vengano eseguite vere e proprie certificazioni BS7799-2 in singole Amministrazioni o in parti di esse.
In questi stessi casi potrà essere raccomandato dal Comitato che almeno i sistemi/prodotti ICT che gestiscono le informazioni e le applicazioni che necessitano di una elevata protezione siano sottoposti a certificazione secondo i Common Criteria o i criteri ITSEC.

---

[14] *(Segue da pag. 38)* Ai fini di una eventuale certificazione Common Criteria di un sistema/prodotto ICT dell'organizzazione, occorrerebbe invece verificare che le suddette funzionalità non contengano difetti realizzativi e siano in grado di resistere, fino ad una soglia fissata dal grado di severità della valutazione, ad un insieme di minacce specificate in un ambiente ben definito

Questa indicazione può considerarsi in linea con quanto previsto nel documento [14] che presenta come consigliabile l'uso della certificazione di sicurezza:

1) per i sistemi che trattano informazioni le quali, sebbene non classificate ai fini della sicurezza nazionale, possono essere considerate critiche o essenziali per lo svolgimento delle funzioni primarie dell'Amministrazione,
2) per i sistemi da cui dipendono l'operatività e/o la manutenzione delle infrastrutture critiche.

Inoltre nel documento [10] viene affermato che il governo statunitense si propone di verificare, dal punto di vista della fattibilità economica, l'estensione dell'obbligo di certificazione ai sistemi/prodotti ICT utilizzati da tutte le agenzie federali, anche nei casi in cui non trattino informazioni classificate. Il governo statunitense prevede peraltro che, qualora tale estensione possa essere effettuata, essa influenzerebbe molto positivamente il mercato dei prodotti ICT consentendo di godere dei relativi benefici anche al di fuori del contesto governativo.

2.4 Documenti di riferimento

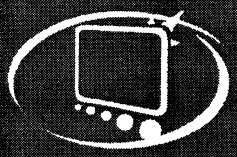
[1] Direttiva 16 gennaio 2002 del Presidente del Consiglio dei Ministri "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali" (pubblicata sulla G.U. n.69 del 22 marzo 2002).
[2] Decreto 24 luglio 2002 del Ministro delle comunicazioni e del Ministro per l'innovazione e le tecnologie "Istituzione del Comitato Tecnico Nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni".
[3] ISO/IEC IS 17799-1 - Information security management - Part 1: Code of practice for information security management - Standard.
[4] BS7799-2 - Information security management systems - Specification with guidance for use.
[5] ISO/IEC TR 13335-1, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 1: Concepts and models of IT security
[6] ISO/IEC TR 13335-2, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 2: Managing and planning IT security
[7] ISO/IEC TR 13335-3, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 3: Techniques for the management of IT security
[8] ISO/IEC TR 13335-4, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 4: Selection of safeguards
[9] ISO/IEC TR 13335-5, Information technology - Security techniques - Guidelines for the management of IT security (GMITS) - Part 5: Management guidance on network security
[10] The National Strategy to Secure Cyberspace - Documento governativo USA - Febbraio 2003.
[11] ISO/IEC IS 15408-1 Evaluation Criteria for Information Technology Security - Part 1: Introduction and general model.
[12] ISO/IEC IS 15408-2 Evaluation Criteria for Information Technology Security - Part 2: Security functional requirements.
[13] ISO/IEC IS 15408-3 Evaluation Criteria for Information Technology Security - Part 3: Security assurance requirements.
[14] National Security Telecommunications and Information Systems Security Committee (NSTISSC) - "National Security Telecommunications and Information Systems

Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products" - Documento governativo USA - Gennaio 2000

2.5 Elenco meccanismi di sicurezza standardizzati da ISO/IEC/JTC1/SC27

ISO/IEC FDIS 7064:	(2002), Data processing - Check character systems (2nd edition, revision of ISO 7064: 1983)
ISO 8372: 1987,	Modes of operation for a 64- bit block cipher algorithm
ISO/IEC 9796-2:	(2002), Digital signature schemes giving message recovery - Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:	1999, Digital signatures schemes giving message recovery - Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:	1999, Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:	(2002), Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-1:	1997, Entity authentication - Part 1: General (2nd edition)
ISO/IEC 9798-2:	1999, Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms (2nd edition)
ISO/IEC 9798-3:	1998, Entity authentication - Part 3: Mechanisms using digital signature techniques (2nd edition)
ISO/IEC 9798-4:	1999, Entity authentication - Part 4: Mechanisms using a cryptographic check function (2nd edition)
ISO/IEC 9798-5:	1999, Entity authentication - Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 9979:	1999, Procedures for the registration of cryptographic algorithms (2nd edition)
ISO/IEC 10116:	1997, Modes of operation for an n-bit block cipher algorithm (2nd edition, in fase di revisione)
ISO/IEC 10118-1:	2000, Hash-functions - Part 1: General (2nd edition)
ISO/IEC 10118-2:	2000, Hash-functions - Part 2: Hash-functions using an n-bit block cipher algorithm (2nd edition)
ISO/IEC 10118-3:	1998, Hash-functions - Part 3: Dedicated hash-functions
ISO/IEC 10118-4:	1998, Hash-functions - Part 4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:	1996, Key management - Part 1: Framework
ISO/IEC 11770-2:	1996, Key management - Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:	1999, Key management - Part 3: Mechanisms using asymmetric techniques
ISO/IEC 13888-1:	1997, Non-repudiation - Part 1: General (in fase di revisione)
ISO/IEC 13888-2:	1998, Non-repudiation - Part 2: Using symmetric techniques
ISO/IEC 13888-3:	1997, Non-repudiation - Part 3: Using asymmetric techniques
ISO/IEC TR 14516:	2002 (ITU-T X.842), Guidelines on the use and management of Trusted Third Party services (in attesa di pubblicazione)

ISO/IEC 14888-1:	1999, Digital signatures with appendix - Part 1: General
ISO/IEC 14888-2:	1999, Digital signatures with appendix - Part 2: Identity-based mechanisms
ISO/IEC 14888-3:	1999, Digital signatures with appendix - Part 3: Certificate-based mechanisms
ISO/IEC 15816:	2002 (ITU-T X.841), Security information objects for access control
ISO/IEC 15945:	2002 (ITU-T X.843), Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:	(2002), Cryptographic techniques based on elliptic curves - Part 1: General (in attesa di pubblicazione)
ISO/IEC 15946-2:	(2002), Cryptographic techniques based on elliptic curves - Part 2: Digital signatures (in attesa di pubblicazione)
ISO/IEC 15946-3:	(2002), Cryptographic techniques based on elliptic curves - Part 3: Key establishment (in attesa di pubblicazione)
ISO/IEC FCD 15946-4:	2002, Cryptographic techniques based on elliptic curves - Part 4: Digital signatures giving message recovery
ISO/IEC TR 15947:	(2002), IT intrusion detection framework (in attesa di pubblicazione)
ISO/IEC 17799:	2000, Code of practice for information security management (in fase di revisione)
ISO/IEC 18014-1:	(2002), Time stamping services - Part 1: Framework (in attesa di pubblicazione);
ISO/IEC FDIS 18014-2:	2002, Time stamping services - Part 2: Mechanisms producing independent tokens
ISO/IEC CD 18014-3:	2002, Time stamping services - Part 3: Mechanisms producing linked tokens
ISO/IEC WD 18028:	2001, Information technology - Security techniques - IT network security
ISO/IEC CD 18031:	2002, Random bit generation
ISO/IEC CD 18032:	2002, Prime number generation
ISO/IEC CD 18033-1:	2002, Encryption algorithms - Part 1: General
ISO/IEC WD 18033-2:	2002, Encryption algorithms - Part 2: Asymmetric ciphers
ISO/IEC CD 18033-3:	2002, Encryption algorithms - Part 3: Block ciphers
ISO/IEC WD 18033-4:	2002, Encryption algorithms - Part 4: Stream ciphers
ISO/IEC WD 18043:	2002, Guidelines for the implementation, operation and management of Intrusion Detection Systems (IDS)
ISO/IEC WD 18044:	2002, Information security incident management
ISO/IEC WD 18045:	2002, Methodology for IT security evaluation



Proposte concernenti le strategie
in materia di sicurezza informatica
e delle telecomunicazioni
per la pubblica amministrazione

Parte seconda
Linee guida per l'attuazione della sicurezza ICT nella PA

3.1 Parte seconda - Linee guida per l'analisi dei rischi

3.1.1 Considerazioni generali

L'analisi del rischio è un processo fondamentale per la pianificazione, realizzazione e gestione di qualsiasi sistema di sicurezza ICT.
Infatti, senza una costante valutazione del valore del patrimonio informativo, dell'intensità delle minacce attuali e potenziali, delle vulnerabilità del sistema e dei potenziali impatti tangibili e intangibili sull'attività e sul posizionamento dell'Amministrazione, risulta impossibile definire un sistema di sicurezza veramente equilibrato e bilanciato rispetto ai rischi ed ai danni/perdite che potrebbero verificarsi.
Nel nuovo sistema di Governo delle P.A. sempre più aperto, cooperante, digitale ed interconnesso, anche a livello internazionale, i confini del rischio non hanno più barriere e le minacce diventano tutte possibili e, in qualche misura, sempre più probabili.
Ciascuna Amministrazione si deve pertanto dotare di un processo continuo di analisi e gestione del rischio conforme agli standard internazionali di sicurezza
L'obiettivo dell'analisi e gestione del rischio è cogliere quali siano i rischi associati agli asset aziendali (individuati, classificati e valorizzati) e concordare quali siano le misure più idonee a ridurre il livello di vulnerabilità a fronte di minacce o a minimizzare l'impatto su violazioni della sicurezza e quindi sul servizio. In sintesi l'Analisi del Rischio è quel processo necessario per identificare i rischi di sicurezza e determinarne la loro ampiezza (compliant BS7799 che è il "Codice professionale per la gestione della sicurezza delle informazioni"). In altri termini l'analisi del rischio è quel processo che definisce le esigenze di sicurezza e concorda su quali siano le più appropriate misure di controllo. Per minaccia s'intende una possibile causa di incidente indesiderato che può comportare danni ad un sistema o a una organizzazione.
Per vulnerabilità s'intende una debolezza di un asset o gruppo di asset che può essere attualizzata da una minaccia. L'analisi del rischio è un'attività considerata parte essenziale e propedeutica all'adozione di efficienti sistemi per una sicurezza globale nell'Amministrazione e comprende essenzialmente i seguenti argomenti:

- Identificazione e Valutazione degli Asset (beni) informativi;
- Assessment delle Minacce e delle vulnerabilità;
- Identificazione dell'esistente e Pianificazione dei Controlli di Sicurezza;
- Risk Assessment;
- Identificazione e Selezione dei Controlli di Sicurezza e Riduzione dei Rischi;
- Accettazione del Rischio.

I risultati di un'analisi del rischio possono contribuire in modo determinante ad aumentare la consapevolezza della Direzione (e di conseguenza di tutta la struttura della PA), verso la sicurezza ma soprattutto verso l'adozione di una forma mentale volta al trattamento degli asset in modo "protettivo". Fornisce altresì un meccanismo pratico per comprendere i pericoli della mancanza o utilizzo incompleto o anomalo dei sistemi di protezione e supporta, con dati qualitativi e quantitativi, la valutazione e selezione delle adeguate misure di sicurezza.
L'analisi del rischio è comunque prevista dal Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali". Si presenta di seguito uno schema di riferimento per indirizzare la stesura, da parte delle Amministrazioni, dei requisiti atti ad identificare e selezionare una metodologia per l'analisi dei rischi adeguata alle esigenze di sicurezza espresse dalla direttiva.

3.1.2 Requisiti di conformità della metodologia

Nella identificazione e selezione di una metodologia di analisi del rischio si dovranno tenere conto delle seguenti caratteristiche di base:

- deve poter valutare oltre al rischio tecnologico, anche il rischio organizzativo, operativo e amministrativo;
- deve poter valutare il rischio di un singolo bene informativo o di un'intera applicazione intesa come unità distinta a supporto di un processo;
- deve essere progettata per essere usata sia per nuove applicazioni in via di sviluppo che per applicazioni esistenti o applicazioni acquisite dal mercato;
- deve essere progettata con l'ottica di supportare l'analisi dei rischi per applicazioni di tutti i tipi e basate su tutte le tecnologie;
- deve supportare coloro che si occupano sia di sicurezza Organizzativa che di sicurezza ICT;
- deve supportare in particolare coloro che hanno la responsabilità di valutare il rischio per l'Amministrazione, della mancanza della fornitura (o di una fornitura alterata), del servizio alla clientela;
- deve essere progettata anche per fornire una guida alla progettazione o selezione di specifiche tecniche di controllo;
- deve essere progettata in conformità degli standard BS7799;
- deve prevedere l'impiego di strumenti automatici e tool per l'analisi generale e per l'analisi specifica del rischio.

3.1.3 Logiche per sviluppare la richiesta di offerta

Sia nel caso che l'Amministrazione decida di svilupparla in casa, sia che scelga di acquisire una metodologia per l'analisi del rischio dall'esterno, occorre che vengano rispettati alcuni requisiti di tipo strutturale e funzionale:

1. un'articolazione in fasi operative, ciascuna finalizzata ad uno o più obiettivi specifici;
2. una serie di attività, per ogni fase, mirate a svolgere le funzioni basilari dell'analisi del rischio.

Per guidare l'individuazione di tali requisiti viene fornito uno schema di riferimento (framework) articolato in fasi ed attività.

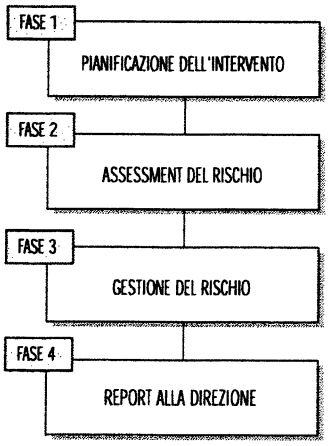
Framework di riferimento

Qualsiasi metodologia di analisi del rischio dovrebbe prevedere almeno 4 fasi consequenziali e interrelate:

- pianificazione dell'intervento;
- valutazione (assessment) del Rischio;
- gestione del Rischio;
- report alla Direzione.

Ciascuna di queste fasi dovrà poi prevedere lo svolgimento di tutte le attività necessarie per conseguire l'obiettivo di fase. Nelle pagine seguenti vengono quindi evidenziati i requisiti di ciascuna fase in termini di passi e di attività che la metodologia prescelta dovrà contenere.

Requisito di articolazione di una metodologia di analisi del rischio



3.1.3.1 Fase 1 - Pianificazione dell'intervento

Descrizione della Fase

Deve essere stabilito, all'inizio del processo di pianificazione del singolo intervento di analisi del rischio da parte del responsabile/delegato della sicurezza, il piano di intervento di analisi e le persone coinvolte.
Ciascun piano di intervento dovrà identificare:

- gli asset da analizzare;
- l'unità organizzativa coinvolta;
- i tempi di intervento;
- il responsabile del prodotto/processo/applicazione;
- le risorse da coinvolgere cioè il project leader, e il gruppo di lavoro nell'analisi.

Inoltre il responsabile/delegato alla sicurezza dovrà predisporre e inviare una lettera di incarico a tutti gli attori coinvolti nell'analisi, in cui sono specificati tempi e responsabilità.

Attività specifiche della Fase

Deve essere definito l'obiettivo di questa fase di pianificazione dell'intervento descrivendo:

- lo scopo della fase di pianificazione;
- le finalità degli interventi di valutazione della situazione di rischio;
- la pianificazione dei passi operativi;
- l'identificazione degli "Attori" coinvolti;
- i compiti di ogni risorsa o entità coinvolta;
- la predisposizione del piano vero e proprio.

3.1.3.2 Fase 2 - Assessment del Rischio

Descrizione della Fase

La fase deve prevedere di identificare il rischio e la sua misura attraverso una valutazione delle minacce e vulnerabilità dell'asset/servizio ed il conseguente impatto sul business.

Dovrà essere previsto di assegnare delle specifiche competenze in termini di "chi fa-che cosa" relativamente a:
- chi decide la tempistica di intervento (pianificata o richiesta specifica);
- chi è responsabile del processo di analisi del rischio;
- chi identifica e definisce l'utilizzo di eventuali strumenti di supporto all'analisi;
- chi effettua l'analisi del rischio "globale" e chi quella settoriale.

Nello sviluppo di questa fase devono venire individuate (e valutate) le contromisure specifiche in essere a protezione del patrimonio informativo e quindi del business.

Attività specifiche della Fase

La fase deve prevedere dei passi procedurali che sviluppino la sequenza dell'assessment e che comunque prevedano almeno la seguente suddivisione:
- un passo che realizzi un assessment circa le minacce esistenti percepite;
- un passo che realizzi un assessment circa le vulnerabilità (incluse le contromisure esistenti);
- un passo che preveda di "individuare" le contromisure già pianificate a protezione del business e di ricalcolare un nuovo indice di vulnerabilità;
- un passo che fornisca il calcolo del rischio relativamente alla situazione esistente ed a quella pianificata, (col calcolo del gap tra i due indici).

In particolare per quanto attiene all'assessment delle minacce dovrà essere possibile:
- individuare e descrivere l'associazione Asset/Minacce;
- valutare le minacce, in particolare riguardo:

- alla verosimiglianza;
- alla frequenza;
- alla probabilità;
- alla gravità;

- fare in modo che venga calcolato l'indice di minaccia come media ponderata delle perdite per minaccia.

In particolare per quanto attiene all'assessment delle vulnerabilità dovrà essere possibile redigere le regole per:
- identificare le vulnerabilità (mancanza o carenza delle contromisure);
- identificare e descrivere l'associazione scoperto/minacce;
- valutare le vulnerabilità (per ciascuna minaccia) come quota di perdita dell'asset in caso di vulnerabilità attuata;
- prevedere le diverse tipologie di calcolo nel caso venissero utilizzati strumenti automatici di analisi.

In particolare per quanto attiene all'identificazione delle contromisure già pianificate, dovrà essere possibile:
- identificare le contromisure pianificate;
- rielaborare l'assessment di vulnerabilità dopo aver considerato e valutato la presenza delle contromisure in essere (pianificate).

In particolare per quanto attiene al calcolo del rischio, dovrà essere possibile:
- fare in modo che venga calcolato il valore di rischio a contromisure attuali;
- fare in modo che venga calcolato il valore di rischio a contromisure pianificate.

3.1.3.3 Fase 3 - Gestione del Rischio

Descrizione della Fase

Questa fase deve esplicitare il modo per definire il rischio residuo accettabile dalla Direzione, derivante dall'applicazione di contromisure, ciascuna delle quali contribuisce, in modo cost-effective, a ridurre marginalmente il rischio iniziale.
Oltre all'individuazione e attribuzione delle specifiche responsabilità, in questa fase devono venire definite le simulazioni sui margini di riduzione del rischio conseguenti all'applicazione delle contromisure e che devono portare all'individuazione del massimo rischio tollerabile per ciascun asset informativo.

Attività specifiche della Fase

La metodologia deve prevedere dei passi procedurali che sviluppino la sequenza della fase di gestione del rischio e che comunque prevedano almeno la seguente suddivisione:

- l'individuazione e la selezione delle contromisure a fronte delle vulnerabilità identificate;
- l'individuazione e calcolo del rischio residuo, in funzione del portafoglio delle contromisure stabilite dopo la valutazione dell'investimento a copertura del rischio netto e dopo aver classificato le contromisure in relazione al margine di riduzione dei rischi;
- la definizione delle regole utili a determinare l'accettazione del rischio residuo dopo l'applicazione delle contromisure.

In particolare per quanto attiene all'individuazione e selezione delle contromisure, dovrà essere possibile:

- individuare i principi di associazione contromisure a vulnerabilità/minacce;
- definire i modelli e gli algoritmi di simulazione dell'andamento dell'indice di rischio secondo le contromisure implementabili;
- definire i metodi di assegnazione a ciascuna contromisura selezionata, della relativa riduzione del margine di rischio conseguibile e delle caratteristiche di costo/efficacia.

In particolare per quanto attiene al calcolo del rischio residuo dovrà essere possibile :

- definire il calcolo dell'investimento a copertura del rischio netto (rischio calcolato meno MRT);
- identificare il portafoglio di contromisure;
- definire il calcolo del rischio residuo.

In particolare per quanto attiene alla definizione del livello di accettazione del rischio si dovrà poter:

- formalizzare i termini dell'accettazione del rischio residuo;
- individuare e sviluppare le specifiche di fattibilità tecnico/organizzativa delle contromisure.

3.1.3.4 Fase 4 - Report alla Direzione

Descrizione della Fase

Questa fase deve prevedere l'analisi delle informazioni scoperte nella fase precedente, al fine di elaborare un report per la Direzione che renda palese quali siano i maggiori rischi che minacciano il business sia di natura organizzativa che tecnologica.
Deve essere altresì formalizzato un piano di azione che assicuri che tutti i necessari miglioramenti in termini di protezione e controllo siano implementati secondo scadenze temporali.

Attività specifiche della Fase

Questa fase deve prevedere almeno due passi procedurali:

- un primo passo che descriva la preparazione, strutturazione e stesura di un report per la Direzione descrivendo specificatamente la (o le) situazione riscontrata/e e gli obiettivi di rischio/sicurezza definiti;
- il secondo che consista nella formalizzazione degli obiettivi negoziati tra le parti coinvolte.

In particolare per quanto attiene la stesura di un report, la metodologia deve prevedere di:

- descrivere le minacce/vulnerabilità all'asset;
- descrivere il valore della potenziale perdita misurata a fronte dei rischi dell'investimento a protezione;
- descrivere il portafoglio di contromisure;
- descrivere le modalità di accettazione del rischio residuo.

In particolare per quanto attiene alla formalizzazione degli obiettivi condivisi sarà necessario prevedere di:

- programmare gli incontri con la Direzione per illustrare/dibattere la relazione;
- programmare gli atti formali (Firma) per presa di visione della relazione.

3.2 Linee guida per lo sviluppo di un piano di Business Continuity

3.2.1 Premessa

Vengono di seguito fornite le linee guida per l'impostazione di un sistema di Business Continuity Management atte ad integrare gli aspetti di organizzazione (ruoli e responsabilità), processi/procedure e le soluzioni tecnologiche di supporto.

3.2.2 Lo scopo del Business Continuity Management

Lo scopo del Business Continuity Management è garantire la continuità dei processi dell'Organizzazione in funzione del loro valore e della qualità dei prodotti/servizi erogati tramite il supporto dell'infrastruttura di ICT, prevenendo e minimizzando l'impatto di incidenti intenzionali o accidentali e dei conseguenti possibili danni.

Gli eventi che potrebbero pregiudicare la continuità del business sono:

- Eventi imprevisti che possono inficiare l'operatività dei sistemi (interruzione dell'alimentazione, incendi, allagamenti, ecc..)
- Malfunzionamenti dei componenti HW e SW
- Errori operativi da parte del personale incaricato della gestione o da parte degli utilizzatori
- Introduzione involontaria di componenti dannosi per il sistema informativo e di rete (es. virus, cavalli di troia, bombe logiche, ecc..)
- Atti dolosi miranti a ridurre la disponibilità delle informazioni (Sabotaggi e frodi; diffusione di virus; bombardamento di messaggi; interruzione di collegamenti; ecc.. .).

Le minacce di tipo doloso possono provenire da operatori/ambienti sia interni sia esterni al Gruppo ed in particolare da utenti connessi alla rete internet.

A fronte di questi possibili eventi, il BCM deve essere focalizzato sulla garanzia di continuità del supporto delle tecnologie ICT ai processi che consentono all'Ente/Organizzazione l'erogazione del/dei servizio/servizi.

3.2.3 Le componenti del Business Continuity Management

Lo sviluppo di un sistema di Business Continuity Management deve tener in considerazione le seguenti componenti:

- Crisis and Incident Management: assicura la gestione dello stato di crisi e la risposta ad incidenti nel caso in cui si verifichi un evento in grado di compromettere la continuità dell'operatività
- Continuity Management: assicura la continuità dei processi durante e dopo un'emergenza attraverso la predisposizione di processi/procedure alternative (spesso manuali) a quelle normalmente supportate dall'infrastruttura di ICT
- Disaster Recovery Management: assicura il recovery delle infrastrutture tecnologiche a supporto dei processi di business
- Business Recovery Management: assicura il recovery dei processi di business dopo un'emergenza e il ritorno alla normalità.

La pianificazione di un Sistema di Business Continuity Management è una misura preventiva nell'ambito della gestione dei rischi, con particolare riferimento ai rischi di disponibilità delle informazioni.

L'esecuzione dei piani e delle procedure previste in caso di eventi in grado di compromettere la continuità operativa deve essere rivolta a ridurre al minimo gli impatti derivanti dal verificarsi di tali eventi.

3.2.4 Il ciclo del Business Continuity Management

Il ciclo di realizzazione del Sistema di Business Continuity Management deve prevedere le seguenti fasi:

- Progettazione del BCM: prevede il disegno e la pianificazione dell'intero sistema sia negli aspetti organizzativi che tecnologici
- Implementazione del BCM: prevede l'implementazione del sistema progettato con particolare attenzione agli aspetti di comunicazione/ sensibilizzazione diffusa e di formazione specifica sulle procedure e sui piani
- Monitoraggio del BCM: prevede il monitoraggio dell'efficacia del sistema implementato attraverso test e simulazioni dei piani e audit periodici specifici
- Mantenimento ed ottimizzazione: prevede l'evoluzione del sistema in relazione ai feedback derivanti dal monitoraggio e ad eventuali ulteriori requisiti interni ed esterni sopraggiunti nel frattempo ed avvia un nuovo ciclo progettuale.

3.2.5 Le strategie per il Business Continuity Management

Gli indirizzi strategici da seguire nella progettazione e realizzazione del Sistema di Business Continuity Management sono le seguenti:

- Considerare le logiche di gestione della continuità come parte integrante e non aggiuntiva della gestione dell'attività di cui ciascun Ente è titolare
- Sviluppare una gestione della continuità in relazione agli impatti che i processi e le infrastrutture di supporto hanno sulle attività dell'organizzazione
- Garantire un mix di interventi di tipo organizzativo e tecnologico adeguato, con una costante attenzione al rapporto costi/benefici
- Assicurare il coordinamento e l'integrazione delle attività di gestione dell'emergenza con le attività di analisi e gestione dei rischi operativi
- Disegnare una struttura di responsabilità chiara e coerente e attribuire esplicitamente le responsabilità aggiuntive ai ruoli già esistenti o nuovi

- Garantire che le nuove logiche di gestione della continuità siano un patrimonio dell'intera Organizzazione e che ciascun dipendente contribuisca affinchè queste diventino parte integrante della cultura organizzativa
- Per garantire l'affidabilità e la continuità di erogazione dell'infrastruttura tecnologica valutare l'opzione strategica di delega in outsourcing attraverso una approfondita e corretta definizione e gestione dei livelli di servizio.

Il ciclo deve essere attivato dalla valutazione degli impatti derivanti da una possibile interruzione dei processi sull'erogazione dei prodotti/servizi, anche ricorrendo, ove possibile, alle esperienze e a situazioni già verificate.
A valle della valutazione degli impatti specifica per ogni Ente, si sceglierà di adottare la soluzione che verrà ritenuta più equilibrata, valutando le alternative, in particolare quelle correlate ai tempi di ripartenza e ripristino.

3.2.6 Le linee guida all'elaborazione dei piani del Business Continuity Management

Il Business Continuity Plan (BCP)

Al fine di ottenere un piano di continuity che possa essere effettivamente adoperato in caso di disastro e, quindi, riesca ad assicurare la continuità, almeno quella minimale e il ripristino dei processi con priorità rispetto a quelli ritenuti chiave, si devono prevedere le seguenti fasi:

1. definizione di obiettivi e ipotesi;
2. definizione della Business Impact analysis;
3. progetto e sviluppo del piano;
4. realizzazione del piano;
5. test del piano di BCP;
6. manutenzione del piano;
7. esecuzione in caso di disastro.

Nel caso specifico il Business Recovery Plan, volto ad assicurare il ripristino dei processi di business dopo l'emergenza, deve essere considerato come un'appendice del BCP, mirato ad assicurare il sostegno ai processi vitali dell'Ente durante e dopo l'emergenza.

1. Definizione di obiettivi e ipotesi

Questa fase si compone di:
- Definizione degli obiettivi;
- Individuazione di uno sponsor;
- Definizione di un Comitato guida (nella fattispecie il Comitato della sicurezza);
- Sviluppo di un piano di progetto;
- Preparazione del budget;
- Definizione di un sistema di reporting.

2. Definizione del Business Impact Analysis

Questa fase consiste nell'identificazione di tutti i processi critici, delle relative dipendenze reciproche, delle tecnologie impattate, dei partners strategici del business, delle principali risorse umane da coinvolgere, delle informazioni vitali da registrare, e degli impatti quantificati che un disastro può avere sull'organizzazione.

Le attività di questa fase dovrebbero essere:
- Identificazione dei rischi organizzativi
- Identificazione dei processi critici
- Definizione dei Tempi di non funzionamento ed impatti finanziari dei processi critici
- Definizione delle interdipendenze dei processi critici allo scopo di determinare l'ordine in cui devono essere riattivati
- Definizione del massimo tempo tollerabile di indisponibilità per ogni processo
- Identificazione del tipo e della quantità di risorse necessarie al ripristino cioè dei dispositivi fisici quali, tavoli, sedie, fax, fotocopie, files, personal computers, stampanti, telefonini per ciascuna attività
- Determinare l'impatto sia finanziario che di reputazione in caso di disastro.

In questa fase i rischi dovrebbero essere definiti in termini qualitativi, di verosimiglianza e di conseguenza sul business. Si noti che le attività di questa fase sono tipicamente identificate nella Metodologia di Classificazione e Valorizzazione degli asset.

3. Progetto e sviluppo del piano

L'obiettivo di questa fase deve essere di definire le strategie operative alternative appropriate per ciascun disastro al fine di fornire un recupero operativo tempestivo per tutti i processi critici e per i processi da questi dipendenti.
Se venisse scelta un'errata strategia di azione per rispondere ad un disastro, le conseguenze del disastro stesso potrebbero essere esacerbate.
Ogni strategia di azione dovrebbe sempre affrontare sia gli aspetti organizzativi che quelli tecnici.
Una strategia di azione di ripristino deve essere sviluppata per il ripristino dei processi del "Core Business" in ottica di sopravvivenza.
Inoltre la singola strategia deve essere scelta in funzione della necessità di tempo di ripristino, inteso come tempo di tolleranza dell'organizzazione senza soffrire perdite significative finanziarie o di immagine (Tempo di Recovery).

4. Realizzazione del piano

Scopo di questa fase è di sviluppare e documentare i processi di ripristino che assicurano la Business Continuity, nel caso si verifichi un disastro, in una formulazione appropriata all'esecuzione in condizioni di emergenza.
Le attività che devono essere incluse in questa fase sono:
- Scelta dei tools per la creazione ed esecuzione del piano di BCP;
- Definizione delle attività di ripristino (sequenze, tempi e responsabilità);
- Definizione dei processi di "escalation" e di ridefinizione delle priorità in funzione della successione degli eventi e della gestione della crisi;
- Identificazione degli individui, dei reparti e delle interdipendenze necessari a effettuare attività specifiche;
- Identificazione e differenziazione dei team di ripristino;
- Identificazione e lista dei contatti chiave, dei fornitori e delle risorse;
- Documentazione del piano ai fini della futura manutenibilità.

5. Test del piano di BCP

L'obiettivo di questa fase è quello di strutturare complete ed efficaci esercitazioni e test per assicurare che il piano funzioni come è stato progettato.

Se il piano non viene testato su basi di regolarità non c'è assicurazione che, nel caso il piano venisse attivato, l'organizzazione sopravviverebbe al disastro.

Gli obiettivi specifici di effettuare i BCP test sono di assicurare che:
- Le procedure di ripristino siano complete ed attuabili;
- La competenza del personale nelle procedure di ripristino possa essere valutata come efficiente;
- Le risorse necessarie a effettuare i processi di ripristino, quali processi, sistemi ICT, personale, risorse fisiche e dati, siano ottenibili ed operative;
- Le procedure manuali di ripristino ed i sistemi ICT di backup siano aggiornati e possano essere o operativi o ripristinabili;
- Il programma di addestramento sia monitorato.

Ci sono tre livelli di test di BCP:
1. verifica del grado di conoscenza del personale coinvolto, per i processi scelti e identificati nella Business Impact Analysis, usando le procedure di BCP nei vari scenari di disastro, tramite sessioni di gruppo;
2. prova di ripristino di alcuni processi scelti, usando le procedure di BCP, comprendendo nelle prove i sistemi IT coinvolti ed il raduno di personale di ripristino in un luogo alternativo a quello usuale;
3. prova di ripristino di tutti i processi critici, con le procedure di BCP, includendo i sistemi critici ed il coordinamento con tutti i gruppi dell'Organizzazione.

Le attività da eseguire sono:
1. Definizione delle strategie di test;
2. Scelta dei metodi di test;
3. Definizione degli obiettivi di test e dei piani di test;
4. Esecuzione dei test;
5. Documentazione delle deviazioni rispetto ai processi critici;
6. Redazione di un report;
7. Ridefinizione del BCP in base ai risultati del test.

6. Manutenzione del piano

L'obiettivo di questa fase è di mantenere il piano aggiornato e pronto al supporto delle attività in caso di emergenza.
Le attività da intraprendere sono:
1. determinare le responsabilità di aggiornamento del piano;
2. identificare i meccanismi organizzativi per innescare i cambiamenti del piano, assicurando che ogni modifica organizzativa, operativa e infrastrutturale, sia comunicata al personale responsabile dell'aggiornamento del piano;
3. determinare delle regole procedurali di manutenzione per assicurare che il piano rimanga aggiornato;
4. determinare i processi per modificare il piano;
5. determinare le regole di controllo dei cambi di versione del piano.

7. Esecuzione in caso di disastro

L'obiettivo di questa fase è la risposta in caso di disastro, ovvero la Gestione della Crisi.

3.2.7 Disaster Recovery Plan

Per Disaster Recovery Plan (DRP) si intendono gli aspetti tecnologici del BCP. Il DRP può essere definito nel modo seguente:
"DRP si riferisce ad un piano focalizzato sull'ICT per ripristinare l'operatività di un sistema, di un'applicazione o di un centro elaborativo in un sito alternativo dopo un emergenza. In particolare non si riferisce quindi a interruzioni minori che non richiedono rilocazione di sito."

Affinchè una organizzazione possa rispondere in maniera efficiente ad una situazione di emergenza, devono essere analizzati:
- I possibili livelli di disastro
- La criticità dei sistemi/applicazioni.

Di seguito viene sintetizzata un'ipotesi di scenari di disastro:
1. Un disastro di primo livello su una locazione può causare, in alcuni casi, la parziale ma non completa distruzione delle operazioni svolte giornalmente. La situazione può essere risolta usando personale nel sito ed effettuando localmente sforzi di ripristino, pur con la riallocazione di alcune persone o funzioni.
2. Un disastro di livello 2 coinvolge diverse locazioni o piani. Le operazioni di routine possono essere distrutte ed i processi critici possono dover essere eseguiti off-site. Personale locale può dover cercare assistenza all'esterno. Il coordinamento delle persone avviene attraverso un centro di operazioni di emergenza.
3. Un disastro di livello 3 può coprire una vastissima zona, ad esempio una regione; tipici esempi di questi disastri sono: inondazioni, terremoti o uragani. In questo caso sono richieste risorse esterne ed assistenza, ma il ripristino completo può comportare settimane o mesi. Generalmente un disastro di questo livello comporta la paralisi delle normali funzioni di business.

I sistemi dovrebbero essere classificati secondo le definizioni seguenti:
Critici
Le relative funzioni non possono essere eseguite senza essere sostituite da strumenti (mezzi) di caratteristiche identiche. Le applicazioni critiche non possono essere sostituite con metodi manuali. La tolleranza in caso di interruzione è molto bassa, di conseguenza il costo di una interruzione è molto alto.

Vitali
Le relative funzioni possono essere svolte manualmente, ma solo per un breve periodo di tempo. Vi è una maggiore tolleranza all'interruzione rispetto a quella prevista per i sistemi critici, conseguentemente il costo di una interruzione è inferiore, anche perchè queste funzioni possono essere riattivate entro un breve intervallo di tempo (generalmente entro cinque giorni).

Delicati
Queste funzioni possono essere svolte manualmente, a costi tollerabili, per un lungo periodo di tempo. Benchè queste funzioni possano essere eseguite manualmente, il loro svolgimento risulta comunque difficoltoso e richiede l'impiego di un numero di persone superiore a quello normalmente previsto in condizioni normali.

Non-critici
Le relative funzioni possono rimanere interrotte per un lungo periodo di tempo, con un modesto, o nullo, costo per l'azienda, e si richiede un limitato (o nullo) sforzo di ripartenza quando il sistema viene ripristinato.
Le procedure applicative, il software di sistema ed i file che sono stati classificati e documentati come critici, devono essere ripristinati prioritariamente.
Applicazioni, software e file classificati come critici hanno una tolleranza molto bassa alle interruzioni. La criticità di applicazioni, software di sistema e dati, deve essere valutata in funzione del periodo dell'anno in cui il disastro può accadere.
Un piano d'emergenza deve prevedere il ripristino di tutte le funzioni aziendali e non solo il servizio ICT centrale.
Per la definizione del DRP devono essere valutate le strategie di ripristino più opportune su: siti alternativi, metodi di back up, sostituzione degli equipaggiamenti e ruoli e responsabilità dei team.
La prolungata indisponibilità del servizio elaborativo derivante in particolare situazione di disastro, e quindi dei servizi primari, rende necessario l'utilizzo di una strategia di ripristino in sito alternativo.

Le più comuni strategie di ripristino in sito alternativo includono i seguenti approcci:

Offsite storage
Tutti i sistemi informativI dovrebbero prevedere un regolare back up ed un sistema di archiviazione delle informazioni in un ambiente protetto in base alla criticità dei sistemi e dei dati, insieme alle licenze Software, le system configurations, e le altre informazioni vitali.

Interoperabilità
Utilizzo di piattaforme e configurazioni standard riducono le spese di recovery e sostituzione delle apparecchiature da sostituire.

Ridondanza
Una ridondanza di data storage, communications paths, alimentazioni e componenti di sistema riducono la probabilità di blocco dei sistemi. Inoltre devono essere valutate le seguenti opzioni in base a criticità dei processi/applicazioni/sistemi e a considerazioni di costo/benefici:

Hot sites (siti "caldi")
Questi centri prevedono una completa configurazione in grado di funzionare entro poche ore. L'apparecchiatura e il software di base devono essere compatibili con l'installazione primaria per la quale si svolge funzione di servizio IT alternativo. Le uniche esigenze addizionali sono il personale, i programmi, i file dati e la documentazione.
Il sito "caldo" è destinato alle operazioni d'emergenza per un periodo di tempo limitato e non ad un esteso utilizzo a lungo termine.
Perciò il sito "caldo" dovrebbe essere considerato come un mezzo per ottenere la continuità delle operazioni essenziali per un periodo di alcune settimane subito dopo un disastro o una grossa emergenza.
Il piano di ripristino per la connettività della rete a un sito caldo che utilizza una rete pub-

blica commutata dovrebbe prevedere la ridondanza e la disponibilità di una sufficiente capacità su diversi percorsi per reinstradare il traffico in caso di necessità. Dovrebbe essere inoltre previsto un instradamento notturno mediante centrali differenti in modo che un problema in un singolo punto non possa rendere inoperante l'intera rete.

Warm sites (siti "tiepidi")
Questi sono siti parzialmente configurati, generalmente con connessioni alle reti e ad unità periferiche specifiche, come unità disco, unità nastro, unità di controllo ma senza l'unità centrale. A volte è presente una CPU di minore potenza.
L'unità centrale può essere ottenuta rapidamente per una installazione di emergenza (fornendo uno dei modelli più comuni).
Dopo l'installazione dei componenti necessari, il centro può essere pronto per il funzionamento in poche ore, anche se l'installazione e l'avviamento dell'unità centrale e delle altre unità mancanti potrebbe richiedere alcuni giorni o settimane.
Questa soluzione è meno dispendiosa rispetto alla soluzione "hot".

Cold sites (siti "freddi")
Questi sono ambienti nei quali sono predisposti gli impianti base (ad esempio cavi elettrici, aria condizionata, pavimenti rialzati) per contenere una sala macchine. Il "cold site" è predisposto per ricevere le apparecchiature ma non dispone di alcun componente prima che questo sia necessario. L'attivazione di simile realtà può richiedere diverse settimane.

Mobile Sites
sono siti trasportabili, personalizzati con equipaggiamenti IT e di telecomunicazioni necessari a soddisfare i fabbisogni di sistema. Il sito è trasferibile e può essere installato al sito alternativo.

Mirrored Sites
sono siti completamente ridondati con mirroring completo. I dati sono elaborati e memorizzati contemporaneamente nei siti primario e alternativo consentendo un'elevata disponibilità del sistema.
Un'opzione strategica da tenere in considerazione è la possibilità di impostare un accordo di reciprocità tra due centri differenti.

Per garantire la fattibilità di una simile soluzione si dovrebbe verificare che:
- Esista una compatibilità di base degli impianti per realizzare una comune infrastruttura
- Esista la disponibilità delle risorse addizionali disponibili
- Siano effettuate regolarmente delle prove di verifica.

Gli accordi reciproci sono accordi tra due o più società con apparecchiature o applicazioni simili.
Le caratteristiche tipiche di questa soluzione prevedono che i partecipanti forniscano tempo macchina agli altri in caso di emergenza.

I vantaggi sono:
- Bassi costi
- Potrebbe essere l'unica alternativa praticabile se non esistessero servizi alternativi con hardware compatibile.

Gli svantaggi sono:
- Di norma non può essere imposto;
- Possibili differenze nella configurazione hardware, spesso impongono delle modifiche ai programmi per renderli funzionanti;
- Cambiamenti non segnalati nel carico di lavoro o nella configurazione delle apparecchiature rendono l'accordo limitato o impraticabile.

Nel piano di Disaster Recovery dovrebbero essere specificate le caratteristiche contrattuali, nel caso di servizi alternativi forniti da terze parti.

Queste dovrebbero coprire i seguenti aspetti:
- Configurazioni
- Definizione di disastro
- Tempestività, cioè in quanto tempo i servizi alternativi saranno disponibili dopo un disastro
- Numero di Utenze per centro per edificio o per area
- Priorità di servizio in caso di disastro comune a più utenti
- Copertura assicurativa per il personale della società operante nei locali del centro alternativo
- Periodo di utilizzo e di disponibilità per l'uso e tipo di supporto tecnico fornito dalle persone del servizio alternativo
- Sistema di comunicazione
- Garanzie che offre il fornitore relativamente alla disponibilità del sito e alla adeguatezza delle strutture
- Diritti di prova
- Affidabilità del centro.

Nell'ambito del Disaster Recovery Plan devono essere previste le procedure di back up e recovery. Le principali sono le seguenti:

Salvataggio dei supporti e della documentazione
La disponibilità di archivi dati adeguati è di cruciale importanza per ripristinare le elaborazioni (internamente o esternamente) in caso di emergenza. La duplicazione dei dati più importanti e della corrispondente documentazione, nonchè la relativa conservazione in adeguati ambienti esterni all'azienda, sono un prerequisito fondamentale per ogni tipo di piano d'emergenza.

Procedure di salvataggio periodiche
Sia gli archivi dati, sia i programmi dovrebbero essere periodicamente copiati. La periodicità di queste operazioni può essere diversa per programmi applicativi e per il software di sistema.
L'utilizzo di sistemi software specifici per la gestione dei nastri (tape management system) e per la schedulazione automatica dei lavori (automated job scheduling), può facilitare la pianificazione periodica di queste operazioni.
Le copie dei dati e dei programmi consentono la gestione continua delle modifiche.
Una copia del file o del record effettuata con periodicità viene conservata per le operazioni di ripristino.

Tutte le modifiche o le transazioni avvenute dall'ultimo salvataggio degli archivi devono essere salvate.
Analogamente, ogni documentazione necessaria alla operatività corrente dell'Amministrazione dovrebbe essere conservata in opportune località esterne.
Analoga considerazione vale per i documenti necessari per ripristinare il database di produzione. Come per i file di dati, anche le copie conservate all'esterno devono essere mantenute aggiornate per assicurarne l'utilizzabilità.

La documentazione da archiviare e conservare esternamente comprende:
- Documentazione sistemistica e dei programmi
- Procedure speciali
- Documenti di INPUT / OUTPUT
- Piano di continuità aziendale.

I dati riservati/critici, posti nell'archivio remoto dovrebbero essere archiviati in appositi armadi ignifughi.

Si dovrebbe mantenere un inventario contenente informazioni quali:
- Il nome del file, il numero di serie del volume, la data di creazione, il periodo contabile di riferimento, il numero di locazione fisica del back-up, per tutti i nastri di back-up.
- Il nome del documento, la sua posizione, il sistema interessato, la data dell'ultimo aggiornamento, per tutta la documentazione critica.

Ripristino delle Reti di telecomunicazioni
Le reti delle telecomunicazioni sono soggette agli stessi disastri naturali dei centri elaborazione dati, ma sono anche esposte ad alcuni eventi disastrosi peculiari delle telecomunicazioni.
Questi potrebbero includere un disastro alla centrale di smistamento, il taglio dei cavi, errori e malfunzionamenti del software per le telecomunicazioni, vulnerabilità nella sicurezza dovute a pirateria informatica (gli hacker delle linee telefoniche sono noti come phracker), e molti altri malfunzionamenti causati dall'uomo.
L'Amministrazione dovrebbe prendere provvedimenti per effettuare il back-up delle proprie infrastrutture di telecomunicazione.
Il piano di Disaster Recovery dovrebbe considerare e fornire adeguate risorse di telecomunicazioni per la continuità delle attività aziendali critiche.
Le infrastrutture di telecomunicazione da prendere in considerazione includono i circuiti di fonia, le reti geografiche (ad esempio per connettersi a centri dati distribuiti), le reti locali (per connettere gruppi di PC) e gli ISV.
La capacità critica dovrebbe essere classificata in varie soglie, cioè 2, 8, 24 ore di fuori servizio, per le diverse risorse di comunicazione.
Le apparecchiature UPS dovrebbero essere sufficienti per fornire un adeguato back-up sia alle apparecchiature trasmissive sia alle apparecchiature elaborative.

I metodi più comuni per fornire continuità di comunicazione sono:
- Ridondanza
- Instradamento alternativo
- Instradamento del traffico tramite il frazionamento dei mezzi infrastrutturali fisici trasmissivi o la loro duplicazione.

- Diversificazione delle reti geografiche grazie al reinstradamento automatico e linee ridondanti per offrire un ripristino istantaneo in caso di caduta
- Ridondanza dei circuiti "all'ultimo miglio".

Il piano deve definire i modi di approvvigionamento delle apparecchiature alternative. Ad esempio si possono valutare le seguenti alternative:

Accordo di fornitura di hardware con un fornitore o terzi
Gli accordi con il venditore dovrebbero pianificare il passaggio da un sito "caldo" a un sito "tiepido" o "freddo

Disponibilità presso il fornitore
I componenti sono facilmente disponibili presso il fornitore in poco tempo e con una minima necessità di speciali predisposizioni.

Immagazzinamento degli equipaggiamenti
Gli equipaggiamenti dovrebbero essere acquistati in anticipo e immagazzinati in un sito alternativo.
Nel piano di Disaster Recovery dovrebbe essere prevista la descrizione della sicurezza del sito alternativo.
Il centro di elaborazione alternativo, deve disporre dello stesso livello di sicurezza e controllo del centro originale.
Questo implica adeguati controlli per l'accesso fisico quali porte chiuse, assenza di finestre, servizio di sorveglianza. Il centro alternativo dovrebbe essere sottoposto a costanti verifiche e controlli ambientali come il centro originale.
Questo comporta il continuo controllo di temperatura, umidità e aria condizionata per raggiungere le condizioni ottimali previste per la conservazione dei supporti magnetici ed, eventualmente, per l'unità centrale e per le diverse unità periferiche.
I controlli ambientali devono prevedere inoltre il pavimento sopraelevato, rilevatori di fumo e di acqua, il gruppo elettrogeno di continuità ed il sistema di spegnimento automatico di incendio adeguatamente provato e funzionante.
L'archiviazione in luoghi esterni di quelle applicazioni che non sono direttamente collegate al mainframe diventa di importanza vitale per sopravvivere in caso di disastro.
Le attività di conservazione per le attività elaborative di supporto all'utente comprenderanno normalmente l'archiviazione in luoghi diversi dei floppy disk e la duplicazione dei file del server.

Al fine di poter riattivare completamente le elaborazioni critiche dell'utente, il centro alternativo dovrebbe comprendere le apparecchiature PC considerate necessarie, le connessioni di telecomunicazione (incluse le connessioni per la fonia) e le apparecchiature ed il software per le LAN.
Il piano dovrebbe prevedere una schedulazione formalizzata delle elaborazioni di tutto il sistema.
Questa schedulazione andrebbe definita per tutti i giorni dell'anno al fine di facilitare l'identificazione di quei sistemi che sono critici al momento in cui avviene il disastro.
La schedulazione andrebbe dettagliata fino al punto da indicare l'ordine da seguire per l'esecuzione di tutti i lavori da elaborare. Il mantenere aggiornata questa sezione del piano di Disaster Recovery è fattore critico se avvengono variazioni all'ambiente elaborativo.

Gestione della crisi
Per Gestione della Crisi si intende il coordinamento complessivo della risposta organizzativa ad una possibile crisi in modo efficace e tempestivo, con lo scopo di evitare o minimizzare i danni al profitto, alla reputazione ed alla capacità di operare dell'Amministrazione.
Le fasi di gestione della crisi dovrebbero essere:
1. Notificazione ed attivazione della crisi
   - Procedure di notifica al personale coinvolto e sequenza delle chiamate
   - Assessment dei danni
   - Piano di attivazione della crisi
2. Recovery dell'emergenza
   - Definizione della sequenza delle attività di recovery
   - Procedure di recovery
3. Ricostituzione dell'operatività
   - Ricostituzione del sito originale
   - Test dell'operatività
   - Termine delle operazioni di emergenza e ripresa dell'operatività normale
4. Attività di gestione post crisi.

La gestione della crisi necessita del coinvolgimento e del coordinamento di team specifici comprendenti le persone incaricate di realizzare i piani di azione.
Queste persone sono generalmente a capo di gruppi creati in corrispondenza di una funzione o compito critico definito nel piano.
A seconda delle dimensioni della struttura organizzativa, questi gruppi si possono anche definire come posizioni di una persona singola.
Ogni team dovrebbe essere addestrato affinchè capisca la funzione del team durante il ripristino, ogni passo da eseguire e come i team si relazionano agli altri team; Il team dovrebbe essere pronto ad operare in ogni momento in caso di necessità di attivazione del piano.

I possibili team identificabili sono i seguenti:

Senior Management Official Team (Gruppo di management)
Questo gruppo è responsabile del coordinamento delle attività di contenimento e contrasto del disastro, supervisiona tutti gli altri gruppi e prende le decisioni chiave per le emergenze interne ed esterne. Il team è responsabile l'attivazione del piano d'emergenza. Il team è guidato da un esponente del Senior Management con l'autorità di prendere decisioni su livelli di spesa, rischio accettabile e coordinamento tra funzioni aziendali e con gli organi esterni di Polizia e Protezione civile.

Management Team (Gruppo per la gestione dell'emergenza)
Questo gruppo funziona come supporto tecnico operativo all'unità di crisi ed opera come "supervisore del disastro". Da esso dipende il coordinamento di tutte le attività degli altri team ed in particolare:
- Recuperare i dati critici e essenziali dal deposito
- Installare e provare il software di sistema e le varie applicazioni presso il sito di recovery del sistema (sito "caldo", sito "freddo", service bureau)
- Identificare, comprare e installare l'hardware opportuno presso il sito di recovery del sistema
- Operare dal sito di recovery del sistema

- Reinstradare il traffico sulle reti di comunicazione
- Reinstallare la rete utente/sistema
- Trasportare gli utenti alla installazione di recovery
- Ricostruire i data base
- Fornire i necessari materiali di ufficio (per es. moduli speciali, scorte di controllo, carta, etc.)
- Coordinare l'uso dei sistemi e i piani di lavoro degli addetti.

Emergency team (Gruppo per le attività di emergenza)
È il gruppo di primo intervento. Sono i componenti delle squadre pompieri e delle cosiddette squadre di emergenza e la loro funzione è il trattamento degli incendi o di altre situazioni d'emergenza. Una delle loro funzioni primarie sarà l'evacuazione ordinata del personale e la salvaguardia di vite umane.

Damage assessment team (Gruppo per la valutazione dei danni)
La funzione di questo gruppo è di valutare le dimensioni dei danni causati dal disastro. Il gruppo dovrebbe comprendere persone in grado di valutare il danno e stimare il tempo richiesto per ripartire con le attività usuali nel sito interessato.
Questo gruppo dovrebbe includere personale esperto nell'uso di apparecchi di collaudo, con conoscenza di sistemi e reti ed addestrato sui regolamenti e procedure di sicurezza da applicare. Inoltre, queste persone avranno la responsabilità di identificare le possibili cause del disastro e il suo impatto in termini di danni e di prevedibile tempo di fermo del sistema.
Altri team si occupano della gestione degli aspetti finanziari del ripristino, del trattamento delle questioni legali derivanti dal disastro, nonchè delle pubbliche relazioni e delle informazioni ai media.

Per queste funzioni sono identificabili anche i seguenti gruppi operativi:

Media Relations Team (Gruppo delle pubbliche relazioni)
Questo gruppo si occupa delle relazioni pubbliche per ridurre i rischi di immagine.

Legal Affairs Team (Gruppo affari legali)
Questo gruppo si occupa di tutti gli aspetti inerenti le implicazioni legali e normative, comprese quelle sulla Privacy e quelle di Responsabilità degli amministratori previste dal DPR. 31/2001.

Physical/Personal Security Team (Gruppo di sicurezza)
Questo gruppo si occupa di tutte le condizioni che impattano i rischi legati alla sicurezza, ambientale fisica e del personale coinvolto nel disastro.
In particolare controlla in modo continuativo durante l'emergenza la sicurezza del sistema e delle comunicazioni; inoltre risolve ogni conflitto di sicurezza che impedisca un rapido recovery del sistema. Assicura l'appropriata installazione ed il funzionamento del pacchetto software di sicurezza.

Procurement (equipment and supplies) Team (Gruppo fornitori)
Questo gruppo ha l'obiettivo di gestire l'approvvigionamento dei materiali e degli equipaggiamenti necessari all'emergenza.

Supporta il lavoro del gruppo hardware utente contattando i fornitori e coordinando la logistica per la fornitura giornaliera del necessario materiale di supporto per il computer e gli uffici.

Altri gruppi di supporto tecnico al Disaster Recovery possono essere i seguenti:

Systems Software Team (Gruppo software di sistema)
È responsabile di effettuare il "restore" dei dischi di sistema, di caricare e provare il software del sistema operativo, e di risolvere i problemi a livello sistemistico.

Server Recovery Team (e.g., client server, web server) (Gruppo di ripristino dei serventi)
È responsabile di tutte le attività sistemistiche ed operative per il ripristino dei serventi e delle server farm.

Application Recovery Team(s) (Gruppo applicativo)
Si reca al sito di recovery del sistema e effettua il restore dei dischi utente e dei programmi applicativi sul sistema. A mano a mano che procede il recovery, questo gruppo può assumere la responsabilità di controllare le prestazioni applicative e l'integrità dei data base.

Operating System Administration Team (Gruppo operativo d'emergenza)
Consiste di operatori e supervisori che, a turno, rimarranno presso il sito di recovery del sistema e gestiranno le operazioni di sistema durante tutta la durata dei progetti di disaster recovery. Un'altra responsabilità potrebbe essere quella di coordinare l'installazione dell'hardware qualora non sia stato scelto come centro di recovery un sito "caldo" o altra installazione con macchine già disponibili.

LAN/WAN Recovery Team (Gruppo di ripristino delle reti)
È responsabile per il reinstradamento delle comunicazioni in voce e dati su larga scala e il ristabilimento dei controlli e degli accessi alla rete su host presso il sito di recovery del sistema.

Network Operations RecoveryTeam (Gruppo operativo delle reti)
Fornisce un supporto continuativo per la trasmissione dati e supervisiona l'integrità delle comunicazioni.

Telecommunications Team (Gruppo delle telecomunicazioni)
Si reca al sito di recovery utente dove lavora insieme con il gruppo di recovery delle reti remote per ristabilire una rete utente/sistema. È anche responsabile per sollecitare e installare hardware per le comunicazioni presso il sito di recovery utente e di lavorare con gli uffici della società dei telefoni locali ed i fornitori gateway nel reinstradamento del servizio locale e accesso ai gateway.

Database Recovery Team (Gruppo della preparazione e registrazione dei dati)
Aggiorna i database applicativi lavorando da terminali installati presso il sito di recovery utente. Supervisiona il personale temporaneo addetto alla immissione dati e assiste ai tentativi di salvataggio dei record acquisendo i documenti originali e altre fonti d'informazione di input.

È responsabile anche di ottenere, imballare e spedire i supporti e altre registrazioni all'installazione di recovery come pure di stabilire e supervisionare un piano per la conservazione delle informazioni create durante l'attività del sito di recovery

Transportation and RelocationTeam (Gruppo di trasporto)
Serve come un gruppo di supporto per localizzare un sito di recovery utente se non ce n'è già uno prefissato ed è responsabile per coordinare il trasporto dei dipendenti dell'azienda a un sito distante di recovery utente. Possono anche aiutare a contattare i dipendenti per informarli sui nuovi luoghi di lavoro e a pianificare e prendere accordi per la sistemazione logistica dei dipendenti stessi.

Hardware Salvage Team (Gruppo dell'hardware utente)
Localizza e coordina la consegna e installazione di terminali utente, stampanti, macchine da scrivere, fotocopiatrici, e altre apparecchiature necessarie. Offre supporto al gruppo delle comunicazioni e a qualsiasi tentativo per il salvataggio di hardware e apparecchiature.

Administrative Support Team (Gruppo di supporto amministrativo)
Fornisce un supporto d'ufficio agli altri gruppi e serve come centro di raccolta/smistamento messaggi per il sito di recovery utente. Può controllare le funzioni di contabilità e stipendi come pure la supervisione giornaliera dell'installazione.

Alternate Site Recovery Coordination Team (Gruppo di rilocazione al sito alternativo)
Dirige il progetto di rilocazione. Fa una valutazione più dettagliata, rispetto a quella fatta inizialmente, dei danni subiti dall'installazione e dalle apparecchiature. Fornisce al gruppo per la gestione dell'emergenza le informazioni necessarie per determinare se i piani devono orientarsi verso la ricostruzione oppure la rilocazione. Fornisce le informazioni necessarie per avanzare richieste di rimborso alle assicurazioni (un'assicurazione è la prima fonte di fondi per il lavoro di ripristino).
Coordina gli sforzi necessari per il salvataggio immediato delle registrazioni (per es. recuperare documenti cartacei, supporti elettronici, etc.).

Original Site Restoration/Salvage Coordination Team (Gruppo di ripristino del sito originale o di salvataggio)
Coordina il trasferimento dal sito caldo ad una nuova locazione o alla locazione originaria ripristinata.
Ciò comporta la rilocazione delle attività elaborative, le comunicazioni e le attività utente. Questo gruppo controlla anche il ritorno verso i normali livelli di servizio.

FEDERCOMIN

Ministro per l'Innovazione e le Tecnologie
Centro Studi

Osservatorio permanente della Società dell'Informazione

Evoluzione dell'innovazione in Italia secondo i parametri eEurope 2005

2° semestre 2004

Executive summary

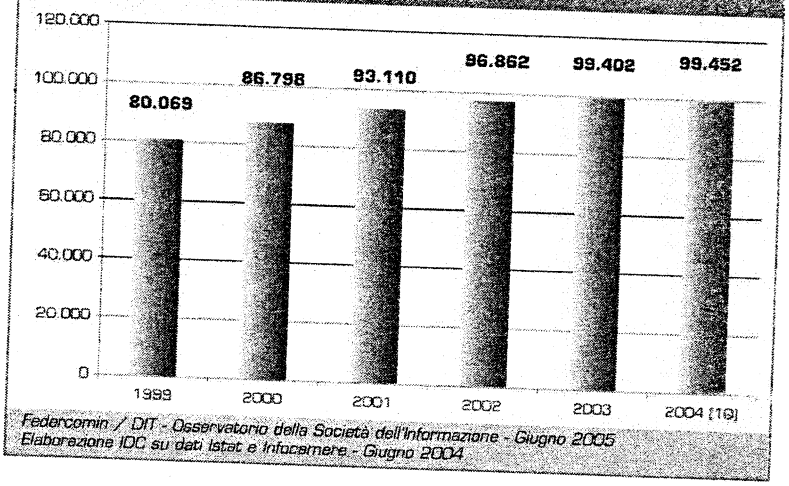
L'Osservatorio della Società dell'Informazione

L'Osservatorio permanente della Società dell'Informazione, realizzato da **Federcomin e Dipartimento per l'Innovazione e le Tecnologie** con la collaborazione di due istituti di ricerca (**IDC e Nielsen//NetRatings**), si propone di diventare il punto di riferimento dello stato di sviluppo della Società dell'Informazione in Italia.
Per raggiungere questo obiettivo si sono seguiti le indicazioni e i parametri del **Piano d'Azione eEurope 2005**, che contiene le linee guida per lo sviluppo e l'utilizzo in ogni Paese europeo di tecnologie informatiche, al fine di supportare lo scambio di informazioni e di servizi tra gli Stati membri.
L'Osservatorio, che ha **periodicità semestrale**, intende analizzare la domanda nei segmenti delle imprese, cittadini ed istituzioni, aggregando i dati intorno a due *focus* principali: **l'utilizzo dell'ICT, come misura della competitività del Paese, e lo sviluppo dei servizi innovativi.**

Il settore ICT in Italia

Il sistema imprenditoriale italiano, e in particolare il settore ICT, è caratterizzato dalla presenza di un numero molto elevato di piccole o *micro* imprese, connotate spesso dall'assenza di una reale struttura aziendale e di addetti. Facendo riferimento a tutte le realtà, comprese quindi le "Partite Iva", **il numero totale delle imprese italiane del comparto ICT è pari, a metà 2004, a circa 100.000 unità**.

FIGURA 1 LE AZIENDE ICT IN ITALIA (unità)



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Elaborazione IDC su dati Istat e Infocamere - Giugno 2004

Scorporando da tale dato (come evidenzia il Rapporto Federcomin del 2004 "*Occupazione e formazione nell'ICT*") le imprese in situazione di criticità (ovvero le aziende in fallimento, in liquidazione o sospese), si arriva a un numero di imprese attive, a fine 2003, pari a **77.300**. Se si considera, poi, il numero di aziende effettivamente strutturate e organizzate con la finalità di svolgere attività di impresa (con addetti, dipendenti o indipendenti), si scende a circa **32.000** imprese. Infine, considerando solo le forme societarie aventi dipendenti, le realtà strutturate del settore ammontano a circa **28.700** unità.
Gli addetti occupati nei settori IT e TLC ammontano, nel 2003 in Italia, al 4,4% del totale della forza lavoro. Nel confronto con gli altri Paesi, l'Italia rimane ancora sotto la media europea.

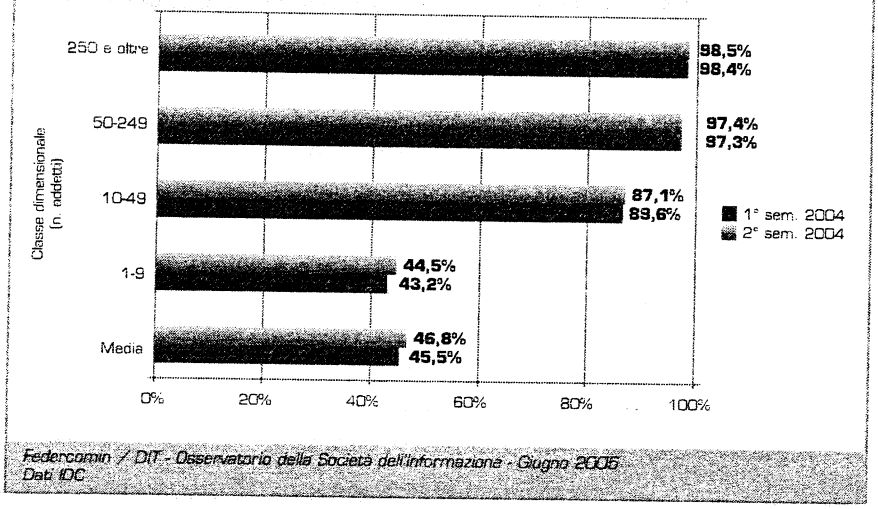
Internet: accesso e utilizzo

Nelle imprese - Considerando il ritardo con cui il mercato italiano ha adottato Internet come strumento di comunicazione e di *business*, si può oggi affermare che una parte significativa del divario iniziale è stato colmato, almeno rispetto agli indicatori di base: **la quasi totalità delle aziende medio-grandi accede ormai a Internet e una quota significativa di esse ha sviluppato una o più piattaforme "a valore aggiunto"** basate su Internet, attraverso le quali collegarsi ai propri dipendenti, ai clienti e fornitori, o alla pubblica amministrazione.

Qualche ritardo emerge nella fascia dimensionale più bassa delle imprese (classe 1-9 addetti), in cui il ricorso a Internet rimane di poco superiore al 43%. Ma anche in queste realtà si assiste all'accelerazione nell'adozione di nuove tecnologie informatiche e nell'accesso a Internet, grazie soprattutto allo sviluppo, nel segmento dei servizi, di nuove iniziative imprenditoriali che coinvolgono soggetti tendenzialmente più propensi ad utilizzare le nuove tecnologie rispetto a quanto accade nelle aziende di piccole dimensioni dei settori più tradizionali.

Il tasso di diffusione dei collegamenti a banda larga mostra una crescita elevata e costante, grazie agli sforzi messi in atto dal Governo (contributi di attivazione, piani di *e-Government*, sensibilizzazione delle aziende), ma anche allo sviluppo di un'offerta molto aggressiva e articolata da parte di tutti i principali *service provider* operanti in Italia, che ha abbassato significativamente le barriere all'ingresso per questa tipologia di servizi permettendone la diffusione. **A giugno 2004 la banda larga veniva utilizzata in Italia dalla quasi totalità (95%) delle aziende con più di 250 addetti e da circa il 45% delle aziende medie e piccole.**

FIGURA 6 IMPRESE CON ACCESSO A INTERNET (%)

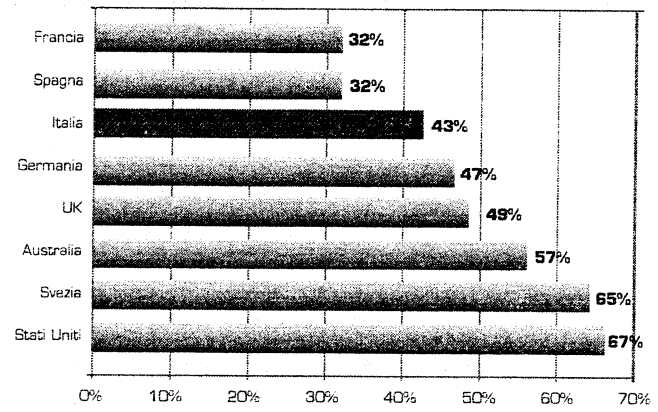


Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati IDC

Nelle famiglie - Un parametro utile per una prima valutazione del grado di informatizzazione dei cittadini italiani è il numero di famiglie che possiedono un Personal Computer in casa. A giugno 2004 **il 56% delle famiglie italiane dispone di un PC domestico**, valore in linea con quelli di altri Paesi dell'Europa centrale, ma abbastanza lontano dal grado di penetrazione del PC nelle famiglie del nord Europa: per esempio in Svezia, Paese che ha sempre dimostrato una elevata predisposizione all'innovazione tecnologica, la penetrazione del PC nelle famiglie è pari al 72%.
Di tutti i PC domestici, l'81% è collegato a Internet, mentre le famiglie con accesso a Internet, sul totale delle famiglie italiane, è pari a circa 42%, con un incremento del 10% negli ultimi dodici mesi. Quello italiano è il secondo tasso di crescita in Europa, dopo il 13% della

Germania. L'Italia si pone dopo la Svezia (circa 64%), UK (45%) e Germania (44%), con un potenziale di sviluppo ancora ampio.
Considerando gli individui maggiori di 14 anni che hanno accesso a Internet, **19,4 milioni sono i navigatori potenziali, mentre 16,4 milioni di questi possono definirsi *navigatori attivi***, ovvero hanno effettuato almeno una connessione alla rete dal computer domestico nel secondo trimestre del 2004.

FIGURA 17 FAMIGLIE CON ACCESSO A INTERNET DA CASA (%)



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati Nielsen//NetRatings - Dicembre 2004

Il navigatore domestico italiano ha un profilo prevalentemente maschile (56%) e adulto, con un buon livello di istruzione (il 66% degli internauti da casa ha almeno un diploma), livelli di occupazione medio-alti (il 12% svolge la libera professione o occupa posizioni di dirigente o quadro). La distribuzione per reddito privilegia le fasce centrali: il 53,2% dichiara di appartenere ad una fascia compresa tra i 15,500 e i 46,499 euro lordi annui. Il 56% degli utilizzatori di Internet ha un'età compresa tra i 25 e i 54 anni.

Sono quasi 6 milioni i navigatori a banda larga a giugno in Italia (per banda larga si intende una velocità di connessione superiore a 128 Kbps), il 38% di tutti gli utilizzatori attivi di Internet da casa. **La penetrazione della banda larga in Italia non è omogenea: in tutto il Nord è superiore al 40%, nel Centro-Sud ha una media del 34%**. Il navigatore in banda larga ha un profilo più maschile di quello a banda stretta. La distribuzione per fasce d'età rivela una maggiore componente di *teen-ager* e di *over* 55 tra gli utilizzatori ad alta velocità.

La fruizione della rete è un'attività che inizia a far parte della quotidianità degli italiani. Due terzi degli utilizzatori accedono almeno una volta alla settimana, il 26,6% tutti i giorni. I più assidui sono gli uomini (il 70,7% dei navigatori uomini si connette almeno una volta alla settimana). Le donne confermano la loro peculiarità di "*light users*" (il 21,6% delle navigatrici si connette meno di una volta al mese). Tra gli utenti più regolari ci sono gli adulti tra i 25 ed i 54 anni (quasi il 30% di tutti gli utilizzatori in quella fascia d'età si connette tutti i giorni) ed i giovani tra i 18 ed i 24 anni (il 43,3% di tutti gli individui in quella fascia d'età si connette almeno una volta alla settimana.

La fotografia dell'Italia connessa non dà l'immagine di un Nord tecnologico e un Sud arretrato. Dei 19,4 milioni di utilizzatori di Internet, il 32% vive nel Nord Ovest, il 28%, ossia oltre 5,4 milioni di individui, nel Sud; meno di 4 milioni accedono alla rete nel Nord Est e circa gli

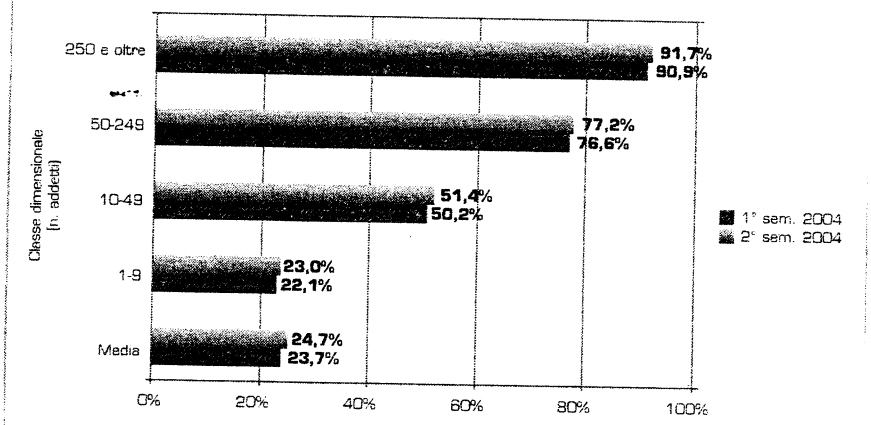
stessi nel Centro. E anche i tassi di utilizzo sono importanti: il 30% di chi si connette complessivamente nel Nord lo fa tutti i giorni, il 41% di chi lo fa nel Centro-Sud almeno una volta alla settimana.

Quali attività sono più diffuse nella rete? Più della metà degli italiani che hanno usato Internet negli ultimi tre mesi lo ha fatto per ricercare informazioni su argomenti di studio o lavoro (56,5%) e per la posta elettronica (52%). Anche reperire informazioni su prodotti, servizi o viaggi svolge un ruolo significativo nella navigazione degli italiani: vi ricorrono il 41,3% degli internauti. Poco più di un navigatore su cinque, invece, consulta i giornali e le *news on-line* (21,5%). E' un'abitudine invece ancora limitata ricorrere al *web* per reperire informazioni in materia sanitaria (9,4% degli utilizzatori Internet) o fare *shopping on-line* (6,8% degli utilizzatori).

La sicurezza *on-line*

Uno dei temi più importanti collegati allo sviluppo dell'*economia in rete*, oltre che di estrema attualità nella situazione internazionale che stiamo vivendo, è quello della sicurezza come condizione di base per supportare e stimolare la crescente apertura in rete dei sistemi informativi aziendali, attraverso l'utilizzo della larga banda, dei servizi mobili e *wireless* di nuova generazione, dei portali, di Intranet e Extranet.
Nelle aziende sopra i 50 dipendenti (ovvero quelle più connesse in rete) la quasi totalità delle imprese ha già adottato più di un sistema di sicurezza informatica. Più scoperte sembrano essere **le realtà di piccole dimensioni,** che **solo nel 22% dei casi dispongono di almeno due sistemi di sicurezza informatica**: ciò è dovuto sia al minore livello di informatizzazione e di utilizzo di Internet rispetto alle aziende di maggiori dimensioni, sia alla relativa semplicità della loro dotazione informatica che nella maggior parte dei casi può essere protetta anche solo da un sistema antivirus.

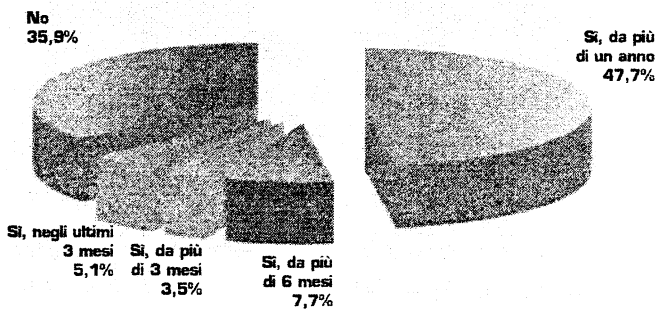
FIGURA 28 IMPRESE CHE UTILIZZANO ALMENO DUE SISTEMI DI SICUREZZA INFORMATICA (%)



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati IDC (% calcolata delle imprese dotate di almeno un PC)

La maggior parte degli utilizzatori Internet da casa (64%) si è dotato di misure di sicurezza per proteggere il computer e di questi il 48% lo ha fatto da più di un anno. Gli aggiornamenti di questi *software* vengono eseguiti direttamente da persone della famiglia (nel 70% dei casi), solo il 13,9% degli utilizzatori ricorre ad un tecnico.

FIGURA 31 UTILIZZATORI WEB CHE ADOTTANO MISURE DI SICUREZZA



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati Nielsen // NetRatings - Giugno 2004

La sensibilità verso un utilizzo consapevole del mezzo Internet è andata crescendo negli ultimi anni parallelamente a un incremento della sua diffusione nelle case e negli uffici degli italiani. La consapevolezza dei potenziali rischi genera frequentemente un atteggiamento di attenzione da parte del navigatore nei confronti dei contenuti che la rete gli propone.
Dei 19,4 milioni di utilizzatori Internet, **il 56,7% dichiara di prestare sempre molta attenzione agli indirizzi digitati** nella barra del *browser* e a certa pubblicità che compare sulle pagine *web*. Il 29,2% alza il livello di attenzione solo sui siti mai frequentati in precedenza. **Il 14,1% non è particolarmente allarmato quando naviga**.

E' ancora molto circoscritto il numero di bambini della scuola elementare che fruiscono della rete: quasi 700 mila hanno navigato nel secondo trimestre del 2004, ovvero il **38,6%** di tutti i bambini in età compresa tra i 6 e gli 11 anni che vivono in famiglie con connessione. E quasi sempre accanto a loro si affianca un adulto (genitore ed insegnante) che li assiste nella navigazione: **solo il 6,8% dei bambini tra i 6 gli 11 anni utilizza Internet senza l'assistenza di un adulto**.

e-Government

Dall'indagine emerge un uso crescente delle nuove tecnologie informatiche e di comunicazione, sia come piattaforme di relazione tra la P.A. e l'universo delle aziende e cittadini, sia come strumento di lavoro all'interno delle stesse amministrazioni. Una spinta importante è venuta da tutte le iniziative di *e-Government* avviate dal Governo, anche se ad oggi la maggior parte dell'interazione tra amministrazioni pubbliche e amministrati è ancora di tipo prevalentemente informativo (prenotazioni, pagamenti, ecc).

I servizi pubblici di base disponibili on-line

	Ottobre 2003	Variazione 2003-2001	Media UE 2003
Imposte sul reddito	100%		88%
Ricerca del lavoro	100%		82%
Assistenza e previdenza sociale	68%	12%	12%
Documenti personali	50%	-	6%
Concessione edilizia	6%	4%	6%
Denunce alla polizia	33%	-1%	24%
Biblioteche pubbliche	100%	95%	35%
Certificati di nascita e di matrimonio	5%	-6%	27%
Iscrizione alla scuola media superiore	32%	5%	35%
Cambio indirizzo	6%	3%	36%
Servizi sanitari	21%	17%	11%

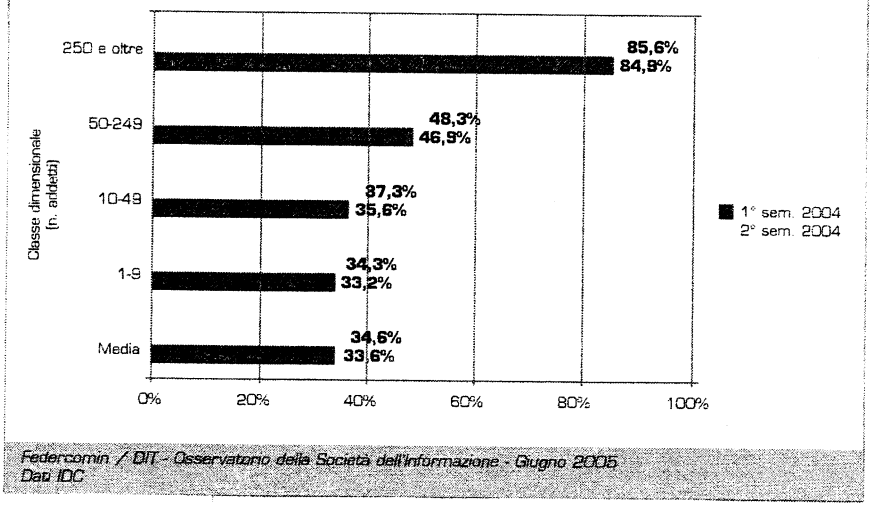
Federcomin / DIT - Osservatorio permanente della società dell'informazione - Ottobre 2004
Elaborazione Centro Studi MIT

Fra Nord e Sud c'è ancora un divario di servizi *on* line da colmare: mentre tra le amministrazioni comunali del Nord e del Centro rendono disponibili servizi per una percentuale pari rispettivamente all'87% e al 90%, al Sud i Comuni che offrono questa possibilità non superano il 50% del totale.

La domanda: le imprese

Circa un terzo (33,6%) delle imprese italiane utilizza regolarmente lo strumento Internet per contattare la Pubblica amministrazione. Questa soglia accomuna in particolare le imprese con meno di 50 addetti; **il contatto con la PA risulta in crescita nella classe di aziende che hanno un numero di addetti compreso tra 50 e 250 (47%), mentre nelle imprese di dimensioni maggiori la comunicazione con gli enti pubblici appare molto diffusa (85%)**.

FIGURA 36 IMPRESE CHE UTILIZZANO INTERNET PER CONTATTARE LA PUBBLICA AMMINISTRAZIONE (%)



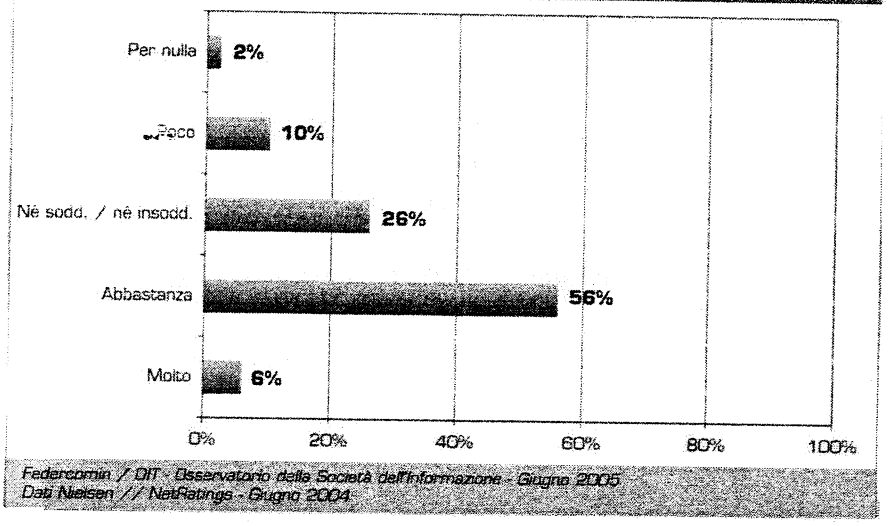
Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati IDC

La domanda: i cittadini

Per quanto riguarda l'utilizzo dei siti della PA da parte dei cittadini, si può parlare di un buon successo: **sono stati consultati, nel secondo trimestre del 2004, da oltre 10 milioni di visitatori unici. Il 17% in più rispetto allo stesso periodo del 2003**.
L'incremento di navigatori che accedono ai siti della PA è un *trend* europeo, con Paesi come Francia e Germania che registrano tassi di crescita superiori al 30% nell'ultimo anno. **L'Italia in questo ambito si pone insieme a Francia e Spagna tra i paesi *leader***: qui la penetrazione di tali siti sul totale della popolazione Internet è superiore al 50%: più di un navigatore su due visita un sito della PA in un trimestre .
In Italia il traffico coinvolge sia i siti delle Amministrazioni locali sia quelli dei Ministeri. Tra questi, il più visitato *on-line* nel secondo trimestre del 2004 è quello dell'Istruzione, Università e Ricerca con oltre 1,8 milioni di utenti unici, seguito dal Ministero dell'Economia e della Finanza con più di 1,6 milioni.

Gli italiani ricorrono all'*e-government* soprattutto per ricercare informazioni (così dichiara il 77,3% degli utilizzatori di questi siti); solo il 38,3% per scaricare moduli. Quote ulteriormente inferiori si evidenziano per inviare moduli compilati (10,8%) o pagare tasse, bollette, canoni (6,2%). I cittadini del nostro paese dimostrano di avere molte aspettative nei confronti di un rapporto digitale con le Amministrazioni e le Istituzioni. Tra i servizi che vorrebbero efficienti *online*, prioritari sono il rilascio di documenti personali, la ricerca di lavoro ed i servizi sanitari. **Ma si dichiarano al contempo soddisfatti dell'offerta attuale** (così si esprime il **62,6%** degli utilizzatori di questi siti).

FIGURA 40 GRADO DI SODDISFAZIONE DEGLI UTENTI DEI SITI DELLA PUBBLICA AMMINISTRAZIONE



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati Nielsen // NetRatings - Giugno 2004

e-Learning

Imprese - Un'area applicativa sulla quale si concentra sempre più l'interesse delle aziende è la formazione del personale, che rappresenta un tema molto sentito dalle imprese, sebbene le modalità, le tecniche e gli strumenti utilizzati siano tra i più disparati. Il **21,6% di imprese con oltre 250 addetti utilizza applicazioni di *e-Learning*** per la formazione del proprio personale, mentre le

classi inferiori di addetti si attestano mediamente tra il 4,6% e il 6,5% di adozione, determinando un dato medio del 4,8%.

Scuola - Per quanto concerne la penetrazione dei computer nelle scuole, i dati indicano un *trend* di crescita positivo. Secondo uno studio del Ministero dell'Istruzione, per un totale di 5,8 milioni di studenti distribuiti nei tre livelli delle scuole dell'obbligo, **sono disponibili oltre 500 mila *computer*: uno ogni 10,9 studenti**. Circa 456 mila di questi *computer* sono anche connessi. Nelle scuole italiane pertanto c'è **un *computer* collegato alla rete ogni 12,8 studenti**.

Cittadini - Si stima che la maggior parte dei navigatori utilizzi Internet per ricercare informazioni su argomenti di studio o di lavoro (con una sostanziale uguaglianza di valori tra uomini e donne), mentre ancora bassa è la percentuali di chi utilizza il *web* in modo più organico, ovvero per seguire reali corsi di formazione.

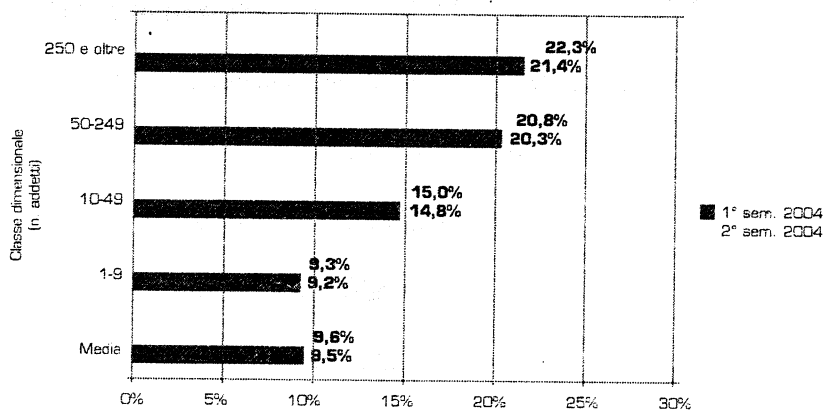
e-Health

Dalla rilevazione **emerge la ridotta presenza di ospedali che consentono di prenotare *online* una visita: solo il 4,4%.** Questa modalità è poco diffusa e **non emergono particolari differenze rispetto alle macro-aree geografiche**. Il contesto territoriale, che con riguardo ad altri indicatori ha fornito evidenza di differenti stadi di sviluppo, sembra influenzare meno questo genere di iniziative. Piuttosto, è la convergenza di diversi fattori, soprattutto a carattere interno alle strutture sanitarie, che rende possibile il verificarsi di condizioni favorevoli alla predisposizione di servizi avanzati, che trovano quindi manifestazione casuale rispetto alla presenza geografica.

e-Business

Le imprese - L'*e-Business* sta modificando il tessuto delle imprese italiane ad iniziare da quelle dimensionalmente maggiori, che presentano strutture e complessità più coerenti con le funzioni delle soluzioni *Internet-based*. Tuttavia, il panorama appare ancora caratterizzato da una sorta di soglia minima di accesso all'*e-Business*, che segna un **limite di demarcazione tra le imprese con almeno 50 addetti e le classi di aziende dimensionalmente più piccole**.
Il commercio elettronico ha introdotto un profondo rinnovamento nei processi di acquisto, sia dei privati sia in ambito *business*. Se ad oggi il valore dei beni e dei servizi scambiati rappresenta, dal punto di vista quantitativo, una minima parte del valore complessivo della produzione (**si stima pari a 3,2% il peso dell'*e-Commerce* sul fatturato delle imprese in Italia** – il primo dei quali calcolato nella sua accezione più allargata, che include il valore degli ordini o impegni all'acquisto inoltrati in ambito B2C e B2B in Italia), il significato più profondo di questo fenomeno è da ricercare nell'approccio e nelle motivazioni che stanno alla base del trasferimento di transazioni dal contesto tradizionale a quello online.
Il raggiungimento di un'integrazione non solo a carattere interno, ma che coinvolga anche *partner* esterni rientra tra gli obiettivi del concetto "impresa estesa", un percorso che si ispira alle sinergie e alle interdipendenza nascenti lungo le filiere produttive e dei servizi, tra operatori a monte e anelli a valle della catena del valore. **La complessità sottesa a questo processo determina però uno stato attuale di integrazione con sistemi informativi di attori esterni ancora ridotta (9,7%), con punte del 21,4% per le aziende di grandi dimensioni**.

FIGURA 46 IMPRESE CHE DISPONGONO DI SISTEMI INFORMATICI COLLEGATI IN RETE AI SISTEMI DI FORNITORI O CLIENTI (%)



Federcomin / DIT - Osservatorio della Società dell'Informazione - Giugno 2005
Dati IDC (% calcolata sulle imprese con accesso a Internet)

Più diffuso è il ricorso ad applicativi di *e-Commerce* grazie sia alla relativa semplicità delle funzionalità di tali applicazioni (almeno nelle forme "*basic*" che, ad esempio, non prevedono che i pagamenti vengano eseguiti *online*) che alla diffusione di portali o *marketplace* all'interno dei quali più aziende possono condividere applicazioni di *e-Commerce*, a costi quindi molto più contenuti (e con una maggiore visibilità in rete) rispetto al caso del sito di *e-Commerce* gestito internamente dall'azienda. Questa seconda soluzione riguarda per lo più le piccole aziende, permettendo loro di sviluppare applicativi di vendita on-line in una percentuale di casi non lontana dalle aziende di maggiori dimensioni.
Dai risultati esposti relativamente al livello di integrazione degli applicativi gestionali aziendali, si può dedurre che nella maggior parte dei casi queste iniziative di *e-Commerce* automatizzino principalmente il *front-end*, rappresentando comunque il primo passo di un processo di integrazione delle attività di *e-Business* all'interno dei sistemi IT aziendali. Questo primo *step* accomuna con intensità simile tutte le fasce d'impresa, con una penetrazione sul totale aziende attorno al 20%.
Il ricorso a servizi bancari e finanziari rientra tra le modalità di utilizzo di Internet che ha avuto più successo negli ultimi anni, incontrando non solo l'interesse della comunità delle imprese ma anche dei privati. L'evoluzione dei servizi offerti, la sofisticazione raggiunta dai sistemi di sicurezza e la maturità generale del mercato rappresentano fattori che trainano il ricorso a questi strumenti, **mediamente utilizzati dal 53% delle imprese con valori comunque superiori al 50% dei casi anche nella fascia dimensionalmente più bassa delle aziende che accedono a Internet**.

I cittadini - L'utilizzo di Internet a finalità di *e-Commerce* è ancora a uno stadio semi-iniziale: **solo il 6,8% del navigatori attivi utilizza il *web* con questa finalità**. Una delle barriere maggiori alla diffusione dell'*e-Commerce* riguarda i già visti ambiti di sicurezza e *privacy*: la scarsa fiducia verso i pagamenti *on-line* e la scarsa propensione a lasciare i propri dati sensibili.

R&S e Università

La spesa in Ricerca e *Sviluppo*

Oltre ai parametri relativi all'utilizzo delle nuove tecnologie informatiche e di comunicazione da parte di cittadini, **un macro-fattore che contribuisce in modo fondamentale alla crescita della competitività di un paese è la spesa in Ricerca e Sviluppo**.

Nel 2003 la spesa pubblica in Ricerca e Sviluppo è stata pari allo 0.54% del Prodotto Interno Lordo; quella privata si è attestata su valori paragonabili (0.56%); la spesa totale in R&S risulta quindi essere stata pari all'1,10% del PIL.
Questo valore è decisamente inferiore alla media Europea, che è pari all'1,94%. Lo stesso parametro riferito a paesi ad alto valore tecnologico quali Svezia e Finlandia presenta valori che oscillano tra il **4% e il 5%**.

I servizi *on-line* offerti dalle università
La percentuale di università che permette di prenotarsi *on-line* agli esami è pari, a metà 2004, al 76% del totale. Più basso il valore degli istituti che permettono di accedere *on-line* agli esiti degli esami scritti (39%) e che permettono di pagare le tasse di iscrizione on-line (19%).

I servizi on-line offerti dalle università (%)	
	1° sem 2004
Università che permettono di prenotarsi agli esami on-line	76%
Università che permettono di accedere agli esiti degli esami scritti on-line	39%
Università che permettono di pagare le tasse di iscrizione on-line	19%
Federcomin / DIT - Osservatorio permanente della società dell'Informazione - Ottobre 2004	
Dati IDC	

REGULATORY REFORM AS A TOOL FOR BRIDGING THE DIGITAL DIVIDE

Abstract

The digital divide touches all regions and economies of the world and threatens to slow progress towards the goal of an all-inclusive information society. Policy makers are faced with the divide's daunting complexity but have a range of policy tools that have proven effective in expanding access throughout the world. Of these tools, regulatory reform has had perhaps the largest impact in both developed and developing economies alike.

The severity of the digital divide in OECD countries is much less than in other parts of the world, due partially to higher income levels, but also as a result of important regulatory reforms initiated over the past several decades. These reforms have paved the way for competitive markets to develop and flourish with minimal intervention.

Regulatory reform can play a key role in non-OECD economies. Policy makers in developing economies should consider the regulatory reforms that have proven the most successful in the OECD, namely liberalizing telecommunication markets, creating a separate telecommunications regulator, opening spectrum for new wireless technologies and promoting the development of human ICT capacity.

As regulatory reforms take effect, telecommunication markets become more efficient and social and economic welfare are enhanced for all stakeholders in an economy via positive externalities. Telecommunications infrastructure can play a key role in economic development, which can create a virtuous cycle where incomes improve and access increases. Telecommunication technologies have also played an important role in enhancing total factor productivity in OECD economies and in employment growth.

As recent events have shown, telecommunication networks can also play a key public safety role in an economy, especially as a tool for disaster warning and recovery efforts. Economies with under-developed telecommunication markets and networks may face higher risks in the face of future catastrophes than economies with extensive networks and public safety systems in place. As a result, this paper includes a section on the need to examine the role of regulatory reform of emergency telecommunication services as a cost-effective and essential way to ensure the optimum contribution of ICTs to disaster warning and recovery.

This paper examines one narrow aspect of the digital divide, the effects of regulatory reform on telecommunication networks. While regulatory reform is only one part of the global digital divide problem, it can play a key role in helping telecommunication markets bridge some of the gaps on their own. It is therefore imperative that policy makers consider regulatory reform as a necessary but not sufficient step towards overcoming the digital divide.

Ministro
per l'Innovazione
e le Tecnologie

PIANO DI INNOVAZIONE DIGITALE PER IL MEZZOGIORNO

Obiettivi, azioni e modalità di attuazione

Premessa

Uno dei maggiori fattori abilitanti alla crescita dei sistemi competitivi e alla diffusione dell'economia della conoscenza è l'innovazione tecnologica. Essa è in grado di generare sviluppo economico solo nei paesi in cui si è raggiunta una certa soglia di penetrazione delle tecnologie dell'informazione e comunicazione che contribuiscono in maniera determinante alla crescita della produttività del lavoro.

Il nostro paese registra un ritardo nello sviluppo della Società dell'Informazione generato da una bassa diffusione di applicazioni e di cultura informatica e da un evidente squilibrio tra nord e sud del paese negli investimenti legati alle tecnologie digitali.

Le politiche governative relative all'Innovazione devono considerare sia gli elementi ostativi relativi al basso utilizzo delle tecnologie digitali nel Mezzogiorno, sia i fattori di impulso allo sviluppo competitivo, quali ad esempio le specializzazioni locali.

E' in questa ottica che il processo di "riforma digitale" avviato dal nostro governo, anche attraverso il mio dicastero, considera la valorizzazione e lo sviluppo del Mezzogiorno Digitale una delle azioni prioritarie da avviare per lo sviluppo del sistema – Paese.

Per la realizzazione delle nostre politiche, nel quadro degli interventi nazionali, abbiamo realizzato il "Piano d'azione per la Società dell'Informazione per il Mezzogiorno". In coerenza con le direttive del Consiglio Europeo e con il piano eEurope 2005 il Piano si articola in due categorie di azioni:

- *stimolare servizi, applicazioni e contenuti sia per i servizi pubblici on line che per l'e-business;*
- *implementare e far evolvere l'infrastruttura di base a banda larga e gli aspetti legati alla sicurezza.*

Il presente Piano è il risultato della fruttuosa collaborazione con il Ministero dell'Economia e con le altre Amministrazioni Centrali e della concertazione attivata attraverso tavoli partenariali con Amministrazioni Regionali.

Lucio Stanca

Ministro per l'innovazione e le tecnologie

Sommario

1. L'Italia e il processo di crescita nella Società dell'informazione

1.1 Lo stato dell'Innovazione Digitale nel Sistema Paese

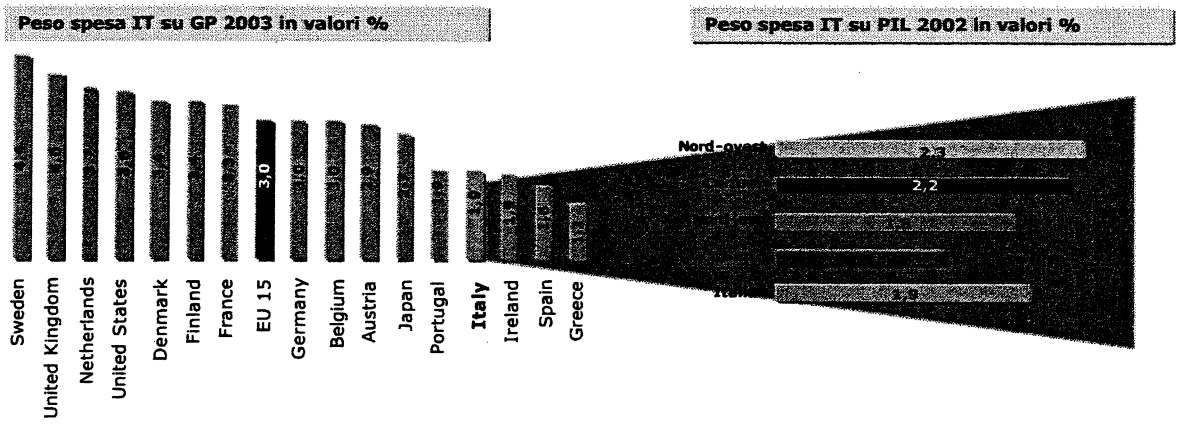
La politica di sviluppo sulla Società dell'Informazione è stata avviata dall'Unione Europea a partire dalla metà degli anni ottanta, attraverso l'incentivazione delle attività di ricerca e sviluppo nel settore dell'Information and Communication Technology, la liberalizzazione delle telecomunicazioni, la definizione di standard e quadri normativi di riferimento. Negli ultimi anni sono state pianificate azioni di medio e lungo periodo per lo sviluppo dell'economia della conoscenza attraverso infrastrutture e servizi su larga banda.

Il piano di azione eEurope 2005 segue il piano di azione 2002 che era soprattutto imperniato sull'estensione della connettività Internet in Europa. Il nuovo piano di azione, approvato dal Consiglio europeo di Siviglia nel giugno 2002, mira a tradurre questa connettività in un aumento della produttività economica e un miglioramento della qualità e dell'accessibilità dei servizi a profitto di tutti i cittadini europei, sulla base di un'infrastruttura a banda larga protetta e ampiamente disponibile.

Nei sistemi economici più dinamici il ruolo dell'innovazione tecnologica e delle tecnologie dell'informazione e della comunicazione è stato determinante[1].

La crisi delle economie occidentali degli ultimi anni ha prodotto un minor investimento in Information Technology rispetto al Prodotto Interno Lordo nei paesi industrializzati, ciò nonostante l'Italia è riuscita a passare dalla 13esima posizione nel 2001 alla decima nel 2003[2] nell'Unione Europea.

Peso della Spesa IT sul PIL nei Principali Paesi e contributo delle aree nazionali



Fonte: Eurostat

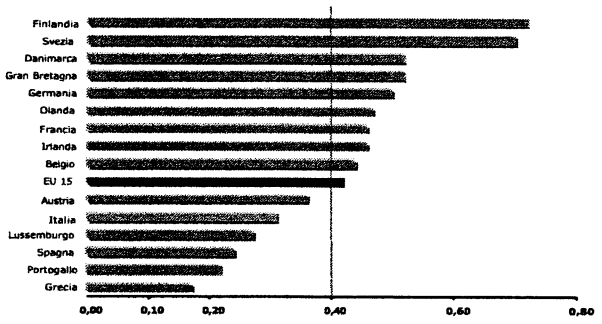
Fonte: Elaborazioni Innovazione Italia su dati Istat Conti regionali 2002/ Assinform Rapporto Regioni 2004

[1] Si veda la recente analisi del Economist Intelligence Unit, aprile 2004 "Reaping the benefits of ICT Europe's productivity challenge"

La posizione italiana, anche se in miglioramento, manifesta un ritardo determinato dalla bassa propensione del sistema agli investimenti. Determinante il basso contributo degli investimenti IT nel Sud del paese.

Il posizionamento del nostro paese nel contesto europeo è dunque ancora di relativa debolezza, soprattutto analizzando i principali indicatori stabiliti dalla Commissione Europea riguardanti i livelli di Innovazione[3]. Nella rilevazione dell'Indice di Innovazione Italia registra un netto miglioramento di posizione: dalla 13esima nel 2001 alla 11esima nel 2003.

Posizionamento Italia nei paesi UE Summary Innovation Index 2003



Fonte: European Innovation Scoreboard, 2003

Sebbene le performance dell'Italia rispetto all'Europa siano migliorate negli ultimi anni, grazie alle politiche governative per il sostegno alla domanda nel settore della pubblica amministrazione, nelle imprese e agli incentivi all'utilizzo della banda larga, esse continuano ad essere condizionate dai forti vincoli allo sviluppo determinati soprattutto dal ritardo del Mezzogiorno.

I risultati sono facilmente confrontabili attraverso gli indicatori stabiliti dalla Commissione Europea per eEurope 2005, al fine di verificare lo stato d'avanzamento della società dell'informazione[4].

Tabella 1 Posizionamento dell'Italia nella classifica europeo rispetto ai 10 indicatori prioritari di sviluppo della Società dell'Informazione – eEurope 2005

AREA	INDICATORE	2001	2002	2003
Accesso cittadini a Internet e utilizzazione	% Popolazione che utilizza internet in ambiente domestico	11	13	8
Accesso delle imprese alle TIC e loro utilizzazione	% di imprese che hanno accesso a internet	11	11	10
	% del fatturato e-commerce sul fatturato delle imprese		10	10
Servizi e-Government Basic	Numero di servizi pubblici di base completamente disponibili on-line	12	9	
	%di utenti internet che visitano siti della Pa	11	11	
e-learning	Numero di PC collegati a Internet per 100 studenti	13	13	
e-health	% di Medici Generici che ha un accesso ad internet o network medico	5	5	
	% di Medici Generici che utilizza referti medici elettronici sui pazienti	9	8	
Penetrazione banda Larga	Connessioni Broadband attive		6	4
	Penetrazione broadband su popolazione residente			12

Fonte: Analisi Innovazione Italia su dati Eurostat, Eito, Eurobarometer, Commissione Europea

---

[2] Fonte Eurostat 2004

[3] European Innovation Scoreboard 2003 presso http://trendchart.cordis.lu/scoreboard2003/index.html

[4] Risoluzione del Consiglio 18 febbraio 2003 Attuazione del piano d'azione eEurope 2005 (2003/C 48/02)

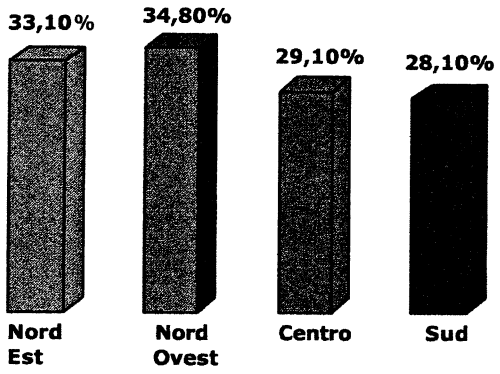
1.2 Il Mezzogiorno: principali vincoli per l'eliminazione del digital divide

L'analisi del panorama nazionale permette di evidenziare il "Digital divide" tra nord e sud del paese e la necessità di avviare politiche di intervento a sostegno della domanda e degli investimenti infrastrutturali nei territori a ritardo di sviluppo. Nei paragrafi successivi evidenziamo tale diversità di utilizzo per categorie socio economiche e per aree geografiche.

a) **I CITTADINI**

Secondo i dati diffusi dal Censis, gli utenti internet in Italia nel 2003 sono 14 milioni, pari al 32 % della popolazione, con una crescita nel triennio 2000-2003 del 49%; proprio in riferimento al 2003 i dati relativi alle aree geografiche, evidenziano una netta differenziazione tra nord (nord-ovest 34,8%, nord est 33,1%) e Sud (in particolare, centro 29,1% e sud 28,1%), con un differenziale di quasi 7 punti percentuali.

Penetrazione di Internet nella popolazione per macroregioni - 2003



Fonte: Censis

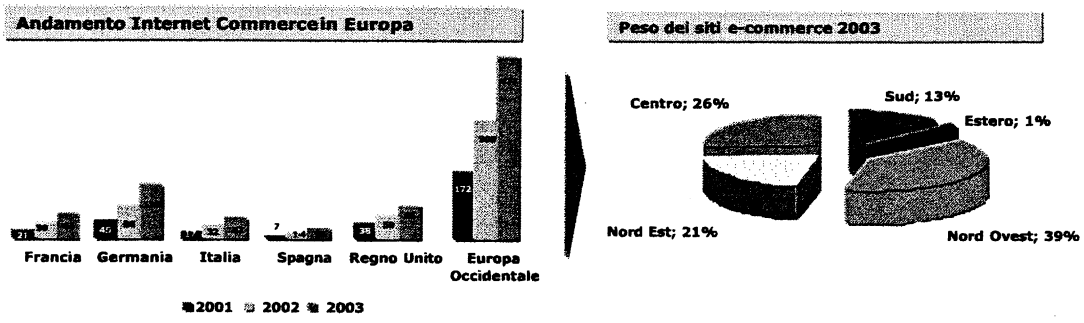
Dati più recenti[5] riferiti al contesto nazionale, indicano che oggi quasi 27 milioni (pari al 47% della popolazione) hanno accesso a Internet da casa . Il 56% delle famiglie italiane dispone di un PC domestico , valore in linea con quelli di altri Paesi dell'Europa centrale, ma abbastanza lontano dal grado di penetrazione del PC nelle famiglie del nord Europa (ad esempio la Svezia ha una penetrazione di PC nelle famiglie pari al 72%). Di tutti i PC domestici, l'81% è collegato a Internet , mentre le famiglie con accesso a Internet, sul totale delle famiglie italiane, è pari a circa 42% , con un incremento del 10% negli ultimi dodici mesi. Quello italiano è il secondo tasso di crescita in Europa, dopo il 13% della Germania. L'Italia si pone dopo Svezia (circa 64%), UK (45%) e Germania (44%), con un potenziale di sviluppo ancora ampio. Le famiglie con collegamento ad Internet, per il 33% sono collegate in banda larga.

---

[5] Federcomin, Dipartimento per l'Innovazione e le Tecnologie, 2004.

b) **IL SISTEMA IMPRENDITORIALE**

Nel 2003 la diffusione di internet all'interno delle imprese italiane si attesta su livelli elevati ma non ancora in linea con la media europea: 83%[6] delle imprese con più di 9 addetti accede a internet. Nell'ultimo triennio dello stesso anno il nostro Paese è cresciuto a ritmi più elevati rispetto alla media europea (26% rispetto al 20%). I ricavi derivanti dall'Internet Commerce (circa 52 Miliardi di € nel 2003) sono cresciuti del 202% rispetto ad una media UE che si attesta sul 178%.



Fonte: Elaborazioni Innovazione Italia su dati EITO, Anee

Nonostante tassi di crescita importanti, in una recente analisi dell'Osservatorio sul Commercio Elettronico Anee[7], viene in evidenza una minor presenza di siti e-commerce nel sud del paese.

Tra i principali ostacoli alla diffusione delle tecnologie digitali all'interno del sistema imprenditoriale italiano c'è il basso livello di alfabetizzazione informatica e la diffidenza delle imprese, in genere medio piccole, nella diffusione di informazioni sensibili on line pena la perdita di autonomia e competività[8].

Nel Sud un ulteriore elemento ostativo alla capacità di investire nell'IT, è costituito dalla bassa propensione all'innovazione delle imprese. Nel 2000 **solo il 16% delle imprese del Mezzogiorno risultano essere innovative rispetto al nord est che si attesta al 24%[9].**

Il nostro sistema economico, a differenza del resto delle economie occidentali, attraverso i distretti industriali trova elementi endemici nella cultura della "rete". Dei circa **140 distretti** e specializzazioni presenti in Italia, **solo 21 sono collocati al sud** e sono prevalentemente nel settore Tessile Abbigliamento.

---

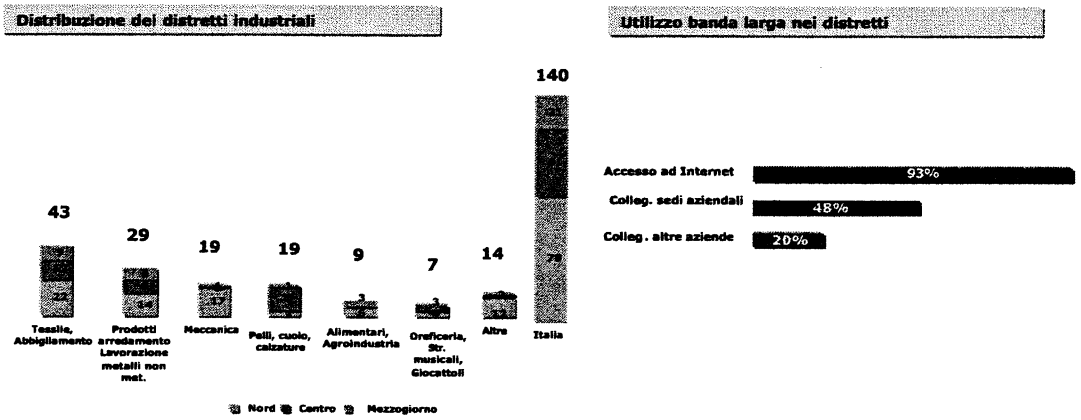
[6] Eurostat

[7] Osservatorio Infocommerce Anee/Assinform 2004

[8] Si vedano i risultati dell'analisi RUR – Censis sui Distretti produttivi digitali 2003

[9] Istat Indicatori di attività innovativa per ripartizione territoriale, periodo 1998 – 2000.

Recenti analisi territoriali[10] sulla diffusione **della banda larga** hanno evidenziato che il 93% delle imprese dei distretti industriali accedono ad internet (10% in più rispetto alla media delle imprese nazionali), evidenziando una maggiore propensione all'utilizzo delle tecnologie IT.



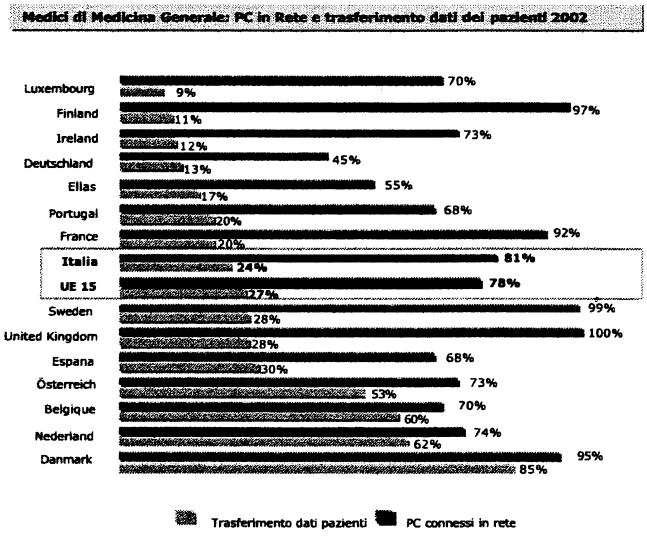
Fonte: Elaborazioni Innovazione Italia su dati IPI, Regione Veneto, Osservatorio Banda Larga

Solo il 20% delle aziende distrettuali tuttavia utilizza la rete per il collegamento ad altre imprese. Risulta quindi necessario avviare politiche di sviluppo e di incentivazione alla diffusione delle cultura dell'innovazione digitale al fine di colmare gli evidenti ostacoli che inibiscono l'innovazione del sistema imprenditoriale e quello dei distretti industriali nel sud del paese.

[10] Osservatorio Between settembre 2003

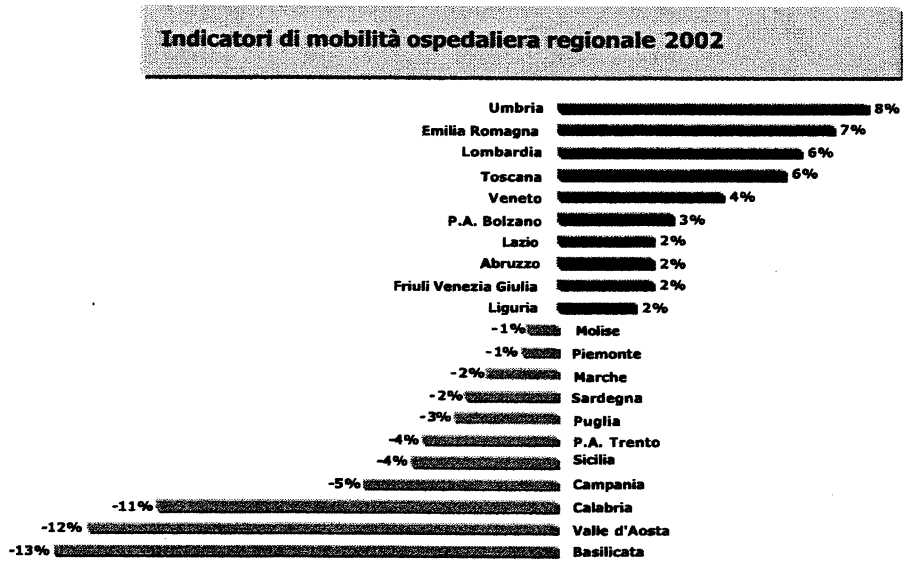
c) I Sistemi Socio - Sanitari Locali

Nonostante l'Italia registri valori esattamente in linea con la media europea nella diffusione dei personal computer tra i Medici di Medicina Generale e nell'utilizzo di internet per il trasferimento dei dati sui pazienti, l'erogazione di servizi sanitari on line verso i cittadini e tra i diversi attori dei sistemi socio sanitari locali è ancora poco diffusa.



Fonte: Elaborazioni Innovazione Italia su dati Eurobarometer 126

L'ostacolo principale allo sviluppo di servizi socio - sanitari in rete è determinato dalla forte disomogeneità (le c.d. isole) dei sistemi informativi presenti presso i diversi attori preposti all'erogazione di servizi socio sanitari. Ancora pochi i casi di front office transattivi (come ad esempio i CUP on line integrati a livello regionale), diffusa a macchia di leopardo l'integrazione degli attori socio sanitari nell'ottica della continuità della cura e della costruzione dell'Electronic Health Record[11] (Lombardia, Veneto, Emilia Romagna, Friuli Venezia Giulia, ...), sporadici o di recente realizzazione le reti di telemedicina e di teleconsulto per la diffusione delle eccellenze (come ad esempio la rete per le patologie oncologiche realizzata da Alleanze contro il Cancro[12]).



Fonte: Elaborazioni Innovazione Italia su dati SDO 2002 Ministero della Salute

Il divario tra nord e sud del paese risulta ancora più evidente analizzando i dati sulla mobilità ospedaliera. Le regioni del sud sono quelle con i più alti tassi di fuga verso le regioni del nord[13]. L'innalzamento

[11] Storia Clinica del Paziente

[12] Progetto finanziato dal Comitato del Consiglio dei Ministri per la Società dell'Informazione, marzo 2003

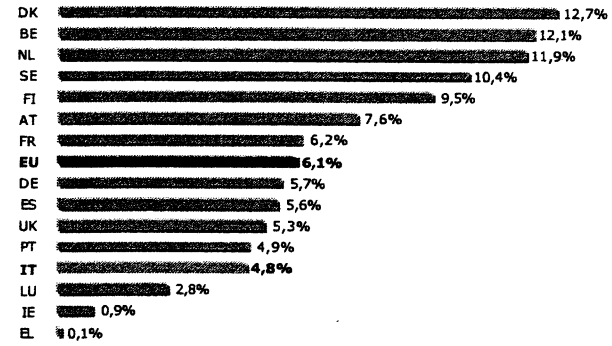
[13] I dati comprendono: che comprendono: Ricoveri per acuti in regime ordinario, Ricoveri per acuti in Day Hospital, Ricoveri riabilitazione in regime ordinario, Ricoveri riabilitazione in Day Hospital, Ricoveri in lungo degenza,

del livello di digitalizzazione delle informazioni sanitarie e l'estensione su tutto il territorio nazionale di servizi diagnostici assistenziali dei Centri di eccellenza e di Alta Specializzazione può garantire a tutti i cittadini, in particolare a quelli residenti nel Mezzogiorno e nelle Isole, prestazioni sanitarie di qualità omogenea ed allineate agli standard di eccellenza.

d) FACILITÀ DI ACCESSO AI SERVIZI

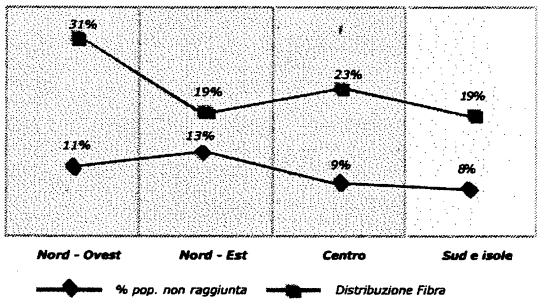
Lo sviluppo della Banda Larga è stato in Italia molto forte, tanto che, nel corso del 2003, il tasso di crescita è stato uno dei più alti dell'Unione con un incremento del 135% negli accessi, grazie agli incentivi pubblici e ad un'offerta sempre più competitiva, sia per quanto riguarda le tariffe che la tipologia dei nuovi servizi.

Penetrazione della Banda Larga in EU (% sulla popolazione)



Communication Commitee EC, gennaio 2004

Digital Divide Italia 2003



Osservatorio Banda Larga, 2004

La disponibilità dei servizi di banda larga è piuttosto omogenea nel territorio nazionale[14]; esistono tuttavia ancora delle zone buie rappresentate soprattutto dai piccoli centri urbani in zone disagiate. I gap infrastrutturali sono al centro delle recenti politiche governative che mirano a colmare i divari esistenti (si vedano le azioni relative alle infrastrutture in Banda Larga nel sud, tra le quali la realizzazione dei Servizi di Pubblica Connettività e la realizzazione di infrastrutture locali attraverso la neo costituita Infratel[15]).

I divario tra nord e sud risiede soprattutto nella fruizione di servizi su banda larga. Sono necessari interventi che permettano ai cittadini e alle imprese di accedere ai servizi con facilità e disponibilità continua.

---

[14] Osservatorio Banda Larga Between

[15] Delibera CIPE 17/2003 che prevede la realizzazione di infrastrutture in banda larga attraverso la società Infratel S.p.A. nata da Sviluppo Italia S.p.A. e Ministero delle Comunicazioni.

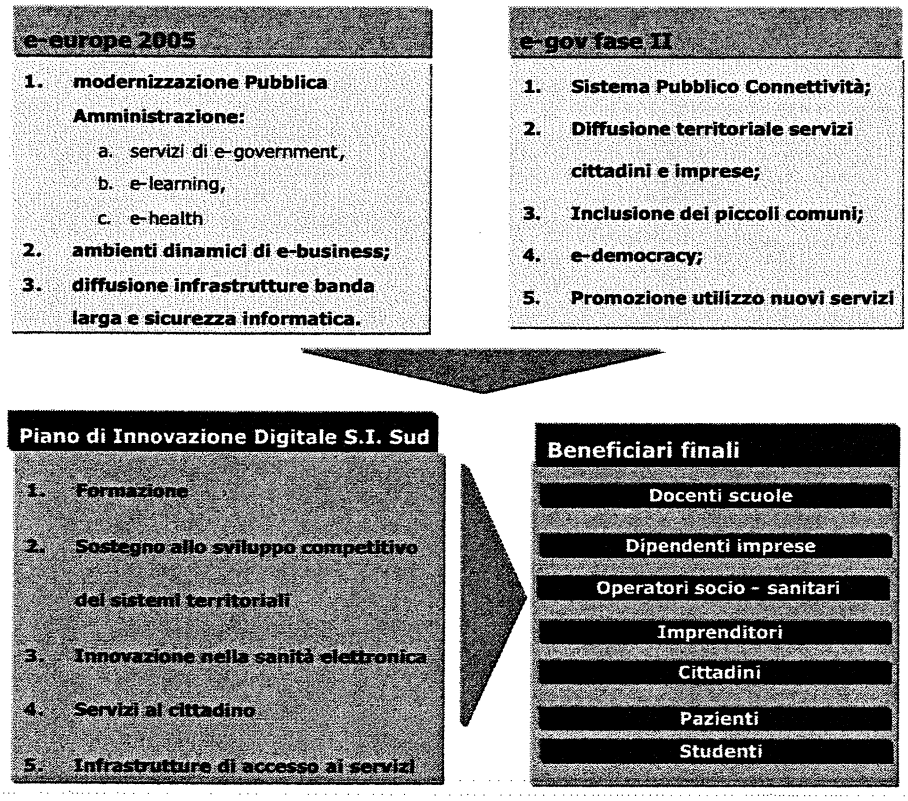
2. Il Piano di Innovazione per la diffusione della Società dell'Informazione nel Mezzogiorno

2.1 La strategia complessiva

In occasione del Consiglio europeo di Lisbona del marzo 2000 è stato definito dalla Commissione Europea, quale obiettivo strategico per il prossimo decennio, la costituzione di una "più competitiva e dinamica economia basata sulla conoscenza nel mondo, al fine di assicurare una crescita economica sostenibile, maggiori e migliori posti di lavoro ed una maggiore coesione sociale". Il piano "eEurope 2005" inoltre, pone come obiettivo la possibilità per tutti, cittadini e imprese, di partecipare alla Società dell'Informazione, promuovendo servizi, applicazioni e contenuti sicuri, basati su infrastrutture di telecomunicazioni accessibili all'intera comunità. Le relative linee d'azione per il 2005 mirano a sostenere:

1. la *modernizzazione della Pubblica Amministrazione* attraverso lo sviluppo dei servizi di e-government, di e-learning, di e-health,
2. lo *sviluppo dei sistemi competitivi* attraverso ambienti dinamici di e-business;
3. la *diffusione delle infrastrutture di banda larga* e della sicurezza informatica.

Dall'analisi dei divari territoriali evidenziati nel capitolo precedente e in rispondenza con le azioni previste dal piano europeo, le iniziative lanciate dal Piano di eGovernment I e II Fase e dai Piani Regionali per la Società dell'Informazione, abbiamo promosso un Piano di Innovazione per la diffusione della Società dell'Informazione nel Sud che prevede 5 linee d'azione che possono essere correlate attivando un circolo virtuoso.



Il territorio di riferimento è costituito dalle **Regioni Obiettivo 1 e le Regioni Abruzzo e Molise.**

Il presente Piano di Innovazione prevede uno stanziamento complessivo di circa **500 Milioni di €**[16]. Le modalità di attuazione prevedono un cofinanziamento dei progetti da parte delle Amministrazioni Regionali per la realizzazione, l'avviamento e la gestione. I progetti saranno realizzati sulla base degli Accordi di Programma Quadro tra il MIT e le amministrazioni regionali. Nella tabella 2 è riportata la ripartizione[17] delle risorse tra gli interventi del presente Piano, descritti nel seguito.

Tabella 2 Quadro economico del Piano

Iniziative per il Sud	Importi in MEURO
Formazione e sviluppo di contenuti digitali nel sistema scolastico	25,9
Formazione nel sistema sanitario locale	22,7
Piano integrato per formare la società nel Sud	12
PMI - sostegno allo sviluppo dei sistemi competitivi tradizionali	133
Sostegno alla creazione di nuove imprese nei settori High Tech	100
Innovazione digitale nei SSL – Telemedicina	4,3
Innovazione digitale nei SSL - Medici di medicina generale	25,8
Servizi ai cittadini - Numero Unico per le emergenze	9,7
Servizi ai cittadini - Sistemi avanzati per la connettività sociale	30
Infrastrutture di accesso – CAPSDA	22,4
Infrastrutture di accesso - Centri di Servizio Territoriali	26,5
Centri territoriali per l'aggregazione dei sistemi di acquisto	8,5
I servizi informativi integrati per la gestione del territorio	26
Ampliamento del sistema pubblico di connettività	26
Ponte digitale nell'area dello Stretto di Messina	4
Integrazione dell'e-gov regionale e centrale nelle regioni del Meridione – IRE-SUD	19
Totale per il SUD	**495,8**

Tutti gli interventi previsti rispondono ad una serie di requisiti fondamentali:

- sostenibilità economica nel lungo periodo;
- possibilità di riuso delle soluzioni previste;
- stimolo all'uso di connessioni in banda larga.

---

[16] Nel totale sono ricompresi anche i 10 milioni di € relativi alla sperimentazione dello scrutinio elettronico, che interessa l'intero territorio nazionale (cfr. pgf. 7).

[17] La Formazione nel sistema imprenditoriale (rif. pgf. 3.3) è una linea di intervento trasversale rispetto ai progetti ricadenti nell'ambito del sostegno allo sviluppo dei sistemi competitivi nel Sud, per cui l'ammontare delle risorse finanziarie è ricompresso nei singoli piani finanziari di tali progetti.

È stata esplicitamente evitata la polverizzazione finanziaria degli investimenti in modo da garantire la rapidità di intervento. La logica seguita ha l'obiettivo di determinare risultati concreti nel breve-medio periodo. Risultati che possano poi essere replicabili anche in altri territori.

2.2 Il modello di governance e il sistema degli attori coinvolti

Il framework degli interventi strategici è il frutto del lavoro cooperativo avviato dal Ministro dell'Innovazione e le Tecnologie con le Amministrazioni Centrali e Locali.

Il modello di governance avviato dal MIT permetterà di condividere progettualità e risultati tra i diversi territori del Sud, mettendo in comune le esigenze e le esperienze. Con tali finalità saranno attivati tavoli di lavoro specifici con gli attori coinvolti nei settori di riferimento (imprese, operatori sanitari, scuole, etc.). Di seguito sono sintetizzate le macro attività relative alla progettazione condivisa con i gli attori territoriali.

Sistema di governance del Piano di Innovazione Digitale nel Sud

1. Definizione del quadro di intervento strategico per il SUD	MIT		
2. Pianificazione finanziaria	MIT, MEF		
3. Definizione delle linee di intervento	MIT		
4. Definizione interventi regionali e centrali		MIT, MEF, MIUR, Tavolo Regioni, Innovazione Italia	
5. Accordi Programma Quadro Regioni		MIT, MEF, Regioni	
6. Progettazione modelli di intervento e architetturali di riferimento		MIT, Innovazione Italia, altri, altri attori di settore	
7. Progettazione e realizzazione degli interventi sul territorio			MIT, Innovazione Italia, Regioni, MIUR
8. Assistenza e comunicazione		MIT, Innovazione Italia	MIT, Innovazione Italia
9. Monitoraggio		MIT, Innovazione Italia	MIT, Innovazione Italia

Il rapporto di collaborazione avviato con le amministrazioni regionali ha reso possibile il coordinamento strategico delle iniziative centrali con quelle locali. Le amministrazioni sono state coinvolte negli studi di prefattibilità con l'esplicita finalità di renderle pienamente partecipi.

La maggior parte degli interventi, infatti, prevede un output locale e un ruolo fondamentale delle amministrazioni regionali. La formalizzazione della progettualità e la sua impostazione finanziaria è in fase avanzata di definizione attraverso lo strumento degli Accordi di Programma Quadro (APQ).

Gli APQ, siglati dal MIT con ogni singola amministrazione, riportano sia le specifiche degli interventi centrali con evidenza della definizione dei ruoli, sia le iniziative locali a supporto di tali interventi.

3. Formazione e sviluppo di contenuti digitali nel sistema economico e sociale del Sud

Gli interventi nell'ambito della formazione riguardano 4 principali categorie di beneficiari: *i docenti delle scuole, gli operatori sanitari, i cittadini e le imprese.*

3.1 La formazione e sviluppo di contenuti digitali nel sistema scolastico del sud

La diffusione delle conoscenze e l'estensione dell'uso della tecnologie all'interno dei percorsi didattici sono elementi fondamentali per l'attuazione della Società dell'Informazione. A tale fine il Dipartimento dell'Innovazione, di concerto con il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) e con i referenti della Società dell'Informazione delle Amministrazioni Regionali, ha previsto una serie di interventi con gli obiettivi sintetizzati nello schema successivo.

Sintesi degli indirizzi strategici e dei relativi strumenti

Indirizzi strategici	Strumenti
• **Diffusione della larga banda**	• Utilizzo della larga banda come fattore abilitante la distribuzione dei contenuti multimediali e la gestione della classe virtuale
• **Coinvolgimento degli insegnanti e promozione dell'incontro fra domanda e offerta**	• Sviluppo di un **ambiente per lo scambio e l'archiviazione/ricerca** dei contenuti digitali (repository collaborativo) • **Coinvolgimento degli insegnanti** nello sviluppo dei contenuti digitali (learning object da inserire nel repository) • Supporto al processo di insegnamento attraverso la **classe virtuale** • **Formazione** degli insegnanti sulla didattica multimediale
• **Sviluppo di contenuti digitali di qualità**	• Sviluppo di **standard** pedagogico didattici, tecnici e di interoperabilità che garantiscano la qualità dei nuovi contenuti • **Riuso dei contenuti già esistenti** con standardizzazione dei formati • Acquisizione di **nuovi contenuti** realizzati dall'editoria
• **Cross medialità**	• Sviluppo di contenuti veicolati attraverso una **molteplicità di strumenti** : ad es. PC, palmare, telefonino, tv digitale terrestre • Linee guida e **standard** pedagogico-didattici e di portabilità
• **e-inclusion**	• Strumenti hardware e software a supporto degli **insegnanti di sostegno**

L'intervento, della durata di circa 3 anni, prevede una attività di formazione intensiva dedicata ai docenti di tutti i livelli scolastici con incentivi alla condivisione delle conoscenze. La formazione sarà specificatamente rivolta all'uso delle tecnologie dell'informazione e della comunicazione (TIC) con applicazioni didattiche, alla gestione di dassi virtuali e all'elaborazione di contenuti per l'e-learning.

La linea d'azione prevede un finanziamento complessivo di **25,9 Milioni di €** destinanti alle Regioni Obiettivo 1 con Abruzzo e Molise. L'attuazione sarà gestita dal Dipartimento per l'Innovazione e dal MIUR che contribuirà dal finanziamento attraverso fondi PON Scuola.

3.2 La formazione nel sistema sanitario locale

Il Dipartimento dell'Innovazione, di concerto con il Ministero della Salute, con i referenti dei sistemi sanitari regionali e con i referenti regionali per la SI, ha previsto una serie di interventi che mirano a incentivare nelle regioni del sud lo sviluppo e l'utilizzo dei sistemi di *formazione a distanza* nell'ambito del programma nazionale di Educazione Continua dei Medici del Ministero della Salute.

Gli interventi riguardano:

1. la *formazione e alfabetizzazione* dei Medici di Medicina Generale e dei Pediatri di Libera Scelta nell'utilizzo dei servizi in rete;
2. la *formazione* nell'ambito dei **servizi di Telemedicina Specializzata Oncologica**;
3. la *formazione degli operatori socio sanitari* attraverso soluzioni **e-learning orientate** *all'Educazione Continua in Medicina*;
4. l'allestimento di *aule multimediali con videoconferenza* per l'erogazione della formazione a distanza.

L'obiettivo è quello di formare **circa 10.000 Medici e collegare circa 515 strutture sanitarie** presenti nel Sud del paese.

La linea d'azione prevede un finanziamento complessivo di ***22,7 Milioni di €*** destinanti alle Regioni Obiettivo 1 con Abruzzo e Molise. L'attuazione prevede il cofinanziamento regionale dei progetti per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida predefinite e attraverso gli Accordi di Programma Quadro Regionali.

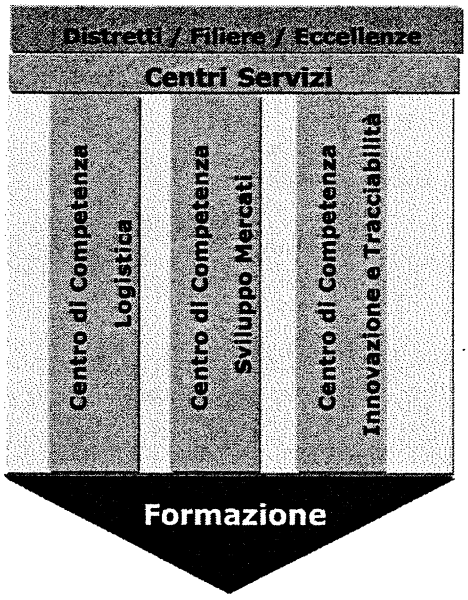
3.3 La formazione nel sistema imprenditoriale nel Sud

Le azioni di sostegno alla formazione del sistema imprenditoriale del Sud sono inserite all'interno di alcuni grandi progetti orientati:

1. allo sviluppo dell'innovazione digitale nelle filiere produttive (tessile e agroalimentare)

2. al sostegno alle Pubbliche Amministrazioni Locali nella promozione delle eccellenze territoriali e della diffusione della conoscenza (Centri Servizi Pubblici per l'accesso ai servizi della PA e per la fruizione di corsi formativi)

Sintesi degli interventi strategici di formazione per le imprese



Gli interventi di formazione alle imprese hanno l'obiettivo di creare la giusta cultura imprenditoriale all'innovazione e diffondere la conoscenza relativa agli strumenti di networking e knowledge management. Inoltre sono lo strumento abilitante per il successo delle iniziative.

In particolare i corsi di formazione, prevalentemente in modalità e-learning, saranno orientati a creare le capacità per utilizzare gli strumenti ICT per il business aziendale, non solo sotto il profilo operativo (interazioni digitali in filiera), ma anche verso l'esterno (approccio nuovi mercati, CRM, Marketing, ecc...).

La diffusione e l'utilizzo sistematico di contenuti digitali crea le condizioni di sviluppo anche delle piccole e medie imprese. Condizioni che si esplicano in una maggiore capacità di interoperabilità e comunicazione tra i sistemi informativi aziendali permettendo scambi rapidi ed efficienti di informazioni.

3.4 Un Piano integrato per formare la società del sud all'utilizzo della rete

In modo trasversale rispetto ai 4 target precedentemente descritti, il Dipartimento per l'Innovazione e le Tecnologie sta sviluppando un **Piano integrato per la formazione** che prevede un sistema di interventi, basati sui seguenti elementi:

a) gli strumenti di formazione a distanza: la TV DIGITALE, l' e-learning ;

b) l' infrastruttura: i centri d'accesso, le aule informatizzate; il sistema pubblico di connettività;

c) i contenuti/servizi.

Obiettivo generale è quello di promuovere iniziative volte a superare ogni possibile causa di "digital divide ", attraverso il coinvolgimento delle generazioni più giovani, l'alfabetizzazione informatica diffusa e la riqualificazione professionale orientata alla creazione di nuove figure lavorative con competenze multidisciplinari.

Il piano è articolato in azioni come segue:

AZIONI	TARGET
Divulgazione e promozione delle conoscenze circa le potenzialità offerte dalle nuove tecnologie per migliorare la produzione e l'accesso ai servizi (pubblici e privati) e favorire l'interazione tra le diverse componenti sociali	Tutte le categorie
Alfabetizzazione informatica di base – progettazione e realizzazione di attività educative finalizzate ad imparare ad usare il computer e internet, e ad utilizzarli attraverso specifici percorsi formativi per ampliare competenze tecniche e tecnologiche.	Scuola - Cittadini
Riqualificazione diffusa delle competenze per lo sviluppo di nuove professionalità correlate con l'utilizzo dei nuovi strumenti informatici	Imprese - Sanità PAL
Formazione informatica specialistica per garantire la disponibilità di nuove figure professionali con competenze specialistiche nel settore della organizzazione aziendale, della progettazione e costruzione di servizi b-web e applicazioni di e-business	Imprese (PMI)
Ulteriori iniziative a supporto della diffusione tecnologica – attraverso la creazione di Università per la terza età, convenzioni per l'acquisizione di PC per le famiglie, decoder e set top box per centri anziani	Cittadini

Il Piano sarà gestito attraverso un'azione coordinata MIT, MEF e regioni; il finanziamento ammonta a **12 milioni di euro**.

4. Il sostegno allo sviluppo dei sistemi competitivi nel Sud

Le politiche di intervento a sostegno dei **sistemi imprenditoriali locali**, dei distretti industriali e delle filiere produttive, possono essere sintetizzate in due macro linee di intervento:

1. *Sostegno allo sviluppo delle imprese che operano nei settori tradizionali*
2. *Sostegno alla creazione di nuove imprese che operano nei settori High tech*

4.1 Le azioni di sostegno allo sviluppo dei settori tradizionali

Gli interventi classificabili in questa categoria possono essere considerati azioni di sostegno allo sviluppo competitivo che mirano a incrementare la competitività delle imprese attraverso nuovi modelli organizzativi e l'innovazione di processo e di prodotto mediante l'introduzione di tecnologie digitali. Tali interventi si declinano in:

1	**SUPPORTO ALLA PROMOZIONE E ALL'INTERNAZIONALIZZAZIONE**	Insieme delle attività e dei servizi a supporto del processo di internazionalizzazione delle imprese, della promozione dei marchi e valorizzazione del "Made in Italy" attraverso l'uso delle tecnologie digitali, in particolare mediante lo sviluppo di network cooperativi e l'utilizzo di applicazioni di E-Business.
2	**SUPPORTO ALLA CREAZIONE DI RETI DI IMPRESE E DI IMPRESE A RETE**	Le azioni volte alla: • creazione di **reti** per favorire l'accesso delle imprese di distretto e di filiera ai sistemi d'integrazione digitale e all'utilizzo delle tecnologie a banda larga; • valorizzazione dei centri servizi esistenti nelle aree distrettuali e, lì dove assenti, creazione di nuove **strutture di servizio** di supporto alle imprese negli ambiti dell'innovazione di processi e prodotti, logistica, tecnologia, qualità, ricerca, promozione della cultura distrettuale, formazione;

3	**SUPPORTO AL TRASFERIMENTO TECNOLOGICO**	Insieme delle azioni volte a promuovere il trasferimento tecnologico tra il mondo universitario e le imprese, promuovendo lo sviluppo e l'innovazione tecnologica e l'eventuale nascita di nuove imprese. In tale ambito saranno creati **centri di competenza** per il trasferimento tecnologico nel Sud nelle seguenti aree: ▪ Logistica ▪ Sviluppo Mercati ▪ Innovazione e Tracciabilità Tali strutture aggregano risorse intellettuali, scientifiche e tecniche; costituiscono le interfacce fra il mondo della ricerca e quello delle imprese, affinché si rafforzino e si accelerino i processi di innovazione. Tale processo viene supportato anche attraverso il ricorso allo strumento del voucher per attività di due diligence, business evaluation, assistenza brevettuale, borse di ricerca.
4	**SUPPORTO ALLA CRESCITA DEL CAPITALE UMANO**	Le azioni mirano a promuovere: • la diffusione delle competenze e delle conoscenze nell'ambito del management dell'innovazione, • la formazione degli addetti per favorire l'uso delle nuove tecnologie.

Gli interventi a sostegno dello sviluppo dei sistemi competitivi nel Sud prevedono un finanziamento complessivo pari a circa **133 Milioni di € .** Le modalità di attuazione prevedono il cofinanziamento da parte delle Amministrazioni Regionali dei progetti per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida definite dal Dipartimento dell'Innovazione e delle Tecnologie e attraverso gli Accordi di Programma Quadro Regionali.

4.2 Lo Strumento per la creazione di nuove imprese nei settori High Tech

E' stato creato un nuovo fondo per favorire la partecipazione pubblica al capitale di rischio di imprese in settori ad alta tecnologia quali l'Information Technology, l'elettronica, le nanotecnologie e microtecnologie, gli strumenti elettromedicali, la meccanica ad alta tecnologia per automazione industriale, sia tramite partecipazione a fondi mobiliari chiusi già costituiti o da costituire, sia attraverso il sostegno diretto alle attività dei Venture Capitalists. Le finalità dello strumento sono:

1. promuovere la nascita o lo sviluppo di imprese innovative nel settore dell'alta tecnologia

2. Promuovere un mercato del capitale di rischio per investimenti su PMI o nuove imprese che per il valore dell' intervento o per tipologia del rischio non attraggono Venture Capital tradizionali

I beneficiari del fondo sono: Start-up in settori ad alta tecnologia, Venture Capitalists, Investitori Istituzionali del Mezzogiorno; le risorse stanziate ammontano a **100 milioni di euro.**

Il Fondo High Tech è costituito con risorse inizialmente provenienti dal fondo aree sottoutilizzate; le Regioni possono partecipare per finanziare investimenti localizzati nei propri territori.

5. L'innovazione digitale nei Sistemi Sanitari Locali

Il Dipartimento dell'Innovazione e le Tecnologie, di concerto con il Ministero della Salute, ha avviato un ambizioso Piano d'Innovazione Digitale nella Sanità che prevede una riorganizzazione complessiva dei sistemi informativi attuali verso architetture e ambienti aperti e cooperativi orientati alla realizzazione dell'Electronic Health Record (Storia Sanitaria del Paziente).

Al centro del nuovo modello di sanità orientata al cittadino ci sono figure fondamentali quali i Medici di Medicina Generale, i Pediatri di Libera Scelta, le strutture territoriali legate all'assistenza socio sanitaria.

Nell'ambito di un quadro di interventi complessi che si concluderà nel 2010 sono stati avviati i progetti nel Sud che prevedono le seguenti linee d'azione:

1. **la formazione**
2. **la telemedicina**
3. **l'integrazione dei medici in rete con le strutture socio sanitarie locali**

5.1 Le eccellenze oncologiche in rete con la telemedicina

Gli ambiti di applicazione della telemedicina possono essere classificati in:

Ospedale (H):	Aziende Ospedaliere, Centri di Eccellenza (IRCCS), etc.
Territorio (T):	Rete integrata di servizi sanitari e socio-sanitari
Ospedale – Territorio (H-T):	inter-relazioni tra le strutture ospedaliere ed il territorio (es. medici di famiglia, UTAP, RSA)
Ospedale – Ospedale (H-H):	interazioni tra differenti strutture ospedaliere (e.g. collegamento con i Centri di Eccellenza).

L'obiettivo principale di tale progetto è di estendere alle regioni *Calabria* e *Sardegna* i servizi diagnostici assistenziali dei Centri di eccellenza oncologici nazionali (teleconsulto specialistico e di condivisione di informazioni/competenze), in modo da garantire a tutti i cittadini prestazioni sanitarie di qualità omogenea ed allineate agli standard di eccellenza nazionale.

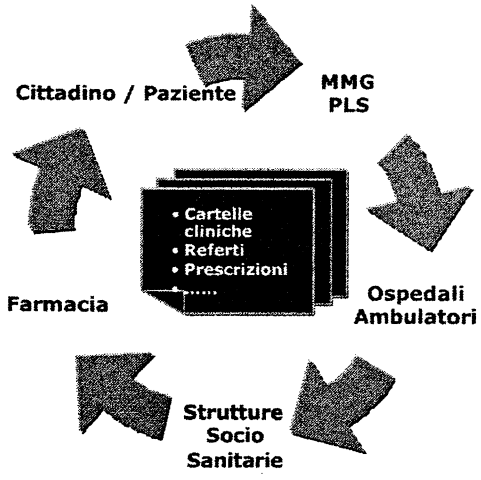
I servizi da realizzare, orientati prevalentemente all'integrazione Ospedale-Territorio ovvero Ospedale-Ospedale, consistono in delivery remoto di expertise specialistiche (teleconsulto, second opinion);

L'intervento per le sole regioni Calabria e Sicilia prevede **4,3 Milioni di €**. Le modalità di attuazione prevedono il cofinanziamento dei progetti da parte delle Amministrazioni Regionali per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida definite dal Dipartimento dell'Innovazione e delle Tecnologie e attraverso Accordi di Programma Quadro Regionali.

5.2 L'integrazione dei medici in rete con le strutture socio sanitarie locali

I Medici di Medicina Generale e i Pediatri di Libera Scelta rappresentano il punto strategico per l'accesso ai servizi di assistenza, prevenzione e cure primarie. Recenti indagini a livello internazionale hanno messo in evidenza come circa l'80% dei medici di base italiani utilizza un PC ed una connessione ad Internet, rispettando all'incirca la media del contesto europeo (82%)[18]. Risulta invece essere del tutto carente l'utilizzo degli strumenti informatici per l'integrazione in rete dei medici con il sistema sanitario locale e nazionale al fine agevolare i processi di assistenza socio sanitaria, di diagnosi e cura.

Percorso di diagnosi e cura del cittadino - paziente



[18] Flash Eurobarometro 126/2002

Gli interventi del Dipartimento dell'Innovazione, in collaborazione con il Ministero della Salute, prevedono la realizzazione di un insieme di servizi per i medici e i pediatri, in grado di consentire l'effettiva comunicazione, la condivisione delle informazioni e la cooperazione con gli altri attori del Servizio Socio Sanitario.

I servizi che saranno realizzati possono essere sintetizzati in :

1. **Servizi di cooperazione e integrazione trasversali** (data set clinici, patient file, ...) definiti in ambito centrale;

2. **Servizi e i sistemi informativi in ambito regionale** (anagrafi assistiti, soluzioni relative ai livelli di assistenza territoriale ed ospedaliero, sistemi di monitoraggio delle prescrizioni, sistemi di EHR Regionali);

L'obiettivo è la messa in rete di **10.000 Medici di Medicina Generale**

L'intervento per tutte le regioni Obiettivo 1 con Abruzzo e Molise prevede **25,8 Milioni di €**. Le modalità di attuazione prevedono il cofinanziamento dei progetti da parte delle Amministrazioni Regionali per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida definite dal Dipartimento dell'Innovazione e delle Tecnologie e attraverso gli Accordi di Programma Quadro Regionali.

6. I servizi ai cittadini

6.1 Azioni a sostegno delle categorie deboli nelle scuole (e-inclusion)

La Scuola italiana si sta progressivamente attrezzando per far fronte alle esigenze di studenti diversamente abili. In questo senso è importante agire secondo due direzioni:

a) azioni dirette agli studenti

b) azioni dirette agli insegnanti per il sostegno.

Per quanto riguarda il primo punto, saranno individuate quelle tecnologie che facilitano l'apprendimento e l'integrazione sociale acquistando le attrezzature necessarie e fornendole alle scuole.

Il corretto utilizzo di tali strumenti è affidato agli insegnanti che verranno adeguatamente preparati con corsi di formazione ad hoc.

6.2 Contenuti digitali

Un passaggio necessario nella promozione della SI del Paese prevede la diffusione di contenuti digitali di qualità a supporto della domanda di Larga Banda e servizi avanzati.

Un importante impulso in questa direzione sarà dato attraverso il progetto "Servizi avanzati nelle Scuole del Sud" tramite il quale sarà promosso l'utilizzo di contenuti digitali nei normali percorsi didattici e nei servizi di supporto all'apprendimento. L'obiettivo sostanziale al termine del ciclo di vita del progetto è quello di rendere disponibile il 50% del materiale didattico tradizionale in forma digitale.

I benefici attesi sono evidenti:

- possibilità per le famiglie di scegliere tra libri scolastici e contenuti multimediali on demand;
- possibilità per gli insegnanti di personalizzare facilmente le loro lezioni;
- maggiore disponibilità di contenuti;
- progressivo avvicinamento degli studenti alle nuove tecnologie.

6.3 Il Numero Unico delle Emergenze

Il progetto NUE 112 si propone di realizzare un **Sistema di Gestione Unificata** delle chiamate di **emergenza** (rendendo l'Italia adempiente rispetto alla specifica Direttiva Europea 2002/22/CE).
In Europa vengono effettuate ogni anno più di 40 milioni di chiamate di emergenza da telefoni mobili. Di queste 3,5 milioni forniscono notizie approssimate sulla localizzazione (p.e. i servizi di emergenza perdono tempo prezioso nell'individuare le vittime) e per 2,5 milioni non si riesce ad ottenere alcuna indicazione sulla localizzazione (p.e. non si può inviare aiuto alle vittime).

Il servizio di Numero Unico delle Emergenze prevede la realizzazione di Centri operativi di prima accoglienza con il compito di recepire tutte le chiamate di emergenza (da rete fissa e mobile) e gestire con efficienza le risposte attraverso nuove tecnologie di integrazione e innovativi modelli organizzativi.

Il nuovo sistema permetterà di:

- Semplificare il processo di richiesta d'aiuto (unico numero 112)
- Migliorare la prima assistenza online
- Offrire un servizio Automatico di Localizzazione delle Chiamate ed Identificazione del Chiamante
- Ridurre le chiamate improprie e la duplicazione degli interventi

L'introduzione del Numero Unico è a rilevante impatto sociale in quanto garantirà un sostanziale **miglioramento della gestione delle emergenze** modificando radicalmente le abitudini dei cittadini.

Per la realizzazione del progetto pilota l'importo stanziato a valere sui fondi CIPE per le regioni Obiettivo 1 è di **9,7 milioni di euro** gestiti centralmente dal Ministro per l'Innovazione e le Tecnologie.

Le province identificate per la sperimentazione sono: Catanzaro, Palermo, Salerno.

6.4 I Sistemi Avanzati per la Connettività Sociale (SAX)

Ad integrazione degli altri interventi nel Mezzogiorno, il Progetto Sistemi Avanzati di Connettività Sociale ha l'obiettivo di ridurre il digital-divide e di favorire l'utilizzo dei servizi innovativi erogati dalle Pubbliche Amministrazioni Locali e Centrali mediante azioni per la diffusione delle infrastrutture di accesso. Sono previste tre azioni integrate:

1. *concessione di un contributo alle famiglie per l'acquisto di un PC connesso ad internet e dotato di lettore di smart card* (SAX-B). E' prevista per i beneficiari la possibilità di richiedere la emissione gratuita, per sé ed eventualmente per i propri familiari, della Carta Nazionale dei Servizi. Le Regioni possono anche decidere di dare un ulteriore contributo per il conseguimento di un titolo riconosciuto a livello europeo all'abilitazione all'uso del PC e per il collegamento a Internet.

2. *concessione di un contributo a soggetti no-profit* (centri per anziani, cooperative sciali, patronati...) *per l'acquisto di PC e relative periferiche per la navigazione in Internet (SAX-P), per fruire di e-learning e del programma "Non e' m@i troppo tardi".* Saranno attrezzati locali aperti al pubblico nei quali poter navigare in Internet in modo gratuito ed assistito. Sono previste azioni formative rivolte ai tutor che assisteranno gli utenti nelle prime fasi di accesso alla rete e di utilizzo dei PC.

3. *distribuzione gratuita di 250.000 Carte Nazionali dei Servizi.* Unitamente alla CNS, per coloro i quali ne siano sprovvisti, è prevista anche la distribuzione gratuita di 200.000 lettori di smart card e del relativo software

L'intervento per tutte le regioni Obiettivo 1, compresi Abruzzo e Molise, prevede un'erogazione di **30 M€, dei quali 14,8 M€ gestiti centralmente dal** Dipartimento dell'Innovazione e delle Tecnologie **(SAX-I e monitoraggio).** Le modalità di attuazione prevedono il cofinanziamento dei progetti da parte delle Amministrazioni Regionali per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida che saranno definite dal **DIT** attraverso la concertazione con le Regioni.

6.5 La sperimentazione dello scrutinio elettronico

Il conteggio informatizzato del voto è una sperimentazione finalizzata alla valutazione dell'efficienza ed applicabilità delle tecnologie informatiche alle operazioni di scrutinio al fine di:

- semplificare e accelerare le operazioni di scrutinio
- facilitare i conteggi ed eliminare gli eventuali errori di trascrizione
- rendere più veloce e sicura la trasmissione dei risultati elettorali
- migliorare l'efficienza delle consultazioni elettorali

L'iniziativa, prevista con Legge 8 aprile 2004 n.90, art.8 (G.U. n. 84 del 9 aprile 2004), si è svolta il 12-13 giugno 2004 in occasione delle elezioni europee in **1.500 seggi elettorali** individuati con decreto del Ministro dell'Interno di concerto con il Ministro per l'Innovazione e le Tecnologie e presenti in 49 città (tutti i capoluoghi di provincia del Sud e di regione del Centro-Nord).

Per l'intervento sono stati stanziati **10 Meuro**, gestiti centralmente dal Ministro per l'Innovazione e le Tecnologie.

La sperimentazione, che si è svolta in parallelo con lo scrutinio tradizionale, ha quindi riguardato tutte quelle fasi che hanno un alto contenuto di manualità, ed in particolare le operazioni di conteggio, verbalizzazione e trasmissione dei risultati elettorali.

La sperimentazione, coerentemente agli obiettivi progettuali, ha permesso di rendere più veloce e sicura la trasmissione dei risultati elettorali e di migliorare l'efficienza delle consultazioni elettorali con riferimento alle "fasi che hanno un alto contributo di manualità". I circa **2mila pc** utilizzati nella sperimentazione sono stati dati in uso alle scuole dove si è svolto lo scrutinio.

I tempi medi di scrutinio sono stati di circa 3 ore. I dati sono pervenuti ai Centri di Servizi in media dopo 5,5 ore dalla chiusura dei seggi e non è stata avvisata alcuna problematicità in merito alle procedure di sicurezza predisposte per la trasmissione delle informazioni.

7. Le infrastrutture di accesso ai servizi

7.1 I Centri di Accesso pubblico ai servizi digitali avanzati

L'intervento prevede la disponibilità sul territorio *Punti e Centri di accesso pubblico dotati di connessioni a banda larga* fornendo nel contempo sia strumenti di accesso ai servizi della Pubblica Amministrazione che opportunità di fruizione di servizi complementari a valore aggiunto (e-learning, teleconference...) a sostegno della alfabetizzazione informatica.

I **Punti** sono delle postazioni autosufficienti dislocate sul territorio, sotto forma di chiosco informatico, dalle quali è possibile accedere ai diversi servizi della Pubblica Amministrazione centrale e locale erogati per via telematica, navigare in internet ed usufruire di alcuni servizi opzionali come la stampa della modulistica o il pagamento di imposte, utenze e simili pratiche.

I **Centri** sono delle strutture che raccolgono postazioni di lavoro dotate di connessione ad alta velocità attraverso cui è possibile accedere sia ai servizi digitali della Pubblica Amministrazione, che navigare in internet ed utilizzare una serie di servizi avanzati quali la videoconferenza, la stampa fotografica, la formazione a distanza etc., usufruendo dell'assistenza sul luogo di personale specializzato.

L'obiettivo è riduzione del digital-divide e la promozione dell'utilizzo di servizi digitali avanzati

L'intervento per tutte le regioni Obiettivo 1 con Abruzzo e Molise prevede **22,4 Milioni di €**. Le modalità di attuazione prevedono il cofinanziamento dei progetti da parte delle Amministrazioni Regionali per la realizzazione, l'avviamento e la gestione. I progetti potranno essere realizzati sulla base delle linee guida definite dal Dipartimento dell'Innovazione e delle Tecnologie e attraverso gli Accordi di Programma Quadro Regionali.

7.2 I Centri di Servizio Territoriali

L'intervento ha come obiettivo quello di garantire la maggiore copertura territoriale della diffusione dei servizi innovativi, al fine di colmare il digital divide tra i Comuni medio piccoli e le altre Amministrazioni e realizzare un efficace sistema per la diffusione ed il riuso delle soluzioni di e-government, attraverso la creazione di Centri di Servizio Territoriali (CST).

La costituzione dei CST permetterà di conseguire risultati in termini di quantità e qualità dei servizi erogati a cittadini e imprese attraverso la realizzazione di sinergie organizzative, tecnologiche ed economiche.

I CST potranno assumere un'organizzazione a matrice nella quale i processi consentiranno un agevole scambio di informazioni, una condivisione delle esperienze maturate e un supporto attivo agli Enti partecipanti.

I principali compiti dei Centri di servizio sono:

- Erogare servizi infrastrutturali agli Enti locali di riferimento
- Erogare servizi applicativi in modalità interattiva per gli Enti locali di riferimento prevalentemente realizzata grazie al riuso delle soluzioni sviluppate con i finanziamenti e-government
- Garantire la coerenza dei flussi di dati tra le Amministrazioni nel rispetto degli standard previsti dal Sistema Pubblico di Connettività
- Supportare/facilitare l'utenza (amministrazioni ed utenti finali) in ambito gestionale, normativo, amministrativo, etc.

L'obiettivo è la riduzione del digital-divide tra i comuni medio-piccoli e medio-grandi nella promozione dell'utilizzo di servizi digitali avanzati

L'intervento per tutte le regioni Obiettivo 1, Abruzzo e Molise prevede un finanziamento di **26,5 Milioni di €.** Il progetto verrà attuato attraverso la concertazione sul territorio da parte delle Amministrazioni Regionali per la realizzazione e l'avviamento dei CST. E' previsto che a regime i CST si autosostengano. I progetti saranno realizzati sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro Regionali.

7.3 Centri Territoriali per l'aggregazione dei processi di acquisto degli Enti Locali delle Regioni del Mezzogiorno

L'intervento Centri Territoriali per l'Aggregazione dei processi di acquisto degli Enti Locali delle Regioni del Mezzogiorno (CAT) ha l'obiettivo di far evolvere le attuali modalità di acquisto delle Amministrazioni regionali verso modalità innovative che prevedano un consistente ricorso all'utilizzo delle tecnologie informatiche (e-procurement).

Le principali finalità sono:

- lo sviluppo di competenze specialistiche sui processi d'acquisto innovativi a supporto delle PA;
- l'introduzione di nuove tecnologie di e-procurement;
- la razionalizzazione della spesa;
- la semplificazione delle attività e la riduzione dei tempi di accesso al mercato;
- l'apertura del mercato di fornitura al fine di favorirne lo sviluppo con particolare riferimento al mercato locale;
- l'aumento dell'offerta dei servizi innovativi per le PA.

Si prevede di realizzare l'intervento nelle seguenti regioni: Basilicata, Calabria, Puglia, Sardegna e Sicilia, con un finanziamento di **8,5 Milioni di €.** Le modalità di attuazione prevedono la concertazione sul territorio da parte delle Amministrazioni Regionali con gli altri Enti locali per la sperimentazione, la realizzazione e l'avviamento. I progetti saranno realizzati sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro Regionali.

7.4 I servizi informativi integrati per la gestione del territorio

L'intervento ha l'obiettivo di incrementare la capacità di governo amministrativo e fiscale del territorio e, più in generale, di migliorare il rapporto su tematiche ambientali e territoriali verso cittadini, professionisti ed imprese, realizzando una infrastruttura dati uniforme, secondo gli indirizzi del progetto europeo INSPIRE, in grado di valorizzare i dati territoriali prodotti dalle amministrazioni pubbliche ed agevolare, nel contempo, il riuso dei dati stessi verso soggetti esterni, anche privati, per realizzare servizi a valore aggiunto, secondo la direttiva comunitaria 2003/98/CE.

L'intervento prevede di realizzare su tutte le regioni meridionali dei Servizi Informativi Territoriali integrati , attraverso moduli di intervento tarati sulla base delle effettive esigenze delle singole regioni. I moduli previsti sono:

- Attivazione della infrastruttura di base del Centro tematico per l'integrazione dei servizi territoriali (acquisto hw, sw e strumenti specifici), come nuova realizzazione o ampliamento/integrazione di risorse già esistenti
- Progettazione e primo impianto della base dati geografica di riferimento
- Attivazione dei servizi a supporto del decentramento catastale, della pianificazione urbanistica e territoriale, a partire dal riuso, adattamento ed ampliamento dei servizi realizzati nell'ambito del progetto di e-government SIGMATER
- Sviluppo di servizi in tema di Difesa del suolo, tutela delle risorse ambientali, protezione civile e calamità naturali
- Sviluppo di servizi per il rilievo e il monitoraggio del sistema viario, sia extraurbano che urbano
- Sviluppo di applicazioni complementari e di servizio verso cittadini e imprese utilizzabili, via WEB (rilascio certificazioni, presentazione istanze, trasparenza amministrativa, conoscenza degli aspetti del territorio di interesse) su tematiche in generale afferenti il territorio.

Lo sviluppo dei servizi territoriali integrati, sostenendo la domanda di servizi specializzati che richiedono servizi di connettività a larga banda, costituisce inoltre una opportunità per tutti gli Enti locali di ottenere un'accurata conoscenza del territorio, sia a supporto delle attività tecnico-amministrative interne sia per migliorare i servizi forniti a cittadini e imprese, semplificando e rendendo trasparenti gli iter burocratici.

L'obiettivo è aumentare la capacità di governo amministrativo e fiscale del territorio e migliorare il rapporto sulle tematiche ambientali e territoriali nei confronti di cittadini, professionisti ed imprese nelle regioni del sud.

L'intervento, destinato a tutte le regioni del Sud, prevede un cofinanziamento di **26 Milioni di €**, a fronte di un cofinanziamento regionale di uguale importo complessivo, e verrà attuato attraverso la concertazione sul territorio da parte delle Amministrazioni Regionali per la realizzazione dei progetti regionali. I progetti saranno realizzati sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro regionali.

7.5 Ampliamento del Sistema Pubblico di Connettività

Lo sviluppo della società dell'informazione può essere realizzato promuovendo la disponibilità di applicazioni e servizi la cui tecnologia abilitante è costituita da reti affidabili ad alta velocità fra loro interconnesse in modo da garantire a tutta l'utenza - sia essa rappresentata dalle imprese, dalla pubblica amministrazione, dai cittadini, condizioni di facilità di accesso, di costi sostenibili e qualità elevata con l'obiettivo (i) di erogare di servizi avanzati di rete, (ii) di ridurre il digital divide mediante l'aumento di servizi di connettività a larga banda in zone periferiche e rurali, (iii) di introdurre tecnologia avanzata sul territorio e (iv) di aumentare l'offerta stimolando più imprese a offrire servizi sul territorio.

Il presente intervento rientra nel quadro di interventi atti a sostenere la domanda di servizi "a larga banda" e la diminuzione del digital divide.

I servizi previsti nell'intervento sono:

1. Diffusione di sistemi di videoconferenza di media/alta qualità sui territori regionali
   - comunicazione audio – video in tempo reale con qualità differenziata per utente/sito
   - scambio dati attraverso un insieme di applicazioni condivise
   - distribuzione di streaming audio/video ad alta qualità
   - funzioni centralizzate di regia, di prenotazione e di regolazione presso il Centro Regionale competente
   - sistema di autenticazione
   - sistema di cifratura per videoconferenza a carattere riservato
   - sistema di accounting e billing
   - sistema di stanze virtuali dedicate.

2. Adeguamento dei Centri Tecnici Regionali per il controllo e la gestione di tali tecnologie.

   Al fine di garantire il corretto funzionamento dell'intero insieme di servizi a larga banda, il progetto prevede l'ampliamento delle funzionalità dei centri tecnici regionali:
   - Funzione di regia per i servizi di videoconferenza
   - Funzione di monitoraggio dei servizi
   - Funzione di prenotazione e trasmissione di streaming video
   - Funzione di cifratura delle comunicazioni ove richiesto

- Gestione dei server per lo streaming
- Gestione della matrice di interoperabilità

3. Introduzione di servizi di rete a larga banda sicuri mediante tecnologia wireless

   La maturazione delle tecnologie wireless terrestri permette la formulazione di un intervento che preveda l'utilizzazione di tali tecnologie per la copertura delle aree regionali a più alto gap infrastrutturale. Tali tecnologie (802.11x - WiFi, 802.16x - Wimax, Navini, Hiperlan, PLC etc.) infrastrutturano il territorio con differenti range fisici per cui è ragionevole prevedere l'utilizzo di un mix tecnologico più che di un'unica tecnologia.

L'intervento di ampliamento del SPC interessa tutte le regioni del sud e prevede un cofinanziamento di **26 Milioni di €,** a fronte di un cofinanziamento regionale di uguale importo complessivo. Esso verrà attuato attraverso la concertazione sul territorio da parte delle Amministrazioni Regionali per la realizzazione degli interventi regionali. I progetti saranno realizzati sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro regionali.

7.6 Ponte digitale nell'area dello stretto di Messina

Il Progetto Ponte Digitale dell'Area dello Stretto mira alla realizzazione di una piattaforma di comunicazione diffusa sul territorio dello Stretto in grado di supportare servizi evoluti a larga banda. Inoltre, il Progetto ha l'obiettivo di creare un marchio di qualità, il MARCHIO PONTE DIGITALE, che sia garanzia di:

a) innovazione

b) eco-sostenibilità

c) qualità sociale dei sevizi offerti.

Il progetto ha una durata complessiva di 18 mesi ed è geograficamente localizzato:

- nelle aree della Provincia di Reggio Calabria e della Provincia Regionale di Messina
- nelle isole minori e le acque marittime territoriali dello Stretto di Messina.

Il finanziamento CIPE delibera N. 20/2004 relativo al progetto è pari a **4,0 Milioni di €.** Il progetto sarà realizzato sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro con le regioni Calabria e Sicilia, ove in tal senso queste decidano d'intesa con le Province interessate e col MIT. I servizi previsti dall'intervento sono elencati nel seguito.

1. Servizi di pubblica utilità

L'obiettivo è delocalizzare (sia su terraferma che durante gli spostamenti sullo Stretto) l'accesso ai seguenti servizi:

- banche dati informative (informazioni istituzionali, svolgimento di pratiche, orari di apertura al pubblico degli uffici, gli orari dei mezzi di trasporto pubblici, accesso ad atti e pratiche pubblici, vademecum per la presentazione di moduli e richieste, scadenziari, autocertificazione)
- servizi transazionali (servizi di certificazione on-line, teleprenotazioni di visite mediche specialistiche, presentazione di dichiarazioni, pagamento di bollette, imposte, tasse e tributi)
- servizi universitari (informazioni su orari e lezioni, corsi di formazione on line, lauree a distanza, eventi e seminari, patente europea del computer)

2. Servizi di supporto al turismo

L'obiettivo è migliorare la fruizione delle risorse culturali, economiche e naturali presenti nell'area dello Stretto.

- Banche di dati turistici sensibili alla posizione (informazioni culturali e non, presenti nelle immediate vicinanze del turista quali notizie relative a monumenti storici, a ristoranti tipici, a negozi con particolari offerte economiche adattate alle esigenze specifiche [lingua, interessi culturali])
- Integrazione dei servizi museali (definizione di percorsi museali comprendenti le strutture di entrambe le sponde)

3. Servizi di gestione avanzata del traffico

L'obiettivo è migliorare la gestione sia del traffico merci che dell'afflusso di turisti soprattutto durante il periodo estivo che convergono sull'area.

- Servizio di mobilità civile assistita (riconoscimento in tempo reale dell'utenza in ingresso nell'Area Metropolitana e assistenza durante il tragitto con informazioni sulle condizioni del sistema viario, sulla scelta di percorsi alternativi e sulla programmazione delle soste)

- Servizio di mobilità assistita alle flotte commerciali di terra (riconoscimento dei TIR in movimento verso il sistema di navigazione e assistenza nella prenotazione dinamica dei traghetti)

4. Telelavoro

Altro elemento qualificante del progetto, è la realizzazione di servizi per l'incentivazione del lavoro e della formazione professionale con iniziative di:

- formazione a distanza
- informa giovani on line
- spin off universitari
- realizzazione di un parco tecnologico

5. Comunicazione multimediale interattiva

Le forme di comunicazione previste dall'intervento sono:

- apprendimento e formazione
- distribuzione di eventi a distanza
- assistenza on-line

6. Marchio di qualità

L'idea del progetto è quella di ideare un marchio del ponte che certifichi l'innovatività dei servizi a cui è assegnato. La creazione di tale marchio prevede un lavoro preliminare, distinto in due fasi, per l'individuazione dei requisiti per la certificazione e del processo per ottenerla.

7.7 Integrazione dell'e-government regionale e centrale nelle regioni del Meridione (IRE-SUD)

La digitalizzazione della Pubblica Amministrazione sul territorio non può svilupparsi completamente senza il coinvolgimento degli uffici periferici delle Pubbliche Amministrazioni centrali, realizzando l'interoperabilità e l'integrazione tra i loro sistemi informativi e quelli delle Autonomie locali. Senza la partecipazione degli uffici periferici delle PAC (oltre 2.500 sul territorio nazionale, di cui circa 1000 nel Mezzogiorno, afferenti alle aree della giustizia, della sicurezza, della scuola, della fiscalità, del lavoro ecc., c 'è il rischio che le azioni innovative delle amministrazioni locali, previste nella prima e soprattutto nella seconda fase del programma di e-government, possano raggiungere solo parzialmente gli obiettivi finali previsti, incidendo pesantemente sulla percezione dei risultati positivi dell'innovazione.

L'obiettivo dell'intervento è quindi l'assicurazione della piena partecipazione all'e-government delle amministrazioni centrali dislocate sul territorio

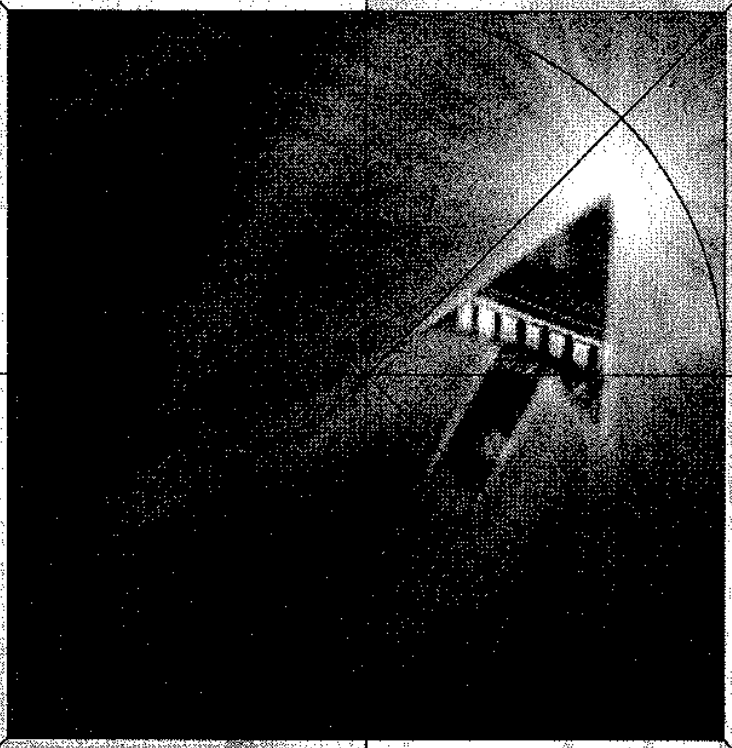
Il progetto proposto vuole favorire questa partecipazione attraverso:

- il sostegno all'accelerazione della informatizzazione degli uffici periferici della PAC, dotando gli uffici periferici che non ne avessero ancora la disponibilità, delle necessarie infrastrutture informatiche di base e sostenendo la digitalizzazione di dati e documenti;
- l'assicurazione della interoperabilità dei sistemi, attraverso l'interscambio informativo tra le Autonomie Locali e gli uffici periferici delle PAC e l'accesso, in sicurezza, alle rispettive basi di dati, quando necessarie alle attività istituzionalei;
- la realizzazione di sistemi tematici integrati, che acquisiscano ed integrino le informazione detenute da tutti i soggetti pubblici rispetto ad un determinato territorio. Tali sistemi, che potranno inizialmente riguardare i temi della sicurezza, dell'ambiente, dello sviluppo economico, dei beni culturali., forniranno supporto alle attiivtà operative, alla definizione delle politiche sul territorio, alla promozione dei territori;
- la formazione di base e specialistica, legata all'interoperabilità e all'integrazione.

Il progetto dovrà poi garantire la governance del percorso innovativo.

L'intervento coinvolge Abruzzo, Molise, Campania, Puglia, Calabria, Basilicata, Sicilia e Sardegna e prevede un cofinanziamento di **19 Milioni di €** nell'arco temporale 2005-2007. La progettazione esecutiva sarà assicurata da Gruppi di Lavoro integrati fra regioni ed amministrazioni centrali coinvolte, con compiti sia di project management e monitoraggio che opererà a supporto del soggetto attuatore (vincitore dell'appalto). I progetti saranno realizzati sulla base delle linee guida definite dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione ed attraverso gli Accordi di Programma Quadro regionali.

II PIANO PER L'INNOVAZIONE DIGITALE NELLE IMPRESE

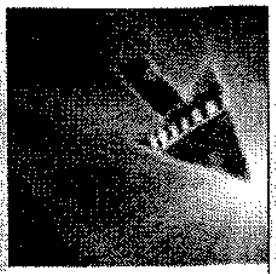


MINISTRO DELLE ATTIVITÀ PRODUTTIVE

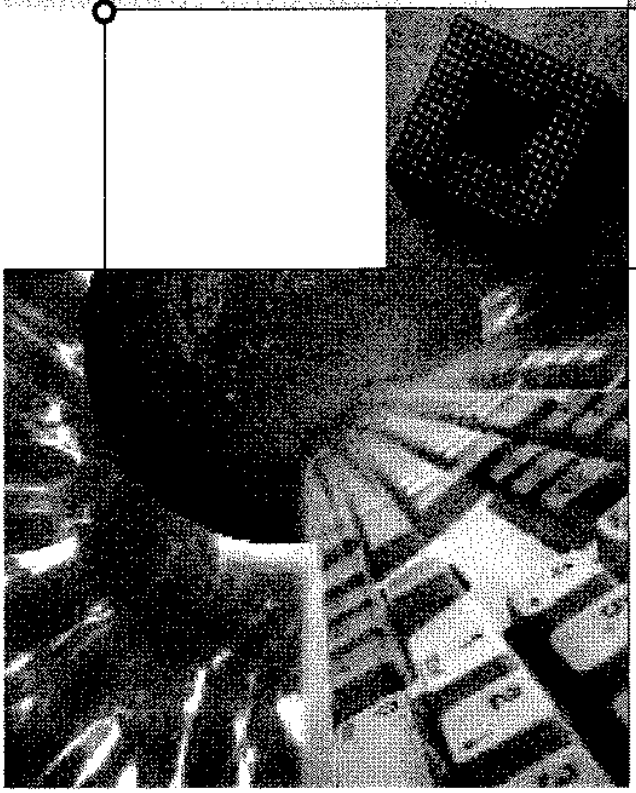
MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

GENNAIO 2005

INDICE



LA SFIDA DIGITALE: IL PIANO PER L'INNOVAZIONE DIGITALE NELLE IMPRESE 2005



A d oltre un anno di distanza dal lancio del **Piano per l'Innovazione Digitale nelle imprese** (Luglio 2003), il Ministro delle Attività Produttive e il Ministro per l'Innovazione e le Tecnologie presentano il Piano 2005, nella rinnovata convinzione che le tecnologie dell'informazione e della comunicazione possano apportare un contributo fondamentale al processo di innovazione, e dunque alla competitività, del sistema produttivo del nostro Paese.

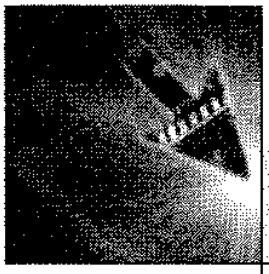
Il Piano 2005 parte da un'attenta valutazione dei risultati ottenuti con il Piano precedente e da un'analisi dello stato dell'arte della diffusione delle tecnologie dell'informazione e della comunicazione nel nostro tessuto produttivo, per giungere all'individuazione delle opportunità e degli spazi offerti dall'innovazione digitale alle imprese italiane in termini di crescita e di sviluppo.

Il nuovo Piano conferma la scelta operata nel 2003 di preferire un approccio concreto, fatto di strumenti, tempi e modalità di intervento a breve e medio termine. L'altro aspetto qualificante del Piano consiste nel riproporre un uso integrato di strumenti d'intervento di diversa natura (finanziaria, normativa e regolamentare, organizzativa e settoriale).

Infine, viene riconfermata la volontà dei due Ministeri di fare squadra e di continuare a lavorare insieme per vincere la sfida digitale che il Piano 2005 lancia anche agli altri Ministeri e alle Regioni affinché tutti i livelli di governo possano insieme partecipare alla costruzione di politiche coordinate in materia di innovazione digitale.

Il Ministro
delle Attività Produttive
Antonio Marzano

Il Ministro
per l'Innovazione e le Tecnologie
Lucio Stanca



IL RUOLO DELL'INFORMATION TECHNOLOGY NEL PROCESSO DI INNOVAZIONE DELLE IMPRESE

A partire dagli anni Novanta, le tecnologie dell'**informazione** hanno registrato progressi tecnologici paragonabili a quelli derivanti dall'introduzione dell'energia elettrica nel secolo scorso: l'evoluzione dell'Information Technology presenta le medesime caratteristiche di **discontinuità tecnologica** in un orizzonte temporale più breve.

Il Personal Computer ha offerto ad un numero crescente di utenti la possibilità di usufruire e di elaborare una quantità sempre maggiore di dati ed informazioni. La creazione delle prime reti locali e la successiva nascita di Internet hanno reso possibile forme di comunicazione e di collaborazione sempre più efficienti come la pubblicazione e la condivisione di informazioni, con un impatto notevole sul **sistema di relazioni sociali, sul sistema economico e su quello politico.**

Maggiore velocità di elaborazione e di trasferimento dei dati, aumentate capacità di archiviazione, collaborazione applicativa, il nuovo canale/mezzo di comunicazione rappresentato da Internet: tutto ciò ha reso **l'Information Technology** uno strumento a supporto delle **imprese di ogni settore** offrendo la possibilità:

- di riorganizzare un numero sempre più importante di attività all'interno delle aziende stesse, attraverso l'automazione e l'integrazione di diverse funzioni;
- di nuove configurazioni della catena del valore delle imprese, determinando cambiamenti sostanziali in diversi settori.

Per questa ragione si è resa indispensabile una vera e propria politica per l'innovazione. Nell'ambito di questa, le tecnologie dell'informazione e della comunicazione rappresentano una priorità rispetto a tre direttrici distinte.

● L'INFORMATION TECHNOLOGY E LE TELECOMUNICAZIONI RAPPRESENTANO SETTORI TRAINANTI DELLE MODERNE ECONOMIE

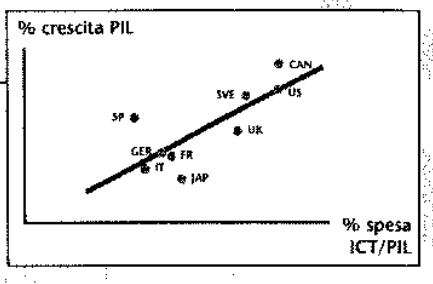
I **settori dell'Information Technology e delle Telecomunicazioni** rappresentano il 7%[1] dell'economia mondiale: sono settori ad alto valore aggiunto che hanno avuto tassi di crescita superiori al 10% negli anni novanta, contribuendo in modo rilevante allo sviluppo dell'economia mondiale. I paesi che hanno mostrato di saper meglio approfittare del progresso tecnologico in questi settori hanno registrato importanti tassi di crescita del prodotto interno lordo.

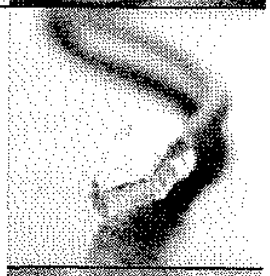
● LE TECNOLOGIE DIGITALI SONO CARATTERIZZATE DA UN ELEVATO GRADO DI INTEGRABILITÀ CON ALTRE TECNOLOGIE

Le tecnologie digitali di base (componentistica, nanotecnologia, microtecnologia, software, tecnologie wireless, fotonica/optoelettronica, sensoristica, telecomunicazioni) hanno un ruolo abilitante e dalla loro combinazione nascono continuamente nuovi prodotti e servizi. È il caso delle **tecnologie digitali degli apparati e dei sistemi**, caratterizzate da un elevato grado di integrazione con altre tecnologie di tipo tradi-

ICT e CRESCITA delle ECONOMIE MODERNE

- Contributo ICT alla crescita del PIL (Italia 95-01): 0,40% su una crescita di 1,98%
- Contributo ICT alla crescita della produttività del lavoro (Italia 95-01): 0,50% su una crescita di 1,13%
- Vi è diretta correlazione tra spesa ICT e crescita del PIL (economie dei principali Paesi OCSE – periodo 1992-01)

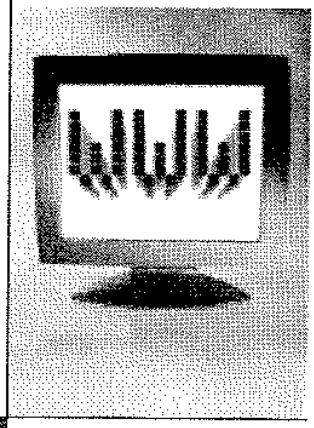




zionale, anche molto diverse fra loro. È evidente che nella definizione delle linee di intervento è opportuno tener conto non solo dello sviluppo delle tecnologie digitali di base nei settori "core" delle loro applicazioni (IT e TLC), ma anche **della loro crescente penetrazione in settori in cui rappresentano il collante tra le tecnologie di base o di sistema tradizionali e sono indispensabili alla crescita del settore stesso** come nei casi della **Domotica**, dell'**Impiantistica**, della **Meccatronica**, degli **Elettrodomestici**, dell'**Elettromeccanica**, del **Telerilevamento**, solo per citarne alcuni.

● L'INFORMATION TECHNOLOGY È UNO STRUMENTO AL SERVIZIO DELLE ORGANIZZAZIONI AZIENDALI, CON POTENZIALITÀ DI CRESCITA DELLA PRODUTTIVITÀ RILEVANTI

Diversi studi hanno dimostrato che **investire in Information Technology comporta un aumento di produttività a condizione che si proceda ad una contemporanea organizzazione dell'azienda e delle risorse umane**. In particolare, un recente studio[2] ha evidenziato una correlazione positiva fra investimenti in IT e produttività a livello aziendale.

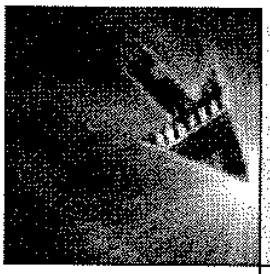


Dall'analisi approfondita di oltre 1.100 aziende statunitensi è emerso che i risultati migliori in termini di produttività si hanno dove l'investimento in Information Technology è inserito in un **insieme organico di investimenti e business practices**, definiti **"Organizzazione Digitale"**, che comprende:

- automazione di numerose attività di routine
- personale altamente qualificato
- processo decisionale più decentralizzato
- miglior flusso informativo sia verticale sia orizzontale
- maggiori incentivi legati alle performance
- maggiore enfasi nella formazione e nel reclutamento

L'investimento in Information Technology deve essere considerato un fattore di competitività che si inserisce nel più ampio insieme di investimenti sopradescritti, e rappresenta, **nei casi di maggior successo, circa il 10% dell'investimento totale** se si considera l'insieme degli investimenti sostenuti dalle aziende relativamente alle risorse umane, alla formazione, ai processi e all'intera organizzazione che rappresentano il 75% del totale.

[1]Fonte Assinform/Netconsulting su dati FMI e WTO
[2]Computing Productivity: Firm-Level Evidence, Erik Brynjolfsson and Lorin M. Hitt, Center for ebusiness at MIT, June 2003.



LA DIFFUSIONE DELL'INNOVAZIONE DIGITALE IN ITALIA

La sensibilità verso l'innovazione digitale in Italia va ancora sostenuta e incoraggiata.

Il **mercato italiano dell'Information Technology** ha registrato, nel 2003, un fatturato di circa 19 miliardi di euro[3], pari all'1,96% del PIL, a fronte di una media europea del 3,1%. Nelle economie più avanzate (Stati Uniti, Gran Bretagna, Francia e Germania), il settore IT rappresenta da un minimo del 3,1% ad un massimo di 4,6% del PIL.

La crescita degli anni '90 è stata guidata prevalentemente da fattori contingenti (internet boom, millennium bug, introduzione euro) piuttosto che dall'emergere di una forte domanda di soluzioni per l'impresa.

Le ragioni alla base delle difficoltà del settore sono riconducibili prioritariamente alla riduzione del livello di investimenti in Information Technology delle imprese italiane, per motivazioni di diversa natura.

Il **settore bancario-assicurativo e quello delle telecomunicazioni** – settori trainanti la crescita della fine degli anni Novanta – hanno registrato un calo sensibile dovuto principalmente al consolidamento degli investimenti realizzati ed alla scomparsa di importanti aziende, in particolare nel comparto delle telecomunicazioni.

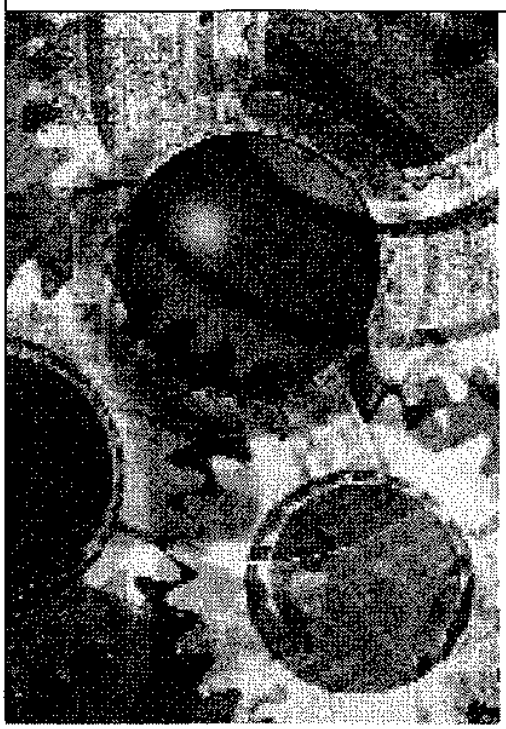
È comunque in questi settori, e soprattutto in quello delle Telecomunicazioni, che le tecnologie dell'informazione e della comunicazione hanno mostrato a pieno il loro impatto innovativo.

L'Italia è un paese all'avanguardia nel campo delle telecomunicazioni, soprattutto relativamente ai servizi di telefonia mobile. Un settore che si è segnalato all'attenzione mondiale per l'introduzione di importanti innovazioni tecnologiche, prima fra tutte le **linee telefoniche prepagate**, che hanno contribuito enormemente alla diffusione della telefonia mobile nel nostro Paese. È il settore in cui la diffusione delle tecnologie digitali, in relazione alle caratteristiche strutturali e tecnologiche che gli sono proprie, ha avuto un duplice impatto in termini di tecnologia digitale di sistema e di soluzioni gestionali al servizio dell'organizzazione aziendale.

Il settore in cui si evidenziano le maggiori criticità è quello dell'Industria manifatturiera in merito agli investimenti delle piccole imprese.

Dal 1991 al 2003 la domanda del comparto industriale ha conosciuto un sostanziale ridimensionamento in termini relativi, passando dal 31% al 23% dell'intero mercato IT. In aggiunta, nel biennio 2002-2003 la contrazione degli investimenti delle aziende industriali è stata maggiore di quella del mercato.

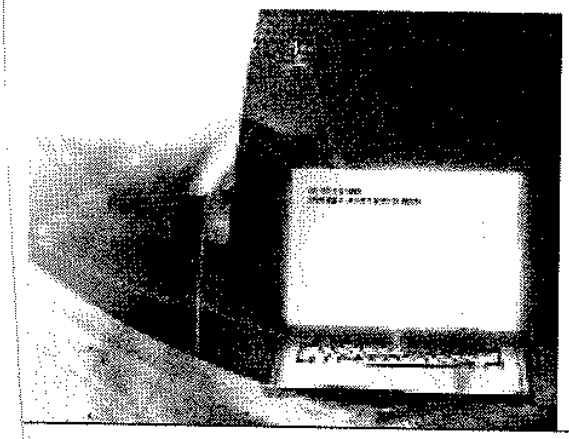
In particolare, nel 2003 gli unici settori che evidenziano un incremento degli investimenti sono quelli



[3] *Dati Assinform/Netconsulting.*

dei **servizi** (+1,5), della **grande distribuzione** (+1,3%) e soprattutto della **Pubblica Amministrazione Locale** (+2,2%), che ha beneficiato dell'avvio di importanti progetti di e-government su scala territoriale. La Pubblica Amministrazione Centrale (-2,2%) risente notevolmente dei vincoli di bilancio dello Stato e dei conseguenti tagli alla spesa.

A fronte di una domanda con le caratteristiche appena



illustrate, il settore italiano dell'Information Technology ha conosciuto nel corso degli ultimi due anni una fase di stallo. Nel 2003, il valore dell'intero mercato è stato stimato pari a 19.396 milioni di euro, di cui circa 5.073 nel segmento Hardware, 945 nell'Assistenza tecnica, 13.378 nel Software e Servizi.

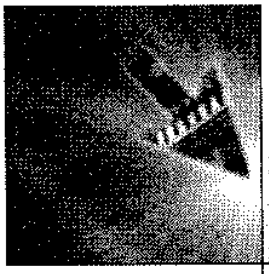
Relativamente all'**Hardware**, a fronte di un calo del fatturato del 5,6%, i dati relativi ai volumi di mercato evidenziano un costante incremento delle unità vendute, con particolare riferimento ai personal computer (+9,8%), trainati dalla diffusione dei portatili. La contrazione della domanda ha portato ad una riduzione generalizzata dei prezzi e delle tariffe anche nel comparto **servizi,** nel quale tutti i sottocomparti registrano un calo rispetto al 2002, ad eccezione dei servizi di *outsourcing* e *facility management*. Il **software** è l'unico comparto a mostrare una crescita (2,2%), sostenuta principalmente dal middleware (+2,4%) e dal software applicativo (+2,4%).

La contrazione della spesa in *Information Technology* contribuisce a rendere particolarmente problematico il posizionamento competitivo delle piccole e medie imprese, in particolare **nei settori del Made in Italy**. In questi settori solo una quota limitata di piccole e medie imprese particolarmente qualificate ha saputo intraprendere nel corso dell'ultimo decennio un processo di investimenti coerente con la sfida competitiva di un'economia globale. La maggior parte delle PMI italiane ha utilizzato le nuove tecnologie in modo limitato, senza ripensare i propri processi aziendali alla luce delle nuove opportunità offerte dall'Information Technology.

Il ritardo accumulato dalle piccole e medie imprese in questo ambito, costituisce **un limite rilevante al rilancio della competitività del Paese nel suo complesso**. Nel breve e medio periodo, la PMI italiana è chiamata ad affrontare relazioni commerciali sempre più complesse a causa dell'allargamento geografico dei canali di vendita e di approvvigionamento e dovrà ridefinire le tradizionali modalità di accesso al credito (accordi Basilea 2). Queste trasformazioni mostreranno, con ancora maggiore evidenza, i limiti della dotazione tecnologica attualmente disponibile e delle competenze in campo informatico effettivamente maturate a livello organizzativo.

In conclusione, le principali motivazioni del ritardo del settore sono:

1. il boom degli anni '90 caratterizzato da fattori congiunturali ed episodici che hanno portato a significativi investimenti ora in fase di consolidamento.
2. La struttura imprenditoriale caratterizzata da PMI poco sensibili a questo tipo di investimenti.
3. I settori trainanti del made in Italy per lo più collocati in produzioni tradizionali.
4. Una ancora lenta implementazione del settore dei servizi.



Il Piano per l'Innovazione Digitale nelle imprese 2005

GLI OBIETTIVI DEL PIANO

Partendo dalle criticità, il Piano propone un'evoluzione delle politiche per l'innovazione digitale volta a:

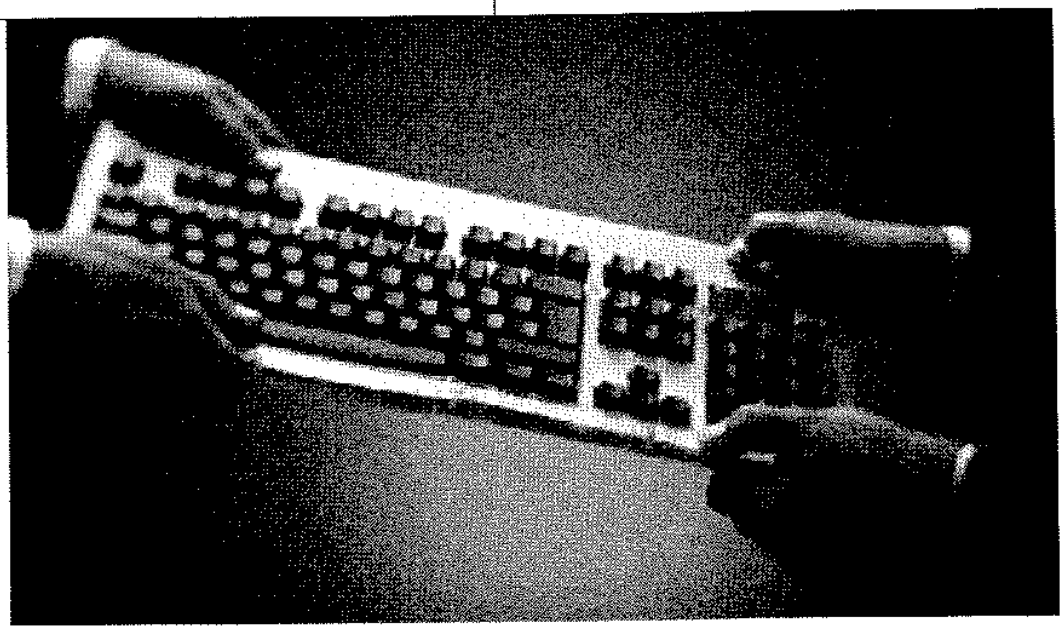
1. **favorire l'utilizzo diffuso di soluzioni applicative innovative a supporto delle organizzazioni aziendali in tutti i settori dell'economia**, ed in particolar modo nelle **piccole e medie imprese** dei **settori tradizionali**;
2. sostenere lo **sviluppo di settori a medio-alta e ad alta tecnologia**, mediante il finanziamento di **programmi di ricerca e sviluppo volti all'integrazione delle tecnologie digitali in nuovi prodotti, servizi e processi produttivi**;
3. sostenere **lo sviluppo e la riqualificazione del settore dell'Information Technology**, al fine di facilitare l'incontro fra domanda ed offerta nei settori, negli ambiti e nei segmenti del mercato illustrati ai punti precedenti.

Relativamente al primo obiettivo, la strategia delineata rientra nell'ambito più generale delle azioni a sostegno alle PMI manifatturiere dei settori tradizionali del c.d. Made in Italy.

È ormai evidente che il vecchio paradigma della competitività italiana in questi settori – contiguità tra meccanica e produzione in settori tradizionali, piccola dimensione e localizzazione in distretti, prezzi competitivi anche grazie a politiche monetarie a favore dell'export – è tramontato a seguito della crescita delle economie asiatiche e dell'introduzione della moneta unica a livello europeo. L'apertura ai mercati internazionali e le nuove sfide competitive rendono necessario un **riposizionamento competitivo** del nostro sistema produttivo verso modelli di business capaci di competere a livello globale: modelli di business più complessi che sfruttino il know-how ed il vantaggio competitivo maturato dal nostro Paese in questi settori.

In questo processo, l'Information Technology costituisce un fattore abilitante per le nuove strategie della moderna impresa. L'offerta IT deve poter valorizzare le caratteristiche vincenti del nostro sistema produttivo, consentendo la transizione verso **un nuovo paradigma competitivo** fondato sia su fattori storicamente vincenti – quali il supporto tecnologico del settore della meccanica, la localizzazione in distretti industriali e l'appeal del design e dei marchi – sia su innovativi modelli organizzativi.

Il secondo obiettivo del Piano fa riferimento a quei settori ad alta e medio alta tecnologia in cui l'Information Techno-



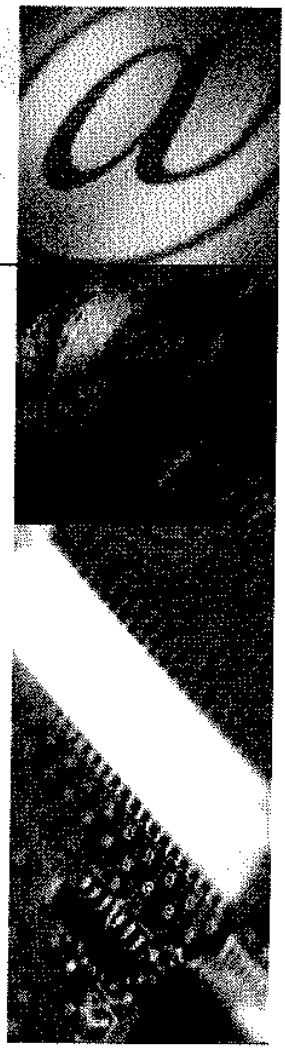
logy è maggiormente diffusa in quanto tecnologia digitale di sistema. Nei settori della Domotica, Impiantistica, Meccatronica, Elettrodomestici, Elettromeccanica e Telerilevamento, **l'Information Technology rappresenta un fattore abilitante a livello di tecnologia incorporata in prodotti, servizi e processi aziendali**. Pertanto, il modello di innovazione che il Governo intende promuovere in questi settori è prevalentemente di tipo architetturale e radicale.

Lo **sviluppo del settore dell'Information Technology,** terzo obiettivo del Piano, rappresenta il presupposto fondamentale affinché le tecnologie digitali possano diffondersi sia come strumento di supporto all'organizzazione e alla strategia dell'impresa, sia come tecnologia integrante degli apparati e dei sistemi. Occorrono interventi **mirati che facilitino l'incontro tra la domanda e l'offerta negli ambiti e nei segmenti di mercato evidenziati ai due precedenti punti** e che pongano le basi per una **riqualificazione ed un consolidamento del settore.**

LA METODOLOGIA DI INTERVENTO

Al fine di conseguire gli obiettivi delineati, il Piano prevede un mix di strumenti d'intervento per la cui definizione si è tenuto conto delle seguenti variabili:

- del **tempo** per il raggiungimento di risultati economici a medio e lungo termine;
- delle esigenze di **modelli di innovazione sostenibili** per le imprese in relazione alla loro **dimensione** ed al **settore merceologico di appartenenza**;
- delle esigenze differenziate per le **imprese localizzate nel Mezzogiorno;**
- della necessità di consentire alle **imprese una programmazione pluriennale sostenibile** degli investimenti in innovazione tecnologica;
- del **complessivo riordino del sistema degli incentivi** che tenga conto della trasformazione dei contributi a fondo perduto in contributi rimborsabili favorendo un maggior ricorso delle imprese a un debito a medio-lungo termine che sia coerente con le nuove strategie dell'impresa, ma anche con i flussi di cassa previsti dall'impresa stessa.



Il Piano propone interventi mirati per i settori del made in Italy

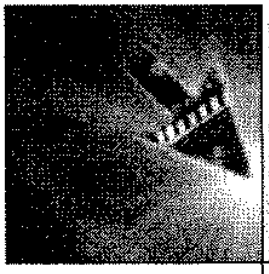
Più in particolare, nel suo approccio metodologico, il Piano propone una segmentazione degli interventi che tenga conto della marcata predominanza nella nostra struttura produttiva dei settori tradizionali del made in Italy (quali l'Agroalimentare, il Tessile, l'Abbigliamento e le Calzature, i Mobili, etc.).

Relativamente a questi settori a *medio-bassa tecnologia*, nei quali gli investimenti in ricerca e sviluppo sono in media inferiori all'1% del valore della produzione, gli interventi saranno rivolti a favorire:

- *in primo luogo*, l'innovazione organizzativa attraverso la reingegnerizzazione dei processi aziendali lungo la catena del valore mediante **investimenti in tecnologie dell'informazione (IT)** con specifico riferimento ai più evoluti applicativi gestionali ed ai servizi di consulenza aziendale.
- *In secondo luogo*, l'innovazione di processo e di prodotto basata **sull'acquisizione di tecnologie** incorporate in macchinari e impianti oppure di licenze su brevetti di altri soggetti.

Nei settori a medio-alta e alta tecnologia - che nell'ambito dell'industria manifatturiera italiana hanno un peso sensibilmente minore rispetto alla media dei primi 5 paesi dell'Unione Europea (Francia, Germania, Gran Bretagna, Italia e Spagna) e che si caratterizzano per una maggiore intensità di ricerca e sviluppo - la competitività delle aziende dipende in modo fondamentale **dalla capacità di sviluppare nuova tecnologia e di incorporarla in prodotti e processi innovativi.**

In questi settori le tipologie di **innovazione** che portano ad un reale vantaggio competitivo sono essenzialmente quelle **di prodotto e di processo.** I modelli di innovazione da perse-



guire sono prioritariamente quelli di tipo architetturale e radicale (soprattutto nei settori ad alto contenuto tecnologico). Gli interventi in questo ambito avranno l'obiettivo di **promuovere lo sviluppo precompetitivo e la ricerca industriale** in imprese di medio-grandi dimensioni su un arco temporale di medio lungo periodo.

Relativamente al primo obiettivo del Piano – diffusione di soluzioni applicative innovative a supporto delle organizzazioni aziendali in settori tradizionali, il Piano prevede – **l'attivazione di garanzie abbinate alla concessione di contributi in conto interessi.**

Per il sostegno allo sviluppo dei settori a medio-alta ed alta tecnologia mediante la diffusione di tecnologie digitali di sistema, **la metodologia d'intervento scelta è quella del finanziamento di progetti rivolti allo sviluppo precompetitivo e alla ricerca industriale.** Sono previsti inoltre interventi di carattere normativo e finanziario per facilitare i processi di trasferimento tecnologico dai Centri di Ricerca/Università e alle imprese.

L'intervento sul **settore dell'Information Technology**, soprattutto relativamente alla sua riqualificazione, sarà, anche in questo caso, basato essenzialmente sul **finanziamento di programmi di investimento in ricerca e sviluppo in ambiti ben definiti.**
Il Piano prevede, inoltre, una serie di **interventi nel Mezzogiorno** finalizzati alla **creazione di nuove imprese e allo sviluppo di eccellenze a livello locale.** Le due finalità descritte impongono un intervento più incisivo in termini di risorse stanziate. **La metodologia d'intervento sarà basata su finanziamenti a tasso agevolato.**
Gli strumenti per il perseguimento di questi obiettivi, concordemente agli orientamenti del Documento di Programmazione Economico-Finanziaria 2005-2008, prevedono il graduale abbandono del modello di intervento incentrato sugli incentivi a fondo perduto, in favore di un approccio basato sia su interventi di carattere più strutturale, volti a creare un ambiente economico favorevole ai processi innovativi ed ai flussi finanziari e tecnologici, sia su interventi diretti in settori e territori definiti.

Alla luce di ciò, le misure individuate dal Piano si ispirano alla nuova filosofia del sistema degli incentivi alle imprese che prevede:

1. il passaggio da un sistema incentrato sull'erogazione di contributi a fondo perduto ad **un sistema basato sulla cooperazione fra istituzioni finanziarie e amministrazione centrale e sull'erogazione di finanziamenti a tasso agevolato, contributi in conto interesse e garanzie sul credito;**
2. una **segmentazione e settorializzazione degli strumenti di incentivo**, che prevedranno diverse tipologie di agevolazione per misura e per natura e diversi procedimenti di istruttoria a seconda della dimensione e del settore di appartenenza dell'impresa;
3. una **maggiore flessibilità degli strumenti stessi**, prevedendo la destinazione di una parte consistente delle risorse stanziate per l'emanazione di bandi tematici, che hanno mostrato la loro efficacia nel corso del biennio 2003-2004;
4. la costante **previsione di premialità per le aggregazioni di impresa e per progetti che prevedano la collaborazione fra Università e aziende.**

Questo nuovo approccio potrà consentire di raggiungere una maggiore efficienza nell'allocazione delle risorse finanziarie pubbliche e degli istituti di credito, un risparmio in termini di risorse stanziate da parte dello Stato ed una maggiore responsabilizzazione delle imprese finanziate.

ARTICOLAZIONE DEL PIANO

Al fine di raggiungere gli obiettivi delineati, il Piano per l'Innovazione Digitale prevede un insieme organico di misure, riconducibili a 5 assi di intervento:

1. **Governance dell'Innovazione Digitale**
2. **Attuazione di misure trasversali**
3. **Interventi diretti a livello settoriale**

4 **Interventi diretti al Mezzogiorno**

5 **Interventi per il miglioramento dei servizi verso le imprese della Pubblica Amministrazione**

1. LA *GOVERNANCE* DELL'INNOVAZIONE DIGITALE

La strategia perseguita dal Piano ha come presupposto fondamentale un coordinamento tra tutti gli attori delle politiche per l'innovazione digitale nelle imprese sia a livello nazionale sia a livello regionale e locale.

Inoltre, le variabili che influenzano il potenziale innovativo di un sistema economico sono molteplici: istruzione e formazione, attività di ricerca, visione imprenditoriale, cultura del progresso. Tematiche che necessitano di un approccio strategico coerente e di una collaborazione stabile tra le Amministrazioni centrali e regionali coinvolte nei processi di innovazione delle imprese e dei territori.

A tal fine, il Ministro delle Attività Produttive ed il Ministro per l'Innovazione e le Tecnologie proporranno la costituzione di un **Comitato permanente** composto dai Ministri competenti in materia di innovazione digitale e dalle Regioni.

MISURA 1.1: COMITATO PERMANENTE PER L'INNOVAZIONE DIGITALE

Descrizione:
Costituzione di un Comitato permanente formato dai Ministri con competenze in materia di innovazione digitale e dai rappresentanti delle Regioni.

Finalità:
Il Comitato svolge un ruolo di coordinamento degli interventi a livello nazionale e regionale, per garantire una programmazione coordinata delle azioni nei diversi settori e qualificare l'offerta di servizi per l'innovazione digitale delle imprese.
Il funzionamento del comitato viene definito, con il concorso delle Regioni, attraverso un decreto interministeriale Ministero Attività Produttive – Dipartimento per l'Innovazione e le Tecnologie.

Il Piano prevede un coordinamento tra tutti gli attori delle politiche per l'Innovazione digitale

Il **Comitato permanente per l'Innovazione Digitale** sarà deputato alla concertazione a livello istituzionale in modo da mettere a fattor comune le esperienze fatte per sviluppare una visione strategica condivisa e per agire in modo sinergico e coordinato.

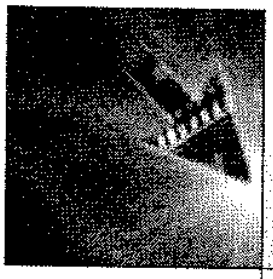
In aggiunta alla costituzione del suddetto Comitato, i Ministri proporranno l'istituzione di un **Comitato consultivo** costituito da rappresentanti delle Università, del mondo delle imprese, del sistema finanziario e delle parti sociali che svolga un'attività di supporto nella definizione degli indirizzi strategici e della programmazione degli interventi nazionali e regionali.

MISURA 1.2: COMITATO CONSULTIVO PER L'INNOVAZIONE DIGITALE

Descrizione:
Costituzione di un Comitato consultivo per l'innovazione digitale composto da rappresentanti delle Università e dei centri di ricerca, delle associazioni imprenditoriali di categoria, del sistema creditizio e finanziario e delle parti sociali. Il comitato svolge un'attività di supporto al Comitato permanente nella definizione degli indirizzi strategici e della programmazione degli interventi nazionali e regionali.

Finalità:
- analizzare gli andamenti ed i processi riguardanti l'ICT offrendo al Comitato permanente informazioni e dati per definire le proprie scelte.
- Individuare e proporre progetti e attività di sviluppo in materia di innovazione digitale.

Le modalità di funzionamento del Comitato verranno definite con apposito atto.



2. ATTUAZIONE DI MISURE TRASVERSALI

● ACCESSO AL CREDITO PER LE PMI

L'accesso alle fonti di finanziamento da parte delle piccole e medie imprese è, soprattutto nella fase iniziale della loro attività, un fattore critico per il successo dell'investimento. Come testimoniato dai numerosi studi della Commissione Europea[4], tale problematica è particolarmente sentita in tutti gli stati membri.

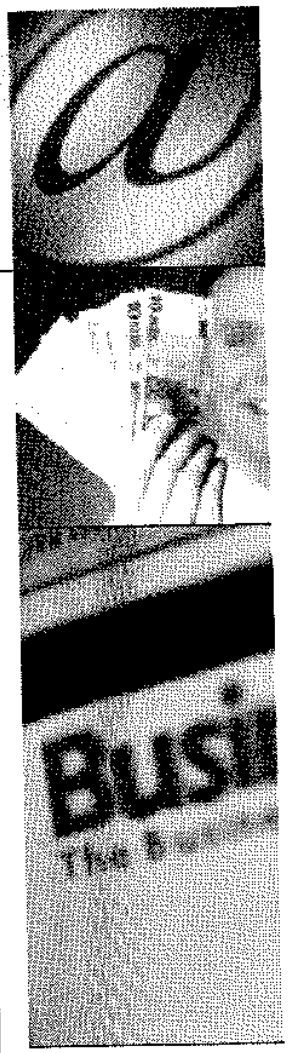
La situazione italiana presenta caratteristiche del tutto particolari rispetto agli altri stati europei, relativamente alla predominanza di piccole e micro imprese. In Italia il numero medio di addetti per impresa è pari a 3,8, il più basso tra i principali paesi europei (nel Regno Unito e in Germania sono oltre i 10 addetti). Inoltre, nella valutazione del merito di credito di un'impresa, si aggiungono considerazioni relative alla rischiosità dell'investimento. Gli investimenti in tecnologie digitali presentano livelli di rischio maggiore rispetto ad investimenti in immobilizzazioni materiali, in quanto non possono essere coperti da garanzie reali sui beni acquistati. Un maggior livello di rischio si traduce in un più alto tasso di interesse.

L'accordo di Basilea 2 e le nuove norme del sistema di contabilità internazionale IAS si sono inserite in questo contesto, aggravando la posizione delle piccole e medie imprese italiane. Dall'esame delle società di rating emerge che il 58% delle aziende italiane potrebbe avere difficoltà a superare l'esame di Basilea 2.

Nell'affrontare la questione dell'accesso al credito per il finanziamento di progetti innovativi basati sull'utilizzo di tecnologie digitali, il Piano prevede 3 misure:

- **istituzione di una sezione speciale "tecnologie digitali" del Fondo di Garanzia per le PMI;**

[4] *Access to finance of small and medium-sized enterprises, Commission communication COM(2003) 713 del 1.12.2003, Credit insurance for European SMEs: A guide to assessing the need to manage liquidity risk, ed altri.*
[5] *Misura in sede di valutazione nel provvedimento competitività per le imprese.*



- **Creazione di una società di rating per le piccole e medie imprese.**
- **un finanziamento agevolato per investimenti in innovazione digitale delle piccole e medie imprese[5]**

La costituzione della sezione speciale "tecnologie digitali" del Fondo di Garanzia per le PMI punta a realizzare l'obiettivo, più volte ribadito in ambito comunitario, di ridurre al minimo il livello di rischio associato al credito e di conseguenza il tasso di interesse passivo mediante la concessione di garanzie sul finanziamento e si inquadra nel più ampio contesto dell'integrazione fra interventi

Fra gli strumenti di intervento l'istituzione di una sezione speciale "tecnologie digitali" del Fondo di Garanzia

MISURA 2.1: ACCESSO AL CREDITO PER LE PMI

SOTTOMISURA 2.1.1: SEZIONE SPECIALE "TECNOLOGIE DIGITALI" DEL FONDO DI GARANZIA PER LE PMI

Descrizione:
Costituzione di una sezione speciale "tecnologie digitali" del Fondo di Garanzia per le PMI per programmi di investimento finalizzati all'introduzione di innovazioni di processo e di prodotto mediante l'uso di tecnologie digitali. La garanzia concessa a valere sulla sezione "tecnologie digitali" è diretta, esplicita, incondizionata e irrevocabile e copre, nei limiti dell'importo massimo garantito pari a 200.000 euro, l'ammontare dell'esposizione dei soggetti finanziatori nei confronti delle PMI.

Finalità:
- agevolare l'accesso al credito a medio lungo termine per le PMI per progetti complessi di innovazione digitale.
- Ridurre il costo complessivo del finanziamento garantito, diminuendo il livello di rischio del credito concesso dagli istituti bancari.
- favorire le aggregazioni di impresa per la creazione di reti interaziendali e metadistretti e l'integrazione di filiere produttive attraverso la ridefinizione degli interventi del Fondo Rotativo per l'Innovazione Tecnologica di cui all'articolo 14 della legge 17 febbraio 1982, n. 46. (cfr. Misura 3.2).

Beneficiari:
Piccole e medie imprese, non iscritte all'albo delle imprese artigiane e valutate economicamente e finanziariamente sane. Non sono ammissibili all'intervento le operazioni relative a PMI operanti nei settori della siderurgia, dell'industria carboniera, della costruzione navale, delle fibre sintetiche, dell'industria automobilistica, dei trasporti e dell'agricoltura.
Risorse Stanziate: 160 milioni di euro.

SOTTOMISURA 2.1.2: FINANZIAMENTO AGEVOLATO PER L'INNOVAZIONE DIGITALE DELLE PMI*

Descrizione:
L'intervento ha l'obiettivo di agevolare finanziamenti per investimenti in innovazione di processi, prodotti e servizi delle PMI attraverso l'adozione di tecnologie digitali. L'attuazione dell' intervento prevede l'utilizzo del Fondo Rotativo di cui all'articolo 1, comma 354 della legge 30 dicembre 2004, n. 311 (legge finanziaria 2005)

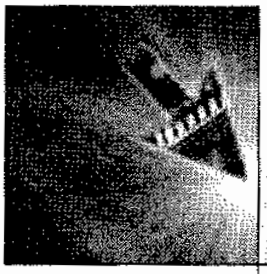
Finalità:
Riduzione dei costi di finanziamento degli investimenti in tecnologie digitali.

Beneficiari:
Piccole e medie imprese.

SOTTOMISURA 2.1.3: CREAZIONE DI UNA SOCIETÀ DI RATING PER LE PMI

Descrizione:
La misura prevede l'introduzione di parametri di valutazione qualitativi delle piccole e medie imprese operanti sul territorio nazionale.

Finalità:
- Agevolare l'accesso al credito per le PMI, in particolare per quelle innovative.

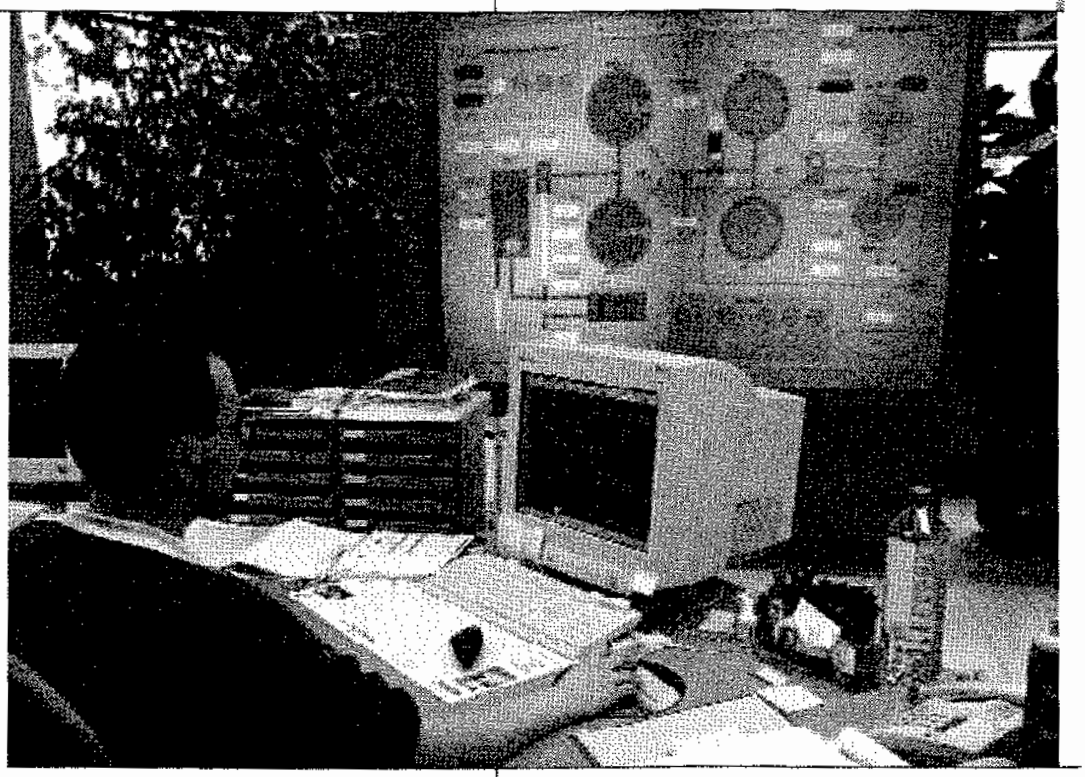


della pubblica amministrazione e istituzioni finanziarie.

La seconda misura non è di carattere finanziariario e mira proprio al tentativo di ridurre l'impatto negativo dell'accordo di Basilea 2 sul nostro sistema di piccole e medie imprese.

colo virtuoso capace di cumulare le conoscenze, moltiplicarne i frutti e sviluppare nelle Università un approccio imprenditoriale.

A tal fine l'individuazione di norme o di regole che faciliti un'azione di rete, consentendo una coesione di



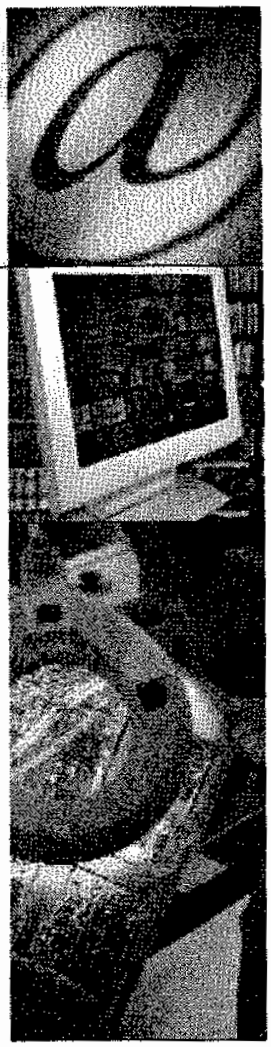
● TRASFERIMENTO TECNOLOGICO

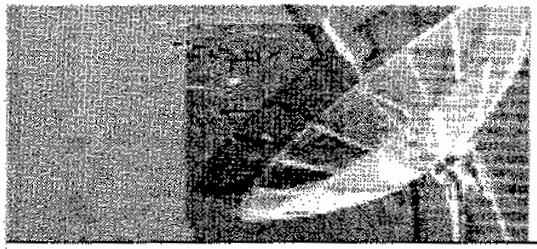
Le misure per il Trasferimento Tecnologico rappresentano l'insieme di attività strategiche che consentono di creare un collegamento tra l'attività di ricerca intesa come produzione di nuova conoscenza ed il mercato al fine di diffondere l'innovazione attraverso nuovi processi e nuovi prodotti ed essere così volano di sviluppo economico.

L'obiettivo delle misure proposte nel Piano è quello di creare un'azione sinergica tra Università, Centri di ricerca pubblici e Industria tale da innescare un circ-

interessi tra i diversi attori, è lo strumento prioritario per raggiungere tale obiettivo.

Il trasferimento della conoscenza tra il mondo della ricerca e l'industria è importante in Italia dove il 50% dell'attività di ricerca è finanziata con fondi pubblici. Per favorire il trasferimento tecnologico all'industria e creare spin out (spin off e start up) occorre agire su: il regime della proprietà, la licenza e lo sfruttamento dei diritti di proprietà industriale che derivano da attività di ricerca realizzata con fondi pubblici.





Occorre creare un'azione sinergica tra Università, Centri di ricerca e Industria

In linea generale, se si considera il ruolo delle Università, il trasferimento della conoscenza all'industria avviene partendo dalla ricerca sia mediante l'attività di formazione (nuovi laureati), sia attraverso l'attività di licensing. In Italia come in Europa il modello di scienza aperta resta ancora il più diffuso: l'Università non detiene alcun diritto di proprietà industriale e quindi non ha la necessità di gestire una politica di trasferimento tecnologico; ci sono pochi incentivi per investire in applicazioni della ricerca; non c'è un impatto diretto sull'economia perché la mancanza di tutela dell'invenzione priva le aziende del vantaggio economico derivante dallo sviluppo delle nuove idee prodotte dalle Università.

Data questa condizione di partenza, ciò che si vuole incentivare è il modello di spin off che può contribuire in modo efficace allo sviluppo e all'ammodernamento dell'economia. La tecnologia trasferita secondo un modello proprietario, ossia adeguatamente tutelata con i diritti di proprietà industriale, è usata come piattaforma per sviluppare nuove attività imprenditoriali finanziate con capi-

MISURA 2.2: DISEGNO DI LEGGE SUL TRASFERIMENTO TECNOLOGICO

Descrizione:
Elaborazione di una legge, ispirata al Bayh-Dole Act statunitense, che consenta alle Università e ai Centri di Ricerca pubblici di acquisire la titolarità dei diritti sui risultati della ricerca finanziata da fondi pubblici, a condizione che tale titolarità venga sfruttata economicamente. Le legge regolerebbe, inoltre, i rapporti fra ente di ricerca e inventore relativamente ai proventi derivanti dallo sfruttamento dell'invenzione (royalties, cessione diritti, creazione spin-off) e vincolerebbe i proventi dell'ente di ricerca/Università al finanziamento di nuovi programmi di ricerca. La nuova normativa prevede, in aggiunta, incentivi per la creazione di uffici per la gestione del trasferimento di tecnologie presso le Università con funzioni di marketing dei risultati della ricerca pubblica presso l'industria ed una priorità attribuita alle PMI italiane/comunitarie nell'assegnazione delle licenze di sfruttamento dell'invenzione.

Finalità:
- incoraggiare la brevettazione delle invenzioni "parcheggiate" nei cassetti delle Università e dei Centri di Ricerca Pubblici
- creare un circolo virtuoso ricerca – brevettazione – trasferimento tecnologico – proventi – ricerca, che realizzi un meccanismo di incentivazione ed autofinanziamento della ricerca pubblica
- consentire alle PMI di attuare strategie basate sull'innovazione tecnologica

Beneficiari:
Università, Enti Pubblici Ricerca , piccole e medie imprese.

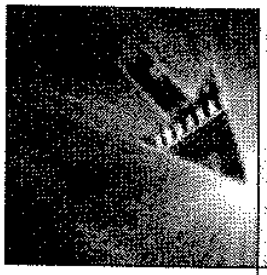
MISURA 2.3: INCUBATORI PER L'AVVIO DI IMPRESE

Descrizione:
I progetti possono riguardare una o più delle seguenti azioni:
- predisposizione di studi di fattibilità tecnica, economica e finanziaria
- realizzazione di infrastrutture, con esclusione delle opere murarie
- assistenza, anche finanziaria, alla fase organizzativa e di avvio dell'impresa
- attività di valutazione economica dei progetti
- attività di formazione per le nuove tecnologie anche con riferimento a quelle dedicate ai formatori

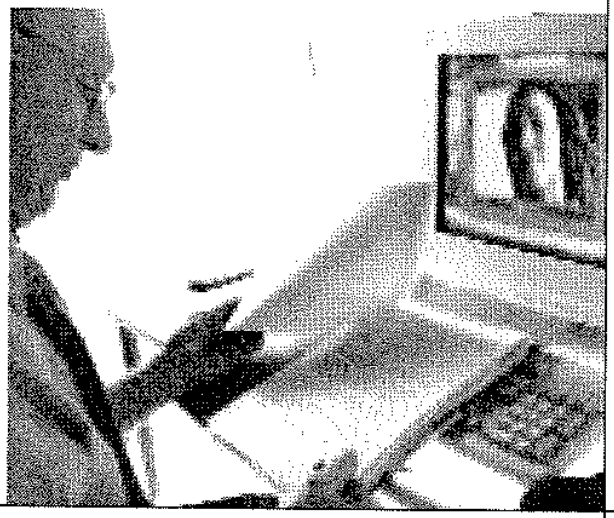
Finalità:
Fornire assistenza tecnica, formativa, consulenziale, logistica ad alto livello a nuove imprese in fase di avvio.

Beneficiari:
Università, enti di ricerca e organismi da essi promossi, e partecipati dai medesimi soggetti in misura complessiva non inferiore al 25%.

Risorse Stanziate:
Erogati fondi per un importo complessivo di contributo concesso pari a 21 milioni di euro. È previsto un ulteriore stanziamento di 22,9 milioni di euro per gli anni futuri.



tale di avviamento. È un processo già avviato in Europa che sta producendo risultati soddisfacenti ma che non funziona spontaneamente. Per questo va individuato un mix equilibrato di misure: capitale di pre-avviamento e di avviamento, incubatori, formazione degli imprenditori,



diffusione di una cultura imprenditoriale anche nel mondo della ricerca pubblica.

Le misure proposte si concentrano solo sugli aspetti normativi che riguardano la gestione dei risultati della ricerca pubblica, rinviando per la trattazione degli incentivi economico-finanziari alla parte del Piano a questi dedicata.

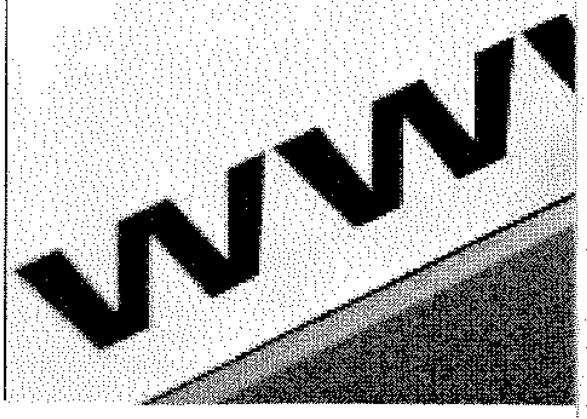
Come già evidenziato nel Piano del 2003, l'esperienza della legge statunitense Bayh-Dole rappresenta un esempio di eccellenza e best practice internazionale dell'efficacia di interventi di tipo regolamentare in materia di trasferimento tecnologico. Concedendo alle Università la titolarità delle invenzioni a condizione che vi sia uno sfruttamento economico delle stesse si mette in moto un meccanismo incentivante che:

- indirizza la Ricerca universitaria verso il mercato;
- incentiva la brevettazione;
- avvicina il mondo accademico all'impresa.

Il Piano prevede la presentazione di un disegno di **legge sul Trasferimento Tecnologico** che regolamenti il sistema appena descritto, tenendo conto delle peculiarità del nostro sistema di ricerca pubblica del quale fanno parte anche le Università. È inoltre previsto il rifinanziamento di 22,9 milioni di euro della **misura per la promozione e assistenza per l'avvio d'impresa (incubatori)** che ha prodotto buoni risultati nell'arco del 2003.

3. INTERVENTI DIRETTI A LIVELLO SETTORIALE

Il Piano intende promuovere anche azioni a sostegno del settore IT (Information Tecnology) e dei settori in cui le tecnologie digitali presentano un elevato grado di integrabilità con altre tecnologie, puntando a rilanciare la qualità dell'offerta e il suo impatto sulla domanda, in particolare rispetto al tessuto industriale della piccola e media impresa.

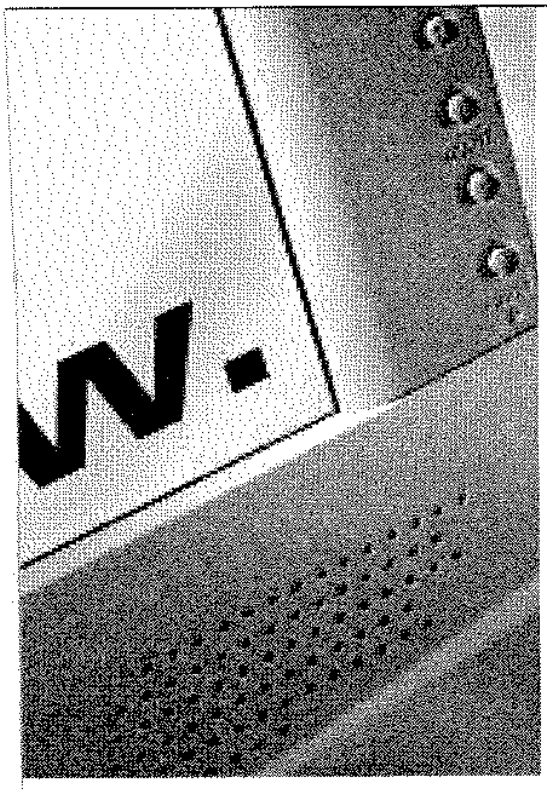


Il nostro Paese può diventare terreno di sperimentazione e di innovazione

Le difficoltà del settore IT non costituiscono un limite rispetto alla possibilità delle imprese italiane di espandersi in ambiti di attività che conosceranno in futuro importanti tassi di crescita, ma mette in discussione la possibilità del sistema industriale italiano di avere accesso a soluzioni Tecnologiche e risorse professionali coerenti con le proprie specificità. I **tratti distintivi del nostro sistema industriale devono essere riconosciuti e valorizzati dall'offerta** IT, nell'auspicio che il nostro Paese diventi terreno di sperimentazione e di innovazione per nuove infrastrutture e nuovi applicativi.

In questa prospettiva, **il Piano identifica tre ambiti di intervento che favoriscono l'incontro fra domanda e offerta di tecnologia:**

- lo sviluppo e la diffusione di applicativi *Open Source* (Misura 3.1),
- la produzione e la diffusione di servizi e contenuti digitali (Misura 3.2),
- la diffusione delle tecnologie digitali in settori ad alta e medio-alta tecnologia (Misura 3.3).

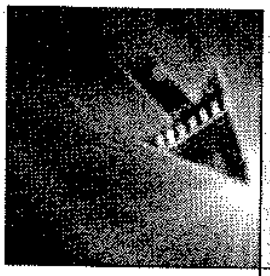


SOFTWARE OPEN SOURCE

L'organizzazione dello sviluppo di software *Open Source* basato su comunità attive in Internet prende piede all'inizio degli anni '90 sulla scia di alcune esperienze di tipo pionieristico promosse nel decennio precedente. Alla base del successo vi sono ragioni diverse: alcune sono riconducibili a fattori strettamente tecnologici ed economici quali, ad esempio, l'aumento della varietà dei collaboratori grazie alla diffusione della rete e il consolidamento di strumenti giuridici innovativi di *licensing* del software. Altre ragioni afferiscono alla sfera culturale e vanno poste in relazione a una crescente consapevolezza di nicchie di utilizzatori di tecnologia e a una richiesta, anche culturale, di autonomia e personalizzazione del software.

La diffusione di sistemi operativi *Open Source* sta conoscendo negli Stati Uniti e in Europa **una crescita costante.** I tassi di adozione si riferiscono prevalentemente a sistemi operativi lato server (Linux) e a web server (Apache). La diffusione di queste tecnologie non dipende solo dal costo di accesso limitato, ma anche dalla loro qualità e affidabilità. L'estensione delle comunità degli sviluppatori di riferimento è tale da garantire un livello di assistenza equivalente a quello fornito dalle imprese che propongono software proprietario.

Oltre ai sistemi operativi lato server, il mondo *Open Source* conosce oggi una progressiva **maturazione di progetti nell'ambito degli applicativi per il mondo delle imprese e della pubblica amministrazione.** Stanno avendo sviluppo e diffusione, in particolare, applicativi per la ge-

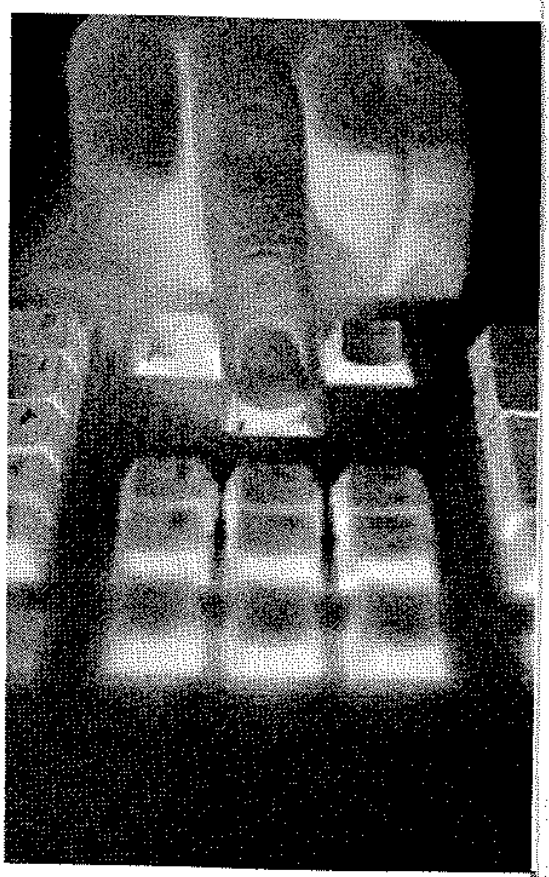


stione della posta elettronica, di *content management*, di collaborazione. Riscontrano un'attenzione crescente anche i progetti relativi allo sviluppo di piattaforme per la gestione integrata di impresa (ERP), di management della relazione con i clienti e di organizzazione della catena di fornitura. Per alcuni di questi progetti sono state avviate iniziative di localizzazione in Italia grazie all'attività di comunità di sviluppatori nel nostro Paese.

In Italia esiste **un'offerta di servizi *Open Source*** oggi in rapida crescita, formata da imprese di nuova generazione, di piccola dimensione, composte prevalentemente da giovani. Le prime ricerche condotte sull'articolazione della filiera dei servizi *Open Source* mettono in evidenza una nuova generazione di operatori di mercato, con ruoli e competenze originali rispetto alla tradizionale organizzazione del settore. I numeri, sebbene ancora limitati in valore assoluto, testimoniano una crescita importante e una domanda sempre più disponibile alla sperimentazione. Le imprese italiane più consolidate attive nel campo dei servizi stanno cominciando a valutare oggi la possibilità di entrare sul mercato sia avviando propri progetti *Open Source* a partire da codice già sviluppato internamente, sia proponendo servizi a partire da progetti già consolidati.

Il software *Open Source* ha ricevuto un'attenzione rilevante nell'ambito della **Pubblica Amministrazione**. A livello europeo, diversi paesi hanno avviato un percorso di sperimentazione puntando prima alla diffusione di sistemi operativi e poi alla crescita degli applicativi. Nel nostro Paese la *Direttiva Open Source* del Ministro per l'Innovazione e le Tecnologie ha esplicitamente previsto, relativamente alle regole ed ai criteri tecnici per l'acquisto ed anche per il riuso del software nella Pubblica amministrazione, l'inclusione di questa nuova tipologia d'offerta tra le soluzioni tecniche, ampliando la gamma delle opportunità e delle possibili soluzioni in un quadro di economicità, equilibrio, pluralismo e aperta competizione.

In considerazione della situazione del mercato IT in Italia, che non possiede grandi aziende IT basate su prodotti software proprietari e che vede le PMI servite prin-



cipalmente da aziende IT locali di piccole/medie dimensioni, il piano individua nello sviluppo dell'offerta Open Source (caratterizzata dalla prevalenza della componente servizi rispetto alla componente licenze), un fattore potenziale di:
significativo sviluppo per le aziende IT italiane;
particolare "appealing" per l'innovazione tecnologica delle PMI italiane.

Il piano intende promuovere lo sviluppo di progetti applicativi *Open Source* e la diffusione di software a codice aperto, in particolare presso la piccola e media impresa, definendo gli spazi di intervento e le tipologie di progetti di interesse nazionale per favorire l'aggregazione di imprese e di sviluppatori attorno a piattaforme consolidate.

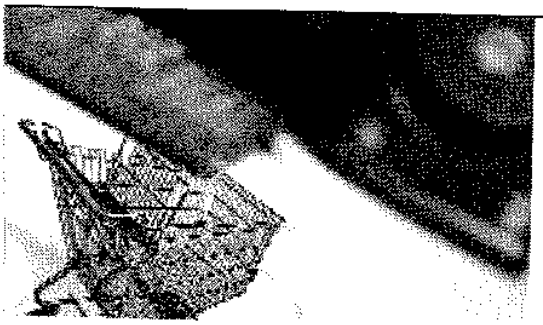
Le azioni da intraprendere nel medio termine sono volte al-

Open Source un'opportunità per le imprese IT

l'obiettivo di **rendere l'opportunità *Open Source* nota e disponibile al settore delle PMI italiane**, in particolare tramite:

- lo sviluppo dell'incontro fra domanda e offerta di servizi attraverso il sostegno di iniziative concepite a favore di filiere produttive o distretti industriali;
- il contributo alla presenza di una comunità italiana dell'*Open Source* attraverso l'incentivazione del dialogo fra mondo delle imprese e mondo della ricerca;
- il sostentamento alla nascita di nuove imprese ed al consolidamento economico e finanziario di aziende già avviate nel settore *Open Source*.

L'intervento in questo ambito (Misura 3.1) sarà attuato sia mediante strumenti consolidati, come il Fondo per l'innovazione tecnologica della legge 46/82, sia mediante la eventuale definizione di strumenti ad-hoc. Le misure intenderanno promuovere lo **sviluppo di competenze** *Open Source* da parte di software house di piccola e media dimensione, lo **sviluppo di applicativi verticali** di tipo *Open Source* per specifiche esigenze delle PMI nelle filiere del made in Italy (sistema casa e sistema moda), la qualificazione di **un'offerta di servizi** su sistemi e applicativi *Open Source* da parte di imprese già attive sul



mercato e la **nascita di nuove imprese** per l'erogazione di servizi su sistemi e applicativi *Open Source*.

● SERVIZI E CONTENUTI DIGITALI

Nel mercato dei contenuti e servizi digitali, strettamente collegato alla diffusione delle tecnologie dell'informazione e della comunicazione, vengono ricomprese diverse attività economiche, delle quali alcune hanno già assunto significativa rilevanza :

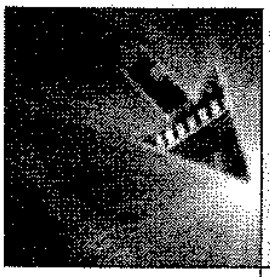
- eCommerce, nell'accezione di commercio elettronico al dettaglio
- eLearning
- contenuti e servizi per la telefonia mobile (Mobile VAS)
- Videogiochi

Nel 2003 il giro d'affari complessivo di questo mercato è stimato pari a 2.557 milioni di euro, dei quali il 57,3% è costituito dai servizi di eLearning e dal fatturato dell'eCommerce, per il 26,7% dai videogiochi per il 16% per i contenuti e servizi da mobile.

L'**eCommerce** ha chiuso il 2003 con un fatturato stimato di 1.206 milioni di euro. È un fenomeno che sembra essere finalmente decollato, con più di un milione di "e-shoppers" e una qualità dell'offerta notevolmente cresciuta nell'ultimo biennio. I settori trainanti della spesa online sono principalmente quello dei libri, dei viaggi, dei generi alimentari e dell'abbigliamento. La crescita è essenzialmente dovuta all'entrata sul mercato di importanti players unita ad una maggiore fiducia dei consumatori.

L'**eLearning** ha mostrato forti tassi di crescita nel 2003, raggiungendo un valore totale di circa 256 milioni di euro. È un mercato che segue il trend positivo degli investimenti in formazione, in costante crescita nel triennio 2001-2003, ma è stato influenzato negativamente dall'andamento dell'intero settore IT e da una domanda in contrazione.

I **videogiochi ed i servizi mobili** a valore aggiunto rappresentano due realtà in costante crescita. Il settore



dei videogiochi è stimato intorno ai 680 milioni di euro e conta su una base di consumatori in continua crescita. I tassi di diffusione delle console e dell'uso del PC per scopi ludici sono dell'ordine del 50% fra i teenagers. La categoria dei teenagers contribuisce in maniera decisiva anche alla crescita dei servizi mobili a valore aggiunto che sono stimati intorno ai 480 milioni di euro. Gli SMS contribuiscono in maniera determinante (64%), ma cresce anche l'apporto di servizi di browsing, delle suonerie polifoniche e dei giochi Java.

La **convergenza dei settori dell'Information Technology, delle telecomunicazioni e dell'elettronica di consumo** sta portando a cambiamenti rilevanti nelle modalità di fruizione dei contenuti e dei servizi: unitamente ai fenomeni già descritti in precedenza, i settori sui quali questo fenomeno si influisce maggiormente sono quelli dell'intrattenimento (TV digitale e servizi connessi, con la forte evoluzione derivante dall'avvio dei primi servizi realmente interattivi quali il *video on demand*) e della cultura (musei, biblioteche e, più in generale, beni culturali).

Di più ampio orizzonte è la cosiddetta **"rivoluzione digitale"**, ben descritta dallo slogan *"world is going digital"*, dove **la visione futura** prevede un mondo in cui una grande maggioranza delle attività umane (lavorative, di apprendimento, di utilizzo del tempo libero) saranno svolte con il **supporto di tecnologie digitali e mediante l'utilizzo di servizi e contenuti digitali**. Tale visione contempla enormi attività di digitalizzazione di contenuti esistenti, di creazione di filiere produttive digitali, di realizzazione di piattaforme per la gestione dei contenuti, dei relativi diritti e dei servizi basati sui contenuti stessi. L'opportunità è evidente, ed è probabilmente uno dei principali fenomeni evolutivi del mondo odierno, capace di supportare nascita di nuove imprese, crescita di imprese esistenti, creazione di occupazione e riconversione di forza lavoro.

Il piano intende promuovere lo sviluppo di servizi innovativi con particolare attenzione rispetto ad ambiti di atti-

vità in cui l'Italia si candida a svolgere un ruolo di leader a livello europeo e internazionale. Il piano vuole, in particolare, specificare alcuni spazi di elezione in termini di contenuti (ad esempio la valorizzazione dei beni culturali nel commercio elettronico), così come in termini di piattaforme tecnologiche di riferimento (ad es. la telefonia mobile e il digitale terrestre).

Da questo punto di vista è opportuno ricordare le attività in corso nella **Commissione Interministeriale sui Contenuti Digitali nell'era di Internet** (coordinata dal Ministro per l'Innovazione e le Tecnologie, con la partecipazione del Ministero dei Beni ed Attività Culturali, del Ministero delle Comunicazioni, del Ministro per le Politiche Comunitarie, del Ministero della Giustizia, del Ministero degli Affari Esteri e del Ministero per le Attività Produttive-Ufficio Italiano Brevetti e Marchi), avviate con l'obiettivo di condurre una approfondita analisi dello sviluppo del mercato dei contenuti digitali ai

fini di individuare, nel rispetto della normativa comunitaria, una proposta di iniziative volte a promuovere lo sviluppo della produzione e della fruizione di contenuti digitali; tali attività saranno completate entro il 28/02/2005 ed i risultati rappresenteranno uno dei principali input al piano per la definizione di azioni di ampio respiro.

La "rivoluzione digitale" può supportare la crescita delle imprese

Le azioni da intraprendere a **medio termine** sono dirette a:

- sostenere la nascita di nuove imprese nel settore a partire da competenze qualificate;
- favorire il consolidamento economico e finanziario di aziende di servizi già avviate;
- promuovere la creazione e la diffusione di standard operativi nell'ambito di servizi innovativi;
- supportare la creazione di piattaforme per lo sviluppo dei servizi basati su contenuti digitali (digitalizzazione, produzione digitale, gestione archivi contenuti e diritti digitali, erogazione contenuti su diverse piattaforme).

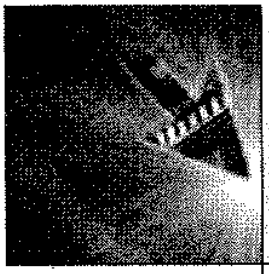
MISURA 3.2: INCENTIVI PER IL COMMERCIO ELETTRONICO

Descrizione:
Concessione di un credito di imposta ex legge 388/2000 per programmi di investimento volti alla realizzazione di soluzioni IT per lo svolgimento dell'attività di commercio elettronico, nonché al lancio dell'offerta on-line e alla formazione digitale del personale. L'assegnazione del credito d'imposta è regolata tramite bando con procedura valutativa ed è soggetta alla regola del de-minimis. L'ammontare minimo dei programmi di investimento ammissibili è pari a 30.000 euro. Sono ammissibili i costi per l'acquisto di hardware, licenze software, per l'acquisizione di servizi di consulenza, per l'acquisto di spazi pubblicitari online e per la formazione del personale. La misura del credito d'imposta è pari al 50% dei costi ammissibili.

Finalità:
- favorire il miglioramento della qualità dell'offerta on-line delle aziende attraverso la realizzazione di soluzioni avanzate per l'eCommerce.
- supportare le imprese che svolgono attività di commercio elettronico nella loro fase di lancio ricomprendendo tra i costi ammissibili anche i costi di internet advertising.

Beneficiari:
Tutte le imprese.

Risorse:
Circa 30 milioni di euro.



Nel **breve termine**, il Piano individua il commercio elettronico quale ambito prioritario di intervento. I buoni risultati ottenuti dal Bando eCommerce del 2003, i dati positivi relativi alla crescita del fenomeno (incremento di circa 70% del fatturato on-line[6] complessivo nel 2003) inducono a stanziare ulteriori risorse per il rafforzamento qualitativo dell'offerta eCommerce, mediante un nuovo credito d'imposta ex legge 388/2000. Lo scorso mese di ottobre il Ministero delle Attività Produttive ha emanato il 3° bando eCommerce con la finalità primaria di migliorare la qualità dell'offerta dell'eCommerce in Italia.

● DIFFUSIONE DELLE TECNOLOGIE DIGITALI IN SETTORI AD ALTA E MEDIO-ALTA TECNOLOGIA

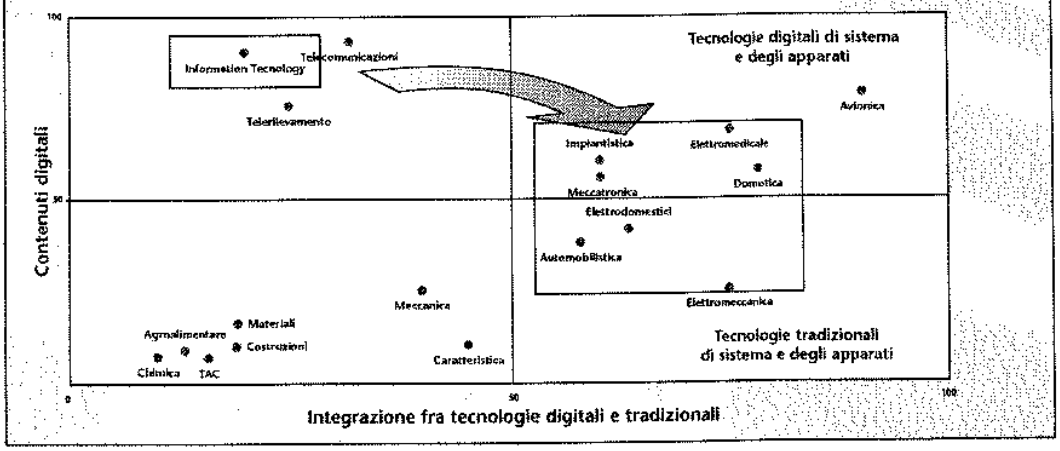
Come illustrato nell'analisi di contesto, le tecnologie digitali di base hanno un ruolo abilitante e dalla loro combinazione nascono continuamente nuovi prodotti e servizi (più o meno complessi). Si parla in questo caso di **tecnologie digitali degli apparati e dei sistemi**, caratterizzate da un elevato grado di integrazione con altre tecnologie di tipo tradizionale, anche molto diverse fra loro.

Le tecnologie digitali degli apparati e dei sistemi sono in grado di guidare l'innovazione nei settori digitali di base richiedendo spesso l'utilizzazione di tecnologie digitali di base al limite delle loro prestazioni e rendendo indispensabile l'interazione fra addetti alla ricerca e sviluppo di entrambi gli ambiti tecnologici.

Relativamente a questo ambito di intervento è prevista **l'emanazione di un bando tematico IT (Misura 3.3) a valere sul Fondo per l'Innovazione Tecnologica nei settori della Domotica, Impiantistica, Meccatronica, Elettrodomestici, Elettromeccanica, del Telerilevamento e dell'Elettromedicale.** L'esperienza recentissima del Bando ICT ha evidenziato enormi potenzialità nell'integrazione delle tecnologie digitali nei suddetti settori.

Obiettivo della politica delineata, quindi, **è quello di sostenere non solo lo sviluppo delle tecnologie digitali di base e i settori *core* delle loro applicazioni, IT e TLC, ma anche di sostenere ed indirizzare lo sviluppo di settori in cui le tecnologie digitali hanno al momento una crescente penetrazione e sono indispensabili alla crescita del settore stesso.** Tale strategia si innesta, pertanto, in un rafforzamento, tramite l'innovazione digitale, delle applicazioni, dei prodotti, e dei servizi, an-

TECNOLOGIE DIGITALI E TECNOLOGIE TRADIZIONALI



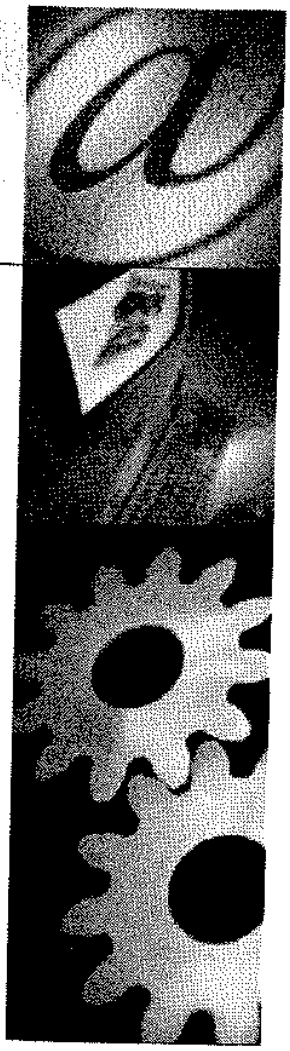
[6] *Dati Anee - Politecnico di Milano.*

che di tipo tradizionale, sui quali il nostro Paese ancora oggi basa il proprio vantaggio competitivo a livello internazionale.

4. INTERVENTI NEL MEZZOGIORNO

Il rafforzamento della competitività del Mezzogiorno trova nell'innovazione digitale uno strumento cruciale. In

questa sezione il Piano individua alcune misure dedicate allo sviluppo delle tecnologie dell'informazione e della comunicazione che abbiano come obiettivo di breve e medio termine quello di qualificare fortemente le imprese del Mezzogiorno mediante la spinta verso processi di aggregazione, mediante la promozione della finanza innovativa (in particolare del Venture capital) nei settori *high tech*, con la valorizzazione di eccellenze territoriali e il potenziamento dei rapporti con il mondo dell'Università e della ricerca. Queste misure si accompagnano naturalmente agli interventi in materia di e-government e alle iniziative di carattere infrastrutturale che il Ministero per l'Innovazione e le Tecnologie ha avviato nel corso degli ultimi anni e ai programmi regionali finanziati dai fondi strutturali.



L'innovazione digitale rafforza la competitività del Mezzogiorno

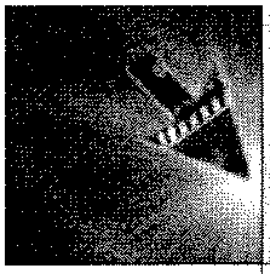
● NASCITA E SVILUPPO DI IMPRESE INNOVATIVE IN SETTORI HIGH-TECH

Al fine di promuovere la nascita e lo sviluppo di imprese high tech nelle Regioni del Mezzogiorno, il Piano prevede la costituzione di un **Fondo per la partecipazione al capitale di rischio di imprese operanti nei settori dell'*Information Technology*, dell'elettronica, delle nanotecnologie e microtecnologie, degli strumenti elettromedicali, della meccanica ad alta tecnologia per automazione industriale.** Il Fondo opererà sia mediante la partecipazione a fondi mobiliari chiusi già costituiti o da costituire, sia mediante il sostegno diretto alle attività di Venture Capital.

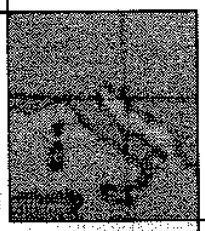
Misure basate sulla costituzione di Fondi per la partecipazione al capitale di rischio di imprese operanti nei settori ad alta tecnologia hanno prodotto risultati molto soddisfacenti in diversi paesi esteri, soprattutto a livello comunitario. Particolarmente significative sono le esperienze della Francia (*CDC Entreprises*), della Gran Bretagna, (*UK High Technology Fund*), dell'Irlanda (*Enterprise Ireland*) e di Israele (*Yozmà*), come risulta da un recente studio di Finlombarda.

I principali vantaggi portati da tali misure sono essenzialmente legati alla riduzione del rischio associato alla sottoscrizione di quote da parte di investitori privati e *venture capitalist*, con un conseguente effetto leva delle risorse pubbliche stanziate.

Nei suddetti casi sono stati previsti diversi meccanismi incentivanti per gli investitori privati, dai più moderati che equiparano l'investimento pubblico e quello privato sia in caso di rendimento positivo sia in caso di perdi-



MISURA 4.1: COSTITUZIONE DEL FONDO HIGH-TECH



Descrizione:
Costituzione di un fondo per la partecipazione pubblica al capitale di rischio di imprese in settori ad alta tecnologia quali l'Information Technology, l'elettronica, le nanotecnologie e microtecnologie, gli strumenti elettromedicali, la meccanica ad alta tecnologia per automazione industriale, sia tramite partecipazione a fondi mobiliari chiusi già costituiti o da costituire o attraverso il sostegno diretto alle attività dei Venture Capital.

Finalità:
- promuovere la nascita o lo sviluppo di imprese innovative nel settore dell'alta tecnologia
- Promuovere un mercato del capitale di rischio per investimenti su PMI o nuove imprese che per il valore dell'intervento o per tipologia del rischio non attraggono Venture Capital tradizionali
- ridurre il costo del riacquisto da parte dell'imprenditore e ridurre il rischio per l'investitore istituzionale attraverso meccanismi di ripartizione differenziata dei rimborsi tra Investitori Pubblici e Privati

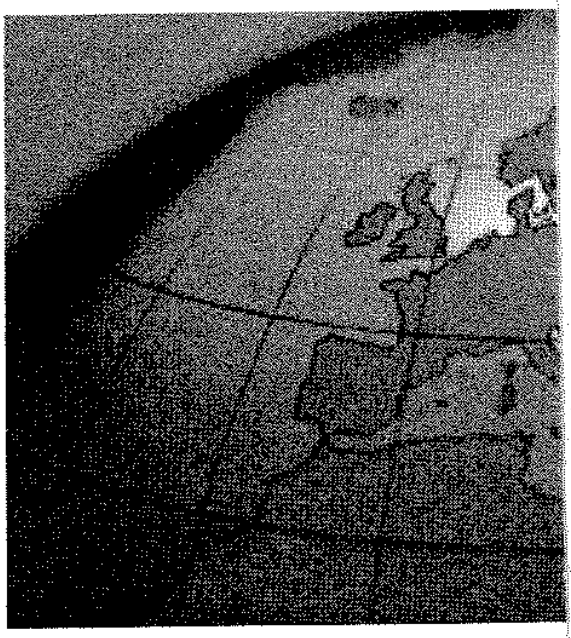
Beneficiari:
Start-up in settori ad alta tecnologia, Venture Capitalists, Investitori Istituzionali del Mezzogiorno.
Risorse Stanziate: 100 milioni di euro per il triennio 2005-2007.

te del fondo target (CDC *Entreprises, Enterprise Ireland*), fino al caso del *UK High Technology Fund* che prevede un rendimento minimo garantito per l'investitore privato.

Relativamente alle performance dei fondi "target", il caso israeliano ha prodotto risultati eccellenti, beneficiando peraltro del *timing* particolarmente favorevole dell'intervento (1993-1998). Riguardo altri casi internazionali è ancora prematuro esprimere un giudizio sulle performance. Le modalità di funzionamento del Fondo High Tech verranno definite dal Ministro per l'Innovazione e le Tecnologie, di concerto con il Ministro delle Attività Produttive e con il Ministro dell'Economia e Finanze.

ICT PER LO SVILUPPO DEL MEZZOGIORNO: IL PROGRAMMA "TERRITORI DI ECCELLENZA"

Il **programma Territori di Eccellenza (delibera CIPE 17 del 2003)** ha come obiettivo lo sviluppo della competitività di specifiche aree del Mezzogiorno attraverso l'utilizzo integrato delle nuove tecnologie dell'informazione e della comunicazione. Esso punta a valorizzare le conoscenze e le competenze professionali già sedimentate nell'ambito di specifici contesti territoriali, avviando progetti in grado di accelerare in modo significativo la crescita delle imprese e del sistema di relazioni in cui operano.

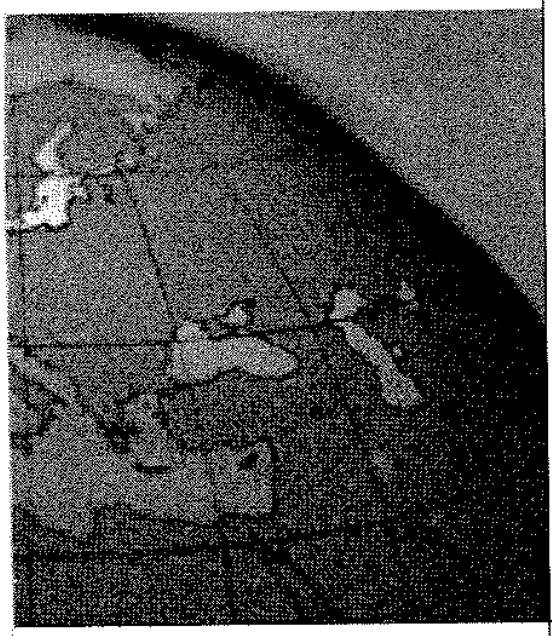


La metodologia di intervento favorisce da un lato lo sviluppo di forme innovative di integrazione e connettività fra persone, imprese e istituzioni all'interno dello specifico ambito territoriale; dall'altro, punta a sviluppare nuove relazioni fra il sistema locale e i circuiti internazionali degli scambi commerciali e dell'innovazione.

La gestione del programma, affidata al Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri, si basa sul coinvolgimento attivo delle Regioni, in

particolare per quanto concerne l'identificazione delle aree geografiche e dei settori di intervento. Gli strumenti che il Dipartimento per l'Innovazione e le Tecnologie intende utilizzare per la realizzazione del programma si focalizzano su quattro direttrici di intervento fra loro complementari: l'innovazione digitale nelle imprese, attraverso l'incentivazione degli investimenti in soluzioni innovative per la gestione aziendale e dei rapporti con le università, l'innovazione dei servizi promossi dalla Pubblica Amministrazione, la qualificazione del capitale umano e la diffusione della banda larga sul territorio.

Nell'ambito del Programma "Territori di eccellenza", **il Piano prevede l'istituzione di un sistema di voucher nelle regioni del Sud.** Come strumento di incentivazione dell'eccellenza, il voucher tecnologico rappresenta uno strumento dai molteplici e potenziali vantaggi. In primo luogo, i voucher sono per loro natura flessibili e proceduralmente veloci, facilmente fruibili e in grado di rispondere alle esigenze dei tempi delle imprese che solitamente sono incompatibili con i tempi più lunghi della pubblica amministrazione.



Obiettivo generale dell'intervento è quello di *migliorare le interazioni fra domanda e offerta*. Il voucher consente

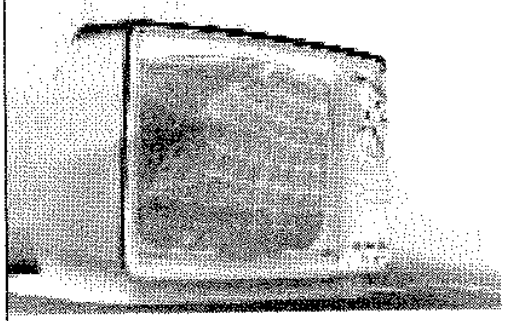
Un utilizzo integrato delle nuove tecnologie per valorizzare l'eccellenza dei territori

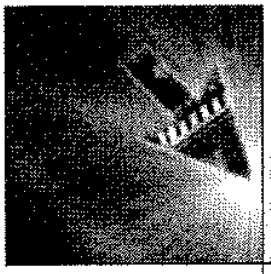
di coprire una quota del rischio legato all'investimento innovativo e quindi di stimolare la domanda di servizi tecnologici. In tal modo **incentiva la cooperazione tra il mondo della ricerca e il mondo dell'imprenditoria stimolando il trasferimento tecnologico.**

L'utilizzo del voucher è funzionale al finanziamento, più che di veri e propri progetti di ricerca ed innovazione tecnologica, **di specifici servizi tecnologici**, come l'assistenza brevettuale, o singole voci di spesa attinenti alla R&S, quale ad esempio la consulenza tecnico scientifica finalizzata alla redazione di uno studio di fattibilità tecnologica di un'idea innovativa in funzione delle specifiche esigenze espresse dalle imprese.

5. INTERVENTI PER IL MIGLIORAMENTO DEI SERVIZI VERSO LE IMPRESE DELLA PUBBLICA AMMINISTRAZIONE

In questo contesto si collocano gli interventi che il CNIPA ha attivato, e che sono tuttora in corso, per contribuire efficacemente al miglioramento dei servizi che la pubblica amministrazione eroga alle imprese.





MISURA 4.2: PROGRAMMA TERRITORI DI ECCELLENZA (DELIBERA CIPE 17 DEL 2003)

Descrizione:
Il Programma promuove una serie di progetti nelle Regioni Abruzzo, Basilicata, Calabria, Campania, Molise, Puglia, Sardegna e Sicilia finalizzate alla qualificazione di aree di eccellenza attraverso l'utilizzo delle nuove tecnologie dell'informazione e della comunicazione. Le risorse del programma sono state assegnate dalla delibera CIPE 17 del 2003 per il rafforzamento della società dell'informazione nelle Regioni del Mezzogiorno.

Finalità:
Il Programma punta a qualificare la competitività di alcune aree territoriali selezionate delle Regioni del Sud attraverso l'utilizzo innovativo delle nuove tecnologie. I territori sono selezionati in base alla loro capacità di ospitare filiere produttive innovative in grado di radicarsi efficacemente nel sistema locale e di confrontarsi con successo con i mercati internazionali. Le nuove tecnologie sono chiamate a supportare lo sviluppo integrato della connettività fra mondo delle imprese, dell'amministrazione e della società nel suo complesso.

Governance:
Il Programma è gestito da un Comitato di indirizzo cui partecipano rappresentanti del Ministero dell'Economia e delle Finanze, del Ministero per l'Innovazione e le Tecnologie e delle Regioni interessate. La durata del programma è triennale. I progetti promossi nell'ambito del programma si concluderanno entro il 31 dicembre 2007.
Risorse a valere sui 100 milioni di euro fonte CIPE.

SOTTOMISURA 4.2.1: VOUCHER TECNOLOGICI

Descrizione:
Istituzione di un sistema-voucher per le Regioni del Mezzogiorno per la concessione di agevolazioni finanziare per attività di:
- assistenza brevettuale
- *due diligence tecnologica*
- business evaluation
- borse per dottorato di ricerca

Attraverso tale meccanismo piccole e medie imprese e persone fisiche potranno usufruire dei suddetti servizi erogati da Centri di Ricerca e Università accreditati presso il Ministero per l'Innovazione e le Tecnologie. Il pagamento dell'ente accreditato viene effettuato direttamente dall'Amministrazione centrale ed è legato alla concessione di un voucher spendibile dall'impresa o dalla persona fisica presso il centro accreditato.

Finalità:
- creare un meccanismo di agevolazione più efficace e più flessibile
- Migliorare l'interazione fra la domanda e l'offerta di servizi di consulenza relativi alle attività di ricerca e sviluppo
- Garantire una selezione più meritocratica dei progetti presentati

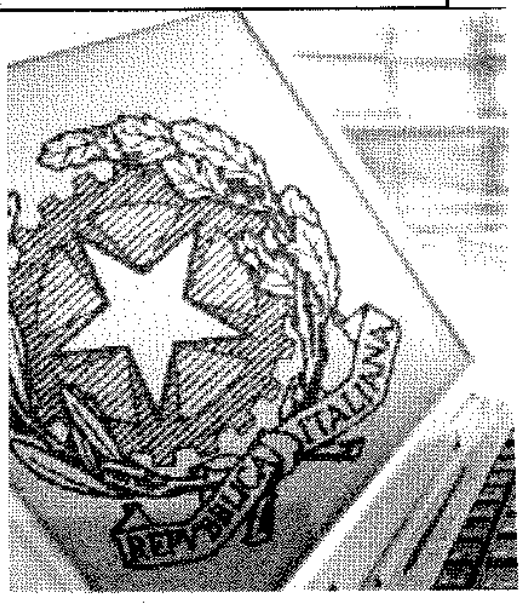
Beneficiari:
Centri di ricerca e Università accreditati del Mezzogiorno in qualità di soggetti erogatori dei servizi. Piccole e medie imprese e persone fisiche del Mezzogiorno in qualità di fruitori del servizio.

Un significativo incremento della competitività del sistema delle imprese richiede una Pubblica Amministrazione in grado di fornire alle imprese da parte di servizi economici, efficaci e tempestivi anche attraverso l'opera di semplificazione amministrativa. Le imprese sono particolarmente sensibili al risparmio di tempi (e costi) che deriva dall'erogazione di servizi da parte della pubblica amministrazione con modalità innovative.

Questi obiettivi generali si ottengono intervenendo su una serie di aspetti, quali:

1 Miglioramento della qualità dell'informazione;

2 Riduzione dei tempi di erogazione del servizio;



Le imprese chiedono una Pubblica Amministrazione efficace e tempestiva

3 Riduzione del costo della burocrazia;
4 Riduzione dei costi;
5 Miglioramento del livello di servizio;
6 Aumento dell'efficienza;
7 Aumento della soddisfazione dell'utente.

Le iniziative avviate dal CNIPA per il miglioramento dei servizi alle imprese si articolano in due filoni principali:

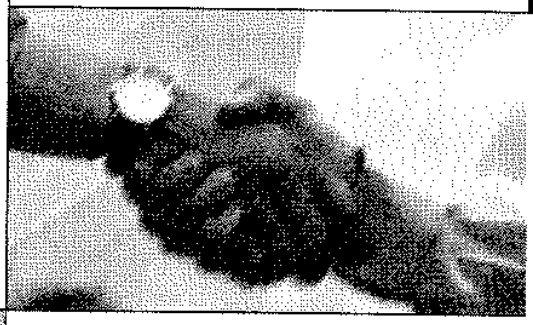
- la promozione e il finanziamento di progetti da parte di Regioni ed Enti Locali, miranti ad introdurre soluzioni innovative per l'erogazione dei servizi della pubblica amministrazione locale (in particolar modo lo Sportello Unico per le Attività Produttive);
- lo sviluppo del portale di servizi integrati alle imprese, al fine di semplificare, attraverso l'integrazione, l'accesso ai servizi per le imprese richiesti dagli adempimenti di legge.

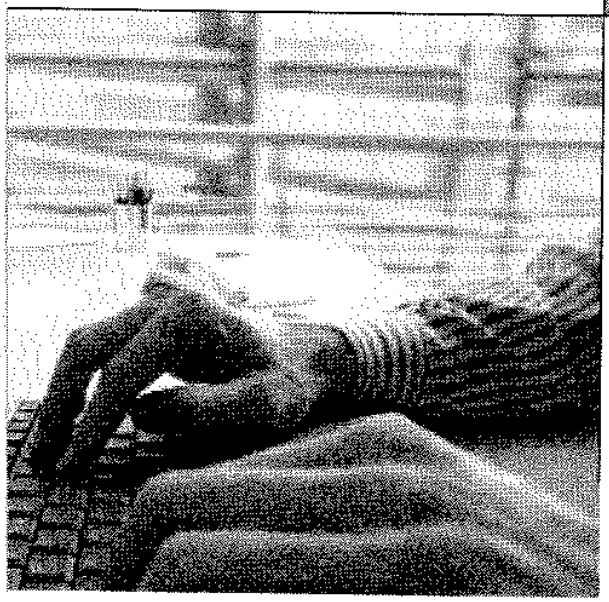
I PROGETTI AVVIATI NELLA PUBBLICA AMMINISTRAZIONE LOCALE

Nell'ambito della prima fase di attuazione dell'e-government locale uno dei principali obiettivi è stato quello di promuovere l'adozione di soluzioni innovative, basate sull'ICT, per il miglioramento dei livelli e della qualità dei servizi che la pubblica amministrazione locale eroga alle imprese. Con questo obiettivo è stato cofinanziato un insieme di progetti proposti dalle Regioni e dagli Enti Locali, per lo sviluppo di soluzioni innovative per l'erogazione dei servizi alle imprese da parte delle Pubbliche Amministrazioni.

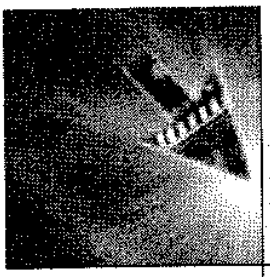
L'insieme dei 21 progetti che sul totale dei 134 finanziati sono finalizzati alla realizzazione dei servizi per le imprese, sono stati cofinanziati per un importo pari a circa 12 milioni di Euro a fronte di un costo totale dei progetti di circa 52 milioni di Euro.

I progetti intervengono su un vasta parte del territorio nazionale, coinvolgendo 11 territori regionali e oltre 900 enti tra regioni, province e comuni. I progetti si trovano in avanzato stato di realizzazione, alcuni sono già conclusi, e prevedono l'attuazione di interventi sugli Sportelli Unici per le Attività Produttive, interventi per servizi specifici in settori di attività d'impresa (agricoltura, commercio, etc.), nonché servizi di promozione del territorio in relazione alla possibilità di insediamenti industriali (marketing territoriale).





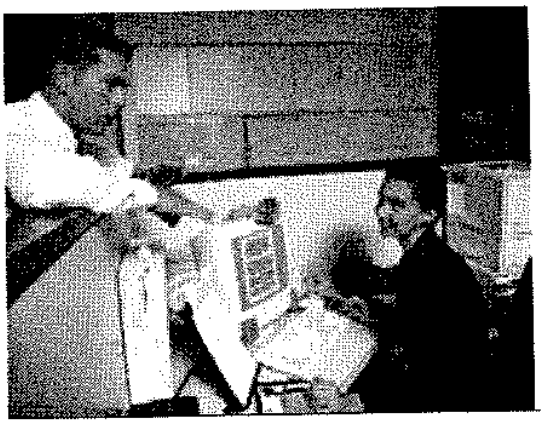
I positivi risultati ottenuti con la prima fase di attuazione spingono alla ricerca di meccanismi in grado di aumentare l'impatto delle soluzioni sviluppate e degli investimenti effettuati. In questo senso è prevista per i prossimi mesi un'estensione e diffusione delle soluzioni di servizi alle imprese verso quei territori che non sono stati interessati dalla prima



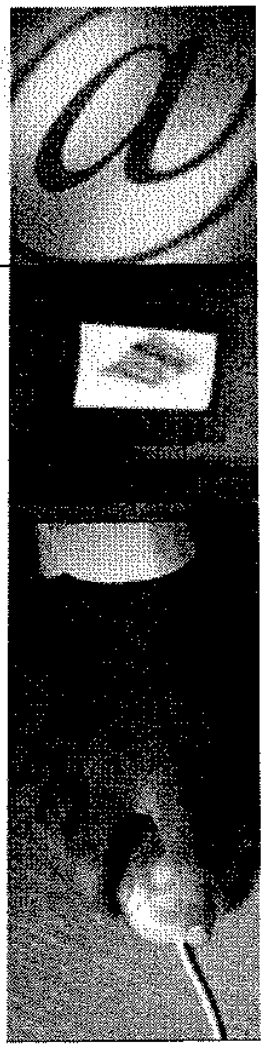
fase. Questa estensione avverrà attraverso progetti di trasferimento e riuso delle soluzioni già sviluppate con successo, che vedrà coinvolte in primo luogo le amministrazioni che hanno già adottato soluzioni innovative e che sono disponibili a trasferire alle altre Pubbliche Amministrazioni il patrimonio di conoscenza ed esperienza accumulato.

● IL SISTEMA INTEGRATO DI GESTIONE DEI SERVIZI ALLE IMPRESE

La volontà di creare un rapporto efficace ed efficiente tra Amministrazione ed imprese si concretizza mediante la semplificazione degli adempimenti a carico di queste ultime. Evitando duplicazioni di comunicazione degli stessi dati alle diverse amministrazioni pubbliche con cui le imprese vengono a contatto nello svolgimento delle proprie attività, si riducono i carichi di lavoro per le imprese e per le amministrazioni per effetto della eliminazione delle ridondanze, delle acquisizioni multiple degli stessi dati, delle anomalie e dei disallineamenti degli archivi informatici.

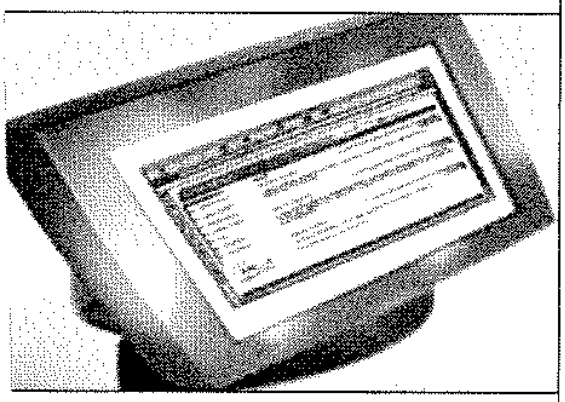


L'opportunità consiste nella identificazione di un unico spazio e di un unico momento in cui l'impresa può agevolmente reperire e produrre le informazioni necessarie per assolvere agli adempimenti di legge e può avviare un unico flusso informativo verso tutti gli enti interessati (INPS, INAIL, Camere di Commercio, Agenzia delle entrate) evitando di accedere alle reti distributive di ogni singolo destinatario.



L'integrazione delle fasi di comunicazione dei dati identificativi delle imprese e della trasmissione di adempimenti multipli, secondo la logica dello sportello unificato delle attività produttive, ha consentito di mettere a punto:

- un repertorio aggiornato e normalizzato delle imprese operanti nel paese;
- una interfaccia unica tra le imprese e ogni ente della Pubblica Amministrazione;
- una interfaccia unica tra enti della PA per lo scambio di informazioni sulle imprese.



I vantaggi offerti dal sistema integrato sono evidenti:

- contenimento dei tempi di lavoro e dei costi del ciclo produttivo pubblico (costo dell'aggiornamento dei dati identificativi delle imprese da parte delle singole amministrazioni);
- riduzione dei costi e dei tempi burocratici a carico dell'impresa (che deve comunicare i dati identificativi una sola volta);
- snellimento delle pratiche di accesso alla PA per la disponibilità di una sola interfaccia;
- integrazione con i servizi sviluppati nell'ambito dello Sportello unico delle Attività Produttive;
- riduzione dei costi e dei tempi nell'ambito pubblico nonché miglioramento della qualità dei dati amministrativi disponibili.

Le risorse principali del modello adottato sono il front-office (o sportello virtuale) utilizzato dalle imprese per usufruire di servizi e il back-office che

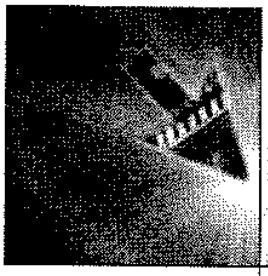
L'impresa deve reperire le informazioni necessarie per assolvere agli adempimenti di legge

consente lo scambio di informazioni tra le PA aderenti secondo uno schema di funzionamento trasversale.

Un ulteriore fattore abilitante del sistema integrato è costituito dal complesso sistema di sicurezza messo a punto che consente di determinare l'identità degli interlocutori, di abilitare l'utenza all'accesso a specifiche funzioni sulla base di predeterminati profili, di trasmettere documenti informatici adottando meccanismi di firma digitale atti a garantire paternità, validità e confidenzialità dei dati contenuti.

Lo sviluppo del progetto, finanziato per un importo di circa 2,5 milioni di euro dal Dipartimento per l'Innovazione e le Tecnologie e per circa 0,6 milioni di euro dall'Inps, è terminato nel mese di settembre 2002. A partire da tale data, sono state rese collaudate sia la componente di front-office - tesa a semplificare il dialogo tra imprese ed enti in una logica di accesso delocalizzato - sia la componente di back-office, il cui fine è agevolare lo scambio di informazioni tra enti della PA.

Il sistema, accessibile all'indirizzo **www.impresa.gov.it**, è stato quindi avviato, in fase di sperimentazione, a partire dal mese di dicembre 2002 presso un limitato numero si province e l'operatività è assicurata dalle principali associazioni di categoria degli intermediari primari (CONFCOMMERCIO, CONFARTIGIANATO, CNA, CONFESERCENTI, CONSULENTI DEL LAVORO) che stanno collaborando nella fase di ottimizzazione dei servizi realizzati. La fase di sperimentazione si concluderà entro il mese di dicembre 2004, data a partire dalla quale è prevista l'entrata in produzione del sistema nel suo complesso.

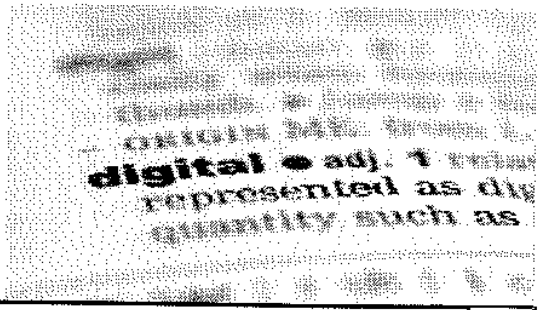


APPENDICE

IL PIANO 2003: I RISULTATI

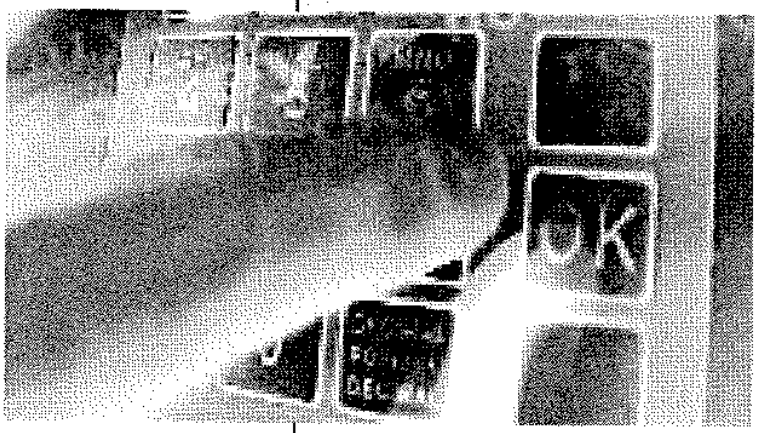
Il Piano lanciato nel 2003 ha inaugurato un nuovo approccio di *Governance dell'innovazione digitale*, caratterizzata da una comune regia da parte del Ministero delle Attività Produttive e del Dipartimento per l'Innovazione e le Tecnologie nella definizione delle politiche e nella implementazione degli interventi. Questo modo di operare è stato oggetto, già in corso d'opera, di grande interesse da parte della Commissione europea che ha espresso, attraverso i Commissari P. Busquin e F. Bolkestein, l'apprezzamento per lo sforzo fatto dall'Italia di coordinare e rendere sinergici gli interventi dei due Ministeri. Nel 2004 il Piano è stato riconosciuto dallo studio di "Benchmarking sulle politiche nazionali e regionali di supporto all'ICT in UE" della DG Imprese della Commissione europea come *best practice* della governance in materia di politiche delle ICT a livello comunitario.

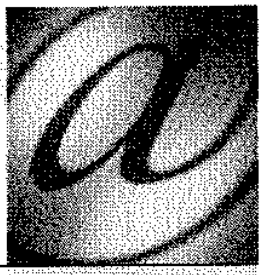
Di seguito si riassume lo stato di attuazione del Piano 2003.

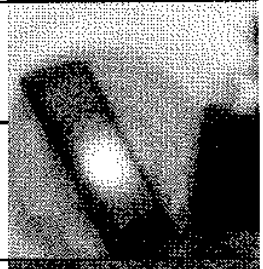


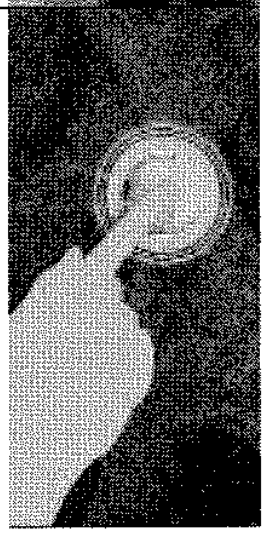
MISURE DI CARATTERE ECONOMICO-FINANZIARIO:

MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
1) Bando tematico per l'innovazione delle PMI *Il Piano per l'innovazione digitale nelle imprese aveva evidenziato come, a differenza di altri Paesi dell'Unione, l'Italia non possedesse uno strumento specifico a sostegno dell'innovazione nel campo delle ICT. A tal fine il Piano annunciava una misura ad hoc – finanziata dal Ministero delle Attività Produttive e dal Dipartimento per l'Innovazione e le Tecnologie – che avesse per obiettivo la riprogettazione dei sistemi tecnico-organizzativi delle PMI attraverso un uso intensivo delle nuove tecnologie della comunicazione e dell'informazione.*	Nel mese di novembre 2003 è stato lanciato il bando tematico Innovazione/ICT, il primo in Italia ad essere mirato in modo specifico al miglioramento dell'efficienza delle PMI attraverso l'applicazione delle tecnologie dell'informazione e della comunicazione (ICT) all'organizzazione aziendale. Il Bando ha interessato l'intero territorio nazionale, ed è stato diretto alle PMI, ai Centri di Ricerca, alle Università e agli enti pubblici di ricerca in partnership con le imprese favorendo le aggregazioni tra PMI ed il coinvolgimento nelle attività di programma di enti pubblici di ricerca e di Università. Attualmente è in corso la procedura di valutazione dei programmi di massima presentati. Dotazione finanziaria – risorse impegnate La misura è stata dotata di risorse per un ammontare di 112,8 milioni di euro. Ai fini della compilazione della graduatoria sono stati selezionati: 63 programmi la cui realizzazione è prevista ad opera di 348 imprese per un ammontare d'investimenti previsto di 87,2 milioni di euro a valere sulle risorse FIT; 43 programmi che verranno realizzati da 278 imprese per le aree Obiettivo 1 a valere sulle risorse nazionali e comunitarie nell'ambito del PON-SIL per un ammontare di investimenti di oltre 65,6 milioni di euro

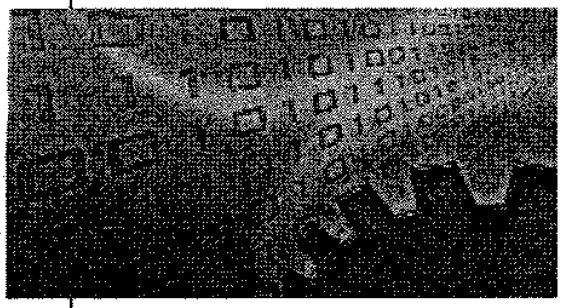


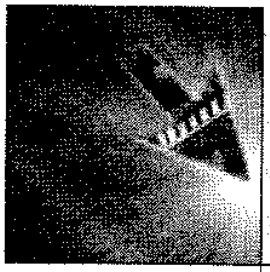




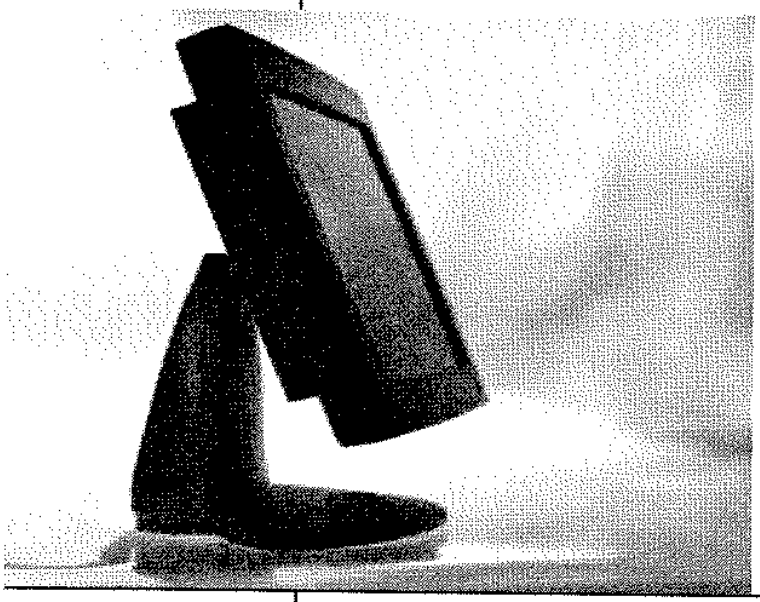


MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
2) Venture capital e capitalizzazione di nuove imprese innovative *Attraverso questa misura, il Piano intendeva favorire l'accesso al capitale di rischio di nuove imprese innovative e di PMI mediante concessione di anticipazioni finanziarie pubbliche a banche e intermediari finanziari, finalizzate alla acquisizione di partecipazioni temporanee e di minoranza.*	Con un decreto del 19 gennaio 2004, il Ministero delle Attività Produttive ha deliberato lo stanziamento di nuovi fondi per il finanziamento di programmi di investimento a sostegno della nascita e del consolidamento delle imprese operanti in comparti ad elevato impatto tecnologico. L'intervento ha per oggetto la concessione ai soggetti accreditati (banche, intermediari finanziari, S.F.I.S.) di anticipazioni finanziarie da utilizzare per l'acquisizione di partecipazioni al capitale di imprese a fronte di programmi pluriennali di sviluppo. In particolare sono ammessi al provvedimento i programmi destinati allo sviluppo di processi produttivi, prodotti e servizi nel campo delle tecnologie dell'informazione e della comunicazione ovvero quei programmi di sviluppo innovativi e ad elevato impatto tecnologico. Sono state, sino ad ora, accreditate presso il MAP 9 Società finanziarie intermediari nell'attuazione della misura. **Dotazione finanziaria – risorse impegnate** Il fondo destinato alla misura è dotato di risorse per 204 milioni di euro di cui 72 milioni di euro provenienti dall'Art. 103 L. 388/00 (proventi UMTS) e da 155 milioni di euro provenienti dall'Art. 106 della medesima legge. Il 15% del secondo importo (33 milioni di euro) sono state destinate agli incubatori delle Università ed ai Centri di Ricerca.
3) Bandi tematici per R&S (ex Art. 56 Finanziaria 2003) *Il Piano prevedeva attraverso la legge finanziaria un fondo per la ricerca applicata. Nell'ambito di questo fondo il DIT disponeva di 35 milioni di euro che sarebbero stati indirizzati al finanziamento di programmi di sviluppo di soluzioni ICT per la reingegnerizzazione dei processo nelle filiere distrettuali e per la logistica integrata.*	La fase di valutazione degli 80 progetti presentati è in corso di chiusura.
4) Leva fiscale *Il Piano proponeva l'introduzione nel nostro sistema di una leva fiscale a favore dell'innovazione, attraverso l'adozione di un meccanismo di detassazione del reddito di impresa e di lavoro autonomo reinvestito, applicato ad una predeterminata tipologia di investimenti in innovazione.*	Una prima applicazione di questo strumento è avvenuta ad opera del Decreto-legge 30/09/2003, n.269 (legge di conversione 24/11/ 2003, n. 326 - supplemento ordinario n. 181/L alla Gazzetta Ufficiale - serie generale - n. 274 del 25/11/2003), che ha introdotto la detassazione degli investimenti in ricerca e sviluppo, export, quotazione in borsa e quelli relativi agli stage aziendali per studenti. La norma non ha però previsto la detassazione degli investimenti in innovazione digitale così come proposto a suo tempo dal MAP e dal MIT.

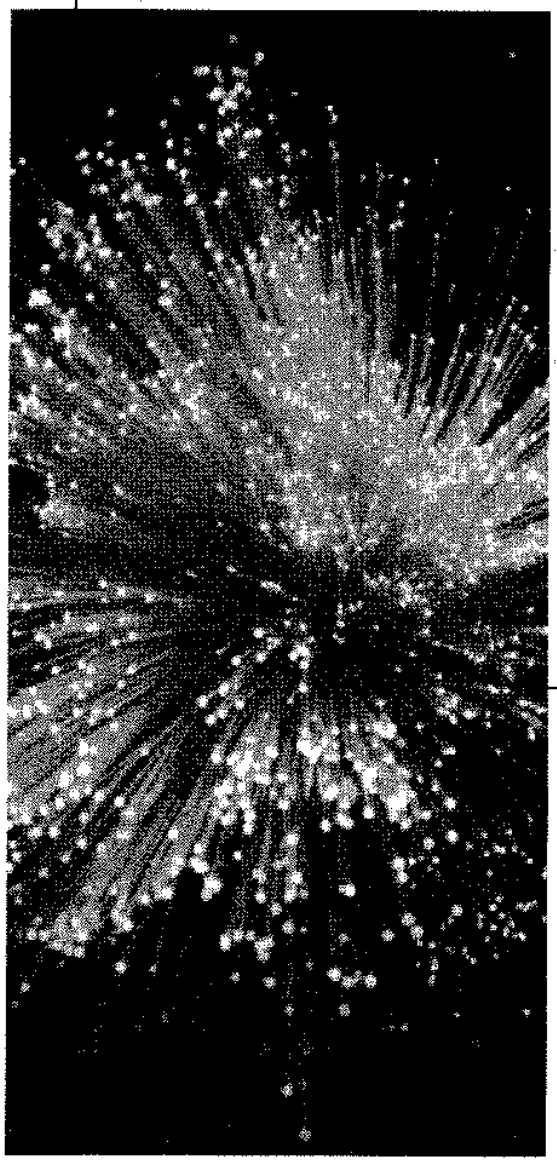




MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
1) Testo unico sulla proprietà industriale *Il Piano indicava quale principale obiettivo da raggiungere attraverso l'elaborazione di un Testo unico/Codice sulla proprietà industriale quello di fornire a tutti gli operatori del settore, una disciplina univoca, sistematica, organica e soprattutto al passo con i tempi.*	Il 23 dicembre 2004, il Consiglio dei Ministri, su proposta del Ministro delle Attività produttive, ha approvato, tramite decreto legislativo, il Codice dei diritti di proprietà industriale, dopo l'esame del Consiglio di Stato e delle competenti Commissioni parlamentari. L'imponente attività di riassetto delle disposizioni vigenti in materia di proprietà industriale e il lavoro di codificazione, svolto da una Commissione Ministeriale di esperti, ha condotto alla ripartizione della materia per settori omogenei, puntando ad un coordinamento formale e sostanziale delle disposizioni vigenti, al fine di garantire coerenza giuridica, logica e sistematica alla materia. Il lavoro della Commissione è stato dedicato anche ad adeguare la normativa alla disciplina internazionale e comunitaria in tema di armonizzazione e semplificazione dei procedimenti amministrativi introdotti con il Trattato sul diritto dei marchi. Il Codice è articolato in 8 capi che trattano rispettivamente dei principi fondamentali e delle disposizioni generali sui diritti di proprietà industriale; la loro disciplina sostanziale; le forme di tutela giurisdizionale; le procedure per l'acquisto ed il mantenimento degli stessi; le procedure speciali; l'ordinamento professionale dei consulenti di proprietà industriale ed infine la gestione dei servizi e dei diritti ad opera dell'Ufficio Italiano Brevetti e Marchi, nonché le disposizione transitorie e finali.
2) Tribunali specializzati in materia di proprietà industriale *La dimensione del contenzioso in materia di proprietà industriale, la necessità di competenze specifiche, la certezza dei tempi della giustizia hanno indotto il Governo a predisporre un Decreto legislativo (168/2003) che prevedeva l'istituzione di tribunali e corti d'appello specializzate nella materia.*	La Misura è stata attuata con l'istituzione di dodici sezioni specializzate che coprono l'intero territorio nazionale (Bari, Bologna, Catania, Firenze, Genova, Milano, Napoli, Palermo, Roma, Torino, Trieste e Venezia).
3) Riorganizzazione dell'Ufficio Italiano Brevetti e Marchi (UIBM) *Il Piano intendeva riorganizzare ed informatizzare l'UIBM attraverso il lancio del progetto di deposito elettronico dei marchi e dei brevetti da realizzarsi in stretta collaborazione con il Dipartimento del Commercio degli Stati Uniti (e, in particolare, con l'USPTO). Il sistema attualmente in uso negli Stati Uniti (cosiddetto TEA'S) verrà modificato a partire da novembre per consentirne la compatibilità con il deposito del marchio internazionale, cui gli USA hanno aderito il 2 novembre 2003.*	Nel corso del 2003 sono stati elaborati gli applicativi per il deposito on-line dei diversi titoli della proprietà industriale attualmente in fase di test presso i mandatari.

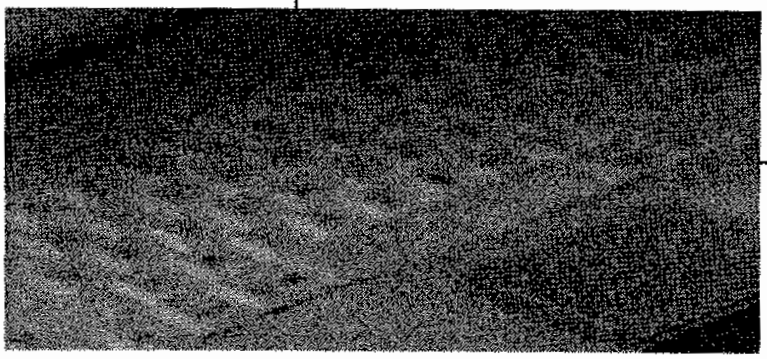


MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
4) Intervento normativo a favore del trasferimento tecnologico Il Piano individuava quale priorità il trasferimento di tecnologia dalle Università al mercato e la valorizzazione economica dei brevetti. A tal fine annunciava la predisposizione di norme dirette a favorire lo sfruttamento economico dell'attività di ricerca ed a premiare adeguatamente i ricercatori.	Nel periodo preso in considerazione dal piano l'UIBM ha lavorato alla predisposizione di un testo normativo per la disciplina della materia in stretto partenariato e concertazione con il mondo delle imprese e della ricerca pubblica. Sono state individuate e sono tuttora in corso di elaborazione alcune norme per l'introduzione dei seguenti principi: • consentire alle Università e ai Centri di Ricerca pubblici di acquisire la titolarità dei diritti sui risultati della ricerca finanziata da fondi pubblici, a condizione che tale titolarità venga sfruttata economicamente; • prevedere incentivi per la creazione di uffici per la gestione del trasferimento di tecnologie presso le Università con funzioni di marketing dei risultati della ricerca pubblica presso l'industria • dare preferenza alle PMI italiane/comunitarie nell'assegnazione delle licenze di sfruttamento dell'invenzione • fornire assistenza, tramite un Ufficio Centrale per il Trasferimento Tecnologico (UTT), per la costituzione di cluster di brevetti, anche appartenenti a diverse Università, che incidono su un particolare settore economico e che più facilmente possano interessare l'industria; • fornire servizi di intermediazione tra Università e mondo delle imprese (anche con l'istituzione di borse per l'innovazione tecnologica), • studiare possibilità di assistenza alle Università per l'avvio di procedure a tutela di brevetti di loro proprietà nonché per la difesa in giudizio degli stessi, in Italia e all'estero. • evitare che le invenzioni di particolare interesse pubblico rimangano inattuate.



MISURE DI CONTESTO

MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
1) Diffusione della cultura dell'innovazione *Il Piano ha previsto tra i suoi assi portanti quello della diffusione della cultura dell'innovazione. E' ormai provato infatti che l'e-business e le ICT aiutano le imprese a ridurre i costi, aumentare la produttività, migliorare l'efficienza dei processi aziendali verso i clienti, i fornitori e i dipendenti. Ma spesso la scarsa informazione e la mancata consapevolezza circa i vantaggi e le soluzioni che l'innovazione può procurare alle imprese ostacola la diffusione di questi strumenti.*	La misura, volta a fornire una risposta concreta al bisogno di conoscenza delle soluzioni IT per le imprese è stata attuata attraverso la realizzazione di 17 seminari informativi per la promozione dell'e.Business nelle imprese. L'iniziativa è stata lanciata dal Comitato e-business del MAP - Direzione Generale Commercio, Assicurazione e Servizi ed è stata attuata da una collaborazione tra IPI e le Associazioni di categoria Confindustria, Confcommercio ed Unincamere. I seminari si sono tenuti su tutto il territorio tra il mese di novembre 2004 e febbraio 2005. Dotazione finanziaria – risorse impegnate La misura conta su un totale di risorse di 200.000 euro. Il cofinanziamento del Ministero ammonta a 80.000 euro.



MISURE DI CARATTERE ORGANIZZATIVO – GESTIONALE

MISURE LANCIATE DAL PIANO 2003	STATO DI ATTUAZIONE E RISULTATI
1) Coordinamento stabile tra Ministri *Il Piano prevedeva la necessità di favorire la collaborazione tra Ministeri con competenze che hanno incidenza sull'innovazione quale elemento chiave per realizzare e rafforzare l'efficacia delle strategie a favore dell'innovazione.*	L'attuazione delle misure del piano è stata garantita da un coordinamento stabile tra le strutture MAP/MIT ed in particolare attraverso l'assegnazione ad una struttura tecnica, l'IPI il compito di assicurare il monitoraggio delle misure. Il raccordo con le parti sociali è stato garantito attraverso i lavori del Comitato e-business che ha permesso un confronto stabile sulla materia.
2) Partenariato socio economico *Il Piano infine prevedeva misure di carattere organizzativo - gestionale che garantissero un coordinamento stabile a livello inter-Ministeriale e con le parti sociali attraverso una struttura specifica.*	Tale misura è stata realizzata attraverso le iniziative attuate dal Comitato e-business, organo flessibile e dinamico specializzato nelle questioni concernenti l'e-business e l'innovazione digitale. È composto dalle principali associazioni di categoria e dei consumatori. Oltre al MAP, vede la partecipazione attiva del DIT. Assicura il dialogo socio economico ed opera al fine di valorizzare i contributi dei suoi partecipanti attraverso interventi, progetti e proposte concreti la materia di competenza.

Credit
A cura del:
Dipartimento Net-Economy - DNE
Direzione Politiche e Progetti di Intervento

IPI - Viale M.llo Pilsudski, 124 - 00197 - Roma
Tel. (+39) 06 809721 - Fax (+39) 06 8072898
info@ipi.it - www.ipi.it

Realizzazione
PRC srl
Via Germanico, 197 - Roma
www.prcsrl.com

Photo
Zefa - Roma

Gennaio 2005

Statistiques en bref

INDUSTRIE, COMMERCE ET SERVICES

POPULATION ET CONDITIONS SOCIALES

SCIENCE ET TECHNOLOGIE

25/2005

Auteur

Christophe DEMUNTER

Contenu

Fin de rédaction: 30.06.2005
Données extraites le : 3.05.2005
ISSN 1561-4859
Numéro de catalogue: KS-NP-05-025-FR-N

Utilisation d'Internet en Europe: sécurité et confiance

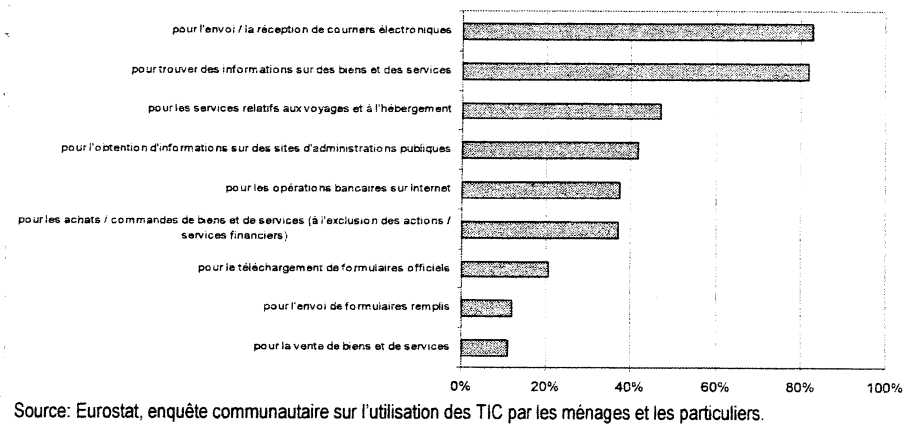
Faits marquants

- Effectuer des achats par Internet est une opération perçue comme étant relativement sûre: la plupart des acheteurs en ligne n'ont en effet signalé aucun problème. Ceux qui en ont signalé ont essentiellement mentionné comme problématiques 'l'incertitude concernant les garanties' et 'des délais de livraison plus longs que ceux qui avaient été annoncés'.
- Parmi ceux qui n'ont jamais effectué d'achats via Internet, 42% (à l'échelle de l'UE-15) ont déclaré être préoccupés par la sécurité et craindre de communiquer des informations relatives à leur carte de crédit via Internet; 60% préfèrent acheter en personne.
- Les "pourriels" ont représenté un problème très répandu en 2004: entre 25% (Portugal) et 58% (Allemagne) d'utilisateurs d'Internet ont reçu des messages électroniques non sollicités; des utilisations frauduleuses de carte de paiement ont été rapportées par moins de 2% des utilisateurs d'Internet, à l'exception du Royaume-Uni.
- Des logiciels antivirus ont été utilisés par presque toutes les entreprises, indépendamment de leur taille; des dispositifs de sécurité plus sophistiqués sont plus répandus dans les grandes entreprises.
- Dans certains pays, une proportion étonnamment élevée d'entreprises n'a toujours pas de dispositifs de sécurité visant à protéger les ordinateurs et les réseaux.
- Une part relativement importante d'entreprises a fait état d'attaques de virus; la situation varie moins en fonction des activités économiques qu'en fonction des pays.

La large utilisation des technologies de l'information et de la communication (TIC) a continué à s'étendre: en 2004, un européen sur deux (49,8% – UE-25) avait eu recours à l'Internet durant les 12 mois précédents; près de 54% des internautes européens se sont connectés à la toile tous les jours ou presque et plus de 82% au moins une fois par semaine. L'Internet offre une variété croissante de fonctionnalités, mais en même temps les utilisateurs sont confrontés à des problèmes tels que les attaques de virus, les "spams" ou l'utilisation frauduleuse d'informations communiquées sur Internet.

La sécurité et la confiance dans l'utilisation d'Internet sont difficiles à évaluer avec précision, car elles ont une composante éminemment subjective. Dans la présente publication, la sécurité et la confiance sont indirectement mesurées à travers une analyse des comportements et des utilisations. Par ailleurs, les chiffres présentés ici (basés sur des enquêtes, voir les notes méthodologiques) risquent d'être faussés en raison d'une faible sensibilisation des personnes interrogées aux risques liés à certains aspects de l'utilisation d'Internet.

Graphique 1: Utilisation d'Internet, par type d'utilisation (% de particuliers qui ont utilisé Internet durant les 3 derniers mois), UE-15 - 2003



Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

Des facteurs attestant la familiarisation du grand public avec les technologies de l'information et de la communication peuvent être observés dans le graphique 1, qui reprend les différents types d'utilisation d'Internet en 2003.

L'utilisation d'Internet pour les achats ou les opérations bancaires est influencée par le niveau d'éducation

Le tableau 1 donne un aperçu de l'accès à Internet par statut socio-professionnel en 2004. Le pourcentage de personnes retraitées qui se sont connectées à Internet au moins une fois par semaine est d'environ 30% au Danemark et en Suède. Bien que ce taux reste très variable au niveau d'UE-25 (entre 8 et 33%), il n'en démontre pas moins que l'Internet s'ouvre à une catégorie de la population réputée réticente à utiliser les TIC.

Parmi les autres groupes socio-professionnels, les taux d'accès à Internet sont élevés, surtout chez les étudiants (ils s'établissent dans une fourchette de 42 à 96%), pour qui Internet fait souvent partie intégrante de la vie quotidienne. Parmi les personnes qui ont un emploi, celles qui se connectent à Internet au moins une fois par semaine sont de plus en plus nombreuses, bien que chez les salariés le taux ait varié de 23% en Turquie à plus de 70% dans les pays nordiques que sont le Danemark, la Finlande, la Suède et l'Islande (voir tableau 1).

En ce qui concerne l'achat de biens et services via Internet, il apparaît que la méfiance à l'égard des paiements en ligne recule au fur et à mesure que les internautes se familiarisent avec les achats en ligne. En 2004, le nombre de particuliers qui ont réglé leurs achats en ligne en communiquant les informations relatives à leur carte de crédit a plus que doublé en Islande, et fortement progressé dans la plupart des pays de l'UE (voir graphique 2).

Cependant, le comportement individuel est directement lié au niveau d'éducation: le graphique 3 montre que les commandes en ligne et les opérations bancaires sur Internet sont plus fréquentes chez les personnes ayant un niveau d'instruction élevé – cette observation est valable pour tous les pays pour lesquels des données sont disponibles.

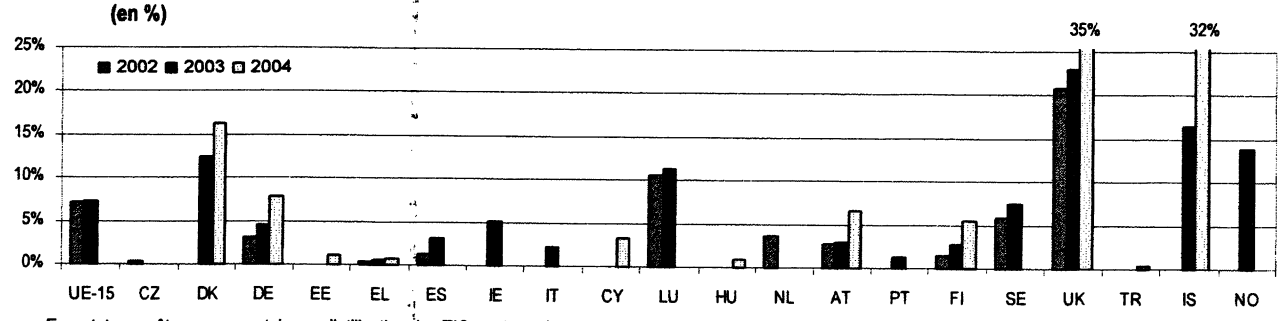
Tableau 1: Proportion de particuliers qui se sont connectés à Internet au moins une fois par semaine en moyenne, durant les 3 derniers mois (en %) - 2004

	Retraités	Salariés	Étudiants	Chômeurs
UE-15	10,6	:	68,3	:
CZ	1,3	:	:	:
DK	29,2	77,0	89,4	56,3
DE	18,0	60,5	84,0	41,7
EE	3,3	52,4	88,6	26,7
EL	0,8	25,2	45,7	11,5
ES	3,7	:	:	:
IE	5,8	:	42,2	:
IT	4,3	34,8	61,8	23,7
CY	6,7	31,3	73,0	39,1
LT	0,9	29,8	76,9	6,2
LU	10,1	:	90,4	:
HU	1,3	25,6	70,0	:
AT	11,7	56,8	89,4	37,8
PT	:	:	71,0	:
SI	:	42,3	81,8	:
FI	14,2	74,6	93,4	48,8
SE	32,9	79,3	94,2	80,7
UK	16,8	57,6	84,4	:
TR	2,1	23,5	44,2	16,6
IS	24,9	78,9	96,3	:
NO	23,7	:	90,7	:

Note: UE-15, CZ, ES, IE, LU, PT, NO: 2003

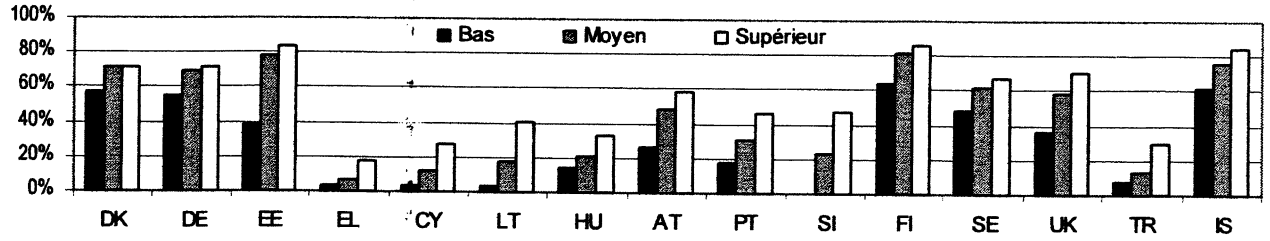
Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

Graphique 2: Nombre de personnes qui ont commandé des biens et services et payé en indiquant leur numéro de carte de crédit sur Internet (en %)



Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

Graphique 3: Nombre de personnes qui ont utilisé Internet, durant les 3 derniers mois, pour effectuer des commandes, des ventes ou des opérations bancaires — par niveau d'éducation* (%) - 2004



* Voir les notes méthodologiques.

Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

La plupart des acheteurs en ligne n'ont pas signalé de problèmes

Comme il ressort du tableau 2, seul un pourcentage relativement faible d'Européens ayant effectué des achats via Internet a rencontré des problèmes en 2004. On peut distinguer deux types de problèmes: le premier apparaît au moment de commander ou d'acheter via Internet, le second lorsqu'il s'agit d'obtenir matériellement les biens ou articles. Moins de 4% de la clientèle Internet a rencontré des problèmes dus à un manque de sécurité des paiements lorsqu'elle a passé commande.

Entre 2% et 6% des clients Internet se sont plaints de difficultés à obtenir réparation après avoir effectué des achats. 'L'incertitude concernant les garanties' a été assez souvent mentionnée à Chypre (12%) et en Slovénie (8%), mais nettement moins souvent en Allemagne (2%). Près de 5% des clients ont été confrontés à la réception de marchandises endommagées (Luxembourg, Royaume-Uni) ou se sont plaints de frais de livraison supérieurs à ceux qui étaient indiqués au moment où ils ont passé commande (Turquie). Les taux sont plus élevés en ce qui concerne les problèmes de livraison (allant de 0,8 à 15,6%), mais ils restent néanmoins bas en termes absolus dans la majorité des pays.

Tableau 2: Problèmes rencontrés lors d'achats via Internet (en % de particuliers ayant commandé des biens ou services via Internet) - 2004

	DE	EL	IE	CY	LU	PT	SI	FI	UK	TR
Recours et réparations difficiles	:	2,1	2,2	6,2	2,2	:	2,2	:	3,8	6,4
Livraison de marchandises endommagées	:	:	1,3	1,6	4,9	:	3,0	:	5,1	3,9
Coûts de livraison plus élevés que ceux annoncés	:	1,9	3,6	2,1	2,1	:	1,2	1,6	3,2	4,6
Incertitude concernant les garanties	2,3	5,5	3,5	12,0	4,0	:	8,4	4,5	5,5	7,4
Prix final plus élevé que ce qui était indiqué	:	3,3	2,1	4,1	1,9	:	1,3	0,2	:	4,1
Pas de réponse satisfaisante suite à une réclamation	:	1,4	3,0	3,3	0,7	:	1,5	:	4,1	7,6
Manque de sécurité des paiements	:	0,6	1,4	1,6	1,5	:	3,7	:	:	3,1
Délais de livraison plus longs qu'indiqué	6,5	3,4	6,9	11,9	9,4	6,7	5,1	14,7	15,6	9,0
Erreur dans les marchandises livrées	4,0	:	2,7	0,8	3,2	:	1,4	3,7	10,5	1,1

Note: EI, IE, LU, UK: 2003

Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

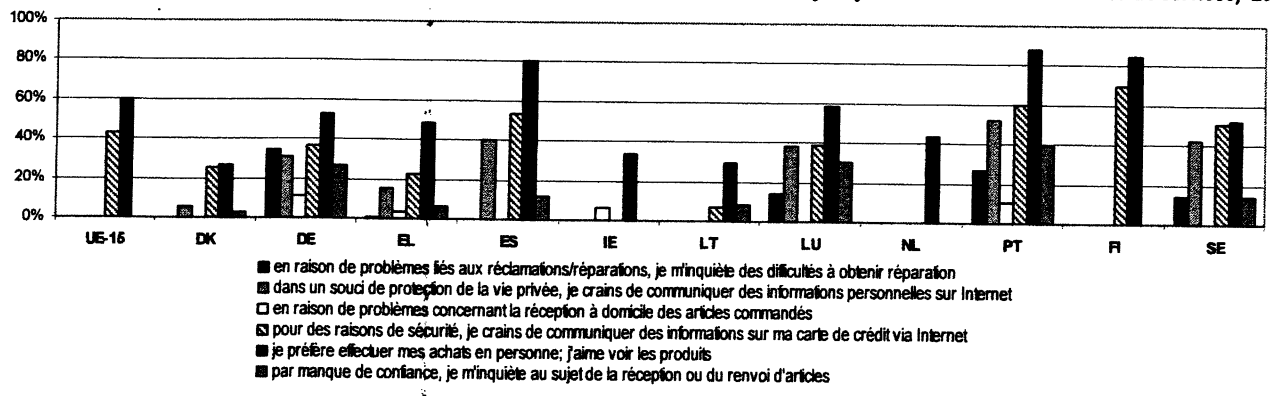
La manière dont les gens font leurs achats ne change que lentement

Même si l'adoption d'outils de communication électroniques est relativement rapide dans toute l'Europe, les habitudes de consommation n'évoluent que lentement. En effet, lorsqu'on demande aux citoyens européens pourquoi ils ne commandent pas de biens ou de services par Internet, entre 25 (Danemark) et 90% (Portugal) des particuliers interrogés répondent qu'ils préfèrent faire leurs achats en personne et voir les produits. C'est la raison qui est invoquée le plus souvent, quel que soit le pays étudié. Entre 10 (Lettonie) et 70% (Finlande) des personnes interrogées s'inquiètent des problèmes de sécurité sur Internet et hésitent à divulguer le numéro de leur carte de crédit en ligne. Des différences notables sont également constatées lorsqu'il s'agit de fournir des informations personnelles sur Internet: alors qu'au Portugal, cette raison est indiquée par 52% des internautes n'ayant jamais effectué aucun achat sur le réseau, elle ne l'est que par 5,4% au Danemark.

Le graphique 4 illustre clairement que ces trois éléments constituent les préoccupations principales dans les différents pays.

Inversement, les personnes qui n'achètent pas via Internet accordent une moindre importance aux craintes de ne pas recevoir les biens commandés à domicile ou de devoir les renvoyer. Cependant, les données disponibles suggèrent que "les problèmes liés à la réception à domicile des marchandises commandées" occupent une moindre place que les inquiétudes quant à la confiance à accorder "concernant la réception ou le renvoi d'articles". Cela laisse à penser que les problèmes potentiels en matière de garantie ainsi que l'absence fréquente de localisation géographique connue pour pouvoir échanger ou faire réparer les articles sont encore source de blocage.

Graphique 4: Raisons invoquées pour ne pas acheter via Internet (en % des particuliers n'ayant jamais commandé de biens ou de services)–2003



Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

Sécurité: prise de conscience de la nécessité d'une protection accrue

L'installation et l'utilisation d'outils de protection contre les virus, les spams, etc. sur les ordinateurs personnels se sont largement répandues dans tous les pays européens au cours des dernières années, mais des différences subsistent (voir tableau 3). Plus d'un quart des particuliers utilisateurs d'Internet ont installé des pare-feu au Danemark, en Allemagne, en Hongrie, au Royaume-Uni et en Islande. De même, les programmes de détection de virus informatiques sont couramment utilisés eux aussi: le pourcentage d'internautes qui ont installé ce dispositif au cours des 3 mois précédant l'enquête va de 18% en Lituanie à près de 60% au Luxembourg. L'Estonie constituait l'exception avec 1%.

Plus particulièrement, le pourcentage d'internautes qui ont récemment installé ou mis à jour leur logiciel antivirus (y compris la mise à jour automatique) ou un pare-feu matériel ou logiciel a dépassé 50% dans 12 des 15 pays pour lesquels des données sont disponibles, ce qui est le signe d'une sensibilisation accrue dans ce domaine. À Chypre, ce pourcentage a atteint 83%.

Les mécanismes d'authentification en ligne, tels que la signature électronique, l'emploi de codes confidentiels ou de mots de passe, sont aussi de plus en plus utilisés. La proportion d'internautes ayant eu recours à ces mécanismes récemment est particulièrement élevée en Slovénie, en Norvège, en Irlande, en Finlande et au Danemark. Inversement, l'authentification en ligne a été moins utilisée par les internautes estoniens, grecs, lituaniens et turcs.

Tableau 3: Mesures prises durant les trois derniers mois pour accroître la sécurité d'utilisation d'Internet (en % des utilisateurs d'Internet) - 2004

	"J'ai installé un programme antivirus"	"J'ai mis à jour un programme antivirus (y compris la mise à jour automatique)"	"J'ai installé ou mis à jour un pare-feu matériel ou logiciel"	"J'ai installé ou mis à jour un programme antivirus ou installé ou mis à jour un pare-feu matériel ou logiciel"	"J'ai eu recours à l'authentification en ligne (mot de passe, code PIN, signature numérique)"
DK	23,4	60,2	25,5	65,2	64,2
DE	39,1	46,4	25,3	54,5	29,1
EE	1,0	0,5	0,1	1,0	0,5
EL	43,0	30,7	13,0	52,1	18,8
IE	30,8	37,8	:	:	68,7
CY	27,9	77,0	9,9	82,5	38,5
LT	18,4	18,5	3,5	26,2	19,8
LU	58,4	57,5	:	:	41,3
HU	54,9	45,6	28,4	63,4	28,0
AT	33,8	42,0	18,5	52,3	28,0
PT	36,4	48,7	18,4	50,4	29,5
SI	37,2	48,1	13,2	57,9	81,0
FI	26,5	47,6	15,0	50,8	66,4
SE	25,4	48,1	20,5	54,2	51,0
UK	38,7	42,2	26,0	58,1	31,6
TR	26,9	23,5	7,7	31,7	10,9
IS	50,0	61,9	26,5	72,4	64,3
NO	25,5	44,0	:	:	72,1

Note: IE, LU, NO: 2003. – Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

Les actions préventives décrites plus haut sont une chose; les problèmes effectivement rencontrés en sont une autre. Ces problèmes se posent en fonction du type de pratique Internet: courrier électronique ou achats en ligne. Un des problèmes les plus fréquemment rencontrés par les internautes européens en 2004 a été la perte de données et de temps suite à une infection de leur PC par un virus (voir tableau 4). La proportion d'utilisateurs d'Internet qui ont fait l'expérience de ce genre de problème (souvent répandu par l'intermédiaire de messages électroniques contenant des pièces jointes 'infectées') a varié entre 12% en Irlande et environ 40% en Lituanie.

Le spam (courrier électronique non sollicité) représente un autre problème majeur: dans de nombreux pays, la plupart des utilisateurs d'Internet en ont fait l'expérience: 81% des internautes islandais ont déclaré qu'ils ont été victimes du spamming, et le pourcentage est nettement supérieur à 40% dans la majorité des pays pour lesquels des données sont disponibles. Quoique le problème du spamming puisse être considéré comme gênant, il n'a cependant pas les mêmes effets que les utilisations frauduleuses de cartes de paiement ou la perte d'informations.

Tableau 4: Problèmes de sécurité des particuliers, par catégorie de problème (en % du nombre de particuliers qui ont utilisé Internet au cours des 12 derniers mois) — 2004

	Usage frauduleux de carte de paiement (carte de crédit ou de débit)	Utilisation abusive d'informations personnelles transmises par Internet	Spams - j'ai reçu des courriers électroniques non sollicités	Virus informatique ayant entraîné une perte d'informations ou de temps
CZ	0,1	0,1	:	15,3
DK	1,1	1,1	54,3	30,1
DE	0,0	2,7	58,3	35,0
EE	0,1	0,0	54,4	19,6
EL	0,1	0,8	27,0	12,0
IE	0,7	2,4	:	11,6
CY	0,9	4,0	42,5	27,0
LT	0,2	0,8	34,3	39,8
LU	1,5	4,1	:	24,9
HU	0,4	1,8	45,2	34,1
AT	1,0	2,1	44,5	29,8
PT	0,0	1,4	25,2	17,5
SI	0,7	1,4	53,5	33,9
FI	0,0	4,5	46,9	26,6
SE	1,2	7,3	39,5	24,7
UK	2,4	3,3	50,6	29,8
TR	1,0	2,1	20,2	21,8
IS	2,8	3,1	80,9	26,8
NO	1,4	3,4	:	19,6

Note: CZ, IE, LU, NO: 2003

Source: Eurostat, enquête communautaire sur l'utilisation des TIC par les ménages et les particuliers.

L'usage frauduleux de cartes de paiement et l'utilisation abusive d'informations personnelles transmises par Internet sont potentiellement plus perturbateurs, car ils touchent à la sécurité et à la vie privée des personnes. Dans la plupart des cas, la part des utilisateurs d'Internet ayant été confrontés à un usage frauduleux de leur carte de paiement reste bien en-deçà de 2%, sauf en Islande (2,8%) et au Royaume-Uni (2,4%). Il convient néanmoins de noter que ce pourcentage se rapporte à tous les utilisateurs individuels, et pas seulement à ceux qui ont effectivement acheté ou commandé des biens ou des services. L'utilisation abusive d'informations personnelles transmises par Internet concerne relativement peu d'internautes: dans la plupart des pays, ce problème a été cité par moins de 4% des utilisateurs, à l'exception de la Suède où ils étaient plus de 7% à s'en plaindre.

Équipements de sécurité dans les entreprises: l'influence des coûts de mise en œuvre

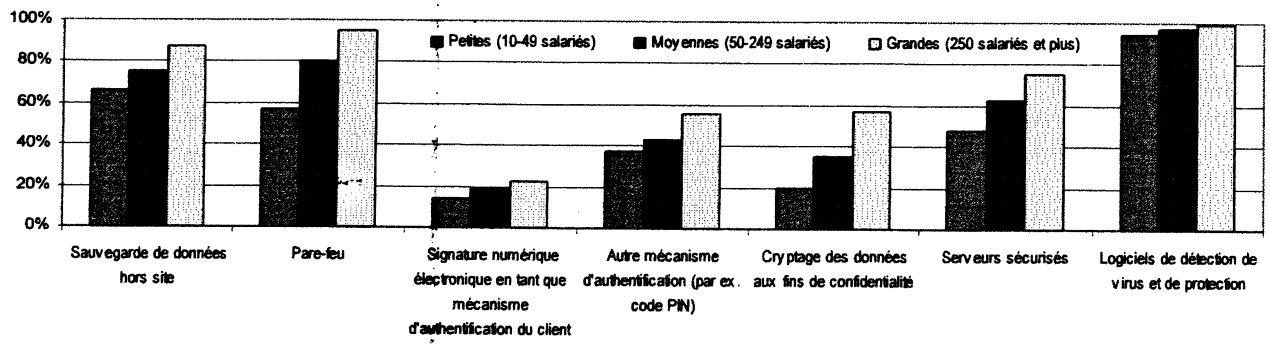
Les entreprises investissent toujours davantage (volontairement ou non) dans la sécurisation de leurs systèmes et réseaux informatiques. Les ressources financières consacrées à cette fin peuvent être considérables. Les dispositifs de protection des systèmes informatiques se répartissent en plusieurs familles, en fonction de l'élément de la chaîne de transmission des données qu'il s'agit de protéger. Que les dispositifs de protection soient plus largement utilisés par les grandes entreprises que par les petites n'est pas surprenant.

Les équipements classiques et relativement peu onéreux, tels que les logiciels de contrôle ou de protection contre les virus, sont largement répandus quelle que soit la taille de l'entreprise. À l'inverse, la signature numérique électronique comme mécanisme d'authentification est relativement récente et n'est pas encore très répandue. Les disparités liées à la taille des entreprises restent faibles.

Indépendamment de la taille de l'entreprise et abstraction faite des logiciels de détection des virus utilisés par plus de 90% des entreprises, les deux principaux systèmes de protection installés (par 60 à 80% des entreprises) sont les systèmes de sauvegarde des données et les pare-feu, bien que ces derniers soient moins courants dans les petites entreprises.

Les systèmes d'authentification, de signature électronique et de cryptage sont moins répandus, notamment en raison d'une mise en œuvre assez complexe et coûteuse. Pour ce qui est de l'installation de serveurs sécurisés, l'écart entre les petites et les grandes entreprises atteint 25%, en relation directe avec le coût et la maintenance de ce type de matériel qui sont souvent difficiles à assumer pour les petites entreprises. Néanmoins, les serveurs sécurisés continuent en général à être plus utilisés (entre 45 et 75% des entreprises) que les systèmes d'authentification et de cryptage (entre 15 et 55%).

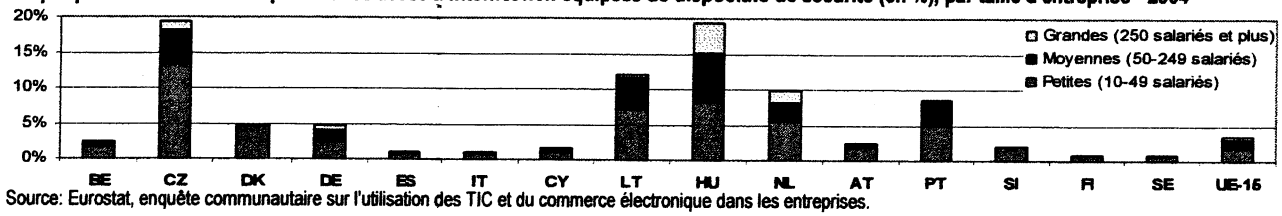
Graphique 5: Dispositifs de sécurité utilisés dans les entreprises, par taille d'entreprise et type de dispositif (en % de toutes les entreprises avec un accès à Internet) – UE-15 - 2004



Source: Eurostat, enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises.

Malgré un éventail de plus en plus large de technologies dans le domaine de la protection des ordinateurs et des réseaux, certaines entreprises n'ont toujours aucun équipement. En 2004, parmi les entreprises n'ayant installé aucun des dispositifs de sécurité cités dans la partie précédente, on comptait surtout les petites entreprises. Cette situation peut être observée dans tous les pays, mais les proportions sont particulièrement élevées en République tchèque et en Hongrie, où près de 20% des entreprises (quelle que soit leur taille) n'étaient pas équipées. Dans une moindre mesure, la Lituanie (12%), les Pays-Bas (10%) et le Portugal (8%) comptaient également une proportion relativement importante d'entreprises ne disposant d'aucun dispositif de sécurité. Ce qui est surprenant, c'est le fait que 4,3% des entreprises hongroises et 2,6% des entreprises néerlandaises font partie, à la fois, de la catégorie des 'grandes entreprises' (250 salariés ou plus) et de la catégorie 'non sécurisées'.

Graphique 6: Nombre d'entreprises avec accès à Internet non équipées de dispositifs de sécurité (en %), par taille d'entreprise - 2004



Source: Eurostat, enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises.

Attaques de virus: les différences se situent davantage entre pays qu'entre secteurs

En dépit du fait que pratiquement toutes les entreprises ont installé des logiciels de contrôle et de protection contre les virus, de nouveaux virus apparaissent régulièrement et les attaques restent monnaie courante. Si l'on considère toutes les activités sélectionnées, entre 23% (Slovaquie) et 53% (Finlande) des entreprises ont dû faire face à une attaque de virus en 2004. Au niveau des pays, tous les secteurs d'activité sont concernés et aucune 'préférence' nette pour une branche en particulier ne peut être décelée.

Il existe cependant une différence notable entre les pays pour lesquels des données sont disponibles: alors qu'en Allemagne et en Italie, entre 20 et 30% des entreprises ont été la cible d'une attaque de virus, la proportion s'est élevée jusqu'à atteindre des taux de 50 à 60% en Finlande, où de telles attaques ont été signalées bien plus souvent que dans la Suède voisine. Les entreprises néerlandaises et irlandaises ont, elles aussi, souvent été confrontées à des attaques de virus. Il convient de garder à l'esprit que ces indications reposent sur des déclarations volontaires.

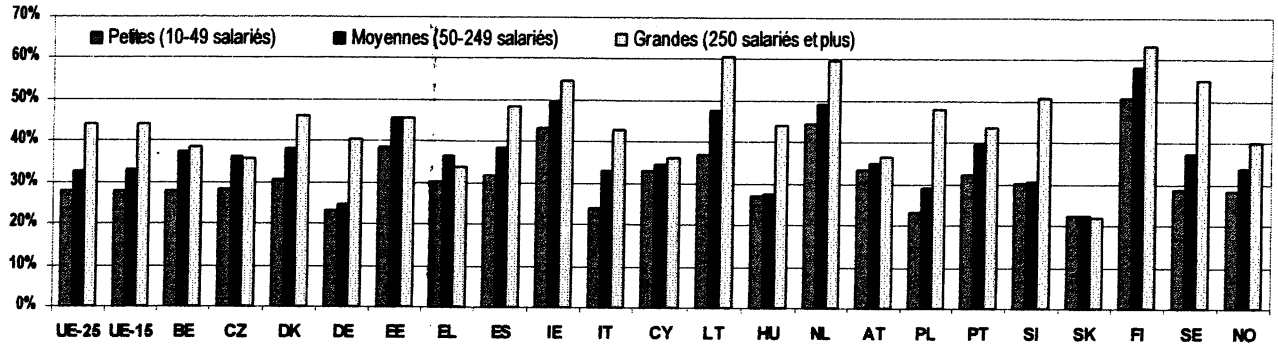
Lorsqu'on considère la taille de l'entreprise, on constate que les grandes entreprises font plus souvent l'objet d'attaques de virus. Des différences sensibles ont été observées en Allemagne, en Hongrie, en Slovénie et en Suède, où les grandes entreprises ont, à l'évidence, constitué les cibles privilégiées des attaques de virus. En Grèce, à Chypre et en Autriche, les différences sont moins marquées. En Slovaquie, les grandes entreprises ont déclaré légèrement moins d'attaques de virus que les petites entreprises.

Tableau 5: Nombre d'entreprises ayant accès à Internet et ayant été la cible d'une attaque de virus en 2004, par secteur économique (%)

	UE-25	UE-15	BE	CZ	DK	DE	EE	EL	ES	IE	IT	CY	LT	HU	NL	AT	PL	PT	SI	SK	FI	SE	NO
Industrie manufacturière	28,5	28,6	30,9	29,7	32,6	23,0	38,5	30,4	33,4	48,9	25,2	32,9	39,5	28,5	45,7	37,0	26,0	32,6	:	23,0	51,8	30,7	32,6
Construction	24,7	24,2	29,5	30,7	22,4	17,0	35,5	29,7	31,0	32,3	20,3	17,0	42,0	23,1	41,6	28,5	25,0	28,1	31,5	26,7	48,0	19,0	24,9
Commerce de gros et de détail	29,4	29,9	29,1	28,9	34,7	22,8	41,6	31,8	33,6	39,9	26,7	35,7	35,8	31,2	47,1	31,9	23,5	34,8	:	23,1	51,2	28,1	25,8
Transports et communications	29,1	29,3	24,3	27,5	32,1	25,0	39,2	34,3	30,6	50,6	25,5	42,9	43,2	28,7	45,7	29,9	22,5	27,1	:	11,9	61,2	29,1	41,5
Immobilier, location et services aux entre	31,0	31,1	30,1	31,1	36,2	23,7	40,8	32,0	35,7	47,0	26,7	41,0	49,9	28,4	46,5	35,3	30,1	40,5	:	21,8	53,0	41,1	27,3
Toutes les activités sélectionnées*	29,2	29,4	29,8	29,8	32,4	24,2	39,9	31,4	33,2	45,1	25,3	33,5	40,3	27,8	45,8	33,8	25,6	33,9	31,3	22,5	52,5	30,8	29,3

* voir les notes méthodologiques — Source: Eurostat, enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises.

Graphique 7: Nombre d'entreprises ayant accès à Internet et ayant été la cible d'une attaque de virus en 2004, par classe de taille (%)



Source: Eurostat, enquête communautaire sur l'utilisation des TIC et du commerce électronique dans les entreprises.

➢ CE QU'IL FAUT SAVOIR - NOTES MÉTHODOLOGIQUES

CODES PAYS

UE : Union européenne, comprenant les 25 États membres (UE-25) : Belgique (BE), République tchèque (CZ), Danemark (DK), Allemagne (DE), Estonie (EE), Grèce (EL), Espagne (ES), France (FR), Irlande (IE), Italie (IT), Chypre (CY), Lettonie (LV), Lituanie (LT), Luxembourg (LU), Hongrie (HU), Malte (MT), Pays-Bas (NL), Autriche (AT), Pologne (PL), Portugal (PT), Slovénie (SI), Slovaquie (SK), Finlande (FI), Suède (SE) et Royaume-Uni (UK).
UE-15 : Union européenne, comprenant 15 États membres (BE, DK, DE, EL, ES, FR, IE, IT, LU, NL, AT, PT, FI, SE, UK).
TR: Turquie – IS: Islande – NO: Norvège

SYMBOLES

":" données non disponibles ou confidentielles.

SOURCES DES DONNÉES

Enquête sur l'utilisation des TIC dans les ménages.
En 2004, 75 016 ménages et 136 452 particuliers ont été interrogés dans les États membres.

Unité d'échantillonnage : ménages et particuliers
Limite d'âge inférieure pour l'enquête sur les particuliers: 16 ans
Limite d'âge supérieure pour l'enquête sur les particuliers : 74 ans
Période de référence: premier trimestre 2004.
Les données individuelles se rapportent aux 3 mois précédant l'enquête.
Pondération des résultats: les résultats ont généralement été pondérés par le nombre de ménages et le nombre de particuliers. Les calculs de données UE-25 et UE-15 ont également été effectués en utilisant la même procédure de pondération à partir des données disponibles.
Niveau d'éducation:
– bas: (CITE 1 et 2) enseignement primaire et enseignement secondaire inférieur, ces deux stades représentent normalement l'enseignement obligatoire,
– moyen: (CITE 3 et 4) enseignement secondaire supérieur et post-secondaire non supérieur, ce niveau commence généralement à la fin de l'enseignement obligatoire;
– supérieur: (CITE 5 et 6) programmes d'enseignement supérieur exigeant normalement l'achèvement des niveaux CITE 3 ou 4, et enseignement supérieur de second cycle conduisant à un titre de chercheur hautement qualifié.

Date d'extraction des données: 1 février 2005

Enquête sur l'utilisation des TIC dans les entreprises.
En 2004, 99 069 entreprises ont été interrogées dans les États membres participants.

Période de référence: premier trimestre 2004.
Pondération des résultats: les résultats ont généralement été pondérés par le nombre d'entreprises.
Classes de taille couvertes: entreprises de 10 salariés ou plus.
Ventilations par classe de taille:
petites entreprises – 10-49 salariés,
moyennes entreprises – 50-249 salariés,
grandes entreprises – 250 salariés et plus.

Date d'extraction des données: 1 février 2005

REMARQUES SPÉCIFIQUES

Tableau 5: Part des entreprises ayant accès à Internet et ayant été la cible d'une attaque de virus en 2003, par secteur économique (%)
Le terme 'toutes les activités sélectionnées' couvre les sections suivantes de la NACE:

NACE D :	Industrie manufacturière
NACE F :	Construction
NACE G :	Commerce de gros et de détail
NACE H :	Hôtels et restaurants (uniquement les groupes 55.1 (Hôtels) et 55.2 (Exploitation de terrains de camping et autres moyens d'hébergement de courte durée)
NACE I :	Transports et communications
NACE K :	Immobilier, location et services aux entreprises
NACE O :	Services collectifs, sociaux et personnels (uniquement les groupes 92.1 (Activités cinématographiques et vidéo) et 92.2 (Activités de radio et de télévision))

AUTRES PUBLICATIONS RÉCENTES SUR LA SOCIÉTÉ DE L'INFORMATION:

- Statistiques en bref 18/2005 – Utilisation d'Internet par les individus et les entreprises en 2004
- Statistiques en bref 09/2005 – e-Gouvernement: le lien Internet avec les entreprises et les citoyens européens
- Statistiques en bref 45/2004 – Clivage régional dans la société de l'information

PUBLICATIONS PRÉVUES:

- Panorama de la Société de l'Information en Europe
- Publications dans la série "Statistiques en bref" sur *les activités faites sur l'Internet*, sur *le commerce électronique*, sur *l'e-gouvernement*, sur *la fracture numérique* et sur *les différences sectorielles en termes de l'utilisation des TIC par les entreprises*

Pour en savoir plus:

Les bases de données

Site web EUROSTAT/Industrie, commerce et services/Statistiques sur la société de l'information

Site web EUROSTAT/Population et conditions sociales/Statistiques sur la société de l'information

Site web EUROSTAT/Science et technologie/Statistiques sur la société de l'information

---

Les journalistes peuvent contacter le service média support :

Bâtiment BECH, Bureau A4/017
L - 2920 Luxembourg

Tel. (352) 4301 33408
Fax (352) 4301 35349

E-mail: eurostat-mediasupport@cec.eu.int

European Statistical Data Support:

Eurostat a mis en place, conjointement avec les membres du "Système statistique européen", un réseau de centres d'appui, qui couvrira presque tous les États membres et certains pays de l'AELE.

La mission de ces centres sera d'aider et d'orienter les utilisateurs qui se procureront des données statistiques européennes sur l'internet.

Vous trouverez sur notre site internet des informations sur ce réseau de centres d'appui:
www.europa.eu.int/comm/eurostat/

Une liste des bureaux de vente dans le monde est disponible à :
l'**Office des publications officielles des Communautés européennes.**

2, rue Mercier
L - 2985 Luxembourg

URL: http://publications.eu.int
E-mail: info-info-opoce@cec.eu.int

UNITED NATIONS EDUCATIONAL,
SCIENTIFIC AND CULTURAL ORGANIZATION

International Conference on Freedom of Expression in Cyberspace

Paris, France
3-4 February 2005

UNESCO Thematic Meeting for the Preparation of the Second Phase of the World Summit on the Information Society (WSIS)

Report

Table of Contents

Report

(a) Date and Place

1. The **International Conference on Freedom of Expression in Cyberspace** was held in **Paris, France, on 3-4 February 2005.**

2. The meeting was hosted by UNESCO and it was organized by the Division of Freedom of Expression, Democracy and Peace, Communication and Information Sector (CI/FED).

(b) Participants

3. The meeting was attended by about 200 participants, representing journalists, publishers, other media professionals, academics, NGO and civil society activists as well as a large number of official representatives of Member States of UNESCO.

4. The meeting was chaired by Director-General Koïchiro Matsuura, Assistant Director General for Communication and Information Abdul Waheed Khan (ADG/CI) and by Mogens Schmidt, Deputy Assistant Director General for Communication and Information (DADG/CI).

5. The Rapporteur of the meeting was Mr. Mogens Schmidt, DADG/CI

6. Panelists included the following experts:

Keynote Speakers

1. **Mr Sandy Starr,** Spiked Ltd, United Kingdom
2. **Ms Helen Darbishire,** Director, Freedom of Information & Expression Program, Open Society Justice Initiative, USA
3. **Mr Miklos Haraszti,** OSCE Representative on Freedom of the Media, Austria
4. **Mr Gus Hosein,** London School of Economics ; Privacy International, UK

Panelists

5. **Ms Sjoera Nas,** Bits of Freedom, The Netherlands
6. **Ms Agnes Callamard,** Executive Director, Article 19, UK
7. **Mr Roberto Saba,** Executive Director, Association for Civil Rights, Argentina
8. **Ms Jane Kirtley,** Director, Silha Center for the Study of Media Ethics and Law, School of Journalism and Mass Communication, University of Minnesota, USA
9. **Mr Indrajit Banerjee,** Secretary-General, Asian Media Information and Communication Centre (AMIC), Singapore
10. **Mr Geoffrey Robertson,** Legal officer, Doughty Street Chambers, UK
11. **Mr Youri Oulianosvky,** ITAR-TASS Representative office in France; Russia
12. **Mr Julien Pain,** Reporters sans frontières, France

13. **Mr Yaman Akdeniz**, CyberLaw Research Unit, Centre For Criminal Justice Studies, University of Leeds, UK
14. **Mr Ronald Koven,** European Representative, World Press Freedom Committee
15. **Mr Chris Kabwato,** Director, HighWay Africa

(c) Objectives

7. The meeting was organized as a thematic meeting for the preparation of the second phase of the World Summit of the Information Society. Its objectives were developed in relation to Paragraphs 4, 55 and 56-69 of the Declaration of Principles adopted by the World Summit on the Information Society (WSIS) in December 2003 in Geneva, Switzerland, and aimed in particular at contributing to Paragraph 24 of the WSIS Action Plan dealing with freedom of expression in Cyberspace.

8. In addition, the meeting aimed at further promoting, discussing and raising awareness of freedom of expression in Cyberspace in general and on the Internet in particular.

(d) Agenda

9. The agenda of the meeting included the following items: (full agenda in Annex I)

- Freedom of Expression on the Internet
- Between Security and Openness. Should There be Limits to Freedom of Expression and Freedom of Information
- Open Internet – Open Media
- Freedom of Expression, Codes and Creativity

Report and recommendations

The conference was organized based on the UNESCO mandate and firm belief that the free flow of information is a fundamental premise of democratic societies where individual freedom is respected and honoured. As embodied in Article 19 of the Universal Declaration of Human Rights, freedom of expression and information must be promoted without exception; this also implies in new media. Freedom of expression is an individual right and the implementation of it is a precondition for a democratic society A corresponding recognition of freedom of expression has been expressed by the WSIS in the Declaration of

Principles, paragraphs 4, 55 and 56-59 and Action Plan, paragraph 24 adopted during the Summit of the first phase of the WSIS in Geneva, December 2003

Furthermore, the conference took its departure from UNESCO's declaration of four principles that must be guiding the development of knowledge societies and that are direct consequences of the organisation's mandate, freedom of expression, universal access, cultural and linguistic diversity, and quality education for all.

As was made clear by the Director General of UNESCO, **Mr. Koïchiro Matsuura** in his opening speech to the conference, the first and most fundamental of these is the principle of freedom of expression, which must apply not only to traditional media but also to new media, including those distributed via the Internet. The challenges of creating inclusive knowledge societies in which all have the chance to participate, be they in the developed or in the developing world, be they man or woman, old or young, rich or poor, is inseparable from ensuring freedom of expression in cyberspace. What kind of universality would it be if censorship were to rule the Internet and what would universal access mean if it were access to only some information, only some ideas, only some images, only some knowledge? Furthermore, how long can knowledge economies prosper or even function, especially in a competitive global environment, if they are starved of ideas and information, asked Mr. Matsuura, and continued, how can knowledge societies become or remain democratic if their citizens are misinformed or ill-informed? How can knowledge societies be secure if the bonds of social identity and belonging are broken by fear, distrust and mutual ignorance?

In both industrialized and developing countries, new digital technologies have the potential to strengthen the institutions of representative democracy and civil society, to enable citizens to gather information and mobilize coalitions around policy issues, and to improve government efficiency and transparency through better communication with citizens.

In cyberspace everybody can be a content provider; the Internet is a vast and in principle unlimited information and communication network and this potential must be realized. The Internet is fast and simple to use. It also reaches much beyond traditional news content and whole new "media outlets", the bloggers, have been developed. Probably it is exactly these

features, together with the speed and the global character of the Internet that has made so many governments worry about granting all citizens full access to the whole World Wide Web.

There is still far to go. In her presentation, **Agnes Callamard** drew attention to the fact that while North America holds 6% of the world population and 41% have on-line access to the Internet, less than 1% of the African population, which is 10% of the world's population, has the same. Furthermore, the 29 OECD states contain 97% of all Internet hosts, 92% of the market in production and consumption of IT hardware, software and services, and 86% of all Internet users. The digital divide is a reality and concerted and targeted efforts are needed to bridge it. All such efforts must however be put in the context of freedom of expression and universal access in order to seriously address global poverty, democratic governance and sustainable development.

The conference agreed that with the rise of the Internet, the fundamental right to freedom of expression is challenged in new ways. The global net holds great potential as a resource for free distribution and reception of information and the creation of dialogue across borders and cultures; however, these qualities may sometimes be undercut by attempts to regulate both access and content. Tools for regulating cyberspace are increasing, as is the impact of the Internet. Even in democratic countries, violations of freedom of expression are growing, and the need to discuss how to prevent undesired side effects of new regulation techniques has become urgent. The press meets barriers on the Internet that would and should not be accepted in traditional media. Free media are essential in creating development and prosperity and in upholding democratic societies and should be hindered neither on a local nor on a global level. A great risk is posed by the institutionalization of constraint, especially in the formative stages of new social development. This is why deliberate restrictions imposed upon the free flow of information are so damaging. Short-term and short-sighted decisions today are perhaps compromising our capacity for effective decision-making tomorrow.

Still, the Internet is through its very architecture a robust, flexible and very resourceful invention that allied with human ingenuity and creativity – and the human instinct for

freedom – will prove to be very resilient and will develop in ways that were unimaginable just a few years ago. This is important to bear in mind when discussing the many challenges before us.

The debate on freedom of expression as an absolute human right does not take place in a vacuum and there are legitimate discussions needed to nuance the very complex legal and practical wickerwork of cyberspace regulations and governance. How for example to assure the protection of Article 19 while respecting individual privacy, national laws and at the same time promoting cultural and linguistic diversity in the global network? How to establish special laws to block Internet sites which are considered to offer ways of obtaining information contrary to certain political, sexual, or moral standards or legislative acts that deal with security or confidentiality laws to protect personal data? How to address cyber crime in all its aspects? Another difficult challenge is the connection between the Internet and protection against terrorism. The balance between measures required for fighting terrorism and respect for fundamental human rights, especially the right to information, is indeed very difficult to find.

The four panels set out to deal with these specific items in four panel discussions.

In the introductory session on Freedom of Expression on the Internet, **Sandy Starr, Agnes Callamard** and **Sjoera Nas** dealt with elements related to the fact that the Internet provides great opportunities to facilitate the use of the freedom rights at low costs and without the obstacles of access and economic barriers common to traditional mass media in the interest of development of prosperity. Still, the Internet is not free of obstacles. **Sandy Starr** took his point of view in the libertarian tradition where freedom of expression is non-negotiable and absolute. He warned against many of the regulation and co-regulation initiatives being advocated as he found that enforcing rights leading to restrictions often came from good motives. He also warned against any legislation trying to oppose hate-speech as such legislation inevitably would create a grey zone that could be abused by those parties in society that wanted to curtail freedom of expression. **Sjoera Nas** listed a series of issues that legislators legitimately would have to deal with at the same time as they should respect all fundamental freedoms as laid out in the UDHR. She underlined that online freedom of

expression starts with offline respect for human rights, including privacy and the right to a fair trial; she mentioned privacy issues, intellectual copy-right issues to avoid piracy on the Internet, spam and RFID. She warned against the fact that many commercial parties, most notably Internet providers were de facto put in a position, often through co-regulation measures, that they should exercise legal assessments on the content they put on the net for third parties. To avoid the haphazardness this could imply she strongly advocated for a set of basic international rules to guide the responsibilities of commercial Internet providers. In this context, transparency is crucial and all ISPs should be obliged by law to publish their rules for notice and take-down as well as yearly statistics about the number of requests and the resulting actions. **Agnes Callamard** stressed the digital divide while pointing to the fact that the divide is not just about technology and thus cannot be addressed by technology solely. Indeed, she said, showering of developing countries with technological gifts might further increase their dependence on the technology and the providers of the industrialized countries. She underscored that freedom of expression is not just about expression but also comprises the right to seek and receive information from others, including the right to freely obtain and read newspapers, to listen to broadcasts, to surf the Internet and to participate in discussions in public and private as a listener. She stressed the right to access publicly held information (freedom of information). She advocated a right to communicate that included access to diverse and pluralistic media; equitable access to the means of communication as well as to the media; the right to use the language of one's choice; the right to participate in the public decision-making process; the right to access information, including from public bodies; the right to be free of undue restrictions on content; and privacy rights.

The second panel, called Between Security and Openness. Should there be Limits to Freedom of Expression and Freedom of Information?, had interventions by **Helen Darbishire**, **Roberto Saba**, **Jane Kirtley**, and **Indrajit Banerjee** and asked the question whether there are any situations that legitimate limiting openness, such as security issues and the threat of terrorism and insecurity, at the expense of freedom of expression and freedom of information? **Helen Darbishire** also stressed the human rights base for all legal frameworks necessary to regulate the Internet. She pointed to the dangerous trend after September 11 where several traditional democracies had compromised the freedom of expression. She underlined that it is the obligation of governments to both defend freedom of expression and

to protect the exercise of this right by all individuals. Much greater efforts must be made in focussing on defining and strengthening governmental obligations with regard to this right. Equally important is to ensure the legal underpinning of the commercial dimensions of cyberspace. Internet providers, for instance, should not be empowered to make decisions amounting to censorship, outside any due process, transparency, and legal framework. The current practice is unaccountable and seriously compromises self- and co-regulation systems. She elaborated further on freedom of information acts and announced a global campaign for ensuring citizens' access to publicly held information. **Roberto Saba** explained how the freedom of information acts had been passed in Argentina and how these acts also comprised online material. He understood access as a non-negotiable human right that should be protected and referred to several decisions of the Inter-American Court. **Jane Kirtley** also took her departure in the changes to fundamental freedoms in the US after 9/11. One would expect that information in digital form would be easier to achieve but that was not the case in the US as Congress had passed limiting amendments to the Freedom of Information Act. She appealed to governments to disclose public interest information to ensure a working participatory democracy. The last panellist, **Indrajit Banerjee**, explained how many countries in Asia were still keeping media un-free; particularly Internet media and how it was still basically governments that were censuring access to the Internet for ordinary citizens. He acknowledged the need for regulation and control when it came to issues of national security but warned against using this as a pretext to exercise even stronger censorship on the media. It was the overall feeling that when needed special national legislation and international police considerations that put restrictions on freedom of expression must be made public so that the authorities can be held accountable.

The speakers in the third panel, Open Media - Open Internet, were **Miklos Haraszti, Geoffrey Robertson, Yuri Oulianovsky**, and **Julien Pain**. They concentrated on news and information media and agreed that free media have imperative significance for democratic societies, ensuring an informed public and facilitating the free flow of information. Freedom of the press is an application of the individual human rights principle of freedom of expression and has a long history. It is however still far from being implemented all over the world. **Miklos Haraszti** gave examples of how, both in traditional and new media, journalists are meeting major challenges when trying to uphold the right to press freedom,

particularly on the increasingly important platform of the Internet. He gave a comprehensive overview of the historic developments in Central and Eastern Europe and concluded that in spite of the many obstacles still existing to fully fledged freedom of the press, huge progress has been made. Earlier, the media were state owned and governments exercised strict control. Today, many media outlets were privately owned and most of these functioned professionally according to reasonable professional standards. More so, there was a beginning understanding of what public service media really implies, also when it comes to ensure freedom of expression in cyberspace. Media are not just commercial outlets and should not be treated like that by their proprietors; media are first of all important channels for the democratic debate. **Geoffrey Robertson**, who is one of the world's leading experts in media legislation, gave some concrete examples of the new legal challenges, the Internet has raised for mass media, especially for internationally oriented media. There were still many attempts to restrict information by simply trying to shut off access the same way as before cows were kept by shutting the gate; but in today's high-tech globalized media environment this would have no lasting effect. He also discussed the country-of-origin legal issue that is still not clarified and he strongly advocated that any legal process against Internet media should be established in the country where the content originated. He also warned against establishing just one set of laws and one regulatory framework for both the media's use of Internet and private individual usage. It is essential that Internet media are granted the same freedoms as print and broadcast media. Likewise, it is important to differentiate limits on freedom of expression of private information and access to public information. The Internet actually provides for cheap and speedy rebuttal procedures. He found the online right to reply a reasonable way forward, also because of the high libel costs. **Youri Oulianovsky** gave an overview of the challenges that traditional news agencies have had to comply with when developing into Internet based media. Internet operations were much cheaper and faster but the risk in the Internet press agencies was that traditional validation of sources was discharged in order to keep up with the speed. He also explained how the 24-hours a day dead-lines were detrimental to the quality of journalism. He warned against unprofessional so-called media outlets on the Internet and many of the news bloggers that did not provide seriously vetted information. He also informed about the fast leap forward in Internet usage in Russia. He showed understanding for governments wanting to exclude certain sites from the net, like in Russia sites that were promoting separatist Chechen interests and in France,

sites that were promoting Nazism. **Julien Pain** was very critical towards the Russian attempts to cut off access to Chechen Internet sites and he described how similar censorship manoeuvres were being put to work in many countries all over the world. He particularly mentioned Tunis as he found it regrettable that the host country for the second phase of the WSIS did not allow for full freedom of expression on the Internet. He encouraged all press freedom institutions and UNESCO to be steadfast in defending the principle of freedom of expression. He also wanted freedom of the press to comprise the new generation of bloggers. As it was now, they were very exposed to violations from the side of censuring governments. Despite the problem some of them had living up to established professional standards for good journalism, they should be protected like any journalist from Le Monde or The Financial Times.

Finally, the last session, called Freedom of Expression, Codes and Creativity, looked at the Internet's decentralized structure, which provides a unique platform for every kind of user to contribute to the production of content and to make use of their right to freedom of expression and which should be safeguarded in any Internet governance system. The four speakers, **Gus Hosein**, **Yaman Akdeniz**, **Chris Kabwato**, and **Ronald Koven** all warned against using the term "harmful content" as an excuse for new regulation of content, not least because it will be extremely difficult to establish solid definitions hereof. **Gus Hosein** also drew attention to the fact "harmful content" is something quite different than "illegal content", which is clearly defined by national and/ or international legislation and against which stake holders need to take appropriate measures. Still, he argued, it was much more important to make efforts to foster creativity on the Internet and to stimulate and promote local content production. Hosein focussed on the paradox of the Internet: never before has the world seen such a powerful information and communication mechanism that was cheap and easy to use and that had a huge potential in the fight against poverty, but at the same time, many governments, including those of the developing countries, concentrated their efforts on restricting and regulating this mechanism with the result that its potential could not be realized. He especially identified two areas that gave reason for concern: the weakening of legal protections of both freedom of expression and – at the other end of the scale – the right to privacy; the surveillance chill reaching from mobile phone tracking to Internet cookies and public cameras. The real challenge is to fully exploit the potential of the

Internet while not compromising civil liberties. **Chris Kabwato** spoke from the point of view of the developing countries and he agreed strongly with **Mr. Hosein** in the identification of the potential of the Internet for creating knowledge societies and for giving voice to indigenous societies. He warned governments of developing countries of giving in to the "contrary spirit" dominated by the fears of the net: fear of technology and fear of free and public debate in the public sphere. On the contrary, one should encourage the development of technical standards for digitally processing local or international languages on the Internet. He commended UNESCO for the Organisation's firm stand for freedom of expression during the WSIS process and for its assistance in adopting the Marrakech Declaration, which he quoted extensively. He also described how Internet creativity and cultural diversity must find a new and internationally accepted interface with existing intellectual property rights agreements by balancing the moral and economic interests of the creators on the one hand and the provision of access to the socio-economic and cultural benefits of such creativity world-wide on the other hand. Finally, he promoted open source and free software, as it was not only cheaper for developing countries but also did not create the same degree of expert dependence as proprietary software. Journalists, knowledge workers, artists and teachers want the space, freedom and platform to share their stories, ideas and experiences, he said, and the Internet can be such a space and platform if it can be freed from the increasing usurpation of corporate interests and the increasing regulations and restrictions by anxious governments. **Yaman Akdeniz** also underlined the decisive distinction between illegal and harmful content and warned against assigning any legal status to the latter. Illegal content is criminalized by national laws while what is defined as harmful content is considered as offensive or disgusting by some people, but is generally not criminalized by national laws. Child pornography, for instance, falls under the illegal content category while adult pornography, in those countries where it is not forbidden by law, falls under the harmful content category. He listed the various responses to both illegal and harmful content: first of all, government regulation, and secondly, self- and co-regulation. The government regulation includes laws at the national level, directives and regulations at the supra-national level (European Union or conventions of the Council of Europe, for example) and UN-level. Self and co-regulation comprises measures such as development of hotlines, codes of conduct, filtering software and rating systems. Although self and co-regulation can provide less costly, more flexible and often more effective alternatives to

prescriptive government legislation, there are a number of problems connected to their functioning. Firstly, they do not apply to all organisations or enterprises; secondly, only a very limited range of sanctions is available in case of breach of rules; and finally, one may question the accountability and impartiality of self-regulatory bodies. For filtering software the problems are even bigger. Most often, the filters cause massive over-blocking leading to both wished and not-wished censorship. A credible self and co-regulation system can only work if it is based upon respect for fundamental human rights such as freedom of expression and privacy and has a strong external consultation and involvement with all relevant stakeholders in the design and operation of the scheme; furthermore the scheme must be based upon clear and intelligible statements of principles and measurable standards, which address real consumer and user concerns. **Ronald Koven** warned against all kind of regulation of the flow of information. He mentioned that codes of conduct and co-regulation measures might be established with the best intentions but that they in the real world often turned against the fundamental freedoms. He also questioned whether keep inter-governmental bodies such as the Council of Europe labelled as self-regulation was in reality different from restrictions inflicted on freedom of expression and freedom of the press. He had no confidence in enforcing journalistic standards and ethics through legislation. Ethics are by definition freely adopted by a category of persons. Once they are embodied in laws, rules or regulations, they can no longer be described as ethics and they become part of a legal system that the group of practitioners no longer has the freedom to interpret and apply for itself. He commended UNESCO for having been firm on stating that ethical standards is something which is completely up to the various groups of professionals to define and develop. He strongly advocated the view that there is no need for any special legislation for the Internet media. There are in fact, he said, a number of existing constraints on freedom of expression in the offline world, such as copyright and other intellectual property arrangements, libel and defamation laws, laws against fraud and other criminal activities, like the sexual abuse of children. Such existing laws in legally developed jurisdictions need only to be adapted and applied to cyberspace. He agreed with **Geoffrey Robertson** on which jurisdiction should get to try offences: it should normally be in the country where the alleged offence is first published, in keeping with the position that press freedom groups and the lawyers who work in this field have generally favoured. Finally, he warned strongly against

introducing new systems for Internet governance that would impede on freedom of expression and the free flow of information.

Closure

Being an experts' meeting, no official Declaration was adopted by the participants, but there was a strong endorsement of the four principles that lay the base for UNESCO's concept of knowledge societies and for assigning to Internet media the same freedoms as print and broadcast media have. The conference was also in agreement to warn against looking at possible necessary Internet regulation as a question of balancing different human rights against each other. Like the rule of law, the Internet should be based upon full human rights, and it is the responsibility of all states to respect and defend these rights when it comes to their application for cyberspace. This message should be clearly included in any new declaration from the countries participating in the WSIS process. Finally, the participants encouraged the development of guidelines that could ensure legal underpinning of commercial Internet enterprises, in particular Internet service providers, and to examine how international legal systems that did not infringe on freedom of expression could be established to minimize spam.

The meeting was concluded by the Assistant Director General for Communication and Information, **Abdul Waheed Khan**, who expressed UNESCO's gratitude to the speakers and the participants and promised that the Organization would continue along the route that had been laid out and that was commended by the conference. It is part of UNESCO's mandate to provide a platform for open discussion and to promote the free flow of ideas, he said, and went on that this is exactly what has been happening over the last two days. The debate has contributed to clarify some of the complex challenges that the international community has to address in order to ensure that free, open and inclusive knowledge societies may flourish, grounded upon the universal principle of freedom of expression. He strongly underlined that the Internet media, as traditional media which still plays maybe the most important

role in the developing world, first of all could play an important role in fighting poverty and encouraging human creativity by contributing to the development of democratic knowledge societies. Along this line, community radio and community multimedia centres must receive greater attention and focus as crucially important communication and information tool in developing communities, bringing them together.

Annex I: Agenda

Programme:

Thursday 3 February

3-3.30pm	Official Opening by Mr. Koïchiro Matsuura, Director-General, UNESCO
3.45-6pm	**Session 1: Freedom of Expression on the Internet** Keynote speech: ▪ Mr Sandy Starr, Spiked Ltd, United Kingdom Chair: ▪ Mr Mogens Schmidt, Deputy Assistant Director-General, Communication and Information Sector, UNESCO Panel: • Ms Agnes Callamard, Executive Director, Article 19, UK • Ms Sjoera Nas, Bits of Freedom, The Netherlands
6pm	Reception

Friday 4 February

9-11am	**Session 2: Between security and openness. Should here be limits to freedom of expression and freedom of information?** Keynote speech: ▪ Ms Helen Darbishire, Director, Freedom of Information & Expression Program, Open Society Justice Initiative, USA Chair: ▪ Ms Elizabeth Longworth, Director, Information Society Division, UNESCO Panel:

- Mr Roberto Saba, Executive Director, Association for Civil Rights, Argentina
- Ms Jane Kirtley, Director, Silha Center for the Study of Media Ethics and Law, School of Journalism and Mass Communication, University of Minnesota, USA
- Mr Indrajit Banerjee, Secretary-General, Asian Media Information and Communication Centre (AMIC), Singapore

11.15am-1pm

Session 3: Open Internet – open media

Keynote speech:

- Mr Miklos Haraszti, OSCE Representative on Freedom of the Media, Austria

Chair:

- Mr Marcello Scarone, Division for Freedom of Expression, Democracy and Peace, UNESCO

Panel:

- Mr Geoffrey Robertson, Legal officer, Doughty Street Chambers, UK
- Mr Youri Oulianosvky, ITAR-TASS Representative office in France; Russia
- Mr Julien Pain, Reporters sans frontières, France

Lunch

3-5pm

Session 4: Freedom of expression, codes and creativity

Keynote speech:

- Mr Gus Hosein, London School of Economics; Privacy International, UK.

Chair:

- Mr Mogens Schmidt, Deputy Assistant Director-General, Communication and Information Sector, UNESCO

Panel:

- Mr Yaman Akdeniz, CyberLaw Research Unit, Centre For Criminal Justice Studies, University of Leeds, UK
- Mr Chris Kabwato, Director, Highway Africa, South Africa
- Mr Ronald Koven, European Representative, World Press Freedom Committee, France

5.15-6.15pm

Closing session:

- Mr Abdul Waheed Khan, Assistant Director-General for Communication and Information Sector, UNESCO

I TESTI UFFICIALI DEL WSIS

Vertice mondiale sulla società dell'informazione

Ginevra 2003 – Tunisi 2005

Documento WSIS-03/GINEVRA/DOC/4-f

12 maggio 2004

Dichiarazione di principi

Costruire la società dell'informazione: una sfida mondiale per il nuovo millennio

A La concezione comune della società dell'informazione

1 **Noi, rappresentanti dei popoli del mondo, riuniti a Ginevra dal 10 al 12 dicembre 2003 per la prima fase del Vertice mondiale sulla società dell'informazione,** proclamiamo la nostra comune volontà e determinazione di edificare una società dell'informazione a dimensione umana, inclusiva e volta allo sviluppo, una società dell'informazione nella quale ognuno abbia la possibilità di creare, ottenere, utilizzare e condividere l'informazione e la conoscenza e nella quale gli individui, le comunità e i popoli possano mettere in opera tutte le loro potenzialità, favorendo il loro duraturo sviluppo e migliorando la qualità della vita, in conformità alle finalità e ai principi della Carta delle Nazioni Unite, e rispettando pienamente e applicando la Dichiarazione universale dei diritti dell'uomo.

2 **La sfida** per tutti noi consiste nel trarre vantaggio dalle possibilità offerte dalle tecnologie dell'informazione e della comunicazione (TIC) a favore degli obiettivi di sviluppo enunciati nella Dichiarazione del Millennio, vale a dire eliminare, l'estrema povertà e la fame, dispensare a tutti l'insegnamento primario, favorire la parità fra uomini e donne e rendere le donne autonome, lottare contro la mortalità infantile, migliorare la salute delle madri, combattere l'AIDS, la malaria e altre malattie, assicurare un ambiente duraturo ed elaborare dei partenariati mondiali per giungere a uno sviluppo favorevole all'instaurazione di un mondo più pacifico, più giusto e più ricco. Noi rinnoviamo anche il nostro impegno ad arrivare a uno sviluppo duraturo, a raggiungere gli obiettivi di sviluppo definiti nella Dichiarazione di Johannesburg, nel suo piano di applicazione e nel Consenso di Monterrey, come in altri testi scaturiti da specifici vertici delle Nazioni Unite.

3 **Noi riaffermiamo** l'universalità, l'indivisibilità e l'interdipendenza di tutti i diritti dell'uomo e di tutte le libertà fondamentali, compreso il diritto allo sviluppo consacrato dalla Dichiarazione di Vienna, come anche l'esistenza di stretti legami fra

loro. Riaffermiamo inoltre che la democrazia, lo sviluppo duraturo e il rispetto dei diritti umani e delle libertà fondamentali, come la buona amministrazione a tutti i livelli, sono dei principi interdipendenti che si rafforzano reciprocamente. Noi ci impegniamo anche a sviluppare il rispetto del primato del diritto negli affari internazionali e nazionali.

4 **Noi riaffermiamo** che, come fondamento essenziale della società dell'informazione e come stabilisce l'articolo 19 della Dichiarazione universale dei diritti dell'uomo, ogni individuo ha diritto alla libertà d'opinione e d'espressione, cosa che comporta il diritto di non essere molestati per le proprie opinioni e quello di cercare, ricevere e diffondere, senza limiti di frontiere, le informazioni e le idee, con qualunque strumento d'espressione. La comunicazione è un processo sociale fondamentale, un bisogno essenziale dell'essere umano e la base di tutta l'organizzazione sociale. E' il cardine della società dell'informazione. Ogni persona, ovunque nel mondo, dovrebbe avere la possibilità di partecipare alla società dell'informazione e nessuno dovrebbe essere privato dei vantaggi che essa offre.

5 **Noi riaffermiamo** anche la nostra fedeltà alle disposizioni dell'articolo 29 della Dichiarazione universale dei diritti dell'uomo, vale a dire che l'individuo ha dei doveri nei confronti della comunità, solo nella quale è possibile il libero e pieno sviluppo della propria personalità, e che nell'esercizio dei propri diritti e nel godimento delle proprie libertà, ogni individuo è sottoposto solo ai limiti stabiliti dalla legge unicamente per assicurare il riconoscimento e il rispetto dei diritti e delle libertà altrui e per soddisfare le giuste esigenze della morale, dell'ordine pubblico e del benessere generale in una società democratica. Questi diritti e queste libertà non possono in alcun caso essere esercitate con spirito contrario alle finalità e ai principi delle Nazioni Unite. Noi, pertanto, incoraggiamo una società dell'informazione nella quale sia rispettata la dignità umana.

6 Fedeli allo spirito della presente Dichiarazione, **noi rinnoviamo il nostro impegno** a difendere il principio dell'uguaglianza sovrana di tutti gli Stati.

7 **Noi riconosciamo che la scienza** svolge un ruolo fondamentale nello sviluppo della società dell'informazione. Molti degli elementi costitutivi della società dell'informazione scaturiscono dai progressi scientifici e tecnici resi possibili dalla condivisione dei risultati della ricerca.

8 **Noi riconosciamo** che l'istruzione, la conoscenza, l'informazione e la comunicazione sono alla base del progresso, dello spirito d'impresa e del benessere della persona umana. Le TIC, pertanto, hanno un'incidenza grandissima su quasi tutti gli aspetti della nostra vita. La rapida evoluzione di queste tecnologie crea occasioni completamente nuove per arrivare a livelli di sviluppo superiori. La loro capacità di superare molti degli ostacoli classici, in particolare quelli costituiti dal tempo e dalla distanza, permette per la prima volta nella storia di far beneficiare del loro potenziale milioni di esseri umani in tutte le regioni del mondo.

9 **Noi siamo consapevoli** che le TIC dovrebbero essere considerate come uno strumento e non come un fine in sé. In condizioni favorevoli, esse possono essere un potente strumento, capace di aumentare la produttività, di stimolare la crescita economica, di favorire la creazione di posti di lavoro e di migliorare la qualità della vita di tutti. Possono, inoltre, favorire il dialogo fra le persone, le nazioni e le culture.

10 **Noi siamo inoltre assolutamente consapevoli** che i benefici della rivoluzione delle tecnologie dell'informazione sono oggi suddivisi in modo ineguale fra i paesi sviluppati e i paesi in via di sviluppo, come anche in seno alle società. Siamo pertanto assolutamente decisi a far sì che questo divario digitale diventi una opportunità per tutti, soprattutto per coloro che rischiano di essere lasciati da parte e di essere ulteriormente emarginati.

11 **Noi siamo decisi** a dare corpo, per noi stessi e per le generazioni future, alla nostra comune concezione della società dell'informazione,. Riconosciamo che i giovani, la popolazione attiva di domani, sono all'avanguardia nella creazione e nell'utilizzo delle TIC. Bisogna dunque offrire loro gli strumenti per agire come apprendisti, sviluppatori, collaboratori, imprenditori e arbitri. Dobbiamo soprattutto prestare attenzione ai giovani che non hanno ancora potuto pienamente beneficiare delle possibilità offerte dalle TIC. Siamo inoltre decisi a creare condizioni propizie allo sviluppo di applicazioni e di servizi TIC che tengano conto dei diritti dei bambini, della loro tutela e del loro benessere.

12 **Noi affermiamo** che lo sviluppo delle TIC offre possibilità immense alle donne, che dovrebbero fare parte integrante della società dell'informazione ed esserne attori chiave. Noi siamo decisi a fare in modo che la società dell'informazione favorisca l'autonomia delle donne e la loro partecipazione piena e totale, in parità con gli uomini, in tutte le sfere della società, a tutti i processi decisionali. Dovremmo favorire l'eguaglianza fra uomini e donne e, a tal fine, utilizzare le TIC come strumento.

13 Nella edificazione della società dell'informazione, **noi dobbiamo prestare particolare attenzione** alle necessità specifiche delle categorie emarginate e vulnerabili, compresi i migranti, i rifugiati, i disoccupati e le persone svantaggiate, le minoranze e i nomadi. Dobbiamo prestare attenzione inoltre ai bisogni specifici degli anziani e degli handicappati.

14 **Noi siamo decisi** ad offrire ai poveri, e in particolare a coloro che vivono in zone isolate o rurali e in zone urbane marginalizzate, i mezzi per rendersi autonomi, accedere all'informazione e avvalersi delle TIC negli sforzi che compiono per sottrarsi alla povertà.

15 Nell'evoluzione della società dell'informazione, particolare attenzione deve essere accordata alla situazione particolare dei popoli autoctoni, e alla conservazione del loro patrimonio ancestrale e culturale.

16 **Noi continuiamo ad accordare** particolare attenzione alle necessità specifiche dei paesi in via di sviluppo, dei paesi ad economia in transizione, ai paesi meno progrediti, ai piccoli Stati insulari in via di sviluppo, ai paesi e territori occupati, ai paesi che emergono da conflitti e a paesi e regioni che hanno bisogni particolari, come a situazioni in cui gravi minacce pesano sullo sviluppo, per esempio le catastrofi naturali.

17 **Noi riconosciamo** che l'edificazione di una società dell'informazione inclusiva esige nuova forme di solidarietà, di partenariato e di cooperazione fra i governi e altri attori, vale a dire il settore privato, la società civile e le organizzazioni internazionali. Consapevoli che l'ambizioso obiettivo di questa Dichiarazione – ridurre il divario digitale e garantire uno sviluppo armonioso, giusto ed equo per tutti – richiederà il serio impegno di tutte le parti coinvolte, lanciamo un appello alla solidarietà informatica sia a livello delle nazioni sia a livello internazionale.

18 Nessun elemento della presente Dichiarazione deve essere interpretato come un'alterazione, una contraddizione o una limitazione delle disposizioni della Carta delle Nazioni Unite e della Dichiarazione universale dei diritti dell'uomo, come anche di nessun altro strumento internazionale o di legislazione nazionale adottato per promuovere questi strumenti, né come una deroga a questi strumenti.

B Una società dell'informazione per tutti: principi fondamentali

19 **Noi siamo decisi**, nella nostra azione, a fare in modo che tutti possano beneficiare delle possibilità che le TIC offrono. Siamo tutti unanimi nel ritenere che, per assolvere questo compito, tutte le parti coinvolte dovrebbero operare insieme per migliorare l'accesso all'infrastruttura e alle TIC, come anche all'informazione e alla conoscenza, per potenziare le capacità, aumentare la fiducia e la sicurezza nell'utilizzo delle TIC, creare un ambiente favorevole a tutti i livelli, sviluppare e ampliare le applicazioni delle TIC, favorire e rispettare la diversità culturale, riconoscere il ruolo dei media, prendere in considerazione le dimensioni etiche della società dell'informazione e incoraggiare la cooperazione internazionale e regionale. Noi riconosciamo che questi sono i principi fondamentali che devono essere alla base di una società dell'informazione inclusiva.

1) Il ruolo dei governi e di tutte le parti coinvolte nella promozione delle TIC per lo sviluppo

20 I governi, il settore privato, la società civile, l'Organizzazione delle Nazioni Unite, come anche altri organismi internazionali hanno una responsabilità e un ruolo

importanti nella edificazione della società dell'informazione e, secondo i casi, nei processi decisionali. L'edificazione di una società dell'informazione a dimensione umana è un'impresa comune che richiede la cooperazione e il partenariato di tutte le parti coinvolte.

21 La connettività ha un ruolo molto importante nell'edificazione della società dell'informazione. Un accesso universale, ubiquitario, giusto e finanziariamente accessibile alle infrastrutture e ai servizi TIC costituisce una sfida per la società dell'informazione e dovrebbe costituire uno degli obiettivi di tutti coloro che partecipano alla sua edificazione. La connettività comprende anche l'accesso all'energia elettrica e ai servizi postali, che dovrebbe essere garantito nel rispetto della legislazione interna di ogni paese.

22 La realizzazione di infrastrutture e di applicazioni di rete d'informazione e di comunicazione sufficientemente sviluppate, rese idonee alle condizioni regionali, nazionali e locali, facilmente accessibili e finanziariamente abbordabili e che utilizzino maggiormente le potenzialità della banda larga e di altre tecnologie innovative, quando esistono, può consentire di accelerare il progresso sociale ed economico dei paesi e favorire la ricchezza di tutti i cittadini, di tutte le comunità e di tutti i popoli.

23 Bisognerebbe concepire e realizzare politiche atte a favorire, a tutti i livelli, la nascita di condizioni favorevoli di stabilità, di prevedibilità e di equità nella concorrenza, non solo per mobilitare maggiormente gli investimenti privati per lo sviluppo delle infrastrutture TIC, ma anche per rispondere agli obblighi di servizio pubblico nelle regioni in cui i meccanismi tradizionali del mercato non funzionano. Nelle zone svantaggiate, l'installazione di punti d'accesso pubblico alle TIC in luoghi quali gli uffici postali, le scuole, le biblioteche e gli archivi può costituire un valido mezzo per favorire l'accesso universale all'infrastruttura e ai servizi della società dell'informazione.

3) L'accesso all'informazione e alla conoscenza

24 In una società dell'informazione inclusiva è essenziale la capacità di ciascuno di accedere all'informazione, alle idee e alla conoscenza e di contribuirvi.

25 La condivisione e il potenziamento della conoscenza mondiale per lo sviluppo possono essere migliorati eliminando gli ostacoli all'accesso equo all'informazione per le attività economiche, sociali, politiche, sanitarie, culturali, educative e scientifiche e facilitando l'accesso all'informazione del settore pubblico, fra l'altro mediante tecnologie di assistenza concepite per essere universali.

26 La crescita della società dell'informazione passa attraverso la creazione di un dominio pubblico ricco, origine e fonte di molteplici vantaggi: formazione del pubblico, creazione di posti di lavoro, innovazione, sbocchi economici e progressi scientifici. Le informazioni di pertinenza del settore pubblico dovrebbero essere facilmente accessibili in modo da sostenere la società dell'informazione e protette da un eventuale uso abusivo. Bisognerebbe rinforzare le istituzioni pubbliche quali le biblioteche, gli archivi, i musei, le collezioni culturali ed altri punti di accesso pubblici per promuovere la tutela degli archivi e un accesso libero ed equo all'informazione.

27 L'accesso all'informazione e alla conoscenza può essere incoraggiato sensibilizzando tutte le parti coinvolte alle possibilità che offrono le varie applicazioni software, in particolare i software proprietari, i software a codice sorgente aperto e i software gratuiti, per potenziare la concorrenza, l'accesso degli utenti e il ventaglio di scelte e per permettere a tutti gli utenti di sviluppare le soluzioni che meglio rispondono alle loro attese. Il possibile accesso ai software dovrebbe essere considerato come un importante elemento di una società dell'informazione veramente inclusiva.

28 Noi ci sforziamo di promuovere un accesso universale, con parità di possibilità per tutti, alle conoscenze scientifiche, come anche alla creazione e diffusione delle informazioni scientifiche e tecniche, comprese le iniziative intraprese per assicurare un accesso aperto alle pubblicazioni scientifiche.

4) Il potenziamento delle capacità

29 Tutti dovrebbero avere la possibilità di acquisire le competenze e le conoscenze necessarie per poter svolgere un ruolo attivo nella società dell'informazione e nell'economia della conoscenza, capirne il funzionamento e beneficiarne integralmente. L'alfabetizzazione e l'insegnamento primario universale sono fattori essenziali per edificare una società dell'informazione veramente inclusiva, dove un'attenzione particolare è accordata ai bisogni specifici delle ragazze e delle donne. Dato l'ampio ventaglio di specialisti delle TIC e dell'informazione richiesti a tutti i livelli, necessita di particolare attenzione il potenziamento della capacità progettuale a livello istituzionale *(Capacity builiding)*

30 Bisognerebbe incoraggiare l'uso delle TIC in tutti gli stadi dell'insegnamento, della formazione e dello sviluppo delle risorse umane, tenendo particolare conto delle necessità degli handicappati e delle categorie svantaggiate o vulnerabili.

31 La formazione permanente e la formazione degli adulti, la riconversione, l'apprendimento costante nel corso della vita, l'apprendimento a distanza e altri servizi speciali, come la telemedicina, possono offrire un contributo essenziale alla offerta/ricerca di lavoro e contribuire all'utilizzo delle nuove possibilità offerte dalle TIC per i lavori tradizionali, i lavori indipendenti e le nuove professioni. La presa di

coscienza e la padronanza delle nozioni di base nel campo delle TIC sono a questo proposito essenziali.

32 I creatori, gli editori e gli autori di contenuti, come anche gli insegnanti, gli educatori, gli archivisti, i bibliotecari e coloro che studiano dovrebbero attivamente contribuire a promuovere la società dell'informazione, soprattutto nei paesi meno progrediti.

33 Per giungere a uno sviluppo duraturo della società d'informazione, bisognerebbe aumentare le capacità nazionali per quanto riguarda la ricerca e lo sviluppo nel settore delle TIC. Un ruolo essenziale, inoltre, dovrebbe essere svolto dai partenariati, specialmente fra paesi sviluppati, paesi in via di sviluppo ed paesi a economia in transizione, nel campo della ricerca e dello sviluppo, del transfer di tecnologie, di produzione e impiego dei prodotti e dei servizi TIC per favorire il potenziamento delle capacità e la partecipazione alla società dell'informazione a livello mondiale. La realizzazione di prodotti TIC apre ampie prospettive nella creazione di ricchezza.

34 La concretizzazione delle aspirazioni che condividiamo, in particolare quella che i paesi in via di sviluppo e i paesi a economia in transizione divengano membri a pieno titolo della società dell'informazione e possano veramente integrarsi nell'economia del sapere, dipende molto dal potenziamento delle capacità nei campi dell'insegnamento, della tecnologia e dell'accesso all'informazione, che costituiscono fattori fondamentali di sviluppo e competitività.

5) Garantire fiducia e sicurezza nell'utilizzo delle TIC

35 Rinforzare il clima di fiducia, soprattutto con la sicurezza dell'informazione e la sicurezza delle reti, con le procedure di autenticazione e con la tutela della vita privata e del consumatore è preliminare allo sviluppo della società dell'informazione e alla nascita della fiducia fra gli utenti delle TIC. E' necessario incoraggiare, sviluppare e realizzare, in collaborazione con tutti i partner e tutti gli organismi internazionali competenti, una cultura globale della cibersicurezza. Questi sforzi dovrebbero essere sostenuti da una solida cooperazione internazionale. In questa cultura mondiale della cibersicurezza, è importante potenziare la sicurezza e assicurare la protezione dei dati e della vita privata, pur migliorando l'accesso e gli scambi commerciali. Questa cultura mondiale della cibersicurezza deve inoltre tenere conto del livello di sviluppo socioeconomico dei paesi e rispettare gli aspetti della società dell'informazione orientati verso lo sviluppo.

36 Pur riconoscendo i principi di un accesso universale e non discriminatorio alle TIC per tutte le nazioni, noi sosteniamo le azioni condotte dalle Nazioni Unite per impedire che le TIC possano essere utilizzate per fini incompatibili con gli obiettivi del mantenimento della stabilità e della sicurezza internazionali e rischino di nuocere

all'integrità delle infrastrutture nazionali, a detrimento della sicurezza degli Stati. Pur rispettando i diritti dell'uomo è necessario evitare che le risorse e le tecnologie dell'informazione siano utilizzate per fini criminali o terroristici.

37 Lo spamming è un problema importante e sempre più grave per gli utenti, le reti e Internet nel suo insieme. Le questioni dello spamming e della cibersicurezza dovrebbero essere trattate nelle sedi appropriate nazionali e internazionali.

6) Creare un ambiente favorevole

38 Per la società dell'informazione è fondamentale un ambiente favorevole a livello nazionale e internazionale. Le TIC dovrebbero essere utilizzate come un importante strumento di buona gestione.

39 E' fondamentale, nell'edificazione di una società dell'informazione a dimensione umana, il primato del diritto, unito ad un quadro politico e regolamentare favorevole, trasparente, propizio alla concorrenza, tecnologicamente neutro, prevedibile e che riflette la situazione reale dei paesi. I poteri pubblici dovrebbero intervenire in modo adeguato per rimediare alle insufficienze del mercato, mantenere un'equa concorrenza, attirare gli investimenti, intensificare lo sviluppo delle infrastrutture e delle applicazioni TIC, ottimizzare i benefici economici e sociali e promuovere il conseguimento delle priorità nazionali.

40 E' indispensabile che gli sforzi nazionali di sviluppo in materia di TIC siano sostenuti da uno sviluppo ambientale internazionale dinamico e propizio, favorevole agli investimenti stranieri diretti, al transfert di tecnologie e alla cooperazione internazionale, soprattutto per quanto riguarda le finanze, l'indebitamento e il commercio, e da una partecipazione piena e totale dei paesi in via di sviluppo alle decisioni che vengono prese a livello mondiale. Migliorare la connettività e renderla finanziariamente accessibile su scala mondiale contribuirebbe in buona parte ad accrescere l'efficacia di questi sforzi di sviluppo.

41 Le TIC costituiscono un potente catalizzatore della crescita perché consentono di realizzare maggiore efficacia e produttività, soprattutto a livello delle piccole e medie imprese (PMI). A questo proposito, per la crescita dell'insieme dell'economia nei paesi sviluppati e nei paesi in via di sviluppo è importante lo sviluppo della società dell'informazione. Sarebbe opportuno favorire la crescita della produttività e le innovazioni rese possibili dalle TIC in tutti i settori d'attività. Un'equa ripartizione degli effetti positivi contribuisce all'eliminazione della povertà e allo sviluppo sociale. Le politiche più vantaggiose saranno probabilmente quelle che incoraggiano gli investimenti produttivi e permettono alle imprese, in particolare alle PMI, di procedere ai cambiamenti necessari per poter beneficiare dei vantaggi offerti dalle TIC.

42 Come è importante tutelare la proprietà intellettuale per incoraggiare l'innovazione e la creatività nella società dell'informazione, così è importante disseminare, diffondere e condividere ampiamente il sapere per incoraggiare l'innovazione e la creatività. Facilitare l'effettiva partecipazione di tutti alla tutela della proprietà intellettuale e alla condivisione del sapere con la sensibilizzazione e il potenziamento delle capacità è un elemento fondamentale di una società dell'informazione inclusiva.

43 Il mezzo migliore per favorire uno sviluppo duraturo nella società dell'informazione è integrare pienamente gli sforzi e i programmi in materia di TIC alle strategie di sviluppo nazionali e regionali. Noi ci rallegriamo del Nuovo partenariato per lo sviluppo dell'Africa (NEPAD) e incoraggiamo la comunità internazionale a sostenere le misure legate alle TIC adottate nell'ambito di questa iniziativa e quelle che riguardano sforzi analoghi compiuti in altre regioni. La suddivisione dei frutti della crescita alimentata dalle TIC contribuisce allo sradicamento della povertà e allo sviluppo duraturo.

44 La normalizzazione è uno degli elementi costitutivi essenziali della società dell'informazione. Bisognerebbe porre l'accento in modo particolare sull'elaborazione e l'adozione di norme internazionali. L'elaborazione e l'utilizzo di norme aperte, compatibili, non discriminatorie e centrate sulla domanda, che tengono conto delle necessità degli utenti e dei consumatori costituiscono un elemento fondamentale per sviluppare e diffondere le TIC e renderne l'accesso più facile, in particolare nei paesi in via di sviluppo. Le norme internazionali hanno come oggetto la creazione di condizioni che permettano di avere accesso ai servizi, in tutto il mondo, qualunque sia la tecnologia utilizzata.

45 Lo spettro delle frequenze radioelettriche dovrebbe essere gestito nell'interesse pubblico e in conformità al principio di legalità, nello stretto rispetto delle leggi e dei regolamenti nazionali e degli accordi internazionali applicabili.

46 Nella edificazione della società dell'informazione, gli Stati sono vivamente incoraggiati a prendere misure adeguate per evitare ed astenersi da ogni azione unilaterale non conforme al diritto internazionale e alla Carta delle Nazioni Unite che potrebbe ostacolare la piena realizzazione dello sviluppo economico e sociale delle popolazioni dei paesi interessati, o nuocere al loro benessere.

47 Considerato che le TIC modificano poco a poco le nostre abitudini di lavoro, è fondamentale creare condizioni di lavoro sicure, affidabili e salubri, idonee all'utilizzo di queste tecnologie e rispettose di tutte le norme internazionali applicabili.

48 Internet è diventato una risorsa pubblica mondiale e la sua gestione dovrebbe essere un punto essenziale dell'ordine del giorno della società dell'informazione. La

gestione internazionale di Internet dovrebbe esercitarsi in modo multilaterale, trasparente e democratico, con la piena partecipazione degli Stati, del settore privato, della società civile e delle organizzazioni internazionali. Dovrebbe inoltre assicurare un'equa ripartizione delle risorse, facilitare l'accesso di tutti e garantire il funzionamento stabile e sicuro di Internet, nel rispetto del multilinguismo.

49 La gestione di Internet abbraccia sia questioni tecniche sia questioni di politica pubblica e dovrebbe riunire tutte le parti coinvolte e le organizzazioni intergovernative o internazionali interessate. A questo proposito si riconosce che:

a) il potere decisionale per quanto riguarda le questioni di politica pubblica legate a Internet è diritto sovrano degli Stati. Questi hanno diritti e responsabilità per quanto concerne le questioni di politica pubblica che hanno portata internazionale;
b) il settore privato ha svolto e dovrebbe continuare a svolgere un ruolo importante nello sviluppo di Internet, sia nel campo tecnico sia in quello economico;
c) la società civile anche ha avuto un ruolo importante per le questione legate a Internet, in particolare a livello comunitario, e dovrebbe continuare a svolgere questo ruolo;
d) le organizzazioni intergovernative hanno facilitato e dovrebbero continuare a facilitare il coordinamento delle questioni di politica pubblica legate a Internet;
e) anche le organizzazioni internazionali hanno svolto e dovrebbero continuare a svolgere un ruolo importante nella elaborazione di norme tecniche e di politiche relative a Internet.

50 I problemi internazionali legati alla gestione di Internet dovrebbero essere trattati in modo coordinato. Noi chiediamo al Segretario generale delle Nazioni Unite di creare un gruppo di lavoro sulla gestione di Internet, nell'ambito di un processo aperto e inclusivo che preveda un meccanismo capace di garantire la piena e attiva partecipazione dei rappresentanti degli Stati, del settore privato e della società civile sia dei paesi sviluppati sia dei paesi in via di sviluppo, e di fare intervenire gli organismi intergovernativi e internazionali e i forum interessati per studiare, da qui al 2005, la gestione di Internet ed eventualmente proporre le misure da prendere.

7) Le applicazioni delle TIC e il loro apporto in tutti i settori

51 L'utilizzo delle TIC dovrebbe contribuire a facilitare la nostra vita quotidiana in tutti i campi. Le loro applicazioni possono rivelarsi molto utili in molti ambiti: amministrazione e servizi pubblici, salute e informazione sanitaria, insegnamento e formazione, lavoro e creazione di posti di lavoro, affari, agricoltura, trasporti, tutela dell'ambiente e gestione delle risorse naturali, prevenzione delle catastrofi naturali, cultura; e favorire l'eliminazione della povertà e raggiungere altri obiettivi di sviluppo. Le TIC dovrebbero inoltre contribuire a instaurare delle strutture durature di tutela e di consumo e attenuare gli ostacoli tradizionali, dando a tutti la possibilità di accedere ai

mercati locali e ai mercati mondiali in modo più giusto. Le applicazioni dovrebbero essere conviviali, accessibili a tutti, abbordabili, adattate alle necessità locali in termini di culture e di lingue e facilitare lo sviluppo duraturo. A tale proposito, converrebbe che le collettività locali assumessero un ruolo più importante nella prestazione di servizi TIC per il bene delle popolazioni interessate.

8) La diversità e l'identità culturali, la diversità linguistica e i contenuti locali

52 La diversità culturale è patrimonio comune dell'umanità. La società dell'informazione dovrebbe essere fondata sul rispetto dell'identità culturale, della diversità culturale e linguistica, delle tradizioni e delle religioni; essa dovrebbe promuovere questo rispetto e favorire il dialogo fa le culture e le civiltà. La promozione, il consolidamento e la conservazione delle diverse identità culturali e delle diverse lingue, che sono oggetto di testi approvati in materia dalle Nazioni Unite e in particolare della Dichiarazione universale dell'UNESCO sulla diversità culturale, costituiranno un'ulteriore ricchezza per la società dell'informazione.

53. Nell'edificazione di una società dell'informazione inclusiva, bisognerà accordare la priorità alla creazione, alla diffusione e alla conservazione di contenuti in diverse lingue e diversi formati, dando particolare attenzione alla diversità d'origine delle opere e al necessario riconoscimento dei diritti degli autori e degli artisti. E' essenziale promuovere la produzione/accessibilità di tutti i contenuti – educativi, scientifici, culturali o ricreativi – in diverse lingue e in diversi formati. L'elaborazione di contenuti locali adattati ai bisogni nazionali o regionali incoraggerà lo sviluppo socioeconomico e stimolerà la partecipazione di tutte le parti coinvolte, in particolare degli abitanti delle zone rurali, isolate o marginalizzate.

54 La conservazione del patrimonio culturale costituisce una componente fondamentale dell'identità e della comprensione di sé che collega una comunità al suo passato. La società dell'informazione dovrebbe valorizzare e salvaguardare il patrimonio culturale per le generazioni future, con tutti i metodi idonei, ivi compresa la digitalizzazione.

9) I *Media*

55 Noi ribadiamo la nostra adesione ai principi della libertà di stampa e della libertà dell'informazione, come a quelli dell'indipendenza, del pluralismo e della diversità dei media, essenziali per la società dell'informazione. La libertà di ricercare, ricevere, diffondere e utilizzare informazioni per la creazione, l'accumulo e la diffusione del sapere è importante per la società dell'informazione. Noi invitiamo i media a dar prova di responsabilità nell'utilizzo e nel trattamento dell'informazione mediante i media in conformità alle norme etiche e professionali più elevate. I media tradizionali, qualunque sia la loro forma, svolgono un importante ruolo nella società dell'informazione e le TIC

dovrebbero contribuirvi. Conviene incoraggiare la diversità delle forme di proprietà dei media, in conformità con le leggi dei paesi e tenuto conto delle relative convenzioni internazionali. Noi ribadiamo la necessità di ridurre le disparità fra i media sul piano internazionale, in particolare per quanto riguarda l'infrastruttura, le risorse tecniche e lo sviluppo delle competenze.

10) La cooperazione internazionale e regionale

60 Noi aspiriamo al pieno utilizzo delle possibilità offerte dalle TIC negli sforzi che mettiamo in atto per raggiungere gli obiettivi di sviluppo decisi a livello internazionale, in particolare quelli della Dichiarazione del Millennio, e per dare concretezza ai principi fondamentali esposti nella presente Dichiarazione. La società dell'informazione è per sua natura universale e gli sforzi delle nazioni devono essere sostenuti da una cooperazione internazionale e regionale efficace fra gli Stati, il settore privato, la società civile e le altre parti coinvolte, in particolare le istituzioni finanziarie internazionali.

61 Per edificare una società dell'informazione mondiale inclusiva, cercheremo e applicheremo in modo efficace approcci e meccanismi internazionali concreti, in particolare per quanto riguarda l'assistenza finanziaria e tecnica. Di conseguenza, pur riconoscendo nel suo giusto valore la cooperazione in corso, con diversi meccanismi, nel campo delle TIC, invitiamo tutte le parti coinvolte ad aderire al "Patto di solidarietà informatica" enunciato nel Piano d'azione. Noi siamo convinti che l'obiettivo stabilito a livello mondiale consiste nel contribuire a ridurre il divario digitale nel promuovere l'accesso alle TIC, nel creare prospettive numeriche e nell'avvantaggiarsi del potenziale che le TIC offrono per lo sviluppo. Prendiamo nota della volontà espressa da alcuni di creare un "Fondo di solidarietà informatica internazionale" alimentato da contributi volontari e di quella espressa da altri di intraprendere studi sui meccanismi esistenti, nonché sull'efficacia e la fattibilità di un tale fondo.

62 L'integrazione regionale contribuisce allo sviluppo della società mondiale dell'informazione e rende indispensabile una stretta collaborazione all'interno delle regioni e fra regioni. Il dialogo regionale dovrebbe contribuire al potenziamento delle capacità nazionali e all'armonizzazione fra le strategie nazionali e gli obiettivi della presente Dichiarazione di principi in condizioni di compatibilità, pur rispettando le specificità nazionali e regionali. In questo contesto, ci rallegriamo per le misure adottate in materia di TIC nel quadro di queste iniziative e incoraggiamo la comunità internazionale a sostenerle.

63 Noi decidiamo di aiutare i paesi in via di sviluppo, i paesi meno progrediti e i paesi a economia in transizione, utilizzando tutte le fonti di finanziamento, fornendo loro un'assistenza finanziaria e tecnica e creando condizioni favorevoli a transfert di tecnologia compatibili con gli obiettivi della presente Dichiarazione e del Piano d'azione.

64 Le competenze fondamentali dell'Unione Internazionale delle Telecomunicazioni (UIT) nel campo delle TIC – assistenza per ridurre il divario digitale, cooperazione internazionale e regionale, gestione dello spettro delle frequenze radioelettriche, elaborazione di norme e diffusione dell'informazione – sono determinanti per l'edificazione della società dell'informazione.

C Verso una società dell'informazione per tutti fondata sulla condivisione della conoscenza

65 **Noi ci impegniamo** a potenziare la cooperazione per cercare risposte comuni ai problemi che si pongono e alle sfide collegate alla realizzazione del Piano d'azione che darà corpo alla concezione di una società dell'informazione inclusiva basata sui principi essenziali enunciati nella presente Dichiarazione.

66 **Ci impegniamo inoltre** a valutare e a seguire i progressi realizzati nella riduzione del divario digitale tenendo conto dei diversi livelli di sviluppo, per raggiungere gli obiettivi di sviluppo approvati a livello internazionale, in particolare quelli enunciati nella Dichiarazione del Millennio, e a valutare l'efficacia degli investimenti e della cooperazione internazionale nell'edificazione della società dell'informazione.

67 **Noi siamo fermamente convinti** che insieme entriamo in una nuova era che offre possibilità immense, quella della società dell'informazione e della comunicazione allargata fra gli uomini. In questa società nascente, l'informazione e la conoscenza possono essere prodotti, scambiati, condivisi e comunicati mediante tutte le reti del pianeta. Se adottiamo le misure necessarie, tutti gli abitanti del pianeta potranno presto edificare insieme una nuova società dell'informazione fondata sulle conoscenze condivise, su una solidarietà mondiale e su una migliore comprensione reciproca fra i popoli e le nazioni. Noi siamo certi che queste misure aprono la strada all'edificazione di una vera società del sapere.

Vertice mondiale sulla società dell'informazione

Ginevra 2003 – Tunisi 2005

Documento WSIS-037GINEVRA7DOC75-F

12 MAGGIO 2004

Piano d'azione

A Introduzione

1. La concezione comune e i concetti fondamentali enunciati nella Dichiarazione di principi trovano la loro applicazione come misure concrete nel presente Piano d'azione. Lo scopo è infatti quello di raggiungere progressivamente gli obiettivi di sviluppo stabiliti a livello internazionale, in particolare nella Dichiarazione del Millennio, nel Monterey Consensus e nella Dichiarazione e nel Piano operativo di Johannesburg, favorendo l'utilizzo dei prodotti, delle reti, dei servizi e delle applicazioni che si fondano sulle tecnologie dell'informazione e della comunicazione (TIC) e di aiutare i paesi a superare il problema del divario digitale (*digital divide*). La società dell'informazione concepita nella Dichiarazione di principi sarà realizzata in collaborazione e in modo solidale dai governi e da tutti le altre parti coinvolte.

2. La società dell'informazione è un concetto evolutivo e il suo stadio di realizzazione differisce da paese a paese in funzione del rispettivo livello di sviluppo. L'evoluzione della tecnologia, insieme ad altri fattori, trasforma rapidamente le condizioni nelle quali questa società prende corpo. Il Piano d'azione è dunque un quadro evolutivo destinato a promuovere la società dell'informazione a livello nazionale, regionale e internazionale. La struttura peculiare del Vertice mondiale sulla società dell'informazione (VMSI), articolato in due fasi, offre la possibilità di tenere conto di questa evoluzione.

3. Tutti le parti coinvolte hanno un importante ruolo da svolgere nella società dell'informazione, soprattutto nel quadro dei partenariati:

a) I governi svolgono un ruolo essenziale nella elaborazione e nella realizzazione, a livello nazionale, di ciberstrategie globali, rivolte verso il futuro e durature. Il settore privato e la società civile, nel dialogo con i pubblici poteri, devono assumere un ruolo consultivo importante nella concezione di ciberstrategie nazionali.

b) L'impegno del settore privato è importante per lo sviluppo e la diffusione delle tecnologie dell'informazione e della comunicazione (TIC), al livello delle infrastrutture, dei contenuti e delle applicazioni. Il settore privato svolge un ruolo, non solo sul mercato, ma anche nell'ambito più ampio di uno sviluppo duraturo.

c) Anche molto importanti per la creazione di una società dell'informazione equa e per la realizzazione di iniziative legate alle TIC a favore dello sviluppo sono l'impegno e la partecipazione della società civile.

d) Le istituzioni internazionali e regionali, ivi comprese le istituzioni finanziarie internazionali, assumono un ruolo chiave quando si tratta d'inserire l'utilizzo delle TIC nel processo di sviluppo e di mettere a disposizione le risorse necessarie per edificare la società dell'informazione e valutare i progressi realizzati.

B Obiettivi, finalità e traguardi

4 Il Piano d'azione ha i seguenti obiettivi: edificare una società dell'informazione inclusiva; mettere il potenziale del sapere e delle TIC a disposizione dello sviluppo; promuovere l'utilizzo dell'informazione e del sapere per la realizzazione degli obiettivi di sviluppo definiti su scala internazionale, in particolare gli obiettivi enunciati nella Dichiarazione del Millennio; affrontare i nuovi problemi che la società dell'informazione pone ai livelli nazionale, regionale e internazionale. La seconda fase del VMSI costituirà l'occasione per valutare i progressi che saranno stati realizzati nella riduzione del divario digitale.

5 Nel quadro delle ciberstrategie nazionali e in conformità alle politiche di sviluppo nazionali, tenuto conto delle condizioni specifiche dei paesi considerati, a seconda delle opportunità, saranno definiti traguardi specifici corrispondenti alla società dell'informazione.

6. Fondati sugli obiettivi di sviluppo approvati a livello internazionale, in particolare quelli della Dichiarazione del Millennio, che si basano sulla cooperazione internazionale, alcuni traguardi indicativi possono servire come riferimento globale per migliorare la connettività e l'accesso alle TIC per la promozione degli obiettivi del Piano, fissati per il 2015. Questi traguardi potranno essere presi in considerazione nella scelta di traguardi nazionali, tenuto conto delle condizioni proprie di ogni paese:

a) connettere alle TIC i villaggi e creare dei punti d'accesso comunitari;
b) connettere alle TIC le scuole secondarie o superiori e le scuole primarie;
c) connettere alle TIC i centri scientifici e i centri di ricerca;
d) connettere alle TIC le biblioteche pubbliche, i centri culturali, i musei, gli uffici postali e gli archivi;
e) connettere alle TIC i centri sanitari e gli ospedali;
f) connettere alle TIC tutte le pubbliche amministrazioni, locali e centrali, e dotarle di un sito web e di un indirizzo elettronico;
g) adattare tutti i programmi delle scuole elementari e secondarie in modo da raccogliere le sfide della società dell'informazione, tenuto conto delle condizioni proprie di ogni paese;
h) garantire l'accesso ai servizi televisivi e radiofonici a tutta la popolazione mondiale;
i) incoraggiare l'elaborazione di contenuti e assicurare le condizioni tecniche atte a facilitare la presenza e l'utilizzo in Internet di tutte le lingue del mondo;

j) consentire che più della metà degli abitanti del pianeta abbia accesso alle TIC facilmente raggiungibili.

7 Nella realizzazione di questi obiettivi, finalità e traguardi, sarà accordata particolare attenzione alle necessità dei paesi in via di sviluppo, e soprattutto a quei paesi, popoli e categorie considerati nei paragrafi da 11 a 16 della Dichiarazione di principi.

C Orientamenti di massima

C1 Il ruolo dei governi e di tutte le parti coinvolte nella promozione delle TIC per lo sviluppo

8. Per lo sviluppo della società dell'informazione è fondamentale l'effettiva partecipazione dei governi e di tutte le parti coinvolte, cosa che implica collaborazione e partenariato da parte di tutti.

a) Tutti i paesi, da qui al 2005, tenuto conto delle condizioni proprie di ogni paese, dovrebbero favorire l'elaborazione di ciberstrategie nazionali, anche per quanto riguarda il necessario potenziamento delle risorse umane.
b) Bisognerebbe stabilire, a livello nazionale, un dialogo strutturato che coinvolga tutte le parti coinvolte, anche grazie a partenariati pubblico/privato, al fine di elaborare delle ciberstrategie per la società dell'informazione e per scambiare le procedure migliori.
c) Nella elaborazione e nella messa in opera di ciberstrategie nazionali, le parti coinvolte dovrebbero tenere conto dei bisogni e delle preoccupazioni ai livelli locale, regionale e nazionale, e in particolare, per ottimizzare i benefici delle iniziative che verranno prese, della nozione di sostenibilità. Il settore privato dovrebbe essere coinvolto nella realizzazione di progetti concreti per sviluppare la società dell'informazione ai livelli locale, regionale e nazionale.
d) I singoli paesi vengono incoraggiati ad avviare, da qui al 2005, a titolo di progetto pilota, almeno un partenariato operativo pubblico/privato (PPP) o fra più settori.
e) Bisognerebbe definire, su scala nazionale, regionale e internazionale dei meccanismi di realizzazione e di promozione di programmi fra le parti coinvolte della società dell'informazione.
f) Bisognerebbe studiare la fattibilità di portali *multi-stakeholder* che venissero creati a livello nazionale per le popolazioni autoctone.
g) Da qui al 2005, le organizzazioni internazionali e le istituzioni finanziarie interessate dovrebbero elaborare delle proprie strategie di utilizzo delle TIC per lo sviluppo duraturo, ivi compresi dei modi duraturi di produzione e di consumo, come mezzo efficace per contribuire alla realizzazione degli obiettivi enunciati nella Dichiarazione del Millennio delle Nazioni Unite.
h) Le organizzazioni internazionali dovrebbero pubblicare, nei loro ambiti di competenza, e in particolare nei loro siti web, informazioni affidabili comunicate dalle parti coinvolte sull'esperienza acquisita nella effettiva integrazione delle TIC.

i) Bisognerebbe favorire l'adozione di un insieme di misure correlate, fra cui: progetti di vivai di imprese, collocamenti di capitale di rischio (ai livelli nazionale e internazionale), fondi pubblici d'investimento (compreso il microfinanziamento di PMI e di micro-imprese), strategie d'incoraggiamento all'investimento, sostegno all'esportazione di software (consiglio commerciale) e sostegno alle reti di ricerca e sviluppo e alla creazione di parchi informatici.

C2 L'infrastruttura dell'informazione e della comunicazione: fondamento essenziale

di una società dell'informazione inclusiva

9 L'infrastruttura è fondamentale per concretizzare l'obiettivo dell'inclusione numerica, se si vuole che l'accesso alle TIC sia universale, duraturo, ubiquitario e finanziariamente accessibile, tenuto conto delle soluzioni appropriate già esistenti in alcuni paesi in via di sviluppo e in altri a economia di transizione, per assicurare connettività e accesso duraturi alle zone remote ed emarginate sia a livello nazionale che regionale.

a) I pubblici poteri dovrebbero adottare delle misure nel quadro delle politiche nazionali di sviluppo per favorire un ambiente concorrenziale e propizio agli investimenti necessari nelle infrastrutture TIC e allo sviluppo di nuovi servizi.
b) Nel contesto delle ciberstrategie nazionali, conviene elaborare politiche e strategie di accesso universale appropriate, nonché i mezzi per la loro applicazione, in conformità con i traguardi indicativi, e stabilire degli indicatori di connettività alle TIC.
c) Nel contesto delle ciberstrategie nazionali, la connettività alle TIC dovrebbe essere assicurata e migliorata in tutte le scuole, le università, le strutture sanitarie, le biblioteche, gli uffici postali, i centri comunitari, i musei ed altre strutture aperte al pubblico, in conformità ai traguardi indicativi.
d) Bisognerebbe sviluppare e potenziare, su scala nazionale, regionale e internazionale, le infrastrutture di rete a banda larga, in particolare per quanto riguarda i sistemi di comunicazione via satellite e altri sistemi, al fine di contribuire a fornire la capacità necessaria per rispondere ai bisogni dei paesi e dei loro abitanti e di assicurare la prestazione di nuovi servizi basati sulle TIC. La realizzazione da parte dell'Unione internazionale delle telecomunicazioni (UIT) e, nel caso in cui questo non fosse possibile, da parte di altre organizzazioni internazionali interessate, di studi tecnici, normativi e operativi, dovrebbe essere sostenuta, al fine di:
    i) ampliare l'accesso alle risorse satellitari e assicurare a livello mondiale l'armonizzazione delle frequenze e la normalizzazione dei sistemi;
    ii) incoraggiare partenariati pubblico/privato;
    iii) promuovere la fornitura di servizi mondiali via satellite ad alta velocità per le regioni mal servite, come le zone lontane e con scarsa densità di popolazione;
    iv) studiare altri sistemi, suscettibili di assicurare una connettività ad alta velocità.

e) Nel contesto delle ciberstrategie nazionali, bisognerebbe rispondere alle necessità particolari delle persone anziane, degli handicappati, dei bambini, e in particolare dei bambini emarginati, e delle altre categorie sfavorite o vulnerabili, soprattutto con misure educative, amministrative e legislative appropriate, per assicurare la loro perfetta integrazione nella società dell'informazione.

f) Incoraggiare lo studio e la produzione di attrezzature e servizi TIC facilmente accessibili, a condizioni finanziarie accessibili a tutti, e in particolare alle persone anziane, agli handicappati, ai bambini, specialmente a quelli emarginati, e alle altre categorie sfavorite o vulnerabili, e promuovere lo sviluppo di tecnologie, applicazioni e contenuti adatti ai loro bisogni, ispirandosi al principio del progetto universale e ricorrendo a tecnologie d'assistenza.

g) Per lottare contro l'analfabetismo bisognerebbe mettere a punto delle tecnologie finanziariamente abbordabili e realizzare delle interfacce informatiche non testuali, così da facilitare l'accesso alle TIC.

h) A livello internazionale dovrebbero essere compiuti degli sforzi a favore della ricerca e dello sviluppo, in modo da mettere a disposizione degli utenti finali delle attrezzature TIC adeguate e finanziariamente abbordabili.

i) E' opportuno incoraggiare l'impiego delle tecnologie *wireless*, compresa quella satellitare, ove non impiegata, nei paesi sviluppati, e in particolare nei paesi in via di sviluppo, per servire le zone isolate, in particolare nei paesi in via di sviluppo e nei paesi a economia di transizione, e ampliare la connettività a basso costo nei paesi in via di sviluppo. Un'attenzione particolare dovrebbe essere accordata ai paesi meno progrediti (PMP) negli sforzi che compiono per istallare una infrastruttura di telecomunicazione

j) Bisognerebbe ottimizzare la connettività fra le principali reti di informazione, incoraggiando la creazione e lo sviluppo di reti federative TIC e di punti dei scambio Internet a livello regionale, per ridurre i costi d'interconnessione e ampliare l'accesso alla rete.

k) Bisognerebbe elaborare delle strategie per sviluppare la connettività mondiale finanziariamente accessibile, e quindi per migliorare l'accesso. I costi di transito e d'interconnessione Internet, negoziati a livello commerciale, dovrebbero essere stabiliti in funzione di parametri oggettivi, trasparenti e non discriminanti, tenuto conto dei lavori in corso.

l) Bisognerebbe inoltre incoraggiare e favorire l'utilizzo congiunto dei mass media tradizionali e delle nuove tecnologie.

C3 L'accesso all'informazione e al sapere

10. Le TIC consentono a ognuno di noi, in ogni parte del mondo, di accedere quasi istantaneamente all'informazione e al sapere di cui i singoli, le organizzazioni e le comunità dovrebbero poter beneficiare.

a) Per la valorizzazione e la promozione delle informazioni nell'ambito del pubblico, sarebbe opportuno elaborare delle linee guida che costituiscano un valido strumento per favorire l'accesso pubblico all'informazione, su scala internazionale.

b) Si incoraggiano i poteri pubblici ad assicurare un adeguato accesso alle informazioni ufficiali di carattere pubblico con diversi mezzi di comunicazione, e in particolare con Internet. Si raccomanda inoltre di stabilire una legislazione sull'accesso alle informazioni e sulla tutela dei dati pubblici, in particolare nel campo delle nuove tecnologie.

c) Si incoraggiano inoltre la ricerca e lo sviluppo volti a mettere le TIC alla portata di tutti, e in particolare delle categorie svantaggiate, emarginate e vulnerabili.

d) I governi e le altre parti coinvolte dovrebbero creare dei punti di accesso comunitario pubblici, multifunzionali e duraturi, che offrano ai cittadini la possibilità di un accesso gratuito alle diverse risorse di comunicazione, e in particolare a Internet. Questi punti d'accesso dovrebbero, per quanto possibile, essere idonei ad offrire assistenza agli utenti nelle biblioteche, nelle scuole, nelle pubbliche amministrazioni, negli uffici postali e in altri luoghi pubblici. L'accento in proposito viene messo in particolare sulle zone rurali e mal servite, nel rispetto dei diritti di proprietà intellettuale (DPI) e incoraggiando l'impiego dell'informazione e la condivisione della conoscenza.

e) Bisognerebbe incoraggiare la ricerca e sensibilizzare tutti le parti coinvolte sulle possibilità offerte da diversi modelli di software e dai mezzi per crearli, ivi compresi i software proprietari, i software a codice sorgente aperto e i software gratuiti, per intensificare la concorrenza, dilatare la possibilità di scelta, rendere i software più accessibili e consentire a tutte le parti coinvolte di valutare le soluzioni che meglio rispondono alle loro necessità.

f) I pubblici poteri dovrebbero attivamente incoraggiare l'utilizzo delle TIC come fondamentale strumento di lavoro per i cittadini e le collettività locali. A questo proposito, la comunità internazionale e le altre parti coinvolte dovrebbero favorire il potenziamento delle capacità delle collettività locali, in modo che l'impiego generalizzato delle TIC consenta una migliore gestione dell'amministrazione locale.

g) Bisognerebbe favorire la ricerca sulla società dell'informazione, in particolare per quanto riguarda le forme innovative di messa in rete, l'adattamento delle infrastrutture TIC, gli strumenti e le applicazioni che facilitano l'accesso di tutti, e in particolare delle categorie svantaggiate, alle TIC.

h) Bisognerebbe sostenere la creazione e l'ampliamento di un servizio di biblioteche e di archivi pubblici digitale, adattato alla società dell'informazione, attualizzando, per esempio, le strategie e le legislazioni nazionali relative alle biblioteche, sensibilizzando tutti i paesi alla necessità di disporre di "biblioteche miste" e favorendo la cooperazione internazionale fra biblioteche.

i) Bisognerebbe favorire le iniziative destinate a facilitare l'accesso, in particolare quello gratuito o a prezzi abbordabili, alle riviste e alle opere in libero accesso, come anche ad archivi di informazione scientifici aperti.

j) E' opportuno sostenere la ricerca e lo sviluppo in fatto di creazione di strumenti utili per tutte le parti coinvolte al fine di migliorare la conoscenza, la stima e la valutazione di diversi modelli e licenze di software, per poter scegliere nelle migliori condizioni i software che meglio potranno contribuire alla realizzazione degli obiettivi di sviluppo nelle condizioni specifiche di ogni paese.

C4 Il potenziamento delle capacità

11. Tutti dovrebbero avere le competenze necessarie per beneficiare in modo totale della società dell'informazione. E' quindi essenziale sviluppare le capacità e assicurare a tutti la possibilità di familiarizzare con le TIC. Le TIC, infatti, possono contribuire all'educazione di tutti in tutto il mondo, mediante la formazione degli insegnanti, nonché al miglioramento delle condizioni necessarie alla formazione permanente, poiché raggiungono le persone anche al di fuori del sistema d'insegnamento ufficiale e permettono di migliorare le competenze professionali.

a) Elaborare politiche nazionali che facciano sì che le TIC siano pienamente integrate nell'insegnamento e nella formazione a tutti i livelli: elaborazione dei programmi scolastici, formazione degli insegnanti e amministrazione e gestione delle strutture, e che favoriscano la formazione permanente.
b) Elaborare e promuovere, a livello nazionale, regionale e internazionale, utilizzando le TIC, programmi di lotta contro l'analfabetismo.
c) Promuovere per tutti lo sviluppo delle competenze nell'ambito dell'informatica, per esempio organizzando corsi d'iniziazione all'informatica per i funzionari delle pubbliche amministrazioni, approfittando delle installazioni esistenti – biblioteche, centri comunitari polivalenti, punti d'accesso pubblico – e creando centri di formazione alle TIC a livello locale, in collaborazione con tutte le parti coinvolte.
d) Nel quadro delle politiche nazionali per l'istruzione e tenuto conto della necessità di sradicare l'analfabetismo degli adulti, fare in modo che i giovani abbiano conoscenze e competenze sufficienti per utilizzare le TIC, in particolare la capacità di analizzare e di trattare l'informazione in modo creativo e innovativo, di condividere le loro conoscenze e di partecipare pienamente alla società dell'informazione.
e) I governi dovrebbero, in collaborazione con le altre parti coinvolte, mettere a punto programmi di aggiornamento che pongano l'accento sulla creazione di una riserva sufficiente di professionisti e di esperti qualificati e competenti in materia di TIC.
f) Realizzare progetti pilota per dimostrare l'interesse dei diversi sistemi d'insegnamento utilizzando le TIC, in particolare per riuscire a raggiungere gli obiettivi della «Educazione per tutti», specialmente quelli attinenti alla formazione di base in informatica.

g) Sforzarsi di abbattere le barriere esistenti fra uomini e donne nel settore dell'insegnamento e della formazione alle TIC, e promuovere le pari opportunità in fatto di formazione nei campi connessi alle TIC per le donne e le giovani. Per le giovani bisognerebbe prevedere programmi d'intervento precoce nelle materie scientifiche e tecniche, essendo uno degli obiettivi quello di accrescere il numero delle donne nelle professioni legate alle TIC. Sarebbe inoltre opportuno promuovere lo scambio delle migliori metodologie nel campo dell'integrazione del principio della parità uomo-donna a proposito della formazione alle TIC.

h) Offrire alle comunità locali, soprattutto nelle zone rurali e mal servite, la possibilità di utilizzare le TIC e promuovere la produzione di contenuti socialmente utili e costruttivi, a beneficio di tutti.

i) Lanciare programmi d'insegnamento e di formazione, se possibile utilizzando le reti d'informazione delle popolazioni autoctone e di tradizione nomadiche, che permettano di partecipare pienamente alla società dell'informazione.

j) Concepire e realizzare una cooperazione regionale e internazionale per potenziare in particolare la capacità dei responsabili e del personale amministrativo nei paesi in via di sviluppo e nei paesi meno avanzati (PMA) e per un adeguato utilizzo delle TIC in tutto il settore educativo, insegnamento extrascolastico compreso, per esempio sul posto di lavoro o a domicilio.

k) Elaborare programmi specifici di formazione all'impiego delle TIC per rispondere alle necessità dei professionisti dell'informazione, come gli archivisti, i bibliotecari, il personale dei musei, gli scienziati, gli insegnanti, i giornalisti, i postelegrafonici, e tutti gli altri professionisti interessati. La formazione dei professionisti dell'informazione dovrebbe essere centrata non solo sulle nuove tecniche e i nuovi metodi di creazione e fornitura di servizi d'informazione e di comunicazione, ma anche sulle competenze necessarie in materia di gestione, per garantire il migliore utilizzo delle tecnologie. La formazione dei docenti dovrebbe vertere essenzialmente sugli aspetti tecnici delle TIC, sull'elaborazione dei contenuti e sulle possibilità offerte dalle TIC, nonché sui problemi che queste pongono.

l) Sviluppare l'insegnamento e la formazione a distanza e altre forme d'insegnamento e formazione nel quadro di programmi di potenziamento delle capacità. Accordare particolare attenzione ai paesi in via di sviluppo e ai PMA in funzione del loro livello di sviluppo delle risorse umane.

m) Promuovere la cooperazione a livello internazionale e regionale nel campo del potenziamento delle capacità, in particolare i programmi per paese stabiliti dalle Nazioni Unite e dalle loro istituzioni specializzate.

n) Avviare progetti-pilota volti a studiare nuovi modi di lavoro in rete mediante l'impiego delle TIC, collegando le strutture d'insegnamento, di formazione e di ricerca dei paesi sviluppati, dei paesi in via di sviluppo e dei paesi a economia in transizione, e questo sia fra i paesi che all'interno degli stessi.

o) Il volontariato, se è conforme alle politiche nazionali e alle culture locali, è molto utile quando si tratta di potenziare le capacità in materia di TIC a favore dello sviluppo, soprattutto nei paesi in via di sviluppo.

p) Elaborare programmi per insegnare agli utenti a sviluppare le loro capacità di auto-apprendimento e di autoformazione.

C5 Stabilire fiducia e sicurezza nell'utilizzo delle TIC

12 La fiducia e la sicurezza sono due dei pilastri principali della società dell'informazione.

a) Promuovere la collaborazione fra i governi nel quadro dell'Organizzazione delle Nazioni Unite, e con tutte le parti coinvolte, nel contesto di altre sedi appropriate per rafforzare la fiducia degli utenti, migliorare la sicurezza e proteggere l'integrità dei dati e delle reti; considerare le minacce esistenti e potenziali che pesano sulle TIC e trattare altre eventuali questioni legate alla sicurezza dell'informazione e delle reti.

b) In collaborazione con il settore privato, i poteri pubblici dovrebbero prevenire e individuare la cibercriminalità e l'utilizzo abusivo delle TIC e porvi rimedio: elaborando linee direttive che tengano conto degli sforzi in corso in questo ambito; progettando una legislazione che autorizzi investigazioni efficaci e azioni giudiziarie in caso di uso illecito; incoraggiando gli sforzi di reciproca assistenza; potenziando l'appoggio istituzionale sul piano internazionale per prevenire e individuare simili incidenti e porvi rimedio; e incoraggiando l'educazione e la sensibilizzazione.

c) I governi, e le altre parti coinvolte, dovrebbero incoraggiare attivamente gli utenti a formarsi e a sensibilizzarsi ai problemi della riservatezza in linea e della protezione della vita privata.

d) Prendere adeguate misure a livello nazionale e internazionale per quanto riguarda lo spamming.

e) Favorire la valutazione interna della legislazione nazionale per superare gli ostacoli all'utilizzo adeguato dei documenti e delle transazioni elettroniche, anche con i mezzi di autenticazione elettronica.

f) Potenziare il quadro di sicurezza e di fiducia adottando iniziative complementari e sinergiche nei campi della messa in sicurezza dell'utilizzo delle TIC, come anche iniziative o linee direttive relative al diritto alla segretezza, alla protezione dei dati e alla protezione dei consumatori.

g) Scambiare le procedure migliori nel campo della sicurezza dell'informazione e della sicurezza delle reti d'informazione e incoraggiare il loro utilizzo da parte di tutte le parti coinvolte.

h) Invitare i paesi interessati a istituire centri di coordinamento per la gestione e il trattamento in tempo reale degli incidenti, e a collegarli in una rete di cooperazione per la condivisione delle informazioni e delle tecnologie relative agli interventi successivi all'incidente.

i) Incoraggiare la ricerca e l'elaborazione di applicazioni sicure e affidabili per facilitare le transazioni in rete.

j) Incoraggiare i paesi interessati a contribuire attivamente alle attività in corso nell'ambito delle Nazioni Unite per aumentare la fiducia e la sicurezza in merito all'utilizzo delle TIC.

C6 Creare un ambiente favorevole

13 Per meglio fruire dei vantaggi socioeconomici e ambientali offerti dalla società dell'informazione, i poteri pubblici devono creare un quadro giuridico, normativo e politico affidabile, trasparente e non discriminante. A tale scopo, bisognerebbe agire nel seguente modo:

a) I poteri pubblici dovrebbero incoraggiare l'elaborazione di un quadro giuridico e normativo propizio, trasparente, prevedibile e favorevole alla concorrenza, che stimoli adeguatamente gli investimenti e lo sviluppo comunitario nel quadro della società dell'informazione.

b) Noi chiediamo al Segretario generale delle Nazioni Unite di creare un gruppo di lavoro sulla gestione di Internet, nell'ambito di un processo aperto e inclusivo al tempo stesso, che garantisca la partecipazione piena e totale dei poteri pubblici, del settore privato e della società civile sia nei paesi in via di sviluppo che nei paesi sviluppati, e che faccia intervenire le organizzazioni intergovernative e internazionali e i forum interessati per studiare, da qui al 2005, la gestione di Internet e formulare delle proposte sulle misure da prendere. Questo gruppo dovrebbe in particolare:
   i) elaborare una definizione pratica della gestione di Internet;
   ii) identificare le questioni di interesse generale che si riferiscono alla gestione di Internet;
   iii) elaborare una concezione comune dei ruoli e delle sfere rispettive di responsabilità dei governi, delle organizzazioni intergovernative, delle organizzazioni internazionali e degli altri forum esistenti, come anche del settore privato e della società civile, sia dei paesi in via di sviluppo sia dei paesi sviluppati;
   iv) elaborare un rapporto sui risultati di quest'attività, da sottoporre ad esame per una eventuale esecuzione nella seconda fase del VMSI (Tunisi, 2005).

c) I poteri pubblici sono invitati:
   i) a facilitare l'istituzione di centri di scambio Internet nazionali e regionali;
   ii) a gestire o a soprintendere, secondo i casi, i rispettivi nomi del loro dominio di primo livello corrispondente a codici di paese (ccTLD)
   iii) a favorire la sensibilizzazione all'uso di Internet.

d) In collaborazione con le parti coinvolte interessate, promuovere l'istituzione di *root servers* regionali e l'impiego di nomi di dominio internazionalizzati per superare gli ostacoli all'accesso.

e) I poteri pubblici dovrebbero continuare ad aggiornare la loro legislazione sulla difesa del consumatore, per tenere conto dei nuovi bisogni della società dell'informazione.

f) Promuovere la partecipazione effettiva dei paesi in via di sviluppo e dei paesi ad economia in transizione ai forum internazionali dedicati alle TIC e consentire scambi di esperienze.

g) I poteri pubblici devono formulare delle strategie nazionali, soprattutto in materia di amministrazione elettronica (*e-government*), per rendere più trasparente, efficace e democratica la pubblica amministrazione.

h) Elaborare un quadro per lo stoccaggio e l'archivio in assoluta sicurezza dei documenti e delle informazioni su supporto elettronico.

i) I poteri pubblici e le parti coinvolte dovrebbero promuovere attivamente la formazione degli utenti e sensibilizzarli ai problemi della riservatezza in linea e della protezione della vita privata.

j) Invitare le parti coinvolte a fare in modo che le pratiche volte a facilitare il commercio elettronico offrano anche al consumatore la scelta di utilizzare o meno i mezzi di comunicazione elettronica.

k) Incoraggiare i lavori in corso sull'efficacia dei sistemi di regolamento delle controversie, in particolare a proposito dei metodi innovativi, suscettibili di facilitare questo compito.

l) I governi sono invitati a formulare, in collaborazione con le parti coinvolte, politiche in materia di TIC atte a stimolare lo spirito d'impresa, l'innovazione e gli investimenti, e in modo assolutamente particolare la partecipazione delle donne.

m) Tenuto conto del potenziale economico delle TIC per le piccole e medie imprese (PMI), è opportuno aiutare queste ultime a una maggiore competitività, razionalizzando le procedure amministrative, facilitando l'accesso al capitale e potenziando la loro capacità di partecipazione a progetti TIC.

n) I poteri pubblici dovrebbero svolgere il ruolo di utenti modello e adottare senza indugio il commercio elettronico, secondo il loro livello di sviluppo.

o) I governi, in collaborazione con le altre parti coinvolte, dovrebbero far conoscere meglio l'importanza delle norme internazionali relative alla interattività per il commercio elettronico mondiale.

p) I governi dovrebbero, in collaborazione con le altre parti coinvolte, promuovere l'elaborazione e l'utilizzo di norme aperte, interattive, non discriminanti e stabilite in funzione della domanda.

q) L'UIT, nella sua qualità di organizzazione abilitata a redigere documenti aventi valore di contratto, coordina e attribuisce le frequenze per facilitare un accesso universale e accessibile.

r) La UIT e altri organismi regionali dovrebbero prendere ulteriori misure per assicurare un utilizzo razionale, efficace ed economico dello spettro delle frequenze radioelettriche da parte di tutti i paesi e il loro equo accesso a questo spettro, sulla base dei relativi accordi internazionali.

C7 Le applicazioni TIC e il loro apporto in tutti i campi

14 Le applicazioni delle TIC possono contribuire a un duraturo sviluppo nei settori dell'amministrazione pubblica, del commercio, dell'insegnamento e della formazione, della salute, del lavoro, dell'ambiente, dell'agricoltura e delle scienze, nel quadro delle ciberstrategie nazionali. Sarebbe opportuno a questo proposito prendere delle misure nei seguenti campi:

15 Amministrazione elettronica

a) Mettere in opera strategie di amministrazione elettronica centrate sulle applicazioni, volte a innovare e a promuovere la trasparenza nei processi

amministrativi e democratici, a migliorarne l'efficacia e a potenziare i rapporti con i cittadini.

b) Elaborare, a tutti i livelli, programmi e servizi nazionali nell'ambito dell'amministrazione elettronica, adattati ai bisogni dei cittadini e delle imprese, per conseguire una più efficace suddivisione delle risorse e dei beni pubblici.

c) Sostenere le iniziative di cooperazione internazionale in materia di amministrazione elettronica, al fine di migliorare la trasparenza, di precisare l'obbligo dei rendiconto, e di potenziare l'efficienza a tutti i livelli dell'amministrazione.

16 Commercio elettronico

a) I governi, le organizzazioni internazionali e il settore privato sono invitati a far conoscere i vantaggi del commercio internazionale e dell'uso del commercio elettronico e a promuovere l'utilizzo di modelli di commercio elettronico nei paesi in via di sviluppo e nei paesi a economia in transizione.

b) I poteri pubblici, instaurando un ambiente favorevole e generalizzando l'accesso a Internet, dovrebbero cercare di stimolare gli investimenti del settore privato e di incoraggiare le nuove applicazioni, lo sviluppo di contenuti e i partenariati pubblico/privato.

c) Le politiche governative dovrebbero incoraggiare la crescita delle PMI e delle microimprese nel settore delle TIC, offrire loro assistenza e aiutarle ad adottare il commercio elettronico, per stimolare lo sviluppo elettronico e la creazione di posti di lavoro nel quadro di una strategia di lotta alla povertà mediante la creazione di ricchezze.

17 Teleinsegnamento (***E-learning)*** (vedere la sezione C4)

18 Informazioni sulla salute *(E-health)*

a) Promuovere la collaborazione fra poteri pubblici, amministratori, professionisti della salute e altri organismi, con la partecipazione di organizzazioni internazionali, al fine di creare dei sistemi di cura della salute e d'informazione sanitaria affidabili, reattivi, di ottima qualità e a costi accessibili, e di promuovere nel campo medico la formazione permanente, l'insegnamento e la ricerca con l'utilizzo delle TIC, pur rispettando e proteggendo il diritto dei cittadini al rispetto della loro vita privata.

b) Facilitare, in tutto il mondo, l'accesso alla conoscenza medica e ai contenuti idonei alle condizioni locali per potenziare i programmi di prevenzione e di ricerca nel campo della salute pubblica e promuovere la salute delle donne e degli uomini, per esempio per quanto riguarda i contenuti sulla sessualità e la salute genetica o sulle malattie sessualmente trasmissibili, come anche le malattie che preoccupano tutti i paesi, come l'AIDS, la malaria e la tubercolosi.

c) Annunciare, sorvegliare e controllare il diffondersi di malattie contagiose grazie al miglioramento dei sistemi comuni d'informazione.

d) Incoraggiare l'elaborazione di norme internazionali per lo scambio di dati sanitari, tenendo in dovuto conto le esigenze di riservatezza.

e) Incoraggiare l'adozione delle TIC per migliorare i sistemi di cura della salute e d'informazione sanitaria ed estenderne la copertura alle zone più lontane o mal servite e alle popolazioni più vulnerabili, riconoscendo il ruolo svolto dalle donne come prestatrici di cure sanitarie nelle loro famiglie e nelle loro comunità.

f) Potenziare e ampliare le iniziative fondate sulle TIC per offrire assistenza medica e umanitaria in caso di catastrofi naturali e in situazioni di emergenza.

19 Lavoro telematico (*E-employment)*

a) Incoraggiare, per i telelavoratori e per i teledatori di lavoro, l'elaborazione di procedure ottimali, basate, a livello nazionale, sui principi di equità e di parità fra uomo e donna, nel rispetto di tutte le norme internazionali applicabili.

b) Promuovere nuovi metodi di organizzazione del lavoro e dell'attività economica, allo scopo di migliorare la produttività, lo sviluppo e il benessere, investendo nelle TIC e nelle risorse umane.

c) Favorire il telelavoro (*teleworking)* per consentire a tutti i cittadini, in particolare nei paesi in via di sviluppo, nei PMA e nei piccoli paesi, di vivere in seno alla loro comunità e di lavorare ovunque, e per aprire alle donne e agli handicappati nuovi sbocchi professionali. Nel quadro della promozione del telelavoro, un'attenzione particolare deve essere rivolta alle strategie che favoriscono la creazione di posti di lavoro e il mantenimento di una manodopera qualificata.

d) Promuovere, nei settori delle scienze e delle tecnologie, programmi d'intervento precoce per le ragazze, per accrescere la presenza femminile nelle professioni legate alle TIC.

20 Ciberecologia

a) I governi, in collaborazione con le altre parti coinvolte, sono invitati a utilizzare e a promuovere le TIC a servizio della tutela dell'ambiente e dell'utilizzo duraturo delle risorse naturali.

b) I poteri pubblici, la società civile e il settore privato sono invitati a prendere misure e a dar vita a progetti e programmi centrati su una produzione e un consumo duraturi e sul riciclaggio, senza pericolo per l'ambiente, dei materiali e dei componenti utilizzati per le TIC gettati fra i rifiuti.

c) Stabilire sistemi di controllo utilizzando le TIC per prevedere le catastrofi naturali e le catastrofi causate dall'uomo e per valutarne l'incidenza, in particolare nei paesi in via di sviluppo, nei PMP e nei piccoli paesi.

21 Ciberagricoltura

a) Assicurare la diffusione sistematica, mediante le TIC, di informazioni sull'agricoltura, l'allevamento, la pesca, la silvicoltura e l'alimentazione, per

facilitare l'accesso a conoscenze e a informazioni complete, aggiornate e dettagliate, in particolare nelle zone rurali.

b) Nel quadro dei partenariati pubblico/privato, cercare di trarre il miglior partito possibile dall'utilizzo delle TIC a servizio del miglioramento (quantitativo e qualitativo) della produzione.

22 Ciberscienza

a) Promuovere connessioni ad Internet ad alta velocità, affidabili ed economiche, per tutte le università e gli istituti di ricerca, per aiutarli, nel ruolo essenziale che è loro specifico, nella produzione d'informazioni e di conoscenza, di insegnamento e di formazione, e per agevolare la creazione di partenariati, la cooperazione e gli scambi fra queste istituzioni.

b) Promuovere programmi di pubblicazione elettronica, di differenziazione dei prezzi e di libero accesso, per rendere le informazioni scientifiche accessibili in tutti i paesi, a condizioni giuste ed eque.

c) Incoraggiare l'utilizzo di tecnologie di scambio fra omologhi per la condivisione delle conoscenze scientifiche e quella delle pre-edizioni e riedizioni di comunicazioni redatte da scienziati che hanno rinunciato al pagamento dei diritti d'autore.

d) Promuovere la raccolta, la diffusione e la conservazione sistematiche ed efficienti dei dati numerici scientifici essenziali, per esempio per quanto riguarda la demografia e la meteorologia, in tutti i paesi e a lungo termine.

e) Sostenere i principi e le norme relativi ai metadati per facilitare la cooperazione, e l'utilizzo efficace delle informazioni e dei dati scientifici raccolti per le necessità della ricerca scientifica.

C8 Diversità e identità culturali, diversità linguistica e contenuti locali

23 Per lo sviluppo di una società dell'informazione fondata sul dialogo fra le culture e sulla cooperazione regionale e internazionale è fondamentale la diversità culturale e linguistica, che porta con sé il rispetto dell'identità culturale, delle tradizioni e delle religioni.

a) Elaborare politiche che favoriscano il rispetto, la tutela, la promozione e il potenziamento della diversità culturale e linguistica e del patrimonio culturale nel contesto della società dell'informazione, come dicono i testi in proposito adottati dalle Nazioni Unite, e soprattutto la Dichiarazione universale dell'UNESCO sulla diversità culturale. Si tratta, fra l'altro, d'incoraggiare i poteri pubblici a concepire politiche culturali favorevoli alla produzione di contenuti culturali, educativi e scientifici e allo sviluppo di industrie culturali locali idonee al contesto linguistico e culturale degli utenti.

b) Elaborare politiche e legislazioni nazionali per consentire alle biblioteche, agli archivi, ai musei e ad altre istituzioni culturali di svolgere pienamente il loro ruolo di fornitori di contenuti – conoscenze tradizionali comprese – nella società

dell'informazione, e in modo particolare di dare accesso in permanenza alle informazioni archiviate.

c) Sostenere gli sforzi volti a sviluppare e ad utilizzare le TIC per la conservazione del nostro patrimonio naturale e culturale, che bisogna continuare a rendere accessibile come elemento vivente della cultura attuale. A questo titolo, è opportuno elaborare sistemi che permettano di dare permanentemente accesso alle informazioni numeriche e ai contenuti multimediali archiviati in banche dati elettroniche e conservare gli archivi, le collezioni culturali e le biblioteche, memoria dell'umanità.

d) Elaborare e organizzare politiche volte a conservare, affermare, rispettare e promuovere la diversità dell'espressione culturale e delle conoscenze e tradizioni delle popolazioni autoctone, grazie alla creazione di contenuti informativi variati e all'utilizzo di diversi metodi, fra cui la digitalizzazione del patrimonio educativo, scientifico e culturale.

e) Sostenere l'elaborazione, la traduzione e l'adattamento dei contenuti locali, la costituzione di archivi digitali e il varo di diverse forme di media tradizionali e digitali da parte delle autorità locali. Queste attività possono anche contribuire a rinforzare le comunità locali e autoctone.

f) Fornire contenuti adattati alla cultura e alla lingua di ognuno nel contesto della società dell'informazione, dando accesso ai servizi tradizionali e digitali dei media.

g) Incoraggiare, nell'ambito di partenariati pubblico/privato, la creazione di contenuti locali e nazionali variati, in particolare quella di contenuti disponibili nella lingua degli utenti, e riconoscere e sostenere le attività basate sulle TIC in tutti i campi artistici.

h) Potenziare le attività che privilegiano i programmi differenziati, nell'insegnamento scolastico o extrascolastico per tutti, e che consentono alle donne di migliorare le proprie capacità di comunicazione e di utilizzo dei media, per rendere le donne e le ragazze più preparate a comprendere ed a elaborare dei contenuti TIC.

i) Sviluppare, a livello locale, le capacità di creazione e di diffusione, da una parte dei programmi informatici nelle lingue locali, dall'altra di contenuti adattati alle diverse categorie della popolazione, ivi compresi gli analfabeti, gli handicappati, le categorie svantaggiate o vulnerabili, in particolare nei paesi in via di sviluppo e nei paesi a economica in transizione.

j) Sostenere i media comunitari e i progetti che si richiamano sia ai media tradizionali che alle nuove tecnologie per facilitare l'uso delle lingue locali, la raccolta d'informazioni sul patrimonio locale e la sua tutela, in particolare per quanto riguarda la diversità dei paesaggi e la diversità biologica, e riconoscere che questi media costituiscono un mezzo per raggiungere le comunità rurali e i gruppi nomadi e isolati.

k) Potenziare le capacità dei popoli autoctoni a elaborare contenuti nelle loro lingue.

l) Collaborare con i popoli autoctoni e le comunità tradizionali per offrire loro i mezzi per utilizzare in modo più efficace le loro conoscenze tradizionali e per beneficiarne nella società dell'informazione.

m) Procedere a scambi di conoscenze, di esperienze e di procedimenti migliori a proposito delle strategie e degli strumenti concepiti per promuovere la diversità

culturale e linguistica a livello regionale e sub-regionale. A tale scopo, affidare a gruppi di lavoro regionali e sub-regionali lo studio di punti specifici di questo Piano d'azione per facilitare gli sforzi d'integrazione.

n) Valutare, su scala regionale, il contributo delle TIC agli scambi culturali e alle relazioni culturali reciproche e, in base ai risultati di questa valutazione, elaborare programmi appropriati.

o) I poteri pubblici dovrebbero promuovere, nell'ambito di partenariati pubblico/privato, tecnologie e programmi di ricerca e di sviluppo in diversi settori, quali la traduzione, l'iconografia o i servizi per l'assistenza vocale, come anche lo sviluppo dei materiali necessari e di diversi modelli di software, fra cui software proprietari, software a codice sorgente aperto e software liberi, quali polizze di caratteri normalizzati, codici di lingua, dizionari, strumenti terminologici e thesaurus elettronici, motori di ricerca plurilingue, strumenti di traduzione automatica, nomi di dominio internazionalizzati, campionamento di contenuti e software generali e di applicazione.

C9 *Media*

24 I media – nelle loro diverse forme e qualunque sia la forma di proprietà – svolgono un ruolo essenziale nella costruzione della società dell'informazione e sono ben noti per il loro importante contributo alla libertà d'espressione e al pluralismo dell'informazione.

a) Incoraggiare i media – stampa, radio e televisione, come anche i nuovi media – a continuare a svolgere il loro importante ruolo nella società dell'informazione.

b) Incoraggiare l'elaborazione di legislazioni nazionali che garantiscano l'indipendenza e il pluralismo dei media.

c) Prendere misure appropriate, compatibili con la libertà d'espressione, per lottare contro i contenuti illeciti e perniciosi nei media.

d) Incoraggiare i professionisti dei media dei paesi sviluppati a organizzare partenariati e reti con i loro omologhi dei paesi in via di sviluppo, in particolare nel campo della formazione.

e) Incoraggiare i media a offrire una immagine equilibrata e diversificata delle donne e degli uomini.

f) Ridurre gli squilibri fra nazioni nel campo dei media, in particolare per quanto riguarda le infrastrutture, le risorse tecniche e la valorizzazione delle competenze umane, avvalendosi a questo proposito dei mezzi TIC.

g) Incoraggiare i media tradizionali a ridurre il divario del sapere e a facilitare i flussi di contenuti culturali, soprattutto nelle regioni rurali.

C10 Dimensioni etiche della società dell'informazione

25 La società dell'informazione dovrebbe essere fondata su valori universali, cercare di promuovere il bene comune ed evitare gli usi nefasti delle TIC.

a) Prendere misure atte a promuovere il rispetto della pace e a conservare i valori fondamentali, quali la libertà, l'uguaglianza, la solidarietà, la tolleranza, la condivisione delle responsabilità e il rispetto della natura.
b) Tutte le parti coinvolte dovrebbero essere maggiormente consapevoli della dimensione etica del loro utilizzo delle TIC.
c) Tutti gli attori della società dell'informazione dovrebbero favorire il bene comune, proteggere la vita privata e i dati personali e prendere le misure necessarie, anche a titolo preventivo, così come sono definite dalla legge, contro le utilizzazioni nefaste delle TIC, come gli atti delittuosi e altri atti dettati dal razzismo, la discriminazione razziale e la xenofobia, come l'intolleranza, l'odio e la violenza che ne risultano, tutte le forme di maltrattamento dei bambini, in particolare la pedofilia e la pornografia infantile, e la tratta e lo sfruttamento degli esseri umani.
d) Invitare le parti coinvolte, in particolare le università, a condurre ricerche sulla dimensione etica delle tecnologie dell'informazione e sulla comunicazione.

C11 Cooperazione internazionale e regionale

26 Per la concretizzazione di questo Piano d'azione è essenziale una cooperazione internazionale fra tutte le parti coinvolte, che deve essere potenziata al fine di promuovere l'accesso universale e ridurre il divario digitale, in particolare mettendo a disposizione i mezzi necessari a questa realizzazione.

a) Nei paesi in via di sviluppo, i poteri pubblici dovrebbero accordare maggiore attenzione ai progetti TIC nelle richieste di cooperazione e di aiuto internazionali riguardanti i progetti di sviluppo d'infrastrutture presentati ai paesi sviluppati e agli organismi di finanziamento internazionali.
b) Nel quadro del Accordo Mondiale delle Nazioni Unite e sulla base della Dichiarazione del Millennio delle Nazioni Unite, ampliare i partenariati pubblico/privato e accelerarne la realizzazione, ponendo l'accento sull'impiego delle TIC per lo sviluppo.
c) Chiedere alle organizzazioni internazionali e regionali d'inserire le TIC nei loro programmi di lavoro e di aiutare i paesi in via di sviluppo, qualunque sia il loro livello di sviluppo, a partecipare alla preparazione e alla concretizzazione di piani d'azione nazionali per sostenere la realizzazione degli obiettivi enunciati nella Dichiarazione di principi e in questo Piano d'azione, pur tenendo conto dell'importanza delle iniziative regionali.

D Patto di solidarietà informatica

27 Il Patto di solidarietà informatica è volto a instaurare le condizioni idonee alla mobilitazione delle risorse umane, finanziarie e tecnologiche necessarie affinché tutti gli uomini e tutte le donne partecipino alla nascente società dell'informazione. E' indispensabile dunque una stretta collaborazione, regionale e internazionale, fra tutte le parti coinvolte nella messa in esecuzione di questo programma. Per risolvere il problema del divario digitale, dobbiamo utilizzare in modo più efficace i metodi e i meccanismi esistenti e considerare in modo approfondito tutte le nuove possibilità per finanziare lo sviluppo delle infrastrutture, le attrezzature, il potenziamento delle capacità e i contenuti, essenziali per la partecipazione alla società dell'informazione.

D1 Priorità e strategie

a) Parte integrante dei piani di sviluppo nazionali dovrebbero essere le ciberstrategie nazionali, ivi comprese le strategie di riduzione della povertà

b) Le TIC dovrebbero essere integrate pienamente nelle strategie di aiuto pubblico allo sviluppo (APS) nel quadro di uno scambio d'informazioni e di un coordinamento più efficaci fra i donatori e grazie all'analisi e allo scambio delle migliori prassi e dell'esperienza scaturita dai programmi «TIC per lo sviluppo».

D2 Mobilitazione delle risorse

a) Tutti i paesi e tutte le organizzazioni internazionali dovrebbero operare per riunire le condizioni idonee ad accrescere la disponibilità delle risorse di finanziamento dello sviluppo e a consentire una mobilitazione efficace di queste risorse, secondo le linee tracciate dal Consenso di Monterrey.

b) I paesi sviluppati dovrebbero prendere provvedimenti concreti per rispettare i propri impegni internazionali di finanziamento dello sviluppo, in particolare il Consenso di Monterrey, nell'ambito del quale ai paesi sviluppati che non l'hanno ancora fatto è richiesto di mettere in atto misure concrete affinché i fondi assegnati all'aiuto pubblico ai paesi in via di sviluppo raggiungano l'obiettivo fissato, vale a dire lo 0,7% del loro prodotto nazionale lordo (PNL) e perché consacrino dallo 0,15 allo 0,20% del loro PNL ai paesi meno progrediti.

c) Per quanto riguarda i paesi in via di sviluppo il cui indebitamento non è sostenibile, ci rallegriamo per le iniziative prese da alcuni per ridurre l'entità del loro debito, e incoraggiamo l'assunzione di altre misure nazionali e internazionali a questo proposito, in particolare, eventualmente, l'annullo del debito e altri accordi. Bisognerebbe rivolgere una particolare attenzione al miglioramento dell'Iniziativa per i paesi poveri molto indebitati. Simili programmi permetterebbero di liberare risorse complementari che potrebbero essere utilizzate per finanziare progetti di applicazione delle TIC per lo sviluppo.

d) Riconoscendo le possibilità offerte dalle TIC, raccomandiamo quanto segue:

   i) sarebbe opportuno che i paesi in via di sviluppo raddoppiassero gli sforzi per ottenere importanti investimenti nazionali ed esteri per le TIC, creando un contesto trasparente, stabile e prevedibile propizio agli investimenti;

ii) sarebbe opportuno che i paesi sviluppati e le organizzazioni finanziarie internazionali tenessero conto delle strategie e delle priorità relative alle TIC per lo sviluppo, inserissero le TIC nei loro programmi d'attività e aiutassero i paesi in via di sviluppo e i paesi a economia in transizione a elaborare, e poi a mettere in esecuzione, le loro ciberstrategie nazionali. In base alle priorità dei piani di sviluppo nazionali e della realizzazione degli impegni precitati, i paesi sviluppati dovrebbero intensificare gli sforzi per fornire ai paesi in via di sviluppo maggiori risorse finanziarie che permettano loro di trarre profitto dalle TIC per lo sviluppo;

iii) sarebbe opportuno che il settore privato contribuisse alla realizzazione del presente Patto di solidarietà informatica.

e) Negli sforzi che mettiamo in atto per ridurre il divario digitale, dovremmo promuovere, nel quadro della cooperazione allo sviluppo, un'assistenza tecnica e finanziaria per il potenziamento delle capacità al livello nazionale e regionale, il trasferimento di tecnologia secondo le condizioni reciprocamente concordate, la collaborazione ai programmi di ricerca e di sviluppo e lo scambio di capacità.

f) Se è vero che è opportuno beneficiare completamente dei meccanismi di finanziamento esistenti, bisognerebbe che prima della fine di dicembre 2004 fosse condotto in porto un attento esame di questi meccanismi, per sapere se sono adeguati e se permettono di far fronte alle sfide delle TIC per lo sviluppo. Tale esame dovrebbe essere affidato a un Gruppo operativo, sotto l'egida del Segretario generale dell'Organizzazione delle Nazioni Unite, e i risultati dovrebbero essere sottoposti all'attenzione dei partecipanti alla seconda fase del Vertice. Sulla base di queste conclusioni, si prenderanno in considerazione miglioramenti e innovazioni riguardanti i meccanismi di finanziamento, in particolare la loro efficacia, la fattibilità e la creazione di un Fondo di solidarietà informatica alimentato da contributi volontari, come indicato nella Dichiarazione di principi.

g) Per ridurre il divario digitale, i paesi dovrebbero pensare a mettere a punto dei meccanismi nazionali che consentano di giungere all'accesso universale nelle zone mal servite, sia rurali che urbane.

E Controllo e valutazione

28 E' possibile elaborare un sistema internazionale realistico di controllo e di valutazione (sia qualitativo che quantitativo) impiegando indicatori statistici paragonabili e i risultati delle ricerche per seguire i progressi realizzati, in riferimento agli obiettivi, agli scopi e traguardi del presente Piano d'azione e tenuto conto delle condizioni proprie di ogni paese.

a) In collaborazione con tutti i paesi interessati, elaborare e realizzare un indice composito di sviluppo delle TIC (opportunità informatiche). Questo indice, che potrebbe essere pubblicato annualmente o ogni due anni in un rapporto sullo sviluppo delle TIC, rifletterebbe l'aspetto statistico, mentre il rapporto presenterebbe un'analisi delle politiche e della loro realizzazione secondo i paesi, anche per quanto riguarda le questioni della parità fra uomo e donna.

b) Indicatori e criteri di riferimento adattati, compresi anche alcuni indicatori di connettività comunitaria, dovrebbero consentire di precisare l'estensione del divario digitale nelle dimensioni nazionale e internazionale e di valutarla a intervalli regolari, per fare il punto sui progressi nell'utilizzo delle TIC realizzati nel mondo per raggiungere gli obiettivi internazionali di sviluppo, in particolare quelli enunciati nella Dichiarazione del Millennio.
c) Gli organismi internazionali e regionali dovrebbero valutare le possibilità di accesso universale alle TIC nei diversi paesi, e rendere regolarmente conto della situazione, per aprire al settore delle TIC nei paesi in via di sviluppo ragionevoli prospettive di crescita.
d) E' opportuno elaborare indicatori sull'utilizzo e sulle necessità specifiche legati al genere, e mettere a punto degli indicatori di performance misurabili per valutare le ripercussioni sulla vita delle donne e delle ragazze dei progetti TIC che beneficiano di un finanziamento.
e) Concepire e realizzare un sito web dedicato alle migliori procedure e ad esempi di successo, che raccolga i contributi di tutti le parti coinvolte, in una presentazione concisa, accessibile e incisiva, conforme alle norme di accessibilità al web riconosciute a livello internazionale. Questo sito potrebbe essere regolarmente aggiornato e divenire uno strumento permanente di scambio di esperienze.
f) Tutti i paesi e tutte le regioni dovrebbero elaborare strumenti e indicatori fondamentali che consentano di disporre di statistiche sulla società dell'informazione, e di analizzarne i principali aspetti. Tenuto conto dei diversi livelli di sviluppo, bisognerebbe dare la priorità a sistemi di indicatori coerenti e confrontabili su scala internazionale.

F Verso la seconda fase del Vertice Mondiale sulla Società dell'Informazione VMSI (Tunisi)

29 Alla luce della Risoluzione 56/183 dell'Assemblea generale, e tenuto conto della prima fase di Ginevra del VMSI, nel primo semestre del 2004 si svolgerà una riunione preparatoria per considerare le questioni relative alla società dell'informazione sulle quali dovrebbe essere fondata la fase di Tunisi del VMSI e per fissare la struttura del processo di preparazione della seconda fase. In conformità alla decisione presa dal presente Vertice a proposito della sua fase di Tunisi, i partecipanti dovrebbero, nel corso della seconda fase del VMSI, considerare, fra gli altri, i seguenti punti:

a) Elaborazione dei testi finali appropriati, fondati sui risultati della fase di Ginevra del VMSI, per consolidare il processo di edificazione di una società dell'informazione universale, ridurre il divario digitale e trasformarla in opportunità numerica.
b) Controllo e realizzazione del Piano d'azione di Ginevra su scala nazionale, regionale e internazionale, e anche al livello delle organizzazioni del sistema delle Nazioni Unite, nell'ambito di un approccio integrato e coordinato, cui tutte le parti coinvolte sono invitate a partecipare. Questa partecipazione dovrebbe essere assicurata, fra l'altro, mediante partenariati fra le parti coinvolte.

sommet mondial sur
la société de l'information
Genève 2003 - Tunis 2005

VERTICE MONDIALE SULLA SOCIETA' DELL'INFORMAZIONE
GINEVRA 2003 – TUNISI 2005

Documento WSIS-05/TUNIS/DOC/007-F
15 novembre
Originale: inglese

IMPEGNO DI TUNISI*

1 **Noi, rappresentanti dei popoli del mondo**, ci siamo riuniti a Tunisi dal 16 al 18 novembre 2005 per la seconda fase del Vertice Mondiale sulla Società dell'Informazione (SMSI) con l'obiettivo di ribadire il nostro indefettibile sostegno alla Dichiarazione di Principi e al Piano di Azione adottati a Ginevra nella prima fase del Vertice Mondiale sulla Società dell'Informazione, nel dicembre 2003.

2 **Ribadiamo** la nostra volontà e il nostro impegno ad edificare una società dell'informazione a dimensione umana, inclusiva e che privilegia lo sviluppo, in conformità con gli obiettivi ed i principi della Carta delle Nazioni Unite, il diritto internazionale ed il multilateralismo, rispettando pienamente e sostenendo la Dichiarazione universale dei diritti dell'uomo affinché ovunque nel mondo le persone possano creare, ottenere, utilizzare e condividere l'informazione e la conoscenza per realizzare l'integralità del loro potenziale e per attuare gli scopi ed obiettivi di sviluppo concordati a livello internazionale, in particolare gli Obiettivi del Millennio per lo Sviluppo.

3 **Ribadiamo** l'universalità, l'indivisibilità, l'interdipendenza e l'interazione di tutti i diritti e delle libertà fondamentali dell'uomo, compreso il diritto allo sviluppo, così come è stato proclamato nella Dichiarazione di Vienna. **Ribadiamo altresì** che la democrazia, lo sviluppo sostenibile e il rispetto dei diritti e delle libertà fondamentali dell'uomo nonché il buon governo a tutti i livelli sono interdipendenti e si rafforzano a vicenda. **Siamo decisi inoltre** a rafforzare il rispetto per la preminenza del diritto sia negli affari internazionali che in quelli nazionali.

4 **Ribadiamo** quanto è stato dichiarato nei paragrafi 4, 5 e 55 della Dichiarazione di Principi di Ginevra. **Riconosciamo** che la libertà di espressione e la libera circolazione delle informazioni, delle idee e della conoscenza sono essenziali per la società dell'informazione e favoriscono lo sviluppo.

5 Il Vertice di Tunisi costituisce per noi un'opportunità unica per far prendere coscienza dei vantaggi che le tecnologie dell'informazione e della comunicazione (TIC) possono portare all'umanità e del modo in cui possono trasformare le attività, i rapporti e la vita delle persone e, di conseguenza, rafforzare la fiducia nel futuro.

6 Questo Vertice costituisce una tappa importante nella lotta che impegna il mondo intero per sradicare la povertà e per attuare gli scopi e gli obiettivi di sviluppo decisi a livello internazionale, in particolare gli Obiettivi del Millennio per lo Sviluppo. Con le decisioni di

* Revisione della traduzione dal francese a cura dell'Unità operativa traduzione e interpretariato del Servizio Affari internazionali.

Ginevra, abbiamo stabilito un legame coerente a lungo termine tra il processo del SMSI ed altri vertici e conferenze importanti e pertinenti dell'Organizzazione delle Nazioni Unite. **Esortiamo** i governi, il settore privato, la società civile e le organizzazioni internazionali ad operare insieme per attuare gli impegni enunciati nella Dichiarazione di Principi e nel Piano di Azione di Ginevra. A questo riguardo, è opportuno segnalare la peculiare importanza che ha rivestito il Vertice Mondiale del 2005 sull'attuazione della Dichiarazione del Millennio.

7 **Ribadiamo gli impegni presi a Ginevra** e ne traiamo ispirazione, qui a Tunisi, dedicandoci ai meccanismi finanziari volti a ridurre il divario digitale, alla *governance* di Internet e alle questioni connesse, nonché ai seguiti e all'attuazione delle decisioni di Ginevra e di Tunisi, stabiliti nell'Agenda di Tunisi per la società dell'informazione.

8 Pur riaffermando il ruolo e le responsabilità importanti di tutte le parti interessate, richiamati dal paragrafo 3 del Piano di Azione di Ginevra, **riconosciamo** il ruolo fondamentale e le responsabilità dei governi nel processo del SMSI.

9 **Ribadiamo la nostra determinazione** nel far sì che ognuno possa beneficiare delle opportunità offerte dalle TIC, ricordando che i governi, così come il settore privato, la società civile e l'Organizzazione delle Nazioni Unite ed altre organizzazioni internazionali, dovrebbero lavorare assieme per migliorare l'accesso alle infrastrutture e alle TIC nonché all'informazione e alla conoscenza, per rafforzare le capacità, accrescere la fiducia e la sicurezza nell'uso delle TIC, creare un ambiente propizio a tutti i livelli, sviluppare e allargare le applicazioni delle TIC, favorire e rispettare la diversità culturale, riconoscere il ruolo dei media, prendere in considerazione le dimensioni etiche della società dell'informazione ed incoraggiare la cooperazione internazionale e regionale. **Ribadiamo** che questi sono i principi fondamentali dell'edificazione di una società dell'informazione inclusiva, di cui viene delineato il progetto nella Dichiarazione di Principi di Ginevra.

10 **Riconosciamo** che l'accesso all'informazione, la condivisione e la creazione delle conoscenze contribuiscono in modo significativo a rafforzare lo sviluppo economico, sociale e culturale, e aiutano dunque tutti i Paesi a raggiungere gli scopi e gli obiettivi di sviluppo stabiliti a livello internazionale, ed in particolare gli Obiettivi del Millennio per lo Sviluppo. Questo processo può essere rafforzato con la rimozione degli ostacoli ad un accesso universale, ubiquitario, equo ed economicamente affrontabile all'informazione. **Insistiamo** sull'importanza della rimozione degli ostacoli alla riduzione del divario digitale, in particolare degli ostacoli che intralciano la piena attuazione dello sviluppo economico, sociale e culturale dei Paesi e del benessere delle loro popolazioni, con particolar riguardo ai Paesi in via di sviluppo.

11 Le TIC, inoltre, consentono ad una platea ampia come mai nel passato di partecipare all'allargamento della base del sapere umano ed alla condivisione della conoscenza in tutte le sfere di attività, contribuendo in particolare alla loro crescita ed applicazione all'insegnamento, alla salute ed alla scienza. Le TIC offrono un enorme potenziale per allargare l'accesso ad un insegnamento di qualità, favorire l'alfabetizzazione e l'istruzione primaria universale e facilitare il processo stesso di apprendimento – per aprire così la via alla costruzione di una società dell'informazione e di un'economia della conoscenza davvero inclusive, che privilegino lo sviluppo e che rispettino la diversità culturale e linguistica.

12 **Insistiamo** sul fatto che l'adozione delle TIC da parte delle imprese svolge un ruolo fondamentale nella crescita economica. Gli effetti positivi, per la crescita e per la produttività, degli investimenti attuati con accortezza nel settore delle TIC possono rafforzare gli scambi commerciali e permettere di creare un maggior numero di posti di lavoro qualificati. Pertanto le politiche di sviluppo dell'impresa e del mercato del lavoro svolgono un ruolo fondamentale nell'adozione delle TIC. **Invitiamo** i governi e il settore privato a rafforzare le capacità delle piccole, medie e micro imprese (PMMI) che, nella maggior parte dei Paesi, costituiscono le più grandi risorse occupazionali. **Lavoreremo insieme,** con tutte le parti interessate, all'attuazione dei quadri politici, giuridici e regolamentari necessari, atti a favorire l'imprenditorialità, con particolar riguardo alle PMMI.

13 **Riconosciamo inoltre** che la rivoluzione delle TIC potrebbe avere numerose ripercussioni favorevoli come strumento di sviluppo sostenibile. L'esistenza, inoltre, di un ambiente propizio a livello nazionale ed internazionale potrebbe prevenire l'aumento delle divisioni sociali ed economiche nonché l'allargamento del divario tra Paesi ricchi e Paesi poveri, tra regioni e tra individui – incluso quello tra uomini e donne.

14 **Riconosciamo inoltre** che per completare la realizzazione di infrastrutture TIC, bisognerebbe privilegiare lo sviluppo delle capacità umane e la creazione di applicazioni TIC e di contenuti digitali in lingue locali, se necessario, in modo d rendere possibile la prospettiva della costruzione di una società mondiale dell'informazione sotto il profilo globale.

15 Prendendo atto dei principi dell'accesso universale e non discriminatorio alle TIC per tutte le nazioni, della necessità di prendere in considerazione il livello di sviluppo sociale ed economico di ogni Paese e nel rispetto degli aspetti della società dell'informazione che previlegiano lo sviluppo, **insistiamo** sul fatto che le TIC sono strumenti efficaci per promuovere la pace, la sicurezza e la stabilità, per rafforzare la democrazia, la coesione sociale, il buon governo e la preminenza del diritto, a livello nazionale, regionale ed internazionale. Le TIC possono servire a promuovere la crescita economica e lo sviluppo delle imprese. Per raggiungere questi obiettivi, è fondamentale sviluppare le infrastrutture, rafforzare le capacità umane e la sicurezza delle reti. **Siamo peraltro consapevoli** della necessità di fare fronte efficacemente alle sfide e alle minacce derivanti dall'uso delle TIC a fini incompatibili con gli obiettivi di mantenimento della stabilità e della sicurezza internazionali, i quali rischiano di nuocere all'integrità delle infrastrutture nazionali, a discapito della sicurezza degli Stati. È necessario prevenire ogni tipo di uso abusivo delle risorse e tecnologie dell'informazione a fini criminali e terroristici, fermo restando il rispetto dei diritti umani.

16 **Ci impegniamo inoltre** a valutare e a seguire i progressi realizzati in vista di ridurre il divario digitale, enendo conto dei diversi livelli di sviluppo, per raggiungere gli scopi ed obiettivi di sviluppo approvati a livello internazionale, in particolar modo gli Obiettivi del Millennio per lo Sviluppo, e a valutare l'efficacia degli investimenti e della cooperazione internazionale nella costruzione della società dell'informazione.

17 **Esortiamo i governi**, utilizzando il potenziale delle TIC, a creare dei sistemi pubblici d'informazione sulle leggi ed i regolamenti, a considerare la possibilità di sviluppare più ampiamente i punti di accesso pubblici e ad agevolare la disponibilità generale di questa informazione.

18 **Dobbiamo pertanto profondere il nostro costante impegno** nella promozione di un accesso universale, ubiquitario, equo e finanziariamente affrontabile alle TIC, compreso quello a tecnologie concepite per essere universali e a tecnologie di facilitazione, a vantaggio di tutte le popolazioni del mondo e in particolare delle persone disabili, in modo tale che i vantaggi siano meglio ripartiti fra le società e all'interno delle società e che il divario digitale sia ridotto, per creare delle opportunità digitali per tutti e sfruttare le possibilità che le TIC offrono allo sviluppo.

19 Sarebbe opportuno che la comunità internazionale prendesse le misure necessarie per far sì che tutti i Paesi del mondo potessero trarre beneficio da un accesso equo ed economicamente affrontabile alle TIC, affinché i vantaggi offerti da queste tecnologie nei settori dello sviluppo socio-economico e della riduzione del divario digitale siano veramente inclusivi.

20 A tal fine, **dobbiamo rivolgere un'attenzione particolare** alle esigenze specifiche dei gruppi sociali emarginati e vulnerabili, compresi i migranti, i profughi e i rifugiati, i disoccupati e le persone disagiate, le minoranze e le popolazioni nomadi, gli anziani e i disabili.

21 A tal fine, **dobbiamo rivolgere un'attenzione particolare** alle specifiche esigenze delle popolazioni dei Paesi in via di sviluppo, dei Paesi con economia in transizione, dei Paesi meno avanzati, dei piccoli Stati insulari in via di sviluppo, dei Paesi in via di sviluppo interclusi, dei Paesi poveri pesantemente indebitati, dei Paesi e territori sotto occupazione e dei Paesi riemergenti dopo un conflitto od una calamità naturale.

22 Nell'evoluzione della società dell'informazione, bisogna rivolgere un'attenzione particolare alla situazione speciale delle popolazioni indigene, nonché alla preservazione della loro eredità, in particolare quella culturale.

23 **Riconosciamo** l'esistenza di un divario tra uomini e donne all'interno del divario digitale, e **riaffermiamo la nostra ferma adesione** alla causa dell'autonomizzazione delle donne e della parità fra i sessi, per poter ridurre tale divario. **Riconosciamo inoltre** che la piena partecipazione delle donne è necessaria nella società dell'informazione, affinché siano in essa garantiti l'inclusione e il rispetto dei diritti umani. **Incoraggiamo** tutte le parti interessate ad appoggiare la partecipazione delle donne in tutti i processi decisionali, affinché possano contribuire ad esercitare la loro influenza in tutti i settori della società dell'informazione, a livello mondiale, regionale e nazionale.

24 **Riconosciamo** il ruolo delle TIC nella protezione e nello sviluppo dell'infanzia. **Rafforzeremo le misure** atte a proteggere i bambini da ogni abuso e a garantire la difesa dei loro diritti nel contesto delle TIC. A questo riguardo, **insistiamo** sul fatto che il superiore interesse del bambino debba essere un fattore di considerazione primaria.

25 **Ribadiamo il nostro impegno** ad autonomizzare i giovani quali protagonisti della costruzione di una società dell'informazione inclusiva. **Coinvolgeremo attivamente** i giovani nei programmi di sviluppo innovativi e basati sulle TIC, e moltiplicheremo le possibilità che si offrono a loro nella partecipazione ai processi delle strategie cibernetiche.

26 **Riconosciamo** l'importanza dei contenuti creativi e delle applicazioni creative per superare il divario digitale e contribuire all'attuazione degli scopi e degli obiettivi decisi a livello internazionale, con particolar riguardo agli Obiettivi del Millennio per lo Sviluppo.

27 **Riconosciamo** che l'accesso equo e sostenibile all'informazione necessita dell'attuazione di strategie per la preservazione a lungo termine delle informazioni digitali create.

28 **Ribadiamo la nostra volontà** di realizzare reti ed applicazioni TIC e di concepire applicazioni, in partenariato con il settore privato, fondate su norme aperte o interoperabili, che siano finanziariamente affrontabili e accessibili in ogni località, in ogni momento e a tutte le categorie di utenti, in modo da costruire una rete ubiquitaria.

29 **La nostra convinzione** è che i governi, il settore privato, la società civile, la comunità scientifica e universitaria e gli utenti possono utilizzare diverse tecnologie e diversi modelli di concessione di licenze, in particolare le tecnologie ed i modelli messi a punto secondo schemi proprietari o a condizioni di fonte aperta e di libero accesso, in base ai loro interessi e alla necessità di disporre di servizi affidabili e di attuare programmi efficaci per le loro popolazioni. Considerata l'importanza dei *software* proprietari nei mercati dei vari Paesi, **ricordiamo** la necessità di incoraggiare e di promuovere lo sviluppo, in collaborazione, di piattaforme compatibili e di *software* liberi e a fonte aperta, secondo modalità in cui convergano le possibilità offerte da tutti i modelli, in particolare per i programmi educativi, scientifici e ad inclusione digitale.

30 Riconoscendo che la riduzione degli effetti delle calamità naturali può contribuire in modo significativo ad uno sviluppo sostenibile ed agevolare gli sforzi diretti a sradicare la povertà, **ribadiamo il nostro impegno** a sfruttare al meglio le capacità ed il potenziale delle TIC, agevolando e rafforzando la cooperazione a livello nazionale, regionale e mondiale.

31 **Ci impegniamo** a lavorare assieme alla realizzazione del patto di solidarietà digitale di cui al paragrafo 27 del Piano di Azione di Ginevra. Fermo restando il rispetto del buon governo a tutti i livelli, la piena e rapida attuazione di questo patto necessita, in particolare, di una soluzione veloce, efficace, completa e durevole al problema del debito dei paesi in via di sviluppo e, all'occorrenza, di un sistema commerciale multilaterale universale, basato su regole, aperto, non discriminatorio ed equo, in grado inoltre di stimolare lo sviluppo in tutto il mondo, nell'interesse dei Paesi in tutte le fasi di sviluppo e richiede altresì la ricerca e l'applicazione effettiva di approcci e meccanismi internazionali concreti diretti a rafforzare la cooperazione e l'assistenza internazionale per ridurre il divario digitale.

32 **Ci impegniamo inoltre** a promuovere l'inclusione di tutti i popoli nella società dell'informazione, attraverso l'uso delle lingue locali e/o indigene nelle TIC. **Continueremo** ad impegnarci a proteggere e promuovere la diversità culturale e delle identità culturali nella società dell'informazione.

33 **Riconosciamo** che, se è vero che la cooperazione tecnica può essere utile, è necessario rafforzare le capacità a tutti i livelli per far sì che siano disponibili le necessarie competenze istituzionali ed individuali.

34 **Riconosciamo che è necessario** mobilitare le risorse, sia umane che finanziarie, in accordo con il capitolo due, per poter accrescere l'uso delle TIC per lo sviluppo e attuare a breve, medio e lungo termine progetti di costruzione della società dell'informazione,

nell'ambito dei seguiti e dell'attuazione dei risultati del SMSI, **e profonderemo il nostro impegno per conseguire tali risultati**.

35 **Riconosciamo** il ruolo centrale delle politiche generali nell'elaborazione del quadro nel quale la mobilitazione delle risorse potrà verificarsi.

36 **Apprezziamo** il ruolo che possono svolgere le TIC per promuovere la pace e prevenire i conflitti che, *fra l'altro,* hanno incidenze negative sull'attuazione degli obiettivi di sviluppo. Le TIC possono essere utilizzate per individuare le situazioni di conflitto grazie a sistemi di allerta avanza, per prevenire i conflitti, promuoverne la pacifica composizione, appoggiare le azioni di aiuto umanitario, con particolar riguardo alla protezione dei civili nei conflitti armati, agevolare le operazioni di mantenimento della pace e contribuire al ristabilimento della pace ed alla ricostruzione dopo i conflitti.

37 **Siamo convinti** che è possibile raggiungere gli obiettivi che ci siamo prefissi grazie alla partecipazione, alla cooperazione e al partenariato dei governi e delle altre parti interessate, ossia il settore privato, la società civile e le organizzazioni internazionali, e che la cooperazione internazionale e la solidarietà a tutti i livelli sono indispensabili se i frutti della società dell'informazione devono essere divisi equamente fra tutti.

38 **I nostri sforzi** non si fermeranno con la conclusione del Vertice. La realizzazione della società mondiale dell'informazione alla quale tutti noi contribuiamo offre sempre maggiori possibilità a tutti i popoli della Terra e alla comunità mondiale, possibilità che erano inimmaginabili solo qualche anno fa. **Dobbiamo** metterle a frutto oggi e far sì che si sviluppino e che si moltiplichino ulteriormente.

39 **Ribadiamo** la nostra ferma determinazione ad attuare una risposta efficace e duratura alle sfide e alle opportunità di costruire una società dell'informazione veramente mondiale che porti beneficio a tutti i popoli della Terra.

40 **Crediamo fermamente** nella completa e rapida attuazione delle decisioni che abbiamo preso a Ginevra e a Tunisi, secondo quanto enunciato nell'Agenda di Tunisi per la società dell'informazione.

25 novembre 2005
Originale: inglese

sommet mondial sur la société de l'information
Genève 2003 - Tunis 2005

Presidente del PrepCom della fase di Tunisi

AGENDA DI TUNISI PER LA SOCIETÀ DELL'INFORMAZIONE

INTRODUZIONE

VERTICE MONDIALE SULLA SOCIETA' DELL'INFORMAZIONE	**Documento WSIS-05/TUNIS/DOC/6(Rév.1)-F**

1 **Siamo consapevoli** che è arrivato il momento di passare dai principi all'azione, pur tenendo conto dei lavori in corso per attuare il Piano di Azione di Ginevra ed individuando i settori in cui i progressi sono stati realizzati, sono in corso o non si sono ancora verificati.

2 **Teniamo a ribadire** gli impegni assunti a Ginevra e ad ispirarci ad essi, qui a Tunisi, soffermandoci sui meccanismi di finanziamento rivolti a ridurre il divario digitale, sulla *governance* di Internet e le questioni connesse, nonché sui seguiti e sull'attuazione delle decisioni di Ginevra e di Tunisi.

MECCANISMI DI FINANZIAMENTO PER RISPONDERE ALLE SFIDE DELLE TIC PER LO SVILUPPO

3 **Ringraziamo** il Segretario Generale dell'ONU per aver creato il Gruppo di Azione sui meccanismi di finanziamento (TFFM) e ci complimentiamo con i membri di questo Gruppo per la relazione da essi stilata.

4 **Ricordiamo** che il TFFM doveva procedere ad un esame approfondito dei meccanismi di finanziamento esistenti per sapere se fossero adeguati e in grado di fare fronte alle sfide delle TIC per lo sviluppo.

5 Dalla relazione del TFFM emerge la complessità dei meccanismi esistenti, privati o pubblici, che assicurano il finanziamento delle TIC nei Paesi in via di sviluppo. La relazione individua i settori nei quali i Paesi in via di sviluppo ed i loro *partner* per lo sviluppo potrebbero conferire un rango di priorità più elevato alle TIC.

6 Tenendo conto della conclusione dell'esame della relazione, **abbiamo preso in considerazione** i miglioramenti e le innovazioni che è stato proposto di introdurre nei meccanismi di finanziamento, in particolare la creazione di un Fondo di Solidarietà Digitale, richiamata nella Dichiarazione di principi di Ginevra.

7 **Riconosciamo** l'esistenza del divario digitale e delle difficoltà che esso pone a numerosi Paesi che si vedono obbligati a scegliere tra un gran numero di obiettivi concorrenti nella pianificazione del loro sviluppo e nelle richieste di crediti di sviluppo, mentre dispongono di risorse limitate.

8 **Siamo consapevoli** dell'entità del problema di ridurre il divario digitale, operazione che esige investimenti adeguati e sostenibili nell'infrastruttura e nei servizi TIC, nonché nel rafforzamento delle capacità e nei trasferimenti di tecnologia per molti anni.

9 **Invitiamo la comunità internazionale** a promuovere, secondo condizioni concordate, il trasferimento delle tecnologie, soprattutto delle TIC, e ad adottare politiche e programmi diretti ad aiutare i Paesi in via di sviluppo a sfruttare la tecnologia nella propria ricerca dello sviluppo, in particolare nell'ambito della cooperazione tecnica e del rafforzamento delle capacità scientifiche e tecnologiche attraverso i nostri sforzi tesi a ridurre il divario digitale e quello dello sviluppo.

10 **Riconosciamo** che gli scopi e gli obiettivi di sviluppo stabiliti a livello internazionale, in particolare gli Obiettivi del Millennio per lo Sviluppo, sono fondamentali. Il consenso di Monterrey sul finanziamento per lo sviluppo è la base dell'attuazione di meccanismi di finanziamento adeguati ed appropriati per promuovere le TIC per lo sviluppo, in conformità con il patto di solidarietà digitale del Piano di Azione di Ginevra.

11 **Riconosciamo – e ne prendiamo atto –** le speciali e specifiche esigenze di finanziamento, menzionate al paragrafo 16 della Dichiarazione di principi di Ginevra[*], del mondo in via di sviluppo, il quale deve risolvere numerosi problemi nel settore delle TIC. Sappiamo che è indispensabile prendere in considerazione queste speciali esigenze di finanziamento per raggiungere gli scopi e gli obiettivi di sviluppo stabiliti a livello internazionale, in particolare gli Obiettivi del Millennio per lo Sviluppo.

12 **Riconosciamo** che il finanziamento delle TIC per lo sviluppo deve inserirsi nel contesto della sempre maggiore importanza del ruolo delle TIC, non solo come mezzo di comunicazione, ma anche come motore di sviluppo e come strumento che consente di raggiungere gli scopi e gli obiettivi di sviluppo stabiliti a livello internazionale, in particolare gli Obiettivi del Millennio per lo Sviluppo.

13 In passato, il finanziamento delle infrastrutture TIC, nella maggior parte dei Paesi in via di sviluppo, era basato sugli investimenti pubblici. Ultimamente, si è verificato un importante afflusso di risorse finanziarie, nel quale la partecipazione del

---

[*] Per una maggiore semplicità, riproduciamo qui sotto il paragrafo 16 della Dichiarazione di Principi di Ginevra:
Continuiamo a rivolgere un'attenzione particolare alle esigenze specifiche delle popolazioni dei Paesi in via di sviluppo, dei Paesi con economia in transizione, dei Paesi meno avanzati, dei piccoli Stati insulari in via di sviluppo, dei Paesi in via di sviluppo interclusi, dei Paesi poveri pesantemente indebitati, dei Paesi e territori sotto occupazione, dei Paesi emergenti da conflitti e dei Paesi e regioni aventi esigenze particolari, nonché alle situazioni che fanno gravare pesanti minacce sullo sviluppo, come per esempio le calamità naturali.

settore privato è stata incoraggiata sulla base di un solido quadro regolamentare e sono state attuate delle politiche generali destinate a ridurre il divario digitale.

14 **Siamo molto incoraggiati** nel constatare che i progressi realizzati nelle tecniche delle comunicazioni e le reti di dati a larga banda offrono ai Paesi in via di sviluppo ed ai Paesi ad economia in transizione sempre maggiori possibilità per partecipare al mercato mondiale dei servizi nati dalle TIC sulla base dei loro vantaggi relativi. Queste nuove possibilità offrono a questi Paesi una solida base commerciale per gli investimenti nelle infrastrutture TIC. I governi devono dunque adottare delle misure, nell'ambito delle politiche nazionali di sviluppo, per contribuire a creare un quadro concorrenziale e propizio agli investimenti necessari nell'infrastruttura delle TIC e allo sviluppo di nuovi servizi. I paesi dovrebbero attuare, inoltre, politiche e misure tali da non scoraggiare, ostacolare od evitare una costante partecipazione di questi Paesi al mercato mondiale dei servizi nati dalle TIC.

15 **Prendiamo atto** del fatto che i problemi incontrati per allargare la portata di un contenuto dell'informazione accessibile e utile nei Paesi in via di sviluppo sono numerosi. Il problema del finanziamento delle diverse forme di contenuto e di applicazione, in particolare, richiede una nuova attenzione perché è stato spesso trascurato in quanto l'accento era posto sull'infrastruttura delle TIC.

16 **Siamo consapevoli** del fatto che, se le TIC hanno attirato degli investimenti, è soprattutto perché l'ambiente era propizio ed è stato caratterizzato da una buona *governance* a tutti i livelli nonché da un quadro politico e regolamentare adeguato, trasparente e favorevole alla concorrenza e adatto alle realtà nazionali.

17 **Abbiamo la volontà** di avviare un dialogo anticipato sulle questioni relative alla responsabilità sociale e alla buona *governance* delle società transnazionali e al loro contributo allo sviluppo economico e sociale dei Paesi in via di sviluppo negli sforzi che facciamo per ridurre il divario digitale.

18 **Ricordiamo** che le forze del mercato non possono assicurare da sole la piena partecipazione dei Paesi in via di sviluppo sul mercato mondiale dei servizi resi possibili dalle tecnologie dell'informazione. **Incoraggiamo dunque** il rafforzamento della cooperazione e della solidarietà internazionale per consentire a tutti i Paesi, soprattutto ai Paesi menzionati al paragrafo 16 della Dichiarazione di principi di Ginevra, di sviluppare infrastrutture TIC e servizi basati sulle tecnologie dell'informazione che siano validi e competitivi a livello nazionale ed internazionale.

19 **Siamo consapevoli** del fatto che, aggiungendosi a quella del settore pubblico, la quota del settore privato nel finanziamento delle infrastrutture TIC svolge ormai un ruolo importante in un gran numero di Paesi in via di sviluppo e che il finanziamento interno è completato dai flussi nord-sud e dalla cooperazione sud-sud.

20 **Siamo consapevoli** del fatto che, data la sempre maggiore entità di investimenti sostenibili del settore privato nelle infrastrutture, i donatori pubblici, a livello multilaterale o bilaterale, riorientano risorse pubbliche verso altre esigenze di sviluppo, con particolar riguardo ai seguenti elementi: documenti di strategia sulla lotta alla

povertà e programmi connessi, riforme politiche ed integrazione delle TIC, rafforzamento delle capacità. **Incoraggiamo** tutti i governi a dare un adeguato livello di priorità alle TIC, incluse le tecnologie tradizionali come la radiodiffusione e la televisione, nelle loro strategie nazionali di sviluppo. **Incoraggiamo d'altro canto** le istituzioni multilaterali ed i donatori pubblici, a livello bilaterale, a prendere in considerazione il fatto di dare un maggiore sostegno finanziario ai progetti d'infrastrutture TIC regionali e ai progetti nazionali su larga scala nonché allo sviluppo connesso delle capacità. Converrebbe che i donatori armonizzassero le loro strategie di assistenza e di associazione secondo priorità fissate dai Paesi in via di sviluppo nelle loro strategie nazionali di sviluppo e in particolare, all'occorrenza, nelle loro strategie di lotta alla povertà.

21 **Siamo consapevoli** che il finanziamento pubblico ha un ruolo capitale da svolgere quando si tratta di assicurare l'accesso alle TIC e ai servizi nelle zone rurali e presso popolazioni svantaggiate, soprattutto dei piccoli Stati insulari in via di sviluppo e dei Paesi in via di sviluppo interclusi.

22 **Osserviamo** che il rafforzamento delle capacità in materia di TIC è un'alta priorità in tutti i Paesi in via di sviluppo e che gli attuali livelli di finanziamento non sono adeguati rispetto alle esigenze, anche se numerosi e diversi meccanismi di finanziamento sono contemplati per le TIC per lo sviluppo.

23 **Sappiamo** che più consistenti risorse finanziarie si rendono necessarie per un certo numero di settori che, d'altronde, non sono stati sufficientemente presi in considerazione negli attuali approcci del finanziamento delle TIC per lo sviluppo. Si tratta dei seguenti settori:

a) programmi di rafforzamento delle capacità delle TIC, documentazione, strumenti, iniziative di finanziamento e di formazione specializzata e d'insegnamento, in particolare per i regolatori e altri impiegati ed enti del settore pubblico;

b) accesso alle telecomunicazioni e connettività per l'erogazione di servizi e di applicazioni TIC nelle zone rurali isolate, nei piccoli Stati insulari in via di sviluppo, nei Paesi in via di sviluppo interclusi ed in altri luoghi che presentino sfide tecnologiche e commerciali non paragonabili ad altre;

c) infrastruttura dorsale regionale, reti regionali, punti di accesso alle reti e progetti regionali connessi, per connettere le reti al di là dei confini e nelle regioni economicamente svantaggiate che possono avere bisogno di politiche coordinate, nonché di quadri giuridici, regolamentari e finanziari, che trarrebbero vantaggio da scambi di esperienze e da prassi ottimali;

d) capacità di banda larga per agevolare la prestazione di un'ampia gamma di servizi e di applicazioni, per promuovere gli investimenti e fornire l'accesso ad Internet a prezzi accessibili, sia agli utenti già registrati che a quelli nuovi;

e) assistenza coordinata, secondo quanto più opportuno, per i Paesi di cui al paragrafo 16 della Dichiarazione di Principi di Ginevra, in particolare i Paesi meno avanzati ed i piccoli Stati insulari in via di sviluppo, per migliorare l'efficacia ed abbassare i costi di transazione associati all'erogazione di un sostegno da parte dei donatori internazionali;

f) applicazioni TIC e contenuto per l'integrazione delle TIC nell'attuazione delle strategie di lotta alla povertà e dei programmi settoriali, con particolar riguardo alle cure sanitarie, all'istruzione, all'agricoltura e all'ambiente;

E' inoltre necessario considerare i seguenti elementi che riguardano le TIC per lo sviluppo e che non sono stati oggetto di adeguata attenzione:

g) sostenibilità dei progetti legati alla società dell'informazione, per esempio, per quanto attiene al mantenimento delle infrastrutture TIC;

h) esigenze specifiche delle piccole, medie e micro imprese (PMMI), esigenze, per esempio, di finanziamento;

i) elaborazione e attuazione locali di applicazioni e di tecnologie TIC da parte dei Paesi in via di sviluppo;

j) attività relative alle riforme istituzionali legate alle TIC e rafforzamento delle capacità riguardanti i quadri giuridici e regolamentari;

k) miglioramento delle strutture amministrative e modifica dei processi di attività economica al fine di ottimizzare l'impatto e l'efficacia dei progetti TIC e degli altri progetti con una forte componente TIC;

l) iniziative degli enti locali e iniziative comunitarie che offrono servizi TIC alle comunità nei settori dell'istruzione, della salute e del miglioramento dei mezzi di sostentamento.

24 Dato che è in primo luogo ai governi che coordinare i programmi pubblici di finanziamento e le iniziative pubbliche di sviluppo delle TIC, **raccomandiamo** un migliore coordinamento intersettoriale e interistituzionale, tanto da parte dei donatori quanto da parte dei beneficiari nel contesto nazionale.

25 Le banche ed istituzioni multilaterali di sviluppo dovrebbero prendere in considerazione la possibilità di adattare i loro meccanismi e, a seconda delle necessità, concepire meccanismi nuovi per fare fronte alle esigenze dello sviluppo delle TIC a livello nazionale e regionale.

26 **Conosciamo** i seguenti requisiti preliminari per un'equa ed universale accessibilità ai meccanismi di finanziamento e per un migliore uso degli stessi:

a) introdurre misure incentivanti in materia di politiche e di normative e provvedimenti a favore dell'accesso universale e della mobilitazione degli investimenti del settore privato;

b) individuare e riconoscere il ruolo essenziale delle TIC nelle strategie di sviluppo nazionali, elaborandole, in modo opportuno, in associazione con strategie cibernetiche;

c) sviluppare capacità istituzionali e meccanismi di attuazione per sostenere l'uso di fondi nazionali a favore del servizio/accesso universale e approfondire lo studio di questi meccanismi diretti alla mobilitazione di risorse interne;

d) incoraggiare lo sviluppo d'informazioni, di applicazioni di servizi, localmente adatti ai Paesi in via di sviluppo e ai Paesi con economia in transizione;

e) favorire il poenziamento di programmi pilota basati sull'uso delle TIC;

f) favorire l'uso delle TIC nel governo come priorità e settore '*target*' essenziale per gli interventi di sviluppo basati sulle TIC;

g) rafforzare le capacità umane ed istituzionali (conoscenze e sapere) a tutti i livelli per attuare gli obiettivi della società dell'informazione, in particolare nel settore pubblico;

h) incoraggiare le realtà del settore privato a contribuire a dar vita ad una più ampia richiesta di servizi TIC offrendo il loro sostegno alle imprese creative, ai produttori locali di contenuti e di applicazioni culturali e alle piccole imprese;

i) rafforzare le capacità per migliorare le possibilità di mobilitazione di fondi ed i mezzi per utilizzarli con efficacia.

27 **Raccomandiamo** di introdurre negli attuali meccanismi di finanziamento i miglioramenti o innovazioni seguenti:

a) migliorare i meccanismi di finanziamento in modo tale che le risorse finanziarie diventino adeguate, più prevedibili, preferibilmente libere da ogni condizionamento e sostenibili;

b) migliorare la cooperazione regionale e creare partenariati fra parti cointeressate, in particolare mediante la creazione di incentivi alla costruzione di strutture dorsali regionali;

c) assicurare un accesso economicamente affrontabile alle TIC, con l'aiuto delle seguenti misure:

i) ridurre i costi Internet internazionali fatturati dai fornitori di infrastruttura dorsale, agevolando segnatamente l'installazione e lo sviluppo di strutture dorsali TIC e di punti di scambi Internet regionali, per ridurre i costi d'interconnessione e allargare l'accesso alla rete;

ii) incoraggiare l'UIT a portare avanti lo studio dell'urgente questione della connettività Internet internazionale, al fine di elaborare le opportune raccomandazioni;

d) coordinare programmi tra governi e grandi attori finanziari per ridurre i rischi di investimenti ed i costi di transazione per gli operatori che sfruttano settori del mercato meno attrattivi (zone rurali o a basso reddito);

e) aiutare ad accelerare lo sviluppo di strumenti finanziari locali, in particolare favorendo gli strumenti locali di micro-finanza, i vivai di piccole imprese di TIC, gli strumenti di credito pubblico, i sistemi di aste inverse, le iniziative di messa in rete su scala comunitaria, la solidarietà digitale e altre innovazioni;

f) migliorare la capacità di accedere ai meccanismi di finanziamento per accelerare il finanziamento delle infrastrutture e servizi TIC, favorendo soprattutto i flussi nord-sud nonché la cooperazione nord-sud e sud-sud;

g) sarebbe opportuno che gli enti multilaterali, regionali e bilaterali di sviluppo considerassero l'utilità di creare un forum virtuale per una condivisione delle informazioni da tutte le parti interessate sui progetti potenziali, sulle fonti di finanziamento e sui meccanismi istituzionali di finanziamento;

h) fare in modo che i Paesi in via di sviluppo siano sempre più in grado di generare fondi per le TIC e sviluppare nuovi strumenti di finanziamento, soprattutto sotto forma di fondi di assegnazione specifica e di capitali di avvio adatti alla loro economia;

i) esortare tutti i Paesi a fare degli sforzi concreti per adempiere ai loro impegni in aderenza al Consenso di Monterrey;

j) sarebbe opportuno che gli enti multilaterali, regionali e bilaterali di sviluppo considerassero la possibilità di collaborare per accrescere le loro capacità di rapida reazione per aiutare i Paesi in via di sviluppo che richiedono un'assistenza nel campo delle politiche TIC;

k) incoraggiare un aumento dei contributi volontari;

l) utilizzare in modo efficace, a seconda delle esigenze, i meccanismi di alleggerimento del debito menzionati nel Piano d'Azione di Ginevra, in particolare le opzioni di annullamento o di scambio di debiti, che possono essere sfruttati per il finanziamento di progetti TIC per lo sviluppo, specialmente nell'ambito delle strategie di lotta alla povertà.

28 Ci rallegriamo per la creazione del Fondo per la Solidarietà Digitale (FSD) con sede a Ginevra, meccanismo finanziario innovatore e volontario, aperto a tutte le parti interessate, che deve permettere di trasformare il divario digitale in opportunità digitali per il mondo in via di sviluppo, focalizzandosi soprattutto sulle esigenze specifiche ed urgenti a livello locale e cercando nuove fonti di finanziamento « di solidarietà ». Il Fondo completerà i fondi già esistenti per finanziare la società dell'informazione, che dovranno continuare ad essere pienamente utilizzati per finanziare la crescita di nuove infrastrutture e nuovi servizi TIC.

GOVERNANCE DI INTERNET

29 Ribadiamo i principi esposti durante la fase di Ginevra dello SMSI, nel dicembre 2003, secondo i quali Internet è diventata una risorsa pubblica mondiale e la sua *governance* dovrebbe costituire una delle priorità essenziali della società dell'informazione. La gestione internazionale di Internet dovrebbe avvenire in maniera multilaterale, trasparente e democratica, con la piena partecipazione degli Stati, del settore privato, della società civile e delle organizzazioni internazionali. Essa dovrebbe assicurare un'equa ripartizione delle risorse, agevolare l'accesso di tutti e garantire un funzionamento stabile e sicuro di Internet, nel rispetto del multilinguismo.

30 Osserviamo che Internet, perno dell'infrastruttura della società dell'informazione, si è evoluto: da rete per i ricercatori e gli universitari, è diventato una risorsa pubblica mondiale.

31 Riconosciamo che la *governance* di Internet, assicurata secondo i principi di Ginevra, è un elemento essenziale di una società dell'informazione a misura d'uomo, aperta, che previlegia lo sviluppo e non discriminatoria. Del resto, ci impegniamo ad assicurare la stabilità e la sicurezza di Internet, come risorsa mondiale, e a garantire la necessaria legittimità della sua *governance*, sulla base della partecipazione piena e

intera di tutte le parti interessate, tanto dei Paesi sviluppati quanto dei Paesi in via di sviluppo, secondo i rispettivi ruoli e responsabilità.

32 **Ringraziamo** il Segretario Generale dell'Organizzazione delle Nazioni Unite per aver creato il Gruppo di Lavoro sulla *Governance* di Internet (GLGI). **Ci congratuliamo** con il Presidente, i membri e il segretario di questo gruppo per il loro lavoro e per la loro relazione.

33 **Prendiamo atto** della relazione del GLGI, i cui membri hanno cercato di impostare una definizione pratica della *governance* di Internet. Questo documento permette di mettere più facilmente a fuoco un certo numero di questioni di interesse generale che si riferiscono alla *governance* di Internet. Ci permette, inoltre, di capire meglio i rispettivi ruoli e responsabilità dei governi, delle organizzazioni intergovernative ed internazionali e di altre istanze, nonché del settore privato e della società civile, nei Paesi in via di sviluppo come nei Paesi sviluppati.

34 Una definizione pratica della *governance* di Internet è l'elaborazione e l'applicazione da parte degli Stati, del settore privato e della società civile, nell'ambito dei rispettivi ruoli, di principi, norme, regole, processi decisionali e programmi comuni atti a modellare l'evoluzione e l'uso di Internet.

35 **Ribadiamo** che la gestione di Internet include questioni sia di ordine tecnico che di politica generale e che essa deve coinvolgere l'insieme delle parti interessate e delle organizzazioni intergovernative ed internazionali competenti. A questo proposito, viene riconosciuto quanto segue:

a) per quanto riguarda le questioni di interesse generale relative a Internet, il potere decisionale dipende dalla sovranità degli Stati, i quali hanno diritti e responsabilità in materia;

b) il settore privato ha sempre avuto e dovrebbe continuare ad avere un ruolo importante nello sviluppo di Internet, sotto il profilo sia tecnico che economico;

c) la società civile svolge anch'essa un ruolo importante in tutte le questioni relative ad Internet, specialmente al livello delle comunità, e deve continuare a svolgere questo ruolo;

d) il ruolo delle organizzazioni intergovernative è sempre stato, e dovrebbe continuare ad essere, quello di agevolare il coordinamento delle questioni di interesse generale che si riferiscono ad Internet;

e) le organizzazioni internazionali hanno esse pure sempre avuto, e dovrebbero continuare ad avere, un ruolo importante nell'elaborazione di norme tecniche riguardanti Internet e le politiche connesse.

36 Riconosciamo il prezioso contributo che gli ambienti universitari ed i settori tecnici, che rientrano nelle parti interessate di cui al paragrafo 35, danno all'evoluzione, al funzionamento e allo sviluppo di Internet.

37 **Cerchiamo di migliorare** il coordinamento delle attività delle organizzazioni internazionali ed intergovernative e delle altre istituzioni coinvolte dalla *governance* di

Internet, nonché gli scambi d'informazione tra queste diverse istanze. Per quanto possibile, dovrebbe essere adottato a tutti i livelli un approccio che tenga conto di una pluralità di parti interessate.

38 **Esortiamo** al rafforzamento delle istituzioni regionali specializzate nella gestione delle risorse Internet per garantire il diritto di ogni singola regione a gestire le proprie risorse Internet, pur assicurando un coordinamento a livello mondiale in questo campo.

39 **Cerchiamo** d'instaurare un clima di fiducia e di sicurezza nell'uso delle TIC, rafforzando le basi di questa fiducia. **Riaffermiamo** che una cultura mondiale della cybersicurezza deve essere incoraggiata, sviluppata e attuata in collaborazione con tutte le parti interessate come indicato dall'Assemblea Generale delle Nazioni Unite nella Risoluzione 57/239 e da alcune istanze regionali competenti. Questa cultura presuppone delle azioni a livello nazionale ed una maggiore cooperazione internazionale per rafforzare la sicurezza, migliorando la protezione della *privacy* e delle informazioni e dati personali. La costante espansione della cultura della cybersicurezza dovrebbe rafforzare l'accesso e gli scambi e deve tenere conto del livello di sviluppo socio-economico di ogni singolo Paese e rispettare gli aspetti della società dell'informazione che previlegiano lo sviluppo.

40 **Sottolineiamo** l'importanza di procedere contro gli autori di cybercrimini, inclusi quelli commessi in un Paese, ma le cui conseguenze si fanno sentire in un altro Paese. **Insistiamo inoltre** sulla necessità di disporre di strumenti e di meccanismi efficaci, a livello nazionale ed internazionale, per promuovere la cooperazione internazionale soprattutto tra le autorità di polizia nel settore della cybercriminalità. **Esortiamo gli Stati** ad elaborare, in collaborazione con le altre parti interessate, la legislazione necessaria per condurre inchieste e per procedere in via giudiziaria contro gli autori di cybercrimini, tenendo conto dei quadri esistenti, per esempio le Risoluzioni 55/63 e 56/121 dell'Assemblea Generale delle Nazioni Unite su *la lotta contro lo sfruttamento delle tecnologie dell'informazione e della comunicazione a fini criminali*, e le iniziative regionali, fra cui la Convenzione sulla cybercriminalità del Consiglio d'Europa.

41 **Siamo decisi a trattare efficacemente** il problema sempre più preoccupante dello spam. **Prendiamo atto** degli attuali quadri vuoi multilaterali, vuoi legati alla pluralità delle parti interessate in tema di cooperazione regionale e internazionale nella lotta allo spam, per esempio la strategia antispam dell'APEC, il Piano d'azione di Londra, il Memorandum di accordo Seul-Melbourne sulla lotta contro lo spam e le attività portate avanti dall'OCSE e dall'UIT in questo campo. Per lottare contro questo fenomeno, **chiediamo** a tutte le parti interessate di adottare, su più fronti, misure quali: sensibilizzazione degli utenti e delle imprese; creazione di una legislazione appropriata ed istituzione di autorità e di meccanismi atti ad applicarla; messa a punto continua di misure tecniche e di autoregolamentazione; elaborazione di migliori prassi; cooperazione internazionale.

42 **Ribadiamo la nostra ferma adesione** alla libertà di cercare, ricevere, trasmettere e utilizzare delle informazioni, in particolare ai fini della creazione,

dell'accumulo e della diffusione della conoscenza. **Affermiamo** che le misure adottate per garantire la stabilità e la sicurezza di Internet e per combattere la cybercriminalità e lo spam devono rispettare la *privacy* ed il diritto di espressione ed essere conformi alle relative disposizioni enunciate nelle pertinanti parti della Dichiarazione Universale dei Diritti dell'Uomo e della Dichiarazione di Principi della fase di Ginevra.

43 **Rinnoviamo** il nostro impegno a favore di un positivo uso di Internet e di altre TIC, nonché dell'adozione di misure appropriate, in particolare preventive, determinate dalla legge, per impedire gli usi abusivi delle TIC, come indicato nella Dichiarazione di Principi e nel Piano di Azione di Ginevra, a tutela della dimensione etica della società dell'informazione.

44 **Sottolineiamo altresì** l'importanza della lotta al terrorismo in tutte le sue forme e in tutte le sue manifestazioni su Internet, nel rispetto dei diritti umani, in conformità con altri obblighi stabiliti dal diritto internazionale, come indicato nell'Articolo 85 del Documento finale del Summit del 2005 (Risoluzione A60/L.1* dell'Assemblea Generale delle Nazioni Unite).

45 **Sottolineiamo** l'importanza della sicurezza, della continuità e della stabilità di Internet, e la necessità di proteggere Internet e altri reti TIC da possibili minacce, tenuto conto della loro vulnerabilità. **Affermiamo** che è necessario trovare un terreno d'intesa sulle questioni che si riferiscono alla sicurezza di Internet e accrescere la cooperazione per agevolare, da una parte, la raccolta e diffusione d'informazioni relative alla sicurezza, e la sensibilizzazione in questo campo e, dall'altra, scambiare buone prassi fra tutte le parti interessate sulle misure dirette a contrastare le minacce che gravano sulla sicurezza, a livello nazionale ed internazionale.

46 **Esortiamo tutte le parti interessate** a garantire il rispetto della *privacy* e la tutela delle informazioni e dei dati personali avvalendosi, a tal fine, di strumenti quali l'approvazione di leggi, l'attuazione di quadri di cooperazione, l'elaborazione di prassi e la messa a punto di misure tecniche e di autoregolamentazione da parte delle imprese e degli utenti. **Incoraggiamo tutte le parti interessate**, in particolare gli Stati, a riaffermare il diritto dei singoli ad accedere all'informazione in base alla Dichiarazione di Principi di Ginevra e ad altri strumenti internazionali concordati, nonché a coordinare la loro azione a livello internazionale, secondo quanto risulterà più opportuno.

47 **Osserviamo** che il commercio elettronico, in tutte le sue forme, cresce sempre più in termini di volume e di valore, a livello sia nazionale che internazionale. **Consigliamo vivamente** l'elaborazione di leggi e prassi nazionali sulla protezione del consumatore, nonché di meccanismi di applicazione, quando necessario, per tutelare i diritti del consumatore che acquisisce beni e servizi '*on line*', e consigliamo altresì vivamente una crescita della cooperazione internazionale, atta a facilitare sempre più, in modo non discriminatorio e in conformità con le vigenti leggi nazionali, la diffusione su ampia scala del commercio elettronico, rafforzando nel contempo la fiducia del consumatore.

48 **Osserviamo con soddisfazione** che i governi utilizzano sempre più le TIC al servizio della popolazione ed incoraggiamo i Paesi che non lo hanno ancora fatto ad elaborare programmi e strategie nazionali di cybergoverno.

49 **Ribadiamo la nostra volontà** di trasformare il divario digitale in opportunità digitali e **ci impegniamo** a vigilare affinché questa evoluzione sia armoniosa, equa e giusta per tutti. **Ci impegniamo** a favorire la presa in considerazione di alcune questioni di sviluppo e a dare consigli al riguardo, nelle disposizioni in materia di *governance* di Internet in senso lato, incluse le questioni di costo di connessione internazionale, di rafforzamento delle capacità e di trasferimento di tecnologie/conoscenze. **Incoraggiamo** l'attuazione del multilinguismo nel contesto dello sviluppo di Internet, e **sosteniamo** lo sviluppo di *software* di facile localizzazione e tali da permettere all'utente di scegliere una soluzione adeguata fra diversi modelli, con particolar riguardo ai programmi informatici a codice fonte aperto, gratuiti e proprietari.

50 **Riconosciamo** che è preoccupante per alcuni Paesi, specialmente quelli in via di sviluppo, che i costi afferenti alla connettività Internet internazionale non siano ripartiti più equamente per rafforzare l'accesso a Internet. **Sollecitiamo** l'elaborazione di strategie favorevoli ad una connettività mondiale più accessibile, il che permetterebbe di fornire un accesso migliorato ed equo per tutti, in particolare al fine di:

a) promuovere i costi di transito e di interconnessione Internet negoziati a livello commerciale in un ambito concorrenziale e stabiliti in funzione di parametri e di obiettivi, trasparenti e non discriminatori, tenendo conto dei i lavori in corso in questo settore;

b) creare reti dorsali Internet a larga banda a livello regionale e punti di scambio Internet a livello nazionale, sub-regionale e regionale;

c) raccomandare ai programmi di donatori e ad altri meccanismi di finanziamento dello sviluppo di considerare la necessità di finanziare iniziative che favoriscano la connettività, i punti di scambio Internet e la produzione di contenuti locali a favore dei Paesi in via di sviluppo;

d) incoraggiare l'UIT a procedere con la massima urgenza nello studio della questione della connettività Internet internazionale, e a comunicare i risultati a fini di disamina e di eventuale attuazione. Incoraggiamo anche altre istituzioni competenti a trattare questa questione;

e) promuovere la messa a punto e lo sviluppo di terminali a prezzi contenuti, accessibili sia ai privati che alla collettività, in particolare per i Paesi in via di sviluppo;

f) incoraggiare i fornitori di servizi Internet ed altri partecipanti ai negoziati commerciali ad adottare prassi dirette a stabilire costi di interconnessione giusti ed equi;

g) incoraggiare le parti competenti a negoziare a livello commerciale costi d'interconnessione ridotti per i Paesi meno avanzati (PMA), in considerazione delle particolari difficoltà di detti Paesi.

51 **Incoraggiamo** i governi ed altre parti interessate, eventualmente nell'ambito di partenariati, a promuovere l'istruzione e la formazione TIC nei Paesi in via di sviluppo,

elaborando strategie nazionali di integrazione delle TIC nell'istruzione e nella formazione del personale e mobilitando le risorse appropriate a questo fine. Bisognerebbe accrescere inoltre la cooperazione internazionale, su base volontaria, in materia di rafforzamento delle capacità nei settori afferenti alla *governance* di Internet. Si potrebbe trattare per esempio di creare degli istituti, e soprattutto dei centri di periti, rivolti ad agevolare il trasferimento di *know how* e lo scambio di prassi migliori, al fine di rafforzare la partecipazione dei Paesi in via di sviluppo e di tutte le parti interessate ai meccanismi di *governance* di Internet.

52 Per garantire una partecipazione efficace alla *governance* mondiale di Internet, **sollecitiamo** le oganizzazioni internazionali, comprese le organizzazioni intergovernative competenti, a vigilare affinché tutte le parti interessate, in particolare i Paesi in via di sviluppo, abbiano la possibilità di partecipare all'assunzione delle decisioni inerenti alle politiche generali che li riguardano e a promuovere e favorire tale partecipazione. *(Adottato)*

53 **Ci impegniamo ad operare con determinazione** a favore del multilinguismo di Internet nell'ambito di un processo multilaterale, trasparente e democratico che consenta l'intervento dei pubblici poteri e delle parti interessate in funzione dei rispettivi ruoli. In questo contesto, **raccomandiamo inoltre** l'uso delle lingue locali per l'elaborazione di contenuti, le opportune traduzioni ed adattamenti, gli archivi digitali e le diverse forme di media digitali e tradizionali, nella consapevolezza che tali attività possono rafforzare anche le comunità locali e autoctone. **Teniamo pertanto ad insistere sulla necessità di:**

a) portare avanti l'adozione del multilinguismo in un certo numero di settori: nomi di domini, indirizzi di posta elettronica, ricerca con parola chiave;

b) attuare programmi che consentano la presenza di nomi di dominio e di contenuti multilingue su Internet ed usare diversi modelli di *software* per fronteggiare il problema del divario digitale linguistico e garantire la partecipazione di tutti nella nuova società emergente;

c) rafforzare la collaborazione tra gli enti interessati in modo da portare avanti l'elaborazione di norme tecniche ed agevolarne l' adozione in tutto il mondo.

54 **Riconosciamo** che un ambiente propizio a livello sia nazionale che internazionale, favorevole all'investimento straniero diretto, al trasferimento di tecnologie e alla cooperazione internazionale, con particolar riguardo alle finanze, all'indebitamento e al commercio, è una condizione essenziale per la costruzione della società dell'informazione, compresi l'espansione e la diffusione di Internet e il suo uso ottimale. In particolare, il settore privato e la società civile, come motore dell'innovazione e dell'investimento privato, svolgono un ruolo fondamentale nello sviluppo di Internet. Si crea valore aggiunto in margine alla rete sia nei Paesi sviluppati sia in quelli in via di sviluppo, quando il quadro di politica internazionale e nazionale incoraggia l'investimento e l'innovazione.

55 **Riconosciamo** che le disposizioni esistenti per la *governance* di Internet funzionano efficacemente ed hanno fatto di Internet il mezzo di comunicazione estremamente affidabile, evolutivo e geograficamente universale che è oggi, incentivato

dal settore privato nel suo funzionamento quotidiano e sempre spinto oltre i suoi limiti dall'innovazione e dalla creazione di valori.

56 Dal momento che Internet continua ad essere un media molto evolutivo, il quadro e i meccanismi concepiti per assicurare la sua *governance* dovrebbero essere inclusivi e dovrebbero permettere di reagire rapidamente di fronte alla sua crescita esponenziale e alla sua rapida evoluzione come spazio comune di sviluppo di numerose applicazioni.

57 La sicurezza e la stabilità di Internet devono essere mantenute.

58 **Riconosciamo** che la *governance* di Internet va al di là delle questioni di denominazione e di indirizzo. Essa include importanti questioni di politica pubblica quali le risorse Internet essenziali, la sicurezza della rete, taluni aspetti relativi allo sviluppo ed alcune questioni attinenti all'uso di Internet.

59 **Riconosciamo** che la *governance* di Internet include questioni di carattere sociale, economico e tecnico relative, fra l'altro, all'accessibilità economica, alla stabilità e alla qualità di servizio.

60 **Riconosciamo inoltre** che i meccanismi oggi in atto non permettono di esaminare come si deve molte politiche pubbliche internazionali multisettoriali che necessitano di un'attenzione particolare.

61 **Siamo convinti** che sia necessario avviare e, se del caso, rafforzare un processo trasparente, democratico e multilaterale, con la partecipazione dei governi, del settore privato, della società civile e delle organizzazioni internazionali, nei rispettivi ruoli. Lungo questo processo, si potrebbe pensare alla creazione di un quadro o di meccanismi adeguati, là dove occorre, per stimolare la dinamica evoluzione in atto delle attuali disposizioni, onde stabilire delle sinergie tra le iniziative prese al riguardo.

62 **Sottolineiamo** che ogni singolo approccio alla *governance* di Internet dovrebbe essere inclusivo e adattabile in modo da continuare ad incoraggiare la realizzazione di un ambiente propizio all'innovazione, alla concorrenza e all'investimento.

63 I Paesi non dovrebbero intervenire nelle decisioni relative al dominio di primo livello corrispondente al codice di Paese (ccTLD) di un altro Paese. I legittimi interessi nazionali, come espressi e definiti da ogni singolo Paese, in modo diverso, in riferimento alle decisioni concernenti i rispettivi ccTLD, devono essere rispettati, difesi e trattati in un quadro e per mezzo di meccanismi flessibili e migliorati.

64 **Riconosciamo** la necessità di elaborare ulteriormente politiche pubbliche applicabili ai nomi di dominio generici di primo livello (gTLD) e di rafforzare la cooperazione fra le parti interessate in tal senso.

65 **Sottolineiamo** che è necessario ottimizzare la partecipazione dei Paesi in via di sviluppo all'assunzione di decisioni relative alla *governance* di Internet, decisioni che

dovrebbero tenere conto dei loro interessi, e che è altresì necessario ottimizzare la partecipazione di questi Paesi allo sviluppo e al rafforzamento delle capacità.

66 Data la costante internazionalizzazione di Internet e del principio di universalità, **conveniamo** di attuare i principi di Ginevra relativi alla *governance* di Internet.

67 **Decidiamo**, fra l'altro, di invitare il Segretario Generale dell'ONU a riunire un nuovo forum al fine di un dialogo tra le numerose parti interessate sulle politiche da seguire.

68 **Riconosciamo** che tutti i governi dovrebbero svolgere un ruolo ed avere pari responsabilità nella *governance* internazionale di Internet nonché nel mantenimento della stabilità, della sicurezza e della continuità di questa rete. **Riconosciamo anche** la necessità per i governi di elaborare politiche pubbliche in consultazione con tutte le parti interessate.

69 **Riconosciamo inoltre** la necessità in futuro di rafforzare la cooperazione per consentire ai governi di svolgere, su un piano di parità, il loro ruolo e le loro responsabilità nelle questioni concernenti le politiche pubbliche internazionali relative a Internet, ma non nelle questioni tecniche ed operative correnti che non hanno nessuna incidenza su quelle di politica pubblica internazionale.

70 Nel rivolgersi alle organizzazioni internazionali competenti, tale cooperazione dovrebbe comprendere l'elaborazione di principi applicabili, a livello mondiale, alle questioni relative alle politiche pubbliche nonché al coordinamento e alla gestione di risorse fondamentali di Internet. A questo riguardo, **esortiamo** le organizzazioni preposte ai compiti essenziali legati ad Internet a favorire la creazione di un ambiente che agevoli l'elaborazione di questi principi.

71 Il processo diretto a rafforzare la cooperazione che il Segretario Generale dell'ONU deve avviare ricorrendo a tutte le organizzazioni competenti entro la fine del primo trimestre 2006 farà intervenire tutte le parti interessate nei rispettivi ruoli, andrà avanti con la massima celerità possibile nel rispetto delle procedure legali e guarderà con favore all'innovazione. Con la partecipazione di tutte le parti interessate, le organizzazioni competenti devono avviare un processo che porti ad un rafforzamento della cooperazione, nel minor tempo possibile e in un'ottica d'innovazione. Queste stesse organizzazioni competenti devono essere invitate a presentare delle relazioni annuali sulle loro attività.

72 **Invitiamo il Segretario Generale dell'ONU** a riunire, secondo un approccio aperto e non esclusivo, entro il secondo trimestre del 2006, un nuovo forum destinato a stabilire tra le numerose parti interessate un dialogo sulle politiche da seguire, il quale, denominato *Forum sulla governance di Internet,* avrà il mandato di:

a) trattare le questioni di politica pubblica relative ai principali elementi della *governance* di Internet come mezzi per contribuire alla vitalità, alla solidità, alla sicurezza, alla stabilità e allo sviluppo di Internet;

b) agevolare il dialogo fra gli organi che si occupano di diverse politiche pubbliche internazionali multisettoriali riguardanti Internet e discutere le questioni che non dipendono dalla competenza di un organo già esistente;

c) mantenere il legame con le organizzazioni intergovernative e altre istituzioni appropriate sulle questioni dipendenti dal loro mandato;

d) agevolare lo scambio di informazioni e di prassi migliori e, al riguardo, avvalersi appieno delle competenze delle comunità universitarie, scientifiche e tecniche;

e) consigliare tutte le parti interessate al fine di proporre i mezzi che permetteranno che Internet sia disponibile e accessibile più rapidamente nel mondo in via di sviluppo;

f) rafforzare ed intensificare l'impegno delle parti interessate, in particolare quello dei Paesi in via di sviluppo, nei meccanismi di *governance* di Internet esistenti e/o futuri;

g) censire le nuove questioni e portarle all'attenzione degli organi competenti e del pubblico in generale e, all'occorrenza, formulare delle raccomandazioni;

h) contribuire al rafforzamento delle capacità ai fini della *governance* di Internet nei paesi in via di sviluppo, basandosi pienamente sulle fonti di conoscenza e sulle competenze locali;

i) promuovere l'opportuna considerazione per i principi del SMSI nei meccanismi di *governance* di Internet e valutarla regolarmente;

j) trattare, fra l'altro, le questioni relative alle risorse fondamentali di Internet;

k) contribuire a trovare le soluzioni ai problemi scaturiti dall'uso e dal cattivo uso di Internet, che preoccupano particolarmente il normale utente;

l) pubblicare i suoi lavori;

73 Il Forum sulla *governance* di Internet avrà, nel suo funzionamento e nella sua funzione, un carattere multilaterale, inclusivo di molteplici parti interessate, democratico e trasparente. A tal fine, il Forum proposto potrebbe:

a) prendere spunto dalle strutture esistenti di *governance* di Internet, ponendo l'accento in particolare sulla complementarità fra tutte le parti interessate che partecipano a questo processo (governi, realtà del settore privato, società civile e organizzazioni intergovernative);

b) essere dotato di una struttura leggera e decentrata ed essere oggetto di regolari esami;

c) riunirsi regolarmente, a seconda delle necessità. Le riunioni del Forum potrebbero, normalmente, essere legate alle grandi conferenze di pertinente interesse delle Nazioni Unite per beneficiare soprattutto del sostegno logistico di cui esse dispongono.

74 **Incoraggiamo** il Segretario Generale a studiare ai fini della riunione del Forum una serie di possibilità che tengano conto delle competenze accertate di tutte le parti interessate alla *governance* di Internet e dell'esigenza di garantire la loro piena partecipazione.

75 Il Segretario Generale dell'ONU farebbe periodicamente relazione agli Stati Membri delle Nazioni Unite sul funzionamento del Forum.

76 **Chiediamo al Segretario Generale dell'ONU** di verificare, consultando formalmente i partecipanti al Forum, se sia auspicabile che il Forum continui le sue attività dopo i cinque anni che seguiranno la sua creazione e di formulare raccomandazioni in merito ai membri delle Nazioni Unite.

77 Il Forum non avrebbe alcuna funzione di controllo e non sostituirebbe i meccanismi, le istituzioni o le organizzazioni esistenti ma permetterebbe loro di intervenire e si avvarrebbe delle loro competenze. Costituirebbe un meccanismo neutro, le sue attività non sarebbero un doppione di altre e non avrebbero carattere vincolante. Non interverrebbe nelle operazioni correnti o tecniche di Internet.

78 Il Segretario Generale dell'ONU dovrebbe invitare tutte le parti interessate ed interlocutrici a partecipare alla riunione inaugurale del Forum nell'ottica di una rappresentanza geografica equilibrata. Dovrebbe anche:

a) attingere alle risorse appropriate che tutte le parti interessate ed interlocutrici possono fornire, in particolare alle assodate competenze dell'UIT, poste in luce dal processo dello SMSI;

b) organizzare un ufficio efficace ed economico per sostenere il Forum assicurando la partecipazione delle molteplici parti interessate.

79 Diverse questioni relative alla *governance* di Internet continuerebbero ad essere trattate in altre sedi competenti.

80 **Incoraggiamo** l'elaborazione di meccanismi inclusivi di una molteplicità di parti interessate a livello nazionale, regionale ed internazionale per instaurare un dialogo ed una collaborazione per un'espansione e diffusione di Internet come mezzo di sostegno agli sforzi di sviluppo diretti al raggiungimento degli scopi ed obiettivi di sviluppo stabiliti dalla comunità internazionale, con particolar riguardo agli Obiettivi del Millennio per lo Sviluppo.

81 **Ribadiamo la nostra volontà** di dare piena attuazione ai Principi di Ginevra.

82 **Prendiamo atto con soddisfazione** della generosa offerta del Governo greco di ospitare la prima riunione del Forum ad Atene entro e non oltre il 2006 e **chiediamo** al Segretario Generale dell'ONU di invitare tutte le parti interessate ed interlocutrici a partecipare alla riunione inaugurale del Forum.

ATTUAZIONE E SEGUITI

83 La costruzione di una società dell'informazione inclusiva e che previlegi lo sviluppo sarà un'operazione di lungo respiro rivolta a numerose parti interessate. **Ci impegniamo dunque** a restare pienamente mobilitati, a livello nazionale, regionale ed internazionale, per dare attuazione e seguito duraturi ai risultati ed impegni scaturiti dal

processo dello SMSI e dalle fasi di Ginevra e di Tunisi del Vertice. Considerati i molteplici aspetti che la costruzione della società dell'informazione andrà a ricoprire, è essenziale che i governi, il settore privato, la società civile, l'Organizzazione delle Nazioni Unite ed altre organizzazioni internazionali cooperino efficacemente, in conformità con i loro diversi ruoli e responsabilità, mediante la mobilitazione delle loro specifiche conoscenze.

84 I governi ed altre parti interessate dovrebbero definire i settori che necessitano ulteriori sforzi e risorse e dovrebbero congiuntamente individuare e, se necessario, elaborare strategie, meccanismi e processi di attuazione dei risultati dello SMSI a livello mondiale, regionale, nazionale e locale, rivolgendo particolare attenzione alle popolazioni e ai gruppi che rimangono emarginati nell'accesso alle TIC ed al loro impiego.

85 Prendendo in considerazione il ruolo fondamentale dei governi in associazione con altre parti interessate nell'attuazione dei risultati dello SMSI, compreso il Piano di azione di Ginevra, a livello nazionale, **incoraggiamo** i governi che non lo hanno ancora fatto ad elaborare, appena possibile e prima del 2010, strategie cibernetiche, comprese le strategie TIC e le strategie cibernetiche settoriali a seconda dei casi[138], che siano globali e rivolte verso il futuro, destinate a durare e che facciano parte integrante dei loro piani di sviluppo e delle loro strategie di lotta alla povertà a livello nazionale.

86 **Appoggiamo** gli sforzi di integrazione regionale ed internazionale diretti a costruire una società mondiale dell'informazione inclusiva, a misura d'uomo, che previlegi lo sviluppo, e **ribadiamo** che una stretta cooperazione all'interno delle regioni e tra di esse è indispensabile per permettere la condivisione della conoscenza. La cooperazione a livello regionale dovrebbe contribuire al rafforzamento delle capacità nazionali e alla messa a punto di strategie di attuazione a livello regionale.

87 **Affermiamo** che lo scambio di punti di vista e la condivisione di prassi e di risorse efficaci sono essenziali all'attuazione dei risultati dello SMSI a livello regionale ed internazionale. A questo fine, bisognerà sforzarsi di fornire e condividere, tra tutte le parti interessate, le conoscenze ed il *know-how* relativi alla concezione, all'attuazione, al controllo e alla valutazione di strategie cibernetiche nazionali e di politiche nazionali, a seconda dei casi. **Riconosciamo** che lottare contro la povertà, rafforzare le capacità a livello nazionale e promuovere i progressi tecnologici su scala nazionale, sono elementi fondamentali per ridurre, in modo duraturo, il divario digitale nei Paesi in via di sviluppo.

88 **Ribadiamo** che, grazie alla cooperazione internazionale dei governi e all'associazione tra tutte le parti interessate, sarà possibile raccogliere la sfida che si offre a noi, ossia mettere a frutto il potenziale delle TIC al servizio dello sviluppo per promuovere l'uso dell'informazione e della conoscenza onde raggiungere gli scopi ed obiettivi dello sviluppo stabiliti a livello internazionale, compresi gli Obiettivi del Millennio per lo Sviluppo, trattare le priorità dello sviluppo a livello nazionale e locale e migliorare così lo sviluppo socio-economico di tutti gli esseri umani.

---

[138] Nella parte che segue del presente documento, il termine "strategie cibernetiche" è inteso come strategie TIC e come strategie cibernetiche settoriali, a seconda dei casi.

89 **Siamo determinati** a migliorare la connettività e l'accesso economicamente praticabile alle TIC e all'informazione a livello mondiale, regionale e nazionale, grazie al rafforzamento della cooperazione internazionale tra tutte le parti interessate, per favorire gli scambi tecnologici ed il trasferimento di tecnologie, nonché lo sviluppo e la formazione delle risorse umane, in modo da migliorare la capacità che hanno i Paesi in via di sviluppo di innovare, partecipare pienamente alla società dell'informazione e dare ad essa il proprio contributo.

90 **Ribadiamo il nostro impegno** a fornire a tutti un accesso equo all'informazione e alla conoscenza, riconoscendo il ruolo che hanno le TIC nella crescita economica e lo sviluppo. **Siamo decisi** a collaborare perché siano raggiunti, entro il 2015, gli obiettivi indicativi enunciati nel Piano di Azione di Ginevra, che servono da riferimenti globali per migliorare la connettività nonché l'accesso universale, ubiquitario, equo, non discriminatorio ed economicamente affrontabile, all'impiego delle TIC, tenendo conto delle specificità nazionali, e ad usare le TIC come strumenti per raggiungere gli scopi ed obiettivi di sviluppo concordati a livello internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo:

a) *integrando e allineando le strategie cibernetiche nazionali* nei piani di azione locali, nazionali e regionali, a seconda dei casi, e in conformità con le priorità di sviluppo a livello nazionale e locale, secondo scadenze;

b) *elaborando e attuando le politiche propizie* che tengono conto della realtà di ogni singolo Paese e che incoraggiano la creazione di un ambiente internazionale favorevole, gli investimenti stranieri diretti e la mobilitazione di risorse nazionali per promuovere e stimolare l'imprenditorialità, in particolare a livello delle piccole, medie, micro imprese, tenendo conto del mercato e del contesto culturale di questi Paesi. Queste politiche dovrebbero iscriversi in un ambito regolamentare trasparente ed equo, per creare un ambiente concorrenziale a sostegno di questi obiettivi e rafforzare la crescita economica;

c) *rafforzando le capacità TIC* di tutti e la fiducia nell'uso delle TIC da parte di tutti – inclusi i giovani, le persone anziane, le donne, le popolazioni autoctone, i disabili e gli abitanti di comunità rurali isolate – mediante il miglioramento e l'attuazione di programmi e di opportuni sistemi di istruzione e di formazione, integrando tra l'altro, l'insegnamento a distanza e la formazione permanente;

d) *attuando una formazione ed un insegnamento efficaci*, in particolare nel campo delle scienze e delle tecnologie TIC, per indurre ed incoraggiare le ragazze e le donne a partecipare e ad interessarsi attivamente alle decisioni legate alla costruzione della società dell'informazione;

e) *rivolgendo una particolare attenzione alla formulazione di concetti a vocazione universale e all'uso di tecnologie di sostegno* atte a facilitare l'accesso di tutti, inclusi i disabili;

f) *incoraggiando l'adozione di misure pubbliche dirette a consentire, a costi contenuti* a tutti i livelli, compresi il livello comunitario, un accesso ai materiali, ai *software* ed alla connettività, grazie ad un ambiente tecnologico sempre più contraddistinto dalla convergenza e grazie al rafforzamento delle capacità e ai contenuti locali;

g) *migliorando l'accesso alle conoscenze sanitarie a livello mondiale* e ai servizi di telemedicina, in particolare, in settori quali la cooperazione mondiale nelle situazioni di emergenza, migliorando anche l'accesso ai professionisti della salute e la loro messa in rete, per contribuire a migliorare la qualità della vita e le condizioni ambientali;

h) *rafforzando le capacità TIC* per migliorare l'accesso alle reti e servizi postali e il loro uso;

i) *usando le TIC per migliorare l'accesso alle conoscenze nel settore agricolo*, lottare contro la povertà e sostenere una produzione di contenuti in relazione con l'agricoltura che sia adatta alle condizioni locali e l'accesso a questi contenuti;

j) *elaborando e attuando applicazioni di cybergoverno* basate su norme aperte per migliorare la generalizzazione e l'interoperabilità dei sistemi di cybergoverno, a tutti i livelli, e facilitare con ciò stesso l'accesso all'informazione e ai servizi pubblici e contribuire alla costruzione di reti TIC e allo sviluppo di servizi disponibili in qualsiasi posto, in qualunque momento e per tutte le categorie di utenti;

k) *sostenendo le istituzioni a scopo educativo, scientifico e culturale*, segnatamente le biblioteche, gli archivi ed i musei, nella loro missione che consiste nell'elaborare e salvaguardare contenuti di vario genere e nell'offrire un accesso equo, aperto e poco costoso a questi contenuti, inclusi i contenuti digitali, per agevolaree l'insegnamento formale e informale, la ricerca e l'innovazione; in particolare, aiutando le biblioteche a svolgere la loro missione di servizio pubblico che consiste nell'offrire un accesso gratuito ed equo all'informazione e nel migliorare la conoscenza delle TIC e la connettività a livello comunitario, specialmente nelle comunità con pochi servizi;

l) *migliorando la capacità delle comunità* di tutte le regioni di elaborare contenuti in lingue locali o vernacolari;

m) *favorendo la creazione di contenuti elettronici di qualità*, a livello nazionale, regionale e internazionale;

n) *incoraggiando l'uso dei media nuovi o tradizionali* per promuovere l'accesso universale all'informazione, alla cultura e alla conoscenza per tutti, in particolare per le popolazioni vulnerabili e gli abitanti dei Paesi in via di sviluppo, e usando soprattutto la radio e la televisione a fini d'istruzione e di apprendimento;

o) *riaffermando l'indipendenza, il pluralismo e la diversità dei media, nonché la libertà dell'informazione*, in particolare, se del caso, mediante l'elaborazione di legislazioni nazionali. Reiteriamo il nostro appello ai media perché dimostrino il loro senso di responsabilità nell'uso e nel trattamento dell'informazione in conformità con le più alte norme etiche e professionali. Riaffermiamo la necessità di ridurre le disparità fra i media a livello internazionale, con particolar riguardo all'infrastruttura, alle risorse tecniche ed allo sviluppo delle competenze. Riaffermiamo questi principi enunciati ai paragrafi 55 - 59 della Dichiarazione di Principi di Ginevra.

p) *incoraggiando vivamente le imprese e gli imprenditori nel settore delle TIC a mettere a punto e ad usare processi di fabbricazione innocui per l'ambiente*

onde ridurre al minimo gli effetti nocivi dell'uso e della fabbricazione delle TIC e dell'eliminazione dei rifiuti TIC sulle popolazioni e sull'ambiente. In questo contesto, è importante rivolgere un'attenzione particolare alle esigenze specifiche dei Paesi in via di sviluppo;

q) *integrando nei piani di azione nazionali e nelle strategie cibernetiche nazionali determinate politiche e quadri di regolamentazione, autoregolamentazione, o di altro genere, per proteggere i bambini ed i giovani* da ogni forma di abuso o di sfruttamento basato sull'uso delle TIC;

r) *favorendo lo sviluppo di reti di ricerca avanzata,* a livello nazionale, regionale ed internazionale, per migliorare la cooperazione nei settori scientifici, tecnologici e universitari;

s) *incoraggiando il volontariato*, a livello comunitario, a contribuire ad ottimizzare l'effetto delle TIC sullo sviluppo;

t) *incoraggiando il ricorso alle TIC per promuovere modalità di lavoro flessibili,* in particolare il telelavoro, che portino ad una migliore produttività ed alla creazione di posti di lavoro.

91 **Riconosciamo** che esiste una relazione intrinseca tra la lotta contro gli effetti delle calamità, lo sviluppo sostenibile e lo sradicamento della povertà e che le calamità, che nuociono gravemente e molto rapidamente agli investimenti, rimangono un ostacolo fondamentale allo sviluppo sostenibile e allo sradicamento della povertà. **Abbiamo piena coscienza** del ruolo particolarmente importante di catalizzatore delle TIC a un triplice livello, nazionale, regionale e internazionale, per quello che riguarda:

a) la promozione della cooperazione tecnica ed il miglioramento della capacità dei Paesi, specialmente dei Paesi in via di sviluppo, di avvalersi di strumenti TIC per le operazioni di allerta avanzata, gestione e comunicazione d'emergenza in caso di calamità, inclusa la diffusione di bollettini d'allerta comprensibili, ad uso delle persone esposte;

b) la promozione di una cooperazione regionale ed internazionale per agevolare l'accesso alle informazioni necessarie alla gestione delle calamità ed allo scambio di tali informazioni, e per studiare modalità atte ad agevolare la partecipazione dei Paesi in via di sviluppo;

c) un fattivo lavoro diretto all'instaurazione di sistemi mondiali normalizzati di sorveglianza e di allerta avanzata collegati alle reti nazionali ed alle reti regionali, destinato ad agevolare le operazioni di emergenza in caso di calamità in tutto il mondo, in particolare nelle zone ad alto rischio.

92 **Incoraggiamo i Paesi e tutte le altri parti interessate, a creare** linee telefoniche d'assistenza per i bambini, tenendo conto della necessità di mobilitare risorse adeguate. Bisognerebbe riservare a questo scopo numeri facili da memorizzare ed utilizzabili gratuitamente da qualunque tipo di telefono.

93 **Vogliamo** digitalizzare i nostri dati storici e il nostro patrimonio culturale nell'interesse delle generazioni future. **Incoraggiamo** politiche efficaci di gestione dell'informazione nel settore pubblico e privato, compreso l'uso dell'archiviazione digitale normalizzata ed il ricorso a soluzioni inedite per ovviare al problema

dell'invecchiamento tecnologico, al fine di assicurare la preservazione a lungo termine delle informazioni, salvaguardandone l'accesso.

94 **Riconosciamo** che tutti, uomini e donne, dovrebbero fruire delle possibilità offerte dalla società dell'informazione. Di conseguenza, **invitiamo** i governi ad aiutare, su base volontaria, i Paesi che sono colpiti da misure unilaterali non conformi al diritto internazionale ed alla Carta delle Nazioni Unite, misure che impediscono la piena attuazione dello sviluppo economico e sociale di tali Paesi, nuocendo al benessere delle loro popolazioni.

95 **Esortiamo** le organizzazioni internazionali o intergovernative a sviluppare, nei limiti di risorse concordate, i loro programmi di analisi delle politiche e di rafforzamento delle capacità, in base ad esperienze concrete e riproducibili di quelle politiche ed azioni in materia di TIC che hanno portato alla crescita economica e alla riduzione della povertà, in particoalre grazie ad una maggiore competitività delle imprese.

96 **Ricordiamo** l'importanza che ricopre la creazione di un quadro giuridico, regolamentare e politico affidabile, trasparente e non discriminatorio. A tal fine, **riaffermiamo** che l'UIT ed alcune organizzazioni regionali dovrebbero adottare misure per assicurare un uso razionale, efficace ed economico dello spettro delle frequenze radioelettriche da parte di tutti i Paesi e il loro equo accesso a questo spettro, in base ai pertinenti accordi internazionali.

97 **Riconosciamo** che la partecipazione di una molteplicità di parti interessate è essenziale alla costruzione di una società dell'informazione a misura d'uomo, inclusiva e che previlegi lo sviluppo, e che i governi potrebbero svolgere un ruolo importante in questo processo. **Sottolineiamo** che una delle chiavi del suo successo è la partecipazione di tutte le parti interessate all'attuazione dei risultati dello SMSI e al loro *follow-up* a livello nazionale, regionale ed internazionale, con l'obiettivo primario di aiutare i Paesi a realizzare gli scopi e gli obiettivi di sviluppo concordati a livello internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo.

98 **Incoraggiamo** il rafforzamento e il proseguimento della cooperazione tra le parti interessate per garantire un'efficace attuazione delle decisioni di Ginevra e di Tunisi, per esempio attraverso la promozione di partenariati impostati su di una molteplicità di parti interessate a livello nazionale, regionale ed internazionale, inclusi i partenariati di tipo pubblico/privato (PPP), incoraggiando la creazione di piattaforme tematiche estese ad una molteplicità di parti interessate a livello nazionale e regionale, nel quadro di uno sforzo e di un dialogo concertati con i Paesi in via di sviluppo ed i paesi meno avanzati, i *partner* dello sviluppo e gli attori del settore delle TIC. A questo riguardo, **ci rallegriamo** per l'istituzione di partenariati quali l'iniziativa « Connettere il mondo » presa dall' UIT.

99 **Conveniamo** di garantire costanti progressi verso l'attuazione degli obiettivi dello SMSI una volta conclusa la fase di Tunisi e d'instaurare pertanto un meccanismo di attuazione e di *follow-up* a livello nazionale, regionale ed internazionale.

100 A livello nazionale, in base ai risultati dello SMSI, **incoraggiamo** i governi, con la partecipazione di tutte le parti interessate e tenendo conto dell'importanza di disporre di un ambiente propizio, a creare un meccanismo nazionale di *attuazione* nel quale:

a) delle strategie cibernetiche nazionali dovrebbero, se del caso, fare parte integrante dei piani di sviluppo nazionali e delle strategie di lotta alla povertà, al fine di contribuire all'attuazione degli obiettivi e degli scopi concordati a livello internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo;

b) le TIC dovrebbero essere totalmente integrate nelle strategie di Aiuto Pubblico allo Sviluppo (APS), nell'ambito di uno scambio d'informazioni e di un coordinamento più efficaci tra partner di sviluppo e grazie all'analisi e allo scambio delle migliori prassi e degli insegnamenti tratti dal programma "Le TIC al servizio dello sviluppo";

c) sarebbe opportuno usare, all'occorrenza, i programmi bilaterali o multilaterali di assistenza tecnica esistenti, inclusi quelli che dipendono dal Piano quadro delle Nazioni Unite per l'assistenza allo sviluppo, per aiutare i governi nei loro sforzi di attuazione a livello nazionale;

d) i "Bilanci comuni di Paesi" dovrebbero comprendere una parte dedicata alle TIC poste al servizio dello sviluppo.

101 A livello regionale

a) Su richiesta dei governi, delle organizzazioni intergovernative regionali, in collaborazione con altre parti interessate, dovrebbero condurre in porto attività di attuazione dei risultati dello SMSI, scambiando informazioni e migliori prassi a livello regionale ed agevolando dibattiti di politica generale sull'uso delle TIC al servizio dello sviluppo, con l'accento sulla realizzazione degli scopi ed obiettivi di sviluppo concordati su scala internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo;

b) su richiesta degli Stati Membri e nei limiti delle risorse di bilancio approvate, le commissioni regionali delle Nazioni Unite potrebbero, in collaborazione con organizzazioni regionali e subregionali, organizzare regolarmente attività regionali di *follow-up* dello SMSI, ed assistere gli Stati Membri, fornendo loro informazioni pertinenti, soprattutto di ordine tecnico, dirette all'elaborazione di strategie regionali e all'attuazione dei risultati delle conferenze regionali;

c) **riteniamo** essenziale l'approccio che guarda ad una molteplicità di parti interessate ed alla partecipazione del settore privato, della società civile, dell'Organizzazione delle Nazioni Unite e di altre organizzazioni internazionali alle attività regionali di attuazione dei risultati dello SMSI.

102 A livello internazionale, tenendo conto dell'importanza di un ambiente propizio:

a) *l'attuazione ed il follow-up* dei risultati delle fasi di Ginevra e di Tunisi del Vertice dovrebbero tenere conto dei temi principali e dei grandi orientamenti enunciati nei documenti del Vertice stesso;

b) ogni singola istituzione delle Nazioni Unite dovrebbe agire nell'ambito del proprio mandato e del proprio ambito di competenza, conformandosi alle decisioni prese dal proprio organo direttivo e nei limiti delle risorse esistenti;

c) l'attuazione ed il *follow-up* dovrebbero includere elementi intergovernativi ed elementi di una pluralità di parti interessate.

103 **Invitiamo** le istituzioni delle Nazioni Unite ed altre organizzazioni intergovernative, in conformità con la Risoluzione 57/270 B dell'Assemblea Generale delle Nazioni Unite, ad agevolare lo svolgimento delle attività tra le diverse parti interessate, società civile e settore privato inclusi, per aiutare i governi dei diversi Paesi nei loro sforzi di attuazione. **Chiediamo** al Segretario Generale dell'Organizzazione delle Nazioni Unite di istituire, nell'ambito del Consiglio dei Capi dei Segretariati degli organismi delle Nazioni Unite (CCS), un gruppo delle Nazioni Unite sulla società dell'informazione, composto dai competenti organismi ed organizzazioni delle Nazioni Unite, incaricato di agevolare l'attuazione dei risultati dello SMSI e di proporre al CCS di tenere conto dell'esperienza e delle attività svolte nell'ambito del processo dello SMSI dall'UIT, dall'UNESCO e dal PNUD, quando egli prenderà in considerazione la possibilità di designare l'istitutuzione o le istituzioni incaricate di dirigere tale gruppo.

104 **Chiediamo inoltre** al Segretario Generale dell'Organizzazione delle Nazioni Unite di fare relazione all'Assemblea Generale delle Nazioni Unite, tramite l'ECOSOC ed entro giugno 2006, sulle modalità del coordinamento interistituzionale dell'attuazione dei risultati dello SMSI, incluse eventuali raccomandazioni sul processo del *follow-up*.

105 **Chiediamo** all'ECOSOC di supervisionare il *follow-up* dei risultati delle fasi di Ginevra e di Tunisi dello SMSI a livello di sistema. A tal fine, chiediamo all'ECOSOC, in occasione della sua sessione di fondo del 2006, di riesaminare il mandato, la missione e la composizione del Comitato consultivo sull'applicazione della scienza e della tecnica allo sviluppo, ed in particolare di studiare il rafforzamento di detto comitato, tenendo conto di un approccio impostato su di una molteplicità di parti interessate.

106 La realizzazione e il *follow-up* dei risultati dello SMSI dovrebbero essere elementi a pieno titolo del *follow-up* integrato - a cura dell'ONU - dei risultati delle grandi conferenze delle Nazioni Unite e dovrebbero contribuire alla realizzazione degli scopi e degli obiettivi concordati a livello internazionale, con particolar riguardo agli Obiettivi del Millennio per lo Sviluppo. Non dovrebbe essere a tal fine necessaria la creazione di nuovi organismi operativi.

107 Le organizzazioni internazionali o regionali dovrebbero valutare le possibilità di accesso universale alle TIC nei diversi Paesi e rendere conto regolarmente della situazione, per aprire al settore delle TIC nei Paesi in via di sviluppo prospettive di crescita eque.

108 **Attribuiamo grande importanza** all'attuazione impostata su di una molteplicità di parti interessate a livello internazionale, che dovrebbe essere organizzata secondo i temi ed i grandi orientamenti del Piano di azione ed inquadrata o coordinata da istituzioni delle Nazioni Unite, a seconda dei casi. Un Allegato al presente documento contiene un elenco indicativo e non esaustivo dei coordinatori o moderatori per i grandi orientamenti del Piano d'Azione di Ginevra.

109 Bisognerebbe ricorrere quanto più possibile all'esperienza e alle attività delle istituzioni delle Nazioni Unite nell'ambito del processo dello SMSI - in particolare dell'UIT, dell'UNESCO e del PNUD. Queste tre istituzioni dovrebbero svolgere il ruolo direttivo principale nell'attuazione del Piano di Azione ed organizzare una riunione dei moderatori/coordinatori per i grandi orientamenti, come indicato nell'Allegato.

110 Il coordinamento delle attività di attuazione impostata su di una molteplicità di parti interessate contribuirebbe ad evitare duplicazioni di attività. Questo coordinamento dovrebbe comprendere in particolare lo scambio d'informazioni, la creazione di conoscenze, lo scambio delle migliori prassi e l'aiuto a favore dell'instaurazione di partenariati impostati su di una molteplicità di parti interessate e di partenariati di tipo pubblico/privato.

111 **Chiediamo** all'Assemblea Generale delle Nazioni Unite di procedere ad un esame complessivo dell'attuazione dei risultati dello SMSI nel 2015.

112 **Raccomandiamo** una valutazione periodica in base ad una metodologia concordata, come quella esposta ai paragrafi 113-120.

113 Opportuni indicatori e criteri di riferimento, inclusi gli indicatori di connettività comunitaria, dovrebbero permettere di precisare l'estensione del divario digitale, nelle sue dimensioni nazionali ed internazionali e di valutarla ad intervalli regolari, per fare il punto sui progressi dell'uso delle TIC realizzati nel mondo al fine di raggiungere gli scopi e gli obiettivi di sviluppo concordati a livello internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo.

114 L'elaborazione di indicatori TIC è importante per misurare il divario digitale. **Notiamo** l'avvio, nel giugno 2004, del *Partenariato sulla misura delle TIC al servizio dello sviluppo* e gli sforzi intrapresi in questo ambito per:

a) elaborare un insieme comune di indicatori TIC fondamentali; accrescere la disponibilità di statistiche paragonabili a livello internazionale nel settore TIC [e istituire un quadro concordato per la loro elaborazione], in vista di un successivo esame e decisione della Commissione delle statistiche delle Nazioni Unite;

b) promuovere il rafforzamento delle capacità dei Paesi in via di sviluppo nella valutazione dell'evoluzione della società dell'informazione;

c) valutare le incidenze attuali e gli effetti potenziali delle TIC sullo sviluppo e la riduzione della povertà;

d) elaborare degli indicatori specifici in funzione dei sessi per misurare il divario digitale sotto i suoi diversi aspetti.

115 **Notiamo inoltre** la creazione dell'*indice di apertura alle TIC* e dell'*indice di apertura al digitale*, che completeranno l'insieme comune di indicatori TIC fondamentali, così come sono stati definiti nell'ambito del *Partenariato sulla misura delle TIC al servizio dello sviluppo*.

116 **Sottolineiamo** che tutti gli indici ed indicatori devono tenere conto dei diversi livelli di sviluppo dei Paesi e delle situazioni nazionali.

117 L'elaborazione di questi indicatori dovrebbe proseguire in uno spirito di cooperazione, in modo da essere economica e da evitare duplicazioni di attività.

118 **Invitiamo** la comunità internazionale a rafforzare le capacità dei Paesi in via di sviluppo in materia di statistiche fornendo loro un sostegno idoneo a livello nazionale o regionale.

119 **Ci impegniamo** a rivedere e a seguire i progressi riguardanti la riduzione del divario digitale, tenendo conto dei diversi livelli di sviluppo dei Paesi, per raggiungere gli scopi ed obiettivi di sviluppo concordati a livello internazionale, inclusi gli Obiettivi del Millennio per lo Sviluppo, valutando l'efficacia degli sforzi d'investimento e di cooperazione dedicati alla costruzione della società dell'informazione, identificando le lacune e le carenze sotto il profilo dell'investimento ed elaborando delle strategie per porvi rimedio.

120 Lo scambio d'informazioni sull'attuazione dei risultati del SMSI è un elemento di valutazione importante. **Notiamo con soddisfazione** la relazione dell'Inventario delle attività dello SMSI, uno degli strumenti che agevoleranno grandemente il *follow-up* dopo la fase di Tunisi del Vertice, e il "Libro d'Oro" delle iniziative avviate durante la fase di Tunisi. **Incoraggiamo** tutte le parti interessate presenti allo SMSI a continuare a comunicare informazioni sulle loro attività per alimentare la banca dati dell'Inventario delle attività dello SMSI gestita dall'UIT e accessibile al pubblico. A questo titolo, **invitiamo** tutti i Paesi a contribuire all'inventario raccogliendo informazioni a livello nazionale con il concorso di tutte le parti interessate.

121 E' necessario sensibilizzare sempre più l'opinione pubblica su Internet per rendere questo mezzo di comunicazione universale veramente accessibile al pubblico. **Chiediamo all'Assemblea Generale delle Nazioni Unite** di dichiarare il 17 maggio Giornata mondiale della società dell'informazione, per contribuire a sensibilizzare, ogni anno, l'opinione pubblica sull'importanza di questo mezzo di comunicazione universale e sulle questioni richiamate nell'ambito del Vertice, in particolare sulle prospettive aperte dall'uso delle TIC nel settore economico e sociale, nonché sulle possibilità di riduzione del divario digitale.

122 **Chiediamo** al Segretario Generale del Vertice di presentare una relazione all'Assemblea Generale delle Nazioni Unite sui risultati del Vertice, in conformità con la Risoluzione 59/220 dell'Assemblea Generale delle Nazioni Unite.

Allegato

Grandi orientamenti	Coordinatori/moderatori possibili
C1. Il ruolo delle istanze pubbliche incaricate della *governance* e di tutte le parti interessate nella promozione delle TIC per lo sviluppo	ECOSOC/COMMISSIONI REGIONALI DELLE NAZIONI UNITE/UIT
C2. L'infrastruttura dell'informazione e della comunicazione	UIT
C3. L'accesso all'informazione e alla conoscenza	UIT/UNESCO
C4. Il rafforzamento delle capacità	PNUD/UNESCO/UIT/CNUCED
C5. Stabilire la fiducia e la sicurezza nell'uso delle TIC	UIT
C6. Creare un ambiente propizio	UIT/PNUD/COMMISSIONI REGIONAL DELLE NAZIONI UNITE/CNUCED
C7. Le applicazioni TIC	
• amministrazione elettronica	PNUD/UIT
• commercio elettronico	OMC/CNUCED/UIT/UPU
• teleinsegnamento	UNESCO/UIT/ONUDI
• telesalute	OMS/UIT
• cyberlavoro	OIT/UIT
• cyberecologia	OMS/OMM/PNUE/ UN-Habitat/UIT/OACI
• cyberagricoltura	FAO/UIT
• cyberscienza	UNESCO/UIT/CNUCED
C8. Diversità e identità culturali, diversità linguistica e contenuti locali	UNESCO
C9. Media	UNESCO
C10. Dimensioni etiche della società dell'informazione	UNESCO/ECOSOC
C11. Cooperazione internazionale e regionale	COMMISSIONI REGIONALI DELLE NAZIONI UNITE/PNUD/UIT/ UNESCO/ECOSOC

APPENDICE

NORMATIVA ITALIANA

Delibera dell'Autorità per le garanzie nelle comunicazioni del 16 marzo 2000, *Linee guida per l'implementazione dei servizi di accesso disaggregato a livello di rete locale e disposizioni per la promozione della diffusione dei servizi innovativi,* in <http://www.agcom.it/attivit_.htm>.

Delibera dell'Autorità per le garanzie nelle comunicazioni del 19 luglio 2000, *Disposizioni in materia di autorizzazioni generali,* in <http://www.agcom.it/attivit_.htm>.

Delibera dell'Autorità per le garanzie nelle comunicazioni 10 ottobre 2001, n. 393/01/CONS, *Offerta Wholesale di linee affittate da parte della società Telecom Italia S.p.a.,* in <http://www.agcom.it/attivit_.htm>.

Legge 8 aprile 2002, n. 59, *Disciplina relativa alla fornitura di servizi di accesso ad Internet*, in <http://www.senato.intranet/index.htm> al *link* "leggi e documenti".

Delibera dell'Autorità per le garanzie nelle comunicazioni del 10 luglio 2002, n. 219/02/CONS, *Aggiornamento dell'elenco degli operatori aventi significativo potere di mercato sul mercato dell'accesso ad Internet,* in <http://www.agcom.it/attivit_.htm>.

Delibera dell'Autorità per le garanzie nelle comunicazioni del 1°dicembre 2004, n. 415 (Allegato B), *Identificazione ed analisi del mercato dell'accesso disaggregato all'ingrosso,* in <http://www.agcom.it/attivit_.htm>.

NORMATIVA COMUNITARIA E COMUNICAZIONI ISTITUZIONALI

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, in <http://www.europa.eu.int/eur-lex/>.

Regolamento (CE) n. 2887/2000 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, relativo all'accesso disaggregato alla rete locale, in <http://www.europa.eu.int/eur-lex/>.

Regolamento CE/733/2002 del Parlamento europeo e del Consiglio del 22 aprile 2002 relativo alla messa in opera del dominio di primo livello .eu, in <http://europa.eu.int/eur-lex/>

Comunicazione della Commissione europea, *eEurope 2005: una società dell'informazione per tutti,* 28 maggio 2002, COM (2002) 263 def, in <http://www.europa.eu.int/eur-lex/>.

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, in <http://www.europa.eu.int/eur-lex/>.

Commissione europea, Prima relazione sull'applicazione della direttiva sulla tutela dei dati (95/46/CE), del 15 maggio 2003, COM (2003) 265 def, in <http://www.europa.eu.int/eur-lex/> al *link* "Prelex" - ricerca semplice.

Comunicazione della Commissione europea, *La regolamentazione e i mercati europei delle comunicazioni elettroniche,* 2 gennaio 2004, COM (2004) 759 def, in <http://www.europa.eu.int/eur-lex/>.

Regolamento (CE) n. 460/2004 del Parlamento europeo e del Consiglio del 10 marzo 2004 che istituisce l'Agenzia europea per la sicurezza delle reti e dell'informazione, in <http://www.europa.eu.int/eur-lex/>.

Regolamento CE/874/2004 della Commissione del 28 aprile 2004 che stabilisce le disposizioni applicabili alla messa in opera e alle funzioni del dominio di primo livello .eu e i principi relativi alla registrazione, in <http://europa.eu.int/eur-lex/>

Comunicazione della Commissione, Verso un partenariato mondiale della società dell'informazione: tradurre in pratica i principi di Ginevra, 13 luglio 2004, COM(2004)480 def, in <http://europa.eu.int/eur-lex/>

LEGISLAZIONE COMUNITARIA IN PREPARAZIONE

Proposta di direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, 20 febbraio 2002, COM(2002)92 def, in <http://europa.eu.int/eur-lex/>.

A5-0238/2003 - Posizione del Parlamento europeo definita in prima lettura il 24 settembre 2003 in vista dell'adozione della direttiva 2003/.../CE del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, in <http://europa.eu.int/eur-lex/>.

Posizione comune definita dal Consiglio dell'Unione europea, in vista dell'adozione della direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, 7 marzo 2005, in <http://europa.eu.int/eur-lex/>.

Comunicazione della Commissione al Parlamento europeo relativa alla posizione comune approvata dal Consiglio in vista dell'adozione di direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, 9 marzo 2005, COM(2005) 83 def, in <http://europa.eu.int/eur-lex/>.

A6-0207/2005, Raccomandazione del Parlamento europeo relativa alla posizione comune del Consiglio in vista dell'adozione della direttiva del Parlamento europeo e del Consiglio relativa alla brevettabilità delle invenzioni attuate per mezzo di elaboratori elettronici, in <http://europa.eu.int/eur-lex/>.

ALTRA DOCUMENTAZIONE

WIPO, *Accord entre l'Organisation mondiale de la propriété intellectuelle et l'Organisation mondiale du commerce*, 1995, in <http://www.wipo.int/treaties/fr/general/>.

WIPO, *Traité de l'OMPI sur le droit d'auteur,* Ginevra, 20 dicembre 1996, in <http://www.wipo.int/treaties/fr/general/>.

ICANN, *Principes directeurs régissant le rglement uniforme des litiges relatifs aux noms de domaine* (UDPR), 26 agosto 1999, in <http://www.icann.org>.

WIPO, *Traité sur le droit des brevets et déclarations communes de la conférence diplomatique,* Ginevra, 1° giugno 2000 (Convenzione europea dei brevetti), in <http://www.wipo.int/treaties/fr/general/>.
WIPO, *Traité de coopération en matire de brevets,* Washington, 19 giugno 1970 (modificato da ultimo il 3 ottobre 2001, in <http://www.wipo.int/treaties/fr/general/>.

Memorandum of understanding between the U.S. department of commerce and ICANN, in <http://www.icann.org>.

Bylaws For Internet Corporation For Assigned Names And Numbers - Statuto nel testo emendato il 19 aprile 2004, in <http://www.icann.org>.

WGIG (*Working Group Internet Governance*), *What to do about ICANN: a proposal for structural reform*, 5 aprile 2005, in <http://www.icann.org>.

SOMMET MONDIAL SUR LA SOCIETE' DE L'INFORMATION, *Rapport du Groupe de travail sur la gouvernance de l'Internet,* giugno 2005, in <http://www.itu.int/wsis/> ai *link* "seconda fase, Tunisi", "documenti".

WTO, *Accord sur les aspects des droits de proprieté intellectuelle qui touchent au commerce (TRIPs),* Allegato 1C, articoli 1-21, in <http://www.wto.org> al *link* "documenti".

REGISTRO DEL ccTLD.it, *Regolamento di assegnazione e gestione dei nomi a dominio sotto il ccTLD "it"* (versione 4.0), in <http://www.nic.it/RA/CR/>.

REGISTRO DEL ccTLD.it, *Compiti e modalità di funzionamento della Commissione per le regole e procedure tecniche costituita nell'ambito dell'Istituto di informatica e telematica del CNR per le attività di Registro del* country code Top Level Domain *"it", conformemente a quanto stabilito nel* Request For Comment (RFC), 1591, ICP-1 ed ICP-2, allegato, in <http://www.nic.it/RA/CR/>.

GLOSSARIO

GLOSSARIO[139]

ADSL — acronimo di *Asymmetric Digital Subscriber Line*, identifica una tecnica trasmissiva asimmetrica (cioè caratterizzata da differenti capacità trasmissive da e verso l'utente) che consente di fornire capacità fino 8 Mbit/s verso l'utente e di 800 kbit/s verso la rete, con doppini di lunghezza massima di 3 km.

ALGORITMO — sequenza ordinata di istruzioni che permette di portare a termine un compito più complesso.

ANALOGICO — segnale di tipo continuo che, con le sue variazioni di ampiezza, rappresenta l'informazione originaria.

ASP — acronimo di *Active Server Pages*. Tecnologia sviluppata dalla Microsoft per migliorare la realizzazione di applicazioni *web*. Si tratta di un linguaggio di *scripting* e viene utilizzato per creare siti che sfruttano *e-commerce* e per la personalizzazione delle pagine in base alle scelte fatte dall'utente.

BACKBONE — è la linea principale di Internet, chiamata "dorsale" alla quale collegata, ad altissima velocità, una serie di potenti computer. Ha come scopo quello di collegare le reti regionali tra di loro grazie a chilometri di cavo. Solitamente rientrano in questa categoria i collegamenti da 2 Megabit/s o multipli superiori.

BIT — acronimo di *Binary Digit*, "cifra binaria". Unità di informazione rappresentata da uno 0 o da un 1. La velocità della trasmissione della informazione è misurata in *bit* al secondo, proprio perché è la più piccola unità di dati che può essere trasmessa. Una combinazione di bit può indicare un carattere alfabetico, una cifra numerica, o effettuare una segnalazione, una commutazione o un'altra funzione. Qualsiasi *file* o informazione è fondamentalmente composto da *bit.*

BPS — acronimo di *Bit* per secondo. Unità di misura per calcolare la velocità di trasmissione dati all'interno di una rete.

---

[139] Le voci indicate sono principalmente tratte da una selezione del Glossario allegato all'opera di F. BRUGALETTA, *Internet per giuristi,* Napoli, Edizioni Simone, 2003, IV Edizione, e da altri glossari relativi ad Internet e alla terminologia tecnologica reperiti *on line*.

BROWSER programma che permette di navigare nel *web*. I più noti sono Netscape Navigator ed Internet Explorer della Microsoft.

BROADBAND cfr. LARGA BANDA

CDN linea dedicata per la trasmissione dei dati ad alta velocità (min 4800 bps, max 2 Mbps) fornita da Telecom Italia.

CLIENT all'interno di una rete ad accesso regolato o in Internet, si definisce *client* un computer che accede a risorse di rete condivise e fornite da un'altra macchina denominata *server*, cui il *client* può lanciare comandi.

CODICI SORGENTE E OGGETTO il *file* (codice) sorgente rappresenta il progetto, ossia lo schema scritto in un linguaggio simile alla lingua naturale. Il *file* (codice) oggetto è invece la traduzione di quello schema in linguaggio macchina (codice binario).

DOMINIO la parte a destra di un indirizzo Internet.

DOWNLOAD operazione di trasferimento di un *file* presente nella rete: è prelevato dal *server* che lo rende disponibile e viene collocato sul proprio computer con la possibilità di utilizzarlo successivamente anche in assenza di collegamento.

FTP acronimo di *File Transfer Protocol*. Protocollo che consente il trasferimento di dati da un *server* ad un computer remoto. Generalmente, gli archivi di *software* presenti in rete utilizzano questo protocollo per consentire il *download* da parte dell'utente. E' possibile che prima di accedere ad un *server* FTP venga richiesta l'immissione di *login* e *password*.

GARR acronimo di Gruppo di Armonizzazione Reti di Ricerca, organismo del C.N.R. che coordina tecnicamente lo sviluppo di Internet in Italia.

HDSL acronimo di *High bit rate Digital Subscriber Line* che identifica una tecnica trasmissiva simmetrica (cio' caratterizzata da uguali

capacità trasmissive da e verso l'utente) che consente di fornire capacità di 2 Mbit/s.

HOST computer o *server* connesso ad una rete e predisposto per fornire prestazioni (materiale d'archivio, programmi) a computer "clienti".

HTML acrononimo di *Hyper Text Markup Language,* linguaggio con il quale si scrivono le pagine *web*.

HTTP acronimo di *Hyper-Text Transfer Protocol*. E' il protocollo di trasmissione utilizzato per il trasferimento di documenti ipertestuali in Internet. L'apposizione di "http" all'inizio di un indirizzo Internet indica il protocollo necessario al trasferimento dal server al proprio sistema.

ICT acronimo di *Information Communication Technology***.** Letteralmente "Tecnologie dell'Informazione e della Comunicazione", insieme delle tecnologie che consentono il trattamento e lo scambio delle informazioni - siano esse testuali, visive o sonore - in formato digitale.

INCUMBENT è l'operatore telefonico dominante in un Paese.

IP acronimo di *Internet Protocol,* numero che identifica in rete un *host*, quale *provider* ad esempio, formato da più cifre separate da un punto. Questo dato viene sempre fornito dai *provider* ai propri abbonati che dovranno inserirlo nei controlli TCP/IP o SLIPP/PPP (a seconda del sistema o della piattaforma utilizzati) per poter effettuare la connessione.

INTERFACCIA punto in cui si verifica il contatto fra due elementi interagenti fra loro. Nel linguaggio informatico lo strumento attraverso il quale l'utente dialoga con il computer.

ISDN Sistema di trasferimento per convogliare voce, video e dati in formato digitale sulla linea telefonica. Chi utilizza una linea ISDN (ed il relativo e specifico *modem*) per il suo collegamento

	ad Internet, può usufruire di una maggiore velocità di connessione (v. anche xDSL).
ISP	acronimo di *Internet Service Provider***.** Letteralmente "fornitori di servizi Internet". Operatori che dispongono di proprie reti di telecomunicazione e forniscono l'accesso ai servizi Internet ad individui e organizzazioni. Gli ISP possono anche rivendere la facoltà di utilizzo della rete e dei servizi ad altri operatori, che possono operare a loro volta come fornitori di servizi utilizzando un proprio marchio e/o il marchio del *Service Provider*.
LAN	acronimo di *Local Area Network***.** E' una rete locale di computer connessi fisicamente l'uno all'altro. Questo tipo di connessione ha il vantaggio di poter condividere programmi, dati e risorse rendendoli disponibili a tutti. Sempre in base all'estensione si classificano altri tipi di rete come la MAN (*Metropolitan Area Network*), la WAN (*Wide Area Network*) e la GAN (*Global Area Network*).
LARGA BANDA	si riferisce al quantitativo di dati che può essere inviato tramite un determinato sistema di comunicazione in un tempo definito. Una grande ampiezza di banda implica una maggiore velocità nel trasferimento dei dati da un punto all'altro della rete che costituisce Internet.
LIC	acronimo di *Local Internet Community,* indica la collettività dei soggetti coinvolti nel mondo di Internet.
MODEM	dispositivo utilizzato per la trasmissione di informazioni tra computer e linea telefonica. In entrata di dati, il *modem* provvede a trasformare in segnali digitali gli impulsi analogici della rete telefonica ("demodulazione"), al contrario, i segnali in uscita, da digitali vengono trasformati in analogici ("modulazione").
MULTICAST	tecnica che consente la trasmissione simultanea a un insieme di utenti dello stesso elemento audio o video.

OLO acronimo di *Other Licensed Operator*. Sono gli operatori nuovi entranti sul mercato di Internet, che forniscono servizi su licenza dell'operatore principale o *incumbent*.

POP acronimo di *Point Of Presence - Post Office Protocol.* Il termine può avere due significati differenti: nel primo caso rappresenta per i *provider*, i nodi di accesso alla rete Internet, mentre, nel secondo, è il sistema di memorizzazione e gestione della posta elettronica all'interno di un *server*.

PROTOCOLLO insieme di regole che sovrintende al trasferimento delle informazioni su Internet.

PROVIDER fornitore dell'accesso ad Internet.

REGISTRATION AUTHORITY ente che provvede alla regolare registrazione di un nome a dominio.

RETE D'ACCESSO è quel segmento della rete di telecomunicazioni che collega fisicamente i nodi periferici (dove sono alloggiate le centrali locali) ai singoli utenti (sia residenziali sia affari), per tratte che possono andare dalle centinaia di metri a oltre 4 km (in Italia la lunghezza media di 1.5 km, ed anche meno in ambito metropolitano). Spesso si usa identificare questo segmento di rete come "ultimo miglio", proprio per sottolineare che si tratta della parte terminale della rete che collega gli utenti.

ROOT SERVER *server* che gestisce il traffico dei dati Internet, lo scambio di *file*, di *e-mail* e l'inoltro delle pagine tramite indirizzo IP, ovvero l'interpretazione dell'URL per trasformarle in indirizzo IP. Da questi *server*, distribuiti in diversi continenti, dipende il funzionamento dei diversi *Domain Name System server*.

SDH acronimo di *Synchronous Digital Hierarchy*. Identifica sistemi trasmissivi sincroni caratterizzati da capacità che vanno dai 155 Mbit/s a 2,5 Gbit/s.

SDSL acronimo di *Symmetrical Digital Subscriber Line*. Sistemi simmetrici per la trasmissione su doppino con una larghezza di banda che può raggiungere le decine di Mbit/s.

SERVER computer dedicato allo svolgimento di un servizio preciso, come la gestione di una rete locale o geografica, alla gestione delle periferiche di stampa (*print server*), allo scambio e condivisione di dati fra i computer (*file server, database server*), all'invio o inoltro di posta elettronica (*mail server*) o a contenere i file di un sito *web* (*web server*). Utilizza un sistema operativo di rete. I computer collegati e che utilizzano il servizio del *server*, si chiamano *client*. A volte lo stesso computer svolge diverse funzioni di *server* (es: sia *file server* che *print server*).

SMTP acronimo di *Simple Mail Transfer Protocol.* Protocollo Internet per i servizi di posta elettronica semplice; il nome del *server* che fornisce il servizio e che permette la ricezione della posta.

SOHO acronimo di *Small Office Home Office*. Indica il mercato dell'informatica diffusa a livello casalingo e di piccolo ufficio.

SPAM posta elettronica non richiesta e spedita per pubblicità.

SPAMMING invio di uno stesso messaggio, a più persone, contemporaneamente.

SOFTWARE è la parte immateriale dell'elaboratore. Si distingue tra *software* di base (sistema operativo) e *software* applicativo (programma propriamente detto). Il sistema operativo racchiude le istruzioni che permettono all'elaboratore di funzionare. Il *software* applicativo permette all'utente di risolvere problemi specifici (contabilità, videoscrittura, disegno, ecc).

TCP/IP *Transmission Control Protocol/Internet Protocol,* è il gruppo di protocolli che permette il funzionamento di Internet.

UNBUNDLING cfr. RETE DI ACCESSO

URL acronimo di *Uniform Resource Locator,* è l'indirizzo del sito su Internet.

VDSL acronimo di *Very High bit rate Digital Subscriber Line*, indica un'evoluzione dei sistemi asimmetrici ADSL verso capacità fino a 50 Mbit/s verso l'utente e dell'ordine di alcuni Mbit/s verso la rete, per doppini di lunghezza massima dell'ordine di alcune centinaia di metri.

VHS acronimo di *Video Home System*. E' un sistema di registrazione del segnale video analogico su nastri magnetici da mezzo pollice.

WDM acronimo di *Wavelength Division Multiplexing.* Insieme delle tecniche di multiplazione a divisione di lunghezza d'onda che consentono di immaginare un incremento considerevole (da 60 a 200 volte l'attuale) della capacità trasportata da ogni singola fibra ottica.

WLL acronimo di *Wireless Local Loop*. Area d'accesso realizzata con tecniche radio. Tipicamente i sistemi WLL operano nel campo delle frequenze da 3 GHz a 43 GHz.

WSIS acronimo di *World Summit on the Information Society.* E' un *summit* internazionale che ha come tema la creazione della società dell'informazione. Nasce da una risoluzione delle Nazioni Unite ed è presentato come un processo dinamico che promette una trasformazione profonda in ogni aspetto della vita di relazione. Il vertice è un processo tripartito basato sulla partecipazione di governi facenti parte delle Nazioni Unite, di privati, della società civile e di agenzie internazionali.

WWW acronimo di *World Wide Web,* letteralmente ragnatela sparsa in tutto il mondo. E' la parte di Internet costituita dagli ipertesti.

xDSL acronimo di *x Digital Subscriber Loop*. Si intende un insieme di tecniche trasmissive che consentono di fornire servizi a larga banda in area d'utente utilizzando, come mezzi trasmissivi, i doppini in rame già installati (v. anche HDSL, ADSL, VDSL).

BIBLIOGRAFIA

BIBLIOGRAFIA

M. BERTANI, *Proprietà intellettuale, antitrust e rifiuto di licenze,* in «Quaderni di AIDA», n. 10 (2004), pp. 1-54.

F. BRUGALETTA, *Internet per giuristi,* Napoli, Edizioni Simone, 2003.

P. COSTANZO, *La democrazia elettronica (note minime sulla c.d.* e-democracy*),* in «Il diritto dell'informazione e dell'informatica», n. 3 (2003), pp. 465-486.

F. FOGLIANI, *Internet Governance in Italia,* in *Tutela del dominio Internet e del marchio, Atti del Convegno dell'Istituto di Ricerca Internazionale*, Milano, 19-20 marzo 2002, disponibile in <http://www.nic.it/NA/present/fog-milano.html>.

F. GUADAGNI, *Nomi e indirizzi Internet: rivoluzione in vista?*, in <http://www.telecomitalialab.com/libri/InternetTouch/aree/guadagni2.pdf>

C. MAGNANINI, *Net economy made in China,* in «L'espresso», n. 33 (agosto 2005), pp. 40-45.

P. MENCHETTI, *Più garanzie per i nomi a dominio aziendale,* in «Guida al diritto», n. 3 (marzo 2005), pp. 130-132.

G. PASCUZZI, *Scoperte scientifiche, invenzioni e protocolli relativi a Internet*, «AIDA», n. 5 (1996), p. 162.

B. PAVOLETTI, *I concetti fondamentali di Internet,* Regione Liguria, Servizio Sistemi Informatici, 1999.

F. POMARICI, *La risoluzione alternativa delle controversie tramite Internet,* Tesi di laurea non pubblicata, Università "La Sapienza" di Roma, Facoltà di giurisprudenza, Istituto di diritto privato, a.a. 2004-2005.

T. PUCCI, *Il diritto all'accesso nella società dell'informazione e della conoscenza. Il* digital divide, in «Informatica e Diritto», marzo 2005, pp. 119-153.

P. RIDOLFI (a cura di), *I disabili nella società dell'informazione,* Milano, Angeli, 2002.

G. ROSATI, *Il Digital Divide in Cina*, 15 gennaio 2003, in <http://www.unarete.org> al *link* "Documenti", in cui sono raccolti riferimenti al *digital divide* nei diversi Paesi del mondo.

G. SANTANIELLO, *I codici di deontologia nel trattamento dei dati personali,* in «Interlex, diritto tecnologia informazione», rivista *on line* disponibile in <http://www.interlex.it/675/santaniello3.htm>.

F. SILVA, *Copyright e mercato,* in *Proprietà intellettuale e cyberspazio*, *Atti del convegno internazionale promosso dall'Osservatorio "Giordano Dell'Amore" sui rapporti tra diritto ed economia*, Stresa, maggio 2001, pp. 31-60.

A. SPERLINGA, *Piccolo corso di Internet, edizione minima*, disponibile in <http://www.alessiosperlinga.it> e in <http://encyclopedie-it.snyke.com/articles/rete_telematica.html>.

A. S. TANENBAUM, *Reti di calcolatori,* Milano, Pearson Education Italia, 2003.

S. TRUMPY, *Internet governance in Italia e nel mondo*, relazione per la Giornata di lavoro *Internet: quale futuro per l'Italia*, a cura del Comitato di Esperti Internet della Presidenza del Consiglio dei Ministri, Roma, 6 novembre 2000.

S. TRUMPY - F. CANESCHI, *Rapporti tra Registri dei nomi a dominio e relativi governi*, relazione per la Tavola rotonda organizzata dalla Sezione italiana di *Internet Society* (ISOC), *Internet Governance: pubblici poteri e partecipazione della "Local Internet Community"*, 22 maggio 2002, disponibile in <http://www.isoc.it/tavolarotonda4/trumpy-caneschi.html >.

P. ZOCCOLI, *Il WTO e la regolazione della liberalizzazione del commercio mondiale per la costruzione del vantaggio competitivo della nazione e delle imprese,* in «Economia e diritto del terziario», n. 2 (2004), pp. 396-413.