We introduce you the inventors of Differentiated Web Surfing

SAFETY WORLD WIDE WEB
FOUNDATION

Via Trebeschi 36
Castegnato - Brescia
Italy
tel.: +39 030 3648400
www.swww.org
www.childkey.org

gestweb
forwarding ideas

Viale Bornata 9
25123 Brescia - ITALY
www.gestweb.com

NAVIGAZIONE DIFFERENZIATA™

NAVIGATION DIFFÉRENCIÉE

DIFFERENTIATED WEB SURFING™

SAFETY WORLD WIDE WEB FOUNDATION

NAVIGAZIONE DIFFERENZIATA™

TECNOLOGIA CHILDKEY™

ChildKey

Accogliendo le raccomandazioni più volte espresse dall'Unione Europea, la società Gestweb spa unitamente alla Fondazione Safety World Wide Web Onlus, hanno elaborato, idealizzato e realizzato la tecnologia Childkey che rappresenta l'unico vero sistema che soddisfa e fa propri tutti i postulati della Navigazione Differenziata.

L'architettura del tecnologia ChildKey si basa sulla possibilità di associare alla richiesta di pagine web il profilo di età (tag-età) dell'utente che le richiede (funzionalità Age Sender).

Per fare questo, è necessario che il profilo dell'utente sia riconoscibile già nel momento in cui avviene la connessione alla rete e comunque prima dell'inizio della navigazione.

Tale riconoscimento è reso possibile da un identificatore di connessione associato all'età dell'utente che questi deve digitare e inoltrare all'atto di connettersi.

L'operazione di identificazione viene svolta dai nuovi autenticatori di Rete ChildKey destinati agli Internet Service Providers con il quale l'utente ha stipulato un contratto di accesso a Internet con il servizio ChildKey.

Tale contratto prevede l'uso degli autenticatori ChildKey in grado di fornire una navigazione differenziata, per l'adulto e per il minore, in base ad un identificatore di connessione associato all'età e rilasciato a ciascun componente la famiglia.

Quando un identificatore di connessione corrispondente a un minorenne viene digitato, l'autenticatore ChildKey indirizza la connessione attraverso la tecnologia di navigazione assistita, attivando la funzionalità Age Sender, Time Limit Control e Total Privacy nonchè tutte le funzionalità di Parsing o Analisi Testuale.

Con AgeSender i servers remoti sono messi in grado di conoscere l'età dell'utente collegato (unica tecnologia al mondo) e quindi di responsabilizzare penalmente i fornitori di contenuti e coloro che li ospitano.

Adeguandosi alla tecnologia ChildKey, i gestori dei siti possono facilmente "moralizzare" il proprio operato apponendo alle pagine dei siti una semplice dichiarazione (metadata ChildKey) concernente la visibilità o non visibilità ai minori dei contenuti messi in rete. E' compito della Fondazione Safety World Wide Web sollecitare tale dichiarazione e controllare che venga eseguita correttamente.

Una ampia diffusione del tecnologia modificherà il "modus operandi" dei Providers e dei Motori di Ricerca nonchè dei fornitori di contenuti in Rete adeguandoli a criteri di responsabilità nei confronti dei minori. Ciò renderà il ricorso alla navigazione differenziata solo quale cautela ma non, come avviene oggi, quale unica misura disponibile.

La tecnologia ChildKey viene diffusa, come tecnologia integrato denominato Keystudent, nelle scuole, biblioteche e tutti quei centri di aggregazione giovanile ove sentita è l'esigenza di protezione dei giovani internauti.

La tecnologia realizzata prevede l'utilizzo da parte del Provider di connessione di un pacchetto software, residente sul server, in grado di gestire un alto livello di sicurezza a garanzia dell'accesso ad Internet dei minori, mentre mantiene una totale trasparenza nella navigazione degli adulti.

Per le scuole, biblioteche e centri di aggregazione giovanile è previsto un'appliance "all in one".

Per i Postulati della Navigazione Differenziata CHildKey vedi a pagina 16.

GLI INVENTORI DELLA NAVIGAZIONE DIFFERENZIATA

ChildKey

Presentato in conferenza stampa al Parlamento Europeo in data 2 settembre 2003 ed in assemblea plenaria delle delegazioni UEN é stato accolto con successo. Ha consentito l'accoglimento delle proposte di modifica al progetto DAPHNE II della Comunità Europea proposte dall'Italia.

Recepito nel Codice di Autoregolamentazione del Ministero delle Comunicazioni firmato a Roma il 19 novembre 2003.

VANTAGGI DERIVANTI DALL'USO DELLA NAVIGAZIONE DIFFERENZIATA

Internet è
"on demand"
ma ora sappiamo
"who is demanding"

- Si utilizza tramite una connessione ad Internet unica per tutta la famiglia, differenziando le password di accesso per i vari membri in funzione dell'età (una per ogni figlio minorenne registrato). ***Art. 3.8 del Codice di Autoregolamentazione***
- Consente l'identificazione del minore già sin dalla richiesta di connessione o comunque prima dell'inizio della navigazione.
- Risponde all'esigenza di sicurezza delle famiglie, permettendo ai bambini una navigazione "senza sorprese" impedendo al bambino l'accesso a siti con contenuto volgare, osceno o violento.
- Informa il bambino che la sua navigazione sarà controllata e dei privilegi a lui spettanti.
- Impedisce la diffusione in Rete dei dati sensibili del minore e del nucleo famigliare.
- Consente di comunicare la presenza del minore all'intera "Rete" notificando ai server visitati il tag-età di presenza del minore che ha richiesto la visualizzazione di contenuti. ***Art. 3.4 del Codice di Autoregolamentazione***

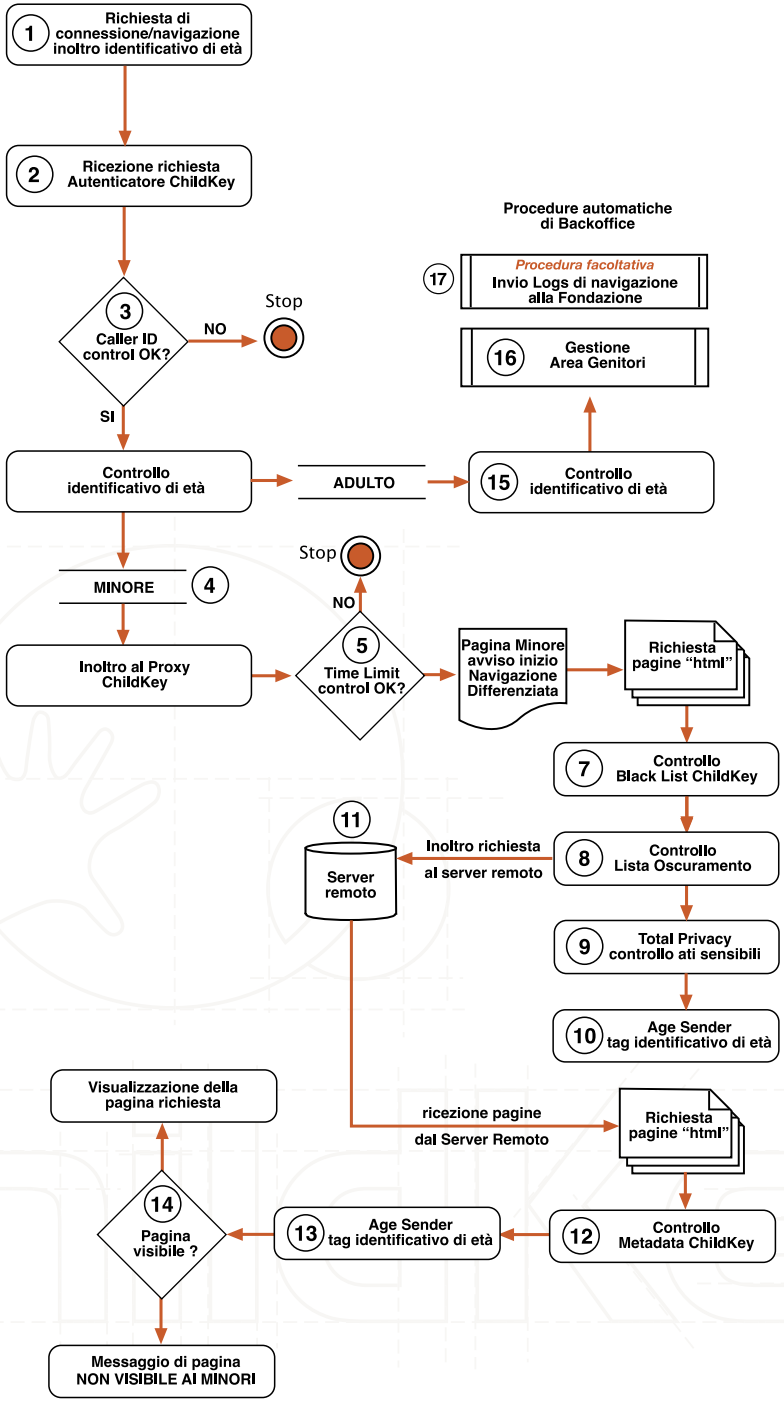
  La nuova informativa crea i presupposti della responsabilizzazione penale di tutti i soggetti che intervengono e operano in Internet.
- Consente di impedire al minore la diffusione in "Rete" dei propri dati sensibili e di quelli del nucleo di appartenenza (Funzione Anti-adescamento).
- Consente ai genitori di tutelare la salute dei figli determinando la durata delle singole connessioni e la durata massima di connessione giornaliera, nonché le fasce orarie di connessione
- Garantisce al genitore di visionare l'attività svolta dal minore in "Rete" (Registri di navigazione e Registro Attività)
- Consente all'adulto di determinare i privilegi di navigazione - via Web - di ogni singolo minore del nucleo famigliare (Area Genitori)
- Non comporta l'installazione di alcun software o hardware sul computer dell'utente
- Consente l'uso della Qualified Mail per una più corretta protezione verso lo spam lesivo dei diritti della famiglia .
- La navigazione degli adulti rimane libera e completamente trasparente al tecnologia
- Offre al Provider la possibilità di dare un servizio a valore aggiunto
- In accordo con gli scopi della **Fondazione Safety World Wide Web onlus**, consente il perseguimento legale nei confronti di quei Providers insensibili agli aspetti legali della diffusione di materiale pornografico o non adatto ai minori.

  La **Fondazione Safety World Wide Web onlus** informa tutti i Prestatori di Servizi che ospitano a qualunque titolo i gestori dei siti visitati dai minori dell'esistenza della tecnologia ChildKey e del mutamento delle responsabilità a loro carico.
- Ai Motori di Ricerca consente di comprendere quando la "ricerca" sia richiesta da un minore e quindi attivare i conseguenti ed "obbligatori" filtri di tutela
- Alle Autorità di ogni singolo Stato di contribuire alla formazione della Lista di Oscuramento contenente tutti i siti con contenuto di natura reatuale (pedo-pornografia, razzismo ecc..)
- I fornitori di contenuti (Registrant) possono autocertificare il contenuto di ogni pagina html pubblicata richiedendo o adottando gratuitamente il metadata ChildKey.

  E' obbligatorio per i destinatari di servizi (proprietari dei siti web) con contenuti non adatti ai minori
- I fornitori di contenuti diventano ora responsabili penalmente di quanto diffuso in "Rete" e ciò grazie alla notifica di presenza del minore (Age Sender)
- Consente di cambiare la Rete imponendo un comportamento etico e consentendo che tutti i contenuti in un prossimo futuro, siano certificati
- Consente inoltre la sparizione di materiale pedo-pornografico dalla Rete poiché il Prestatore di Servizi (Provider che ospita i contenuti a qualunque titolo) non potrà più accettare contenuti da anonimi e non classificati nel qual caso sarà correo dello stesso reato previsti all'art. 600 quater del codice penale.

COSA ACCADE QUANDO CI SI CONNETTE E SI NAVIGA

FLOW CHART

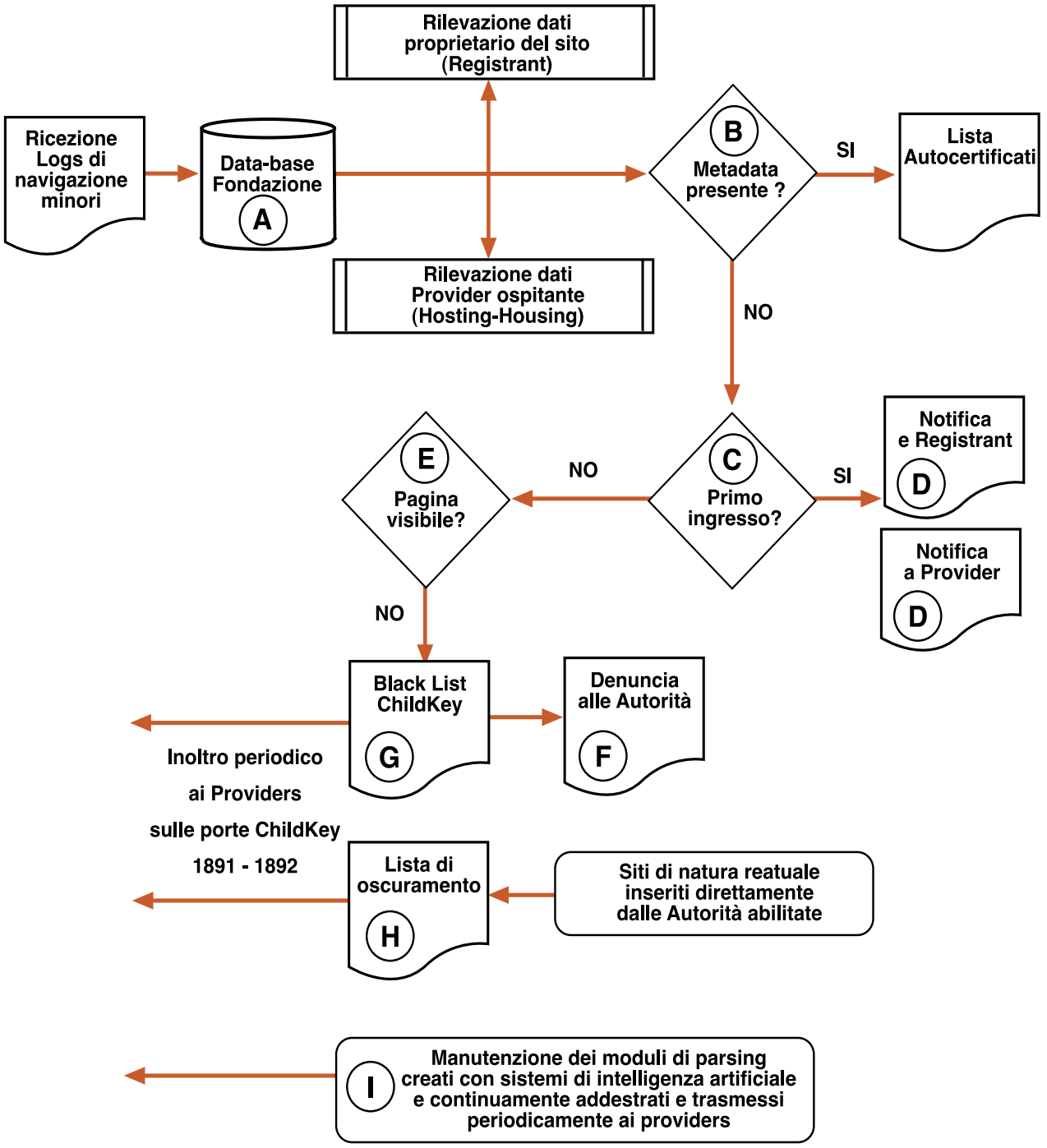


FLOW CHART DETAILS

Identificazione e riconoscimento del minore	Fase che attiene alla sfera privata tra Provider e proprio Utente. Attraverso l'invio del tag-età (ChildKey) il Provider Childkey è posto in condizioni di identificare il minore all'atto della richiesta di connessione o, in caso di linea cable, prima che inizi la navigazione. • il Provider ChildKey rilascia tanti identificatori di connessione associati all'età quanti sono i componenti del nucleo famigliare;	1 2 3 4
Trasparenza ed informativa	Il minore viene informato, dopo l'avvenuta identificazione, nella "Home Page Famiglia", che trattasi di navigazione differenziata e dei privilegi per esso fissati e dei tempi residui di navigazione spettantigli.	2
Navigazione Libera per l'adulto	Non pone restrizioni di sorta alla navigazione dei maggiorenni. Esiste la possibilità di applicare la Lista di Oscuramento anche all'adulto; in tal modo verrebbe sottratta utenza al mercato alla pedo-pornografia.	15 16
Time Limit Control Tutela della salute	Consente all'adulto di determinare la durata delle connessioni e le fasce orarie abilitate e precisamente: • durata di una singola connessione continuativa; • durata massima del totale delle connessioni giornaliere; • fasce orarie abilitate per la connessione.	5
Area Genitori	Consente di determinare i privilegi di navigazione di ogni singolo minore e di visualizzare e controllare: Configurazione privilegi per il settaggio dei filtri di navigazione di ogni singolo minore incluso il Time Limit Control; Registri di Navigazione i reports di navigazione di ogni singolo minore sono disponibili per il controllo via Web o possono essere inviati tramite posta elettronica e consentono l'informativa costante e dettagliata dell'operato del minore; Registri di Attività i reports di navigazione di tutta la famiglia con indicazione di data e durata delle singole connessioni giornaliere.	16
Black-List ChildKey	Lista dei siti, precedentemente notificati, che hanno rifiutato l'autocertificazione e considerati a rischio per il minore. La Black-List ChildKey viene periodicamente trasmessa ai Providers.	7 G
Lista di Oscuramento	Lista dei siti con contenuto reatuale (pedo-pornografia) e direttamente inseriti nel data-base della Fondazione dalle Autorità competenti a ciò preposte e abilitate. La Lista di Oscuramento viene distribuita ai Providers.	8 H
Total Privacy Antiadescamento	Impedisce l'adescamento del minore impedendo la diffusione in rete dei dati sensibili del nucleo famigliare. Impedisce anche che le Black-List possano essere eluse. Impedisce l'aggiramento delle Black-List o del Parsing tramite i siti "cleaner" o pulitori.	9 16

Autocertificazione dei contenuti Metadata ChildKey	L'inserimento del metadata ChildKey (<meta name ="swww.childkey" content="childkey.red">) o(<meta name ="swww.childkey" content="childkey.green">) in tutte le pagine html visibili, siano esse statiche o dinamiche, consente alla Tecnologia ChildKey di discriminare tra contenuti visibili e non visibili ai minori. L'adozione di un metadata consente alla tecnologia una standardizzazione e una diffusione a costo zero per tutti i costruttori e web masters di siti Internet.	**12 D E**
Age Sender Notifica di presenza del minore alla rete	Fase che attiene alla sfera pubblica tra Provider e la Rete Internet. Consiste nella notifica di presenza del minore a tutta la Rete Internet con l'uso di un identificatore riconoscibile da tutti e quindi pubblico inserito nell' header di richiesta. Ad ogni richiesta di pagine da parte del minore, la Tecnologia ChildKey notifica al server interpellato anche il tag età del minore: tale funzione è effettuata dal modulo Age Sender ed è coperta da brevetto. Il Provider riceverà una comunicazione come nell'Esempio 2, cioè modificata dal modulo Age Sender:	**10**
	Esempio senza Age Sender : http- request: GET / HTTP / 1.0 Connection: Keep-Alive User-Agent: Mozilla/4.0 Host: www.apple.com Accept: */* Accept-Language: en, it	Esempio con Age Sender : http - request: GET / HTTP / 1.0 Connection: Keep-Alive User-Agent: Mozilla/4.0 Host: www.apple.com Accept: */* Accept-Language: en, it **My age is: minor**
	Tale funzione genera una informazione che produce ripercussioni in campo penale creando i presupposti della responsabilità penale in capo ai fornitori di contenuti e dei Providers che li ospitano e dei Motori di Ricerca.	
Parsing Dinamico Modelli da intelligenza semantica	Impedisce la visualizzazione al minore di pagine pornografiche e pedo-pornografiche attraverso l'uso di moduli creati ed addestrati con sistemi di intelligenza artificiale e costantemente aggiornati dalla Fondazione. L'interpretazione del contenuto testuale e di altri parametri coperti da brevetto consentono l'identificazione del 98% delle pagine a rischio.	**13 I**
Sensore di presenza minore Snasa ChildKey	L'uso software Snasa Childkey consente ai Motori di Ricerca ed ai servers dei Providers di "comprendere" se la richiesta di pagine "html" è effettuata da un minore. ***Alternativamente basterà una clausola contrattuale che imponga l'identificazione del proprietario dei contenuti e la c ertificazione degli stessi con il metadata ChildKey.***	**11 D**
Inoltro automatico dei reports di navigazione (Procedura facoltativa)	I reports o logs di navigazione dei minori, con esclusione delle anagrafiche a tutela della Privacy, vengono inoltrati alla Fondazione Safety World Wide Web Onlus per il trattamento dei dati e le conseguenti azioni di tutela dei minori.	**17 A D**

FLUSSO ELABORAZIONE DATI DELLA FONDAZIONE



Ricezione reports navigazione	Il data base della Fondazione riceve sulle porte 1891 e 1892 i reports di navigazione dei minori da tutti i Providers che utilizzano la tecnologia ChildKey. I reports non contengono anagrafiche e ciò a tutela della Privacy del minore.	**17 A**
Controllo Metadata ChildKey	In tale fase La tecnologia controlla la presenza del Metadata ChildKey. In caso positivo la pagina "html" del sito viene catalogata tra quelle autocertificate. L'inserimento di un metadata in tutte le pagine html visibili, siano esse statiche o dinamiche, consente alla Tecnologia ChildKey di discriminare tra contenuti visibili e non visibili ai minori. L'adozione di un metadata consente alla tecnologia una standardizzazione e una diffusione a costo zero per tutti i costruttori e web masters di siti Internet. Il mancato inserimento del metadata ChildKey da parte dei gestori di siti visitati da minori comporta l'inclusione del sito nella Black-List dei siti sconsigliati ai minori, compilata e aggiornata dalla fondazione Safety World Wide Web Onlus. L'informativa di presenza di minore comporta l'obbligatorietà all'autocertificazione se i contenuti diffusi in rete non sono visibili ai minori conformemente alle disposizioni legislative vigenti in italia o in Europa. L'uso del Metadata è licenziato gratuitamente e così pure il software per l'inserimento automatico dello stesso se il sito contiene molteplici pagine . Le condizioni di licenza prevedono che l'autocertificazione avvenga sulla base delle norme Europee o Italiane inerenti la protezione dei minori. Come è formulato il metadata ChildKey: per siti visibili ai minori: <meta name ="swww.childkey" content="childkey.green"> per siti non visibili ai minori: <meta name ="swww.childkey" content="childkey.red"> N.B. Il metadata ChildKey certifica ogni singola pagina Html del sito e non il sito. Quindi un sito potrebbe contenere sia pagine visibili che pagine non visibili ai minori, mantenere anche in presenza di queste ultime le barre di navigazione (sempre che le stesse siano visibili). I siti con metadata "green" vengono comunque sottoposti a Parsing a titolo cautelativo.	**B**
Analisi di incongruenza	Il sistema accetta la dichiarazione di non visibilità per i minori e conseguentemente trasmette al minore la pagina di cortesia. Nel caso invece di dichiarazione di visibilità, provvede comunque a controllarne il contenuto al fine di evitare una errata o mendace dichiarazione, in tale caso, il test di incongruenza evidenzia tale situazione e la Fondazione agirà non solo in sede penale ma anche in sede civile per ciolazione di licenza.	**12**

FLOW CHART DETAILS

Identificazione Registrant e Provider	La Fondazione provvede con un tecnologia automatica ad identificare, in corrispondenza dell'URL visitato dal minore, il Registrant o Proprietario del sito ed il Provider che lo ospita.	**D**
Controllo notifica	In questa fase si controlla se al Registrant ed al Provider sia già stata inviata l'informativa di cui al punto E. In caso affermativo e stante l'assenza del metadata autocertificatore, si procede alla fase successiva F.	**C**
Controllo contenuti	Utilizzando il Parsing Dinamico utilizzato dalla Tecnologia ChildKey si verifica se tale pagina "html" abbia contenuti non idonei ai minori. In caso affermativo si procede ad inserire l'URL nella Black-List ChildKey F ed ad effettuare l'esposto-denuncia H	**E**
Parsing Modelli Semantici	La Fondazione ha cura di aggiornare ed addestrare i sistemi di Intelligenza Semantica per l'ottenimento dei Modelli da cui sono estratti i vocabolari per l'analisi dei contenuti delle pagine "html". La Fondazione cura anche l'uso di altre metodi di riconoscimento. I modelli semantici aggiornati sono trasmessi ai Providers sulle porte 1891/92.	**I**
Esposto denuncia	La Fondazione si fa carico di procedere a formulare gli esposti-denuncia nel caso di violazione dei diritti di minori che navigano in rete. In tal caso fornisce tutta la documentazione tecnica necessaria.	**F**
Black-List ChildKey	Viene realizzata la Black-List dei siti non autocertificati e con contenuti ritenuti a rischio per i minori. Tale Black-List è costantemente monitorata e aggiornata e viene distribuita ai Providers sulle porte 1891/92.	**G 7**
Private White and private Black Lists	In ossequio alla sentenza della Corte Suprema Usa del 29 giugno 2004, il sistema non fa uso di Liste cosruite da terzi o comunque realizzate privando i soggetti inseriti della possibilità di autocertificazione. Le Private White and Black Lists sono l'espressione del massimo rispetto morale, religioso e politico della famiglia, scuola o altro sistema educativo che ne faccia uso. Difatti le stesse sono costruite dagli stessi educatori nel rispetto della propria linea di pensiero.	
Lista di Oscuramento	Lista dei siti con contenuto reatuale e direttamente inseriti nel data-base della Fondazione dalle Autorità competenti a ciò preposte e abilitate. La Lista di Oscuramento viene distribuita ai Providers sulle porte 1891/92.	**H 8**

OBBLIGHI DELLA FONDAZIONE

Obbligo istituzionale della Fondazione Safety World Wide Web è operare e vigilare affinché non vengano offesi e/o violati i diritti dei minori che navigano in Internet servendosi della Tecnologia ChildKey. In particolare, essa provvede a catalogare, archiviare e trattare i reports dei siti visitati dai minori che le vengono periodicamente inviati dagli Internet Service Providers che erogano il servizio ChildKey.

In base a questi dati, la Fondazione invia a tutti i responsabili dei siti visitati dai minori che non abbiano ancora provveduto ad autocertificare i contenuti delle proprie pagine web mediante il metadata ChildKey, una e-mail seguita da raccomandata, in cui li informa della visita di un minore e li invita ad adeguare il loro comportamento ai criteri di responsabilità che tale informazione rende obbligatori.

La Fondazione procede a redigere una Black-List dei siti a rischio (cioè non ancora dotati di metadata ChildKey e risultati, dopo esame diretto, non adatti ai minori) e si impegna ad aggiornarla con continuità.

La Fondazione si impegna a rimuovere dalla lista quei siti che nel frattempo hanno adottato il metadata ChildKey autocertificando correttamente il contenuto delle loro pagine.

La Black-List è trasmessa periodicamente a tutti gli Internet Service Providers che erogano il servizio di protezione ChildKey, i quali possono impiegarla nella procedura di analisi delle pagine web richieste dai minori.

La Fondazione effettua il monitoraggio, cataloga e informa costantemente Providers ed i Motori di Ricerca per controllare se il loro comportamento si sia adeguato a criteri di responsabilità per la tutela dei minori.

Scuole e centri di aggregazione giovanile

La Fondazione propone e diffonde la tecnologia ChildKey per l'uso nelle scuole, biblioteche e altri centri di aggregazione giovanile. KeyStudent, un prodotto della tecnologia ChildKey, è un sistema integrato brevettato, applicato all'interno della rete scolastica, che inibisce la consultazione di pagine internet dai contenuti non idonei, quali: la pornografia, senza la necessità di installare software aggiuntivi sulle postazioni PC. Attraverso un'intuitiva interfaccia web, il supervisore potrà, per ogni studente, determinare dei privilegi di navigazione.

Diffusione in licenza gratuita del software

La Fondazione propone e diffonde il software Snasa ChildKey - senso di presenza del minore - per Providers e Motori di ricerca e diffonde l'autocertificatore metadata ChildKey per tutti i siti che ne facciano richiesta nonchè lo SpiderCk per l'individuazione delle pagine non autocertificate giacenti sui servers dei Prestatori di contenuti.

Rapporto con le Autorità e Lista di Oscuramento

La Fondazione, a fini antipedofilia, consente alle Autorità di ogni singolo Stato che ne facciano richiesta, di inserire direttamente nel proprio data-base i siti a contenuto reatuale. Questi formano la Lista di Oscuramento anche'essa trasmessa periodicamente ai Providers. Il collegamento viene effettuato in procedura protetta (https) e viene rilasciato su richiesta e compatibilmente con le disposizioni legislative vigenti.

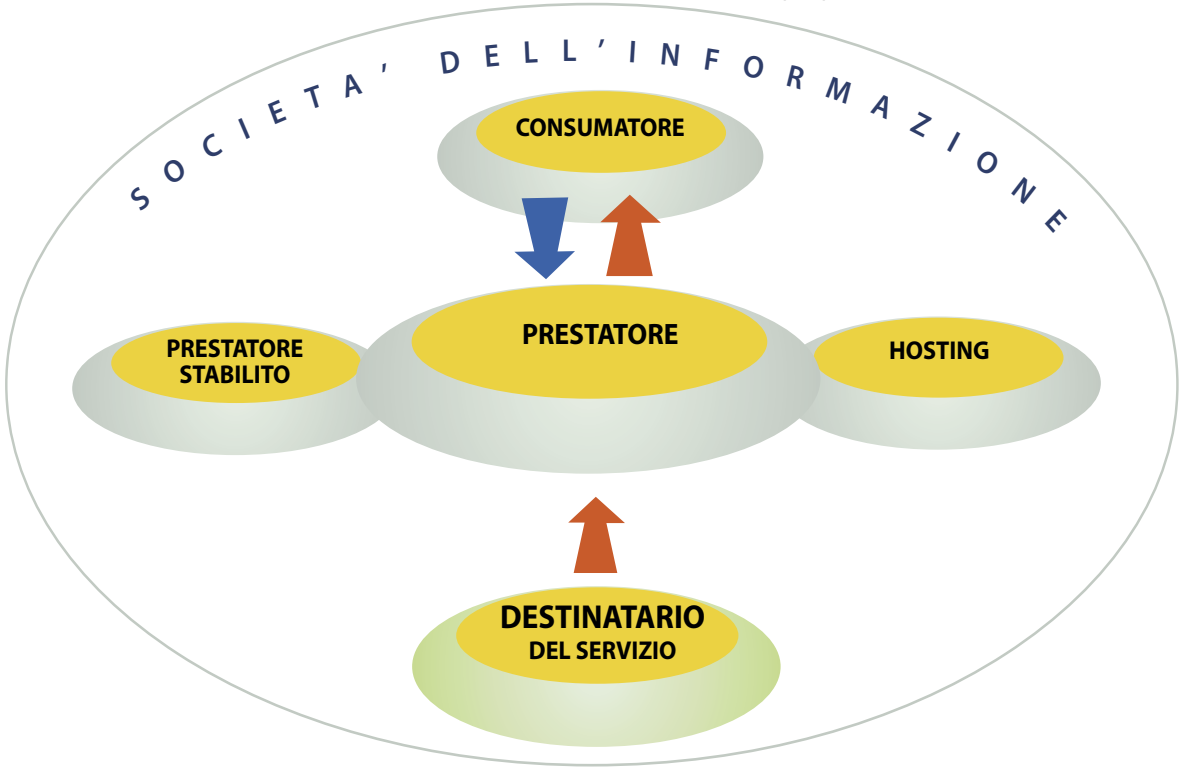
Rapporti con il RIR (RIPE NCC - ARIN - APNIC)

La Fondazione a cura di informare i tre enti che assegnano gli IP per gli utenti finali di Internet con:

- Inoltro al RIR della Lista di Oscuramento con richiesta di oscuramento dell'IP.
  Tale procedura, se accettata, comporterebbe la non visibilità a livello mondiale di tutti quei siti che le Autorità di ogni singolo Stato hanno ritenuto essere reatuali per natura (siti pedo-pornografici e altri) e quindi non visibili né da minori né da adulti.
- Inoltro al RIR della Lista di Incongruenze tra dati del Registrant (proprietario del sito) e l'effettivo proprietario.
  Tale Lista nasce in conseguenza delle "notifiche" effettuate dalla Fondazione ai Registrant o ritenuti tali.
  Si è potuto constatare che i dati di taluni Registrant non corrispondono ai dati effettivi per cui la "notifica" non ha esito positivo.
  Tali incongruenze sono segnalate al RIR.

I SOGGETTI DELLA RETE

La rete vista dalla Direttiva 2000/31/CE dell'8 giugno 2000



Per poter comprendere appieno la responsabilità di ogni singolo soggetto che opera in Internet è opportuno fare riferimento alla distinzione effettuata dalla Normativa Europea con la Direttiva 2000/31/CE.

In tale Direttiva si identificano i seguenti soggetti:

Società dell'informazione:

i servizi ai sensi dell'articolo 1, punto 2, della direttiva 98/34/Ce, come modificata dalla direttiva 98/48/CE;

Prestatore:

la persona fisica o giuridica che presta un servizio della società dell'informazione;

Prestatore stabilito:

il prestatore che esercita effettivamente e a tempo indeterminato un'attività economica mediante un'installazione stabile. La presenza e l'uso dei mezzi tecnici e delle tecnologie necessarie per prestare un servizio non costituiscono di per sé uno stabilimento del prestatore;

Hosting:

prestazione di un servizio della società dell'informazione consistente nella memorizzazione di informazioni fornite da un destinatario del servizio a richiesta di un destinatario del servizio;

Destinatario del servizio:

la persona fisica o giuridica che, a scopi professionali e non, utilizza un servizio della società dell'informazione, in particolare per ricercare o rendere accessibili delle informazioni;

Consumatore:

qualsiasi persona fisica che agisca a fini che non rientrano nella sua attività commerciale, imprenditoriale o professionale.

Con l'avvento della Navigazione Differenziata tale visione della Rete va modificata come nello schema illustrato nella pagina seguente.

Responsabilità penale in Rete

Oggi, grazie alla tecnologia ChildKey ed all'avvento della Navigazione Differenziata, i Prestatori di servizio sono posti in grado di sapere se chi è connesso in quel momento e sta effettuando una richiesta di pagina web sia un minore o un maggiore.

Tale informazione impone ai Prestatori si Servizio ed ai Destinatari di Servizio (Motori di Ricerca, Siti ecc..) di adeguare il loro comportamento ai criteri di responsabilità. Ciò potrà essere fatto utilizzando il metadata ChildKey per i siti o lo Snasa ChildKey (software che rileva la presenza del minore) entrambe licenziati gratuitamente dalla Fondazione Safety World Wide Web Onlus.

Riteniamo che già oggi esistano, grazie a tale informativa, i presupposti di applicabilità del cod.pen. per la violazione degli artt. 40, 528 e 600 ter e quater.

Aspetti legislativi: le responsabilità

La legislazione dell'Unione Europea e di molti altri paesi ha già disciplinato vari reati di tipo informatico per combattere la diffusione su Internet di informazioni illegali, di pornografia (in particolare di quella infantile), di affermazioni razziste e di informazioni che incitano alla violenza. L'autore o i fornitori dei contenuti possono essere chiamati a risponderne in sede penale. Anche i fornitori di servizi sono coinvolti: potendo dimostrare l'accesso illecito di un minore, infatti, si possono configurare gli estremi di un accesso incontrollato e quindi legalmente perseguibile, dal punto di vista penale e/o amministrativo.

Secondo il codice penale italiano, infatti, chi espone in luogo pubblico o aperto al pubblico o acquista, detiene o mette in circolazione scritti, disegni, immagini o altri atti osceni di qualsiasi specie, è perseguibile penalmente (art. 528 c.p.), laddove si considerano osceni gli atti e gli oggetti che, secondo il comune sentimento, offendono il pudore. I reati possono essere commessi anche omissivamente, in altre parole non facendo nulla per evitare che avvenga qualcosa che costituisce reato.

Inoltre, per quanto riguarda lo specifico campo della pornografia infantile, la Decisione emanata il 29 maggio 2000 dal consiglio dell'Unione Europea, prevede che gli Stati membri esaminino le misure appropriate ad

eliminare la pornografia infantile e le misure per sollecitare i fornitori di servizi Internet a :

- ✔ togliere dalla circolazione il materiale di pornografia infantile di cui sono stati informati o di cui sono venuti a conoscenza e che è diffuso attraverso tali servizi
- ✔ conservare i dati relativi a tale traffico
- ✔ predisporre sistemi di controllo per combattere la produzione, il trattamento, il possesso e la diffusione di materiale di pornografia infantile
- ✔ fornire consulenza alle autorità circa il materiale di pornografia infantile di cui sono stati informati o di cui sono venuti a conoscenza e diffuso per loro tramite.

In adesione alla Convenzione sui diritti del fanciullo, il legislatore italiano ha previsto, con apposita modifica del codice penale (Legge 269/98), le norme per la tutela dei fanciulli contro ogni forma di sfruttamento e violenza sessuale a salvaguardia del loro sviluppo fisico, psicologico, spirituale, morale e sociale.

Si vedano altresì gli art. 600 ter e quater per quanto attiene a materiale pedo-pornografico.

LA RETE VISTA OGGI CON LA NAVIGAZIONE DIFFERENZIATA

1. Identificazione Minore/Adulto
2. Richiesta pagine "html"
3. Inserimento Tag Minore
4. Richiesta contenuti certificati
5. Memorizzazione contenuti certificati
6. Ritiro pagine "html"
7. Visualizzazione pagine "html" per tutti
8. Visualizzazione pagine "html" per adulti

CLASSIFICA DELLE RESPONSABILITA'

1 IL DESTINATARIO DEL SERVIZIO

Il Destinatario del servizio è sicuramente il soggetto su cui ricade l'obbligo di classificare e autocertificare i contenuti pubblicati.

La mancata autocertificazione lo rende responsabile di "diffusione di materiale offensivo dei diritti dei minori a minore".

2 IL PRESTATORE DI CONTENUTI

Il Prestatore (di contenuti) è posto in grado di conoscere se la richiesta di pagine html è effettuata da un minore.

Ciò consente di esigere dal Destinatario del Servizio, la classificazione dei contenuti.

Riteniamo possa sussistere in caso contrario la responsabilità prevista dall'art. 40 c.p.

A ciò potrà ovviare se:

1 ***la memorizzazione dei dati da diffondere in Rete avvenga previa identificazione del Destinatario del servizio;***

2 ***saranno previste clausole contrattuali che impongano al Destinatario del servizio la classificazione o autocertificazione dei contenuti con il metadata CHildKey.***

3 IL PRESTATORE DI CONNESSIONE

Il Prestatore (di connessione) non riveste particolari tipi di responsabilità. Riteniamo che comunque abbia il dovere di offrire il servizio di Navigazione differenziata alle famiglie, anche avvalendosi di terze parti (Gestori della Navigazione differenziata).

GIUDICE COMPETENTE

Trattandosi di reato di tipo "evento" il Giudice "naturale" è quello del Paese dove le immagini sono state visualizzate o tentate di visualizzare.

Quindi per quanto attiene all'Italia, sarà competente la Procura Italiana ove la famiglia del minore o il minore risiedono.

AZIONE PENALE

La Fondazione, unitamente alle Associazioni che collaborno, si fa altresì carico di procedere a formulare gli esposti-denuncia a carico di coloro, sia Italiani che esteri, che abbiano attuato comportamenti ritenuti contrari e che violano i diritti dei minori fornendo parimenti tutta la documentazione necessaria alle Autorità.

Per quanto attiene al nostro Paese ci sono ben tre Progetti di Legge specifici per l'adozione della Navigazione Differenziata.

In particolar modo la Proposta di Legge presentata dal deputato On.le Francesca Martini in data 8 ottobre 2002 e dell'On.le Cima in data 30 agosto 2002 n.3122, preso atto che la tecnologia ChildKey è in grado di consentire ai Providers di riconoscere un minore che si è connesso, pone a questi, all'art.1, l'obbligo di dotarsi di mezzi idonei alla protezione dei minori stessi.

La Proposta di Legge prevede all'art. 3, con l'introduzione dell'art. 528 bis del codice penale, pene molto dure per i providers o fornitori di servizi di connessione alla rete che non ottemperino ad disposto dell'art.1.

Vi è poi un Disegno di Legge d'iniziativa della senatrice Alberti Castellati del 12 gennaio 2004 n.2683 ed anche in esso si prende atto dell'opportunità di utilizzare la tecnologia di Navigazione Differenziata CHildKey.

Un grande successo per la Fondazione Safety World Wide Web Onlus ed un enorme passo avanti per la protezione dei minori che navigano in Internet.

AUDIZIONE FONDAZIONE alla COMMISSIONE GIUSTIZIA

DISEGNO DI LEGGE N.4599 13 GENNAIO 2004

PROPOSTA LEGISLATIVA DELLA FONDAZIONE IN COMMISSIONE GIUSTIZIA IL 21 OTTOBRE 2004

Nel corso dell'audizione del 21 ottobre 2004 inerente il Disegno di Legge n. 4599, si è provveduto ad illustrare il funzionamento della tecnologia di Navigazione Differenziata e di come questa sia in grado di far conoscere a tutti i Prestatori di Servizi Hosting (il soggetto indicato all'art. 2 della Direttiva n. 2000/31/CE dell'8 giugno 2000 in Gazzetta Ufficiale n° L 178 del 17/7/2000 che memorizza i dati per renderli disponibili e diffonderli in Internet) se il fruitore di tali contenuti sia un minore.

Il disegno di legge, nella sua attuale formulazione, affronta il problema esclusivo della pedo-pornografia che rappresenta meno dello 0,0001% del materiale osceno disponibile in Internet e di cui possono fruirne i minori senza che ciò, nonostante la nota all'art. 18 del Progetto di Legge Prestigiacomo preveda tale ipotesi, trovi una sua autonoma norma sanzionatoria.

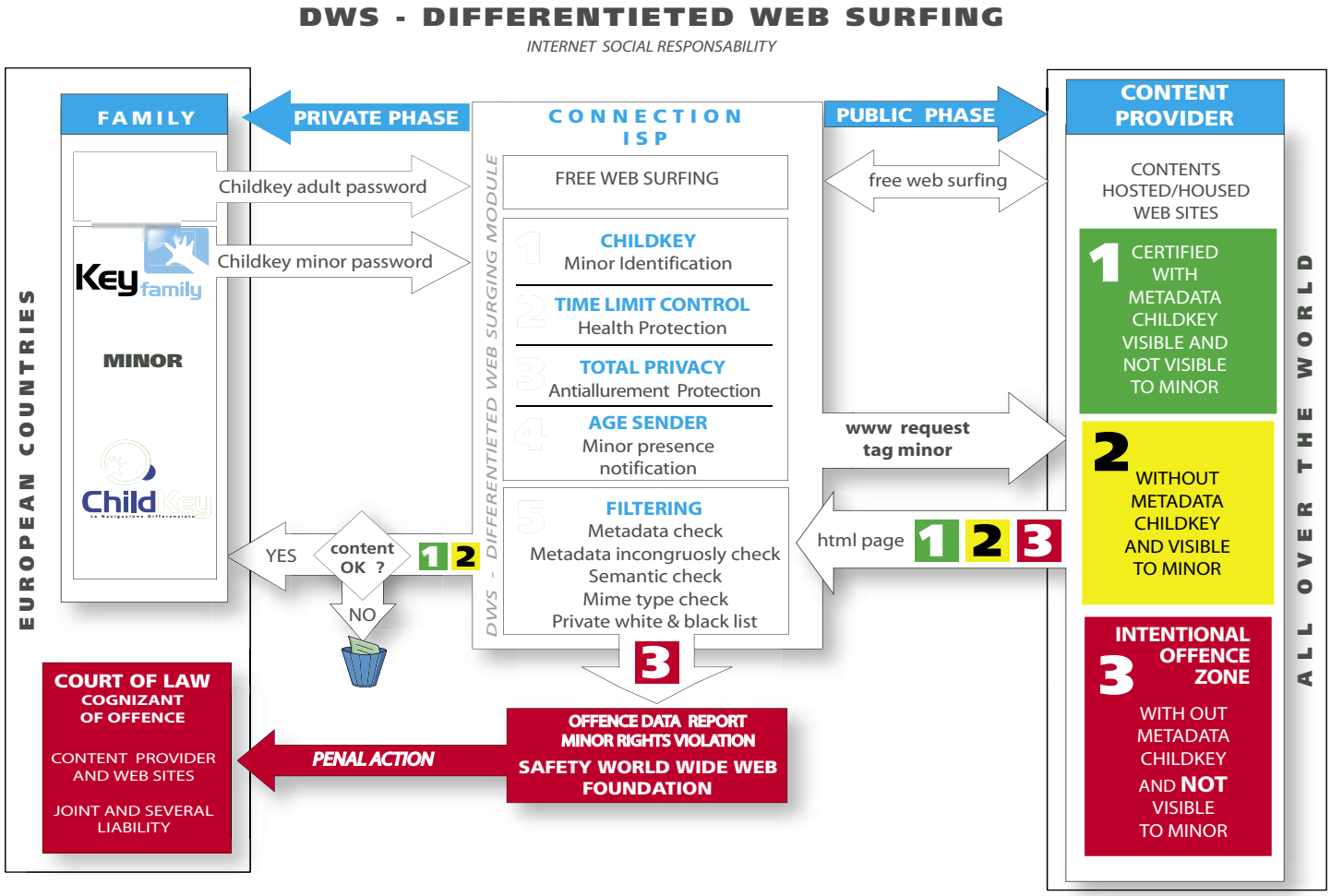
Difatti la nota all'art.18 recita:
"L'articolo 18 introduce nel codice penale il nuovo articolo 528-bis.
Con lo stesso ci si ripropone di **tutelare i minori non solo in quanto soggetti utilizzati per la produzione di materiale pornografico minorile** – obiettivo cui sono consacrati gli articoli sin qui descritti – **ma anche in quanto fruitori di materiale pornografico « adulto », in particolare di quello diffuso a mezzo INTERNET**. Cio`al fine di consentirne, anche da tale prospettiva, un corretto sviluppo psichico."

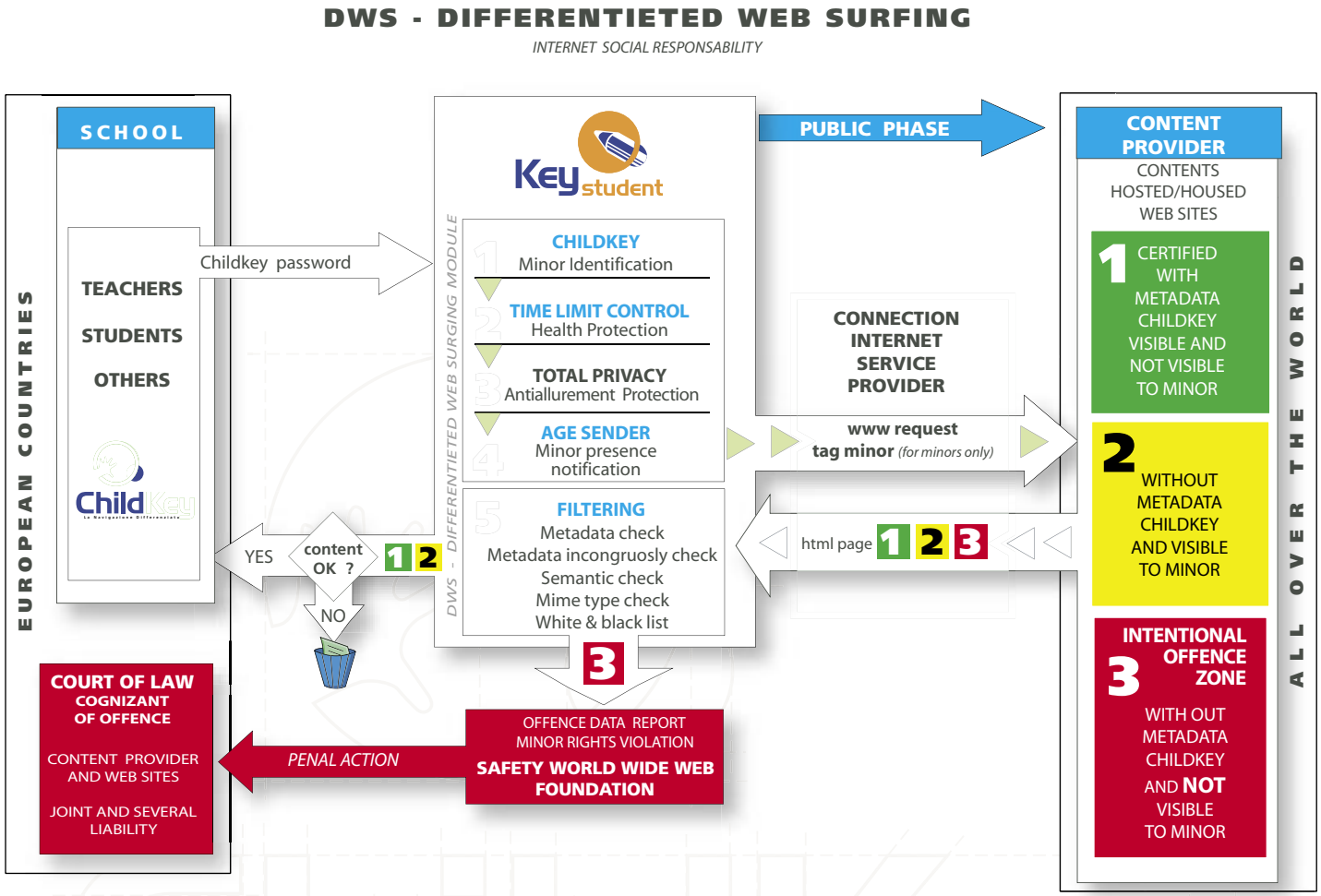
Le tecnologie attuali, così come descritte nella Proposta di Legge Martini n.3235, consentono di far conoscere al Prestatore di Servizi Hosting, se il destinatario dei contenuti richiesti sia un minore.

Ed ecco quindi l'esigenza di introdurre un nuovo articolo 528ter che sanzioni la fattispecie prevista dalla nota all'art.18 del Progetto di Legge sopraripRodotta e definitivamente punisca non solo chi realizza i contenuti ma anche chi ne consente la diffusione.

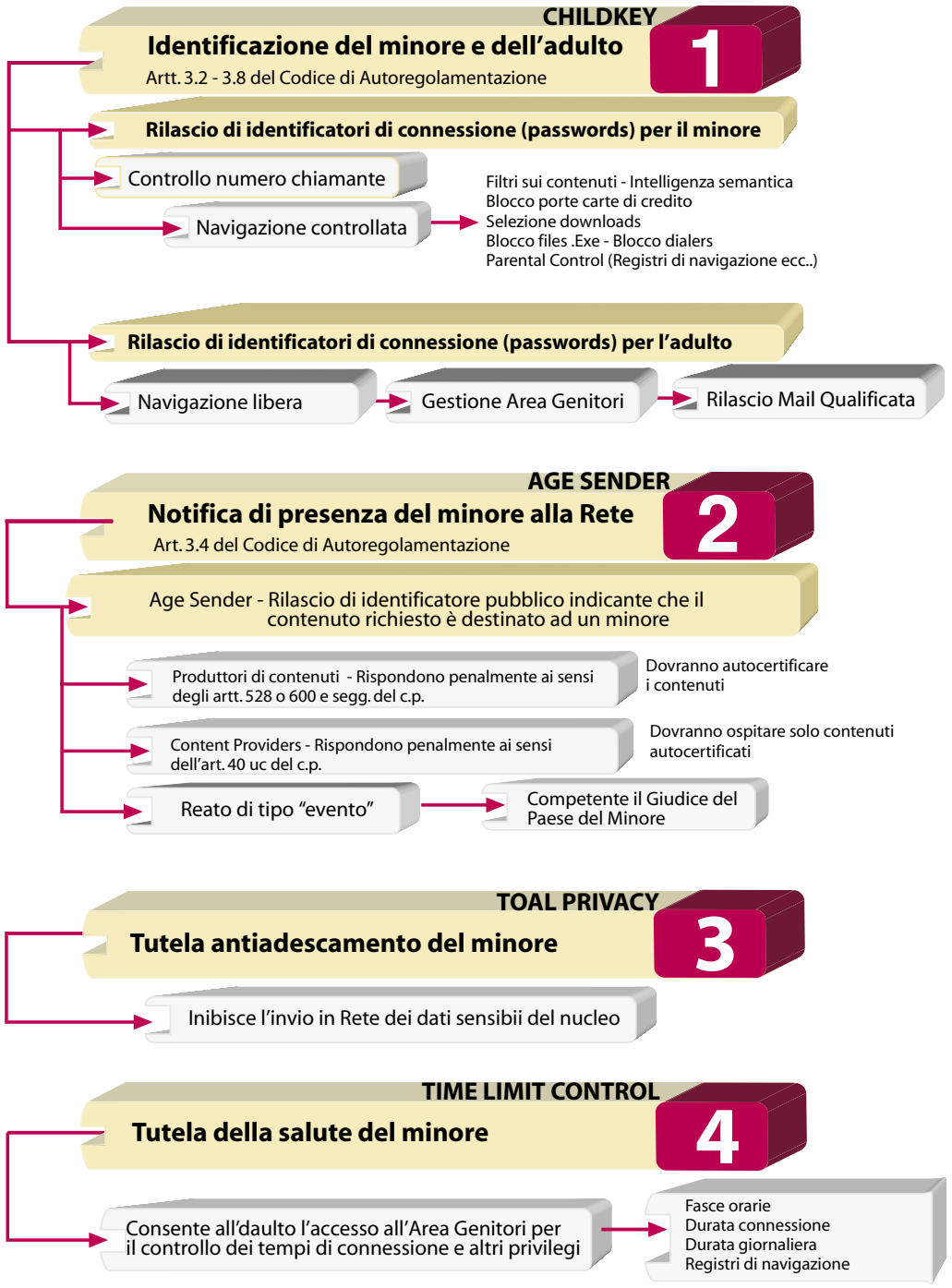
"ART. 528-ter (Inserimento sulla rete internet di scritti, disegni o immagini osceni).
Salvo che il fatto costituisca più grave reato, chiunque inserisce o lascia inserire in un sito Internet scritti, disegni o immagini osceni, senza adottare mezzi tecnici idonei ad impedirne la visione ai navigatori di cui conosca, o sia in grado di conoscere usando la diligenza professionale, l'età inferiore a 18 anni, è punito ai sensi dell'articolo 528. Ai fini dell'applicazione della presente norma, sono equiparati il destinatario ed il prestatore dei servizi della società dell'informazione, come definiti dall'art. 2 della Direttiva n. 2000/31/CE dell'8 giugno 2000."

KeyFamily CONCEPTUAL MAP

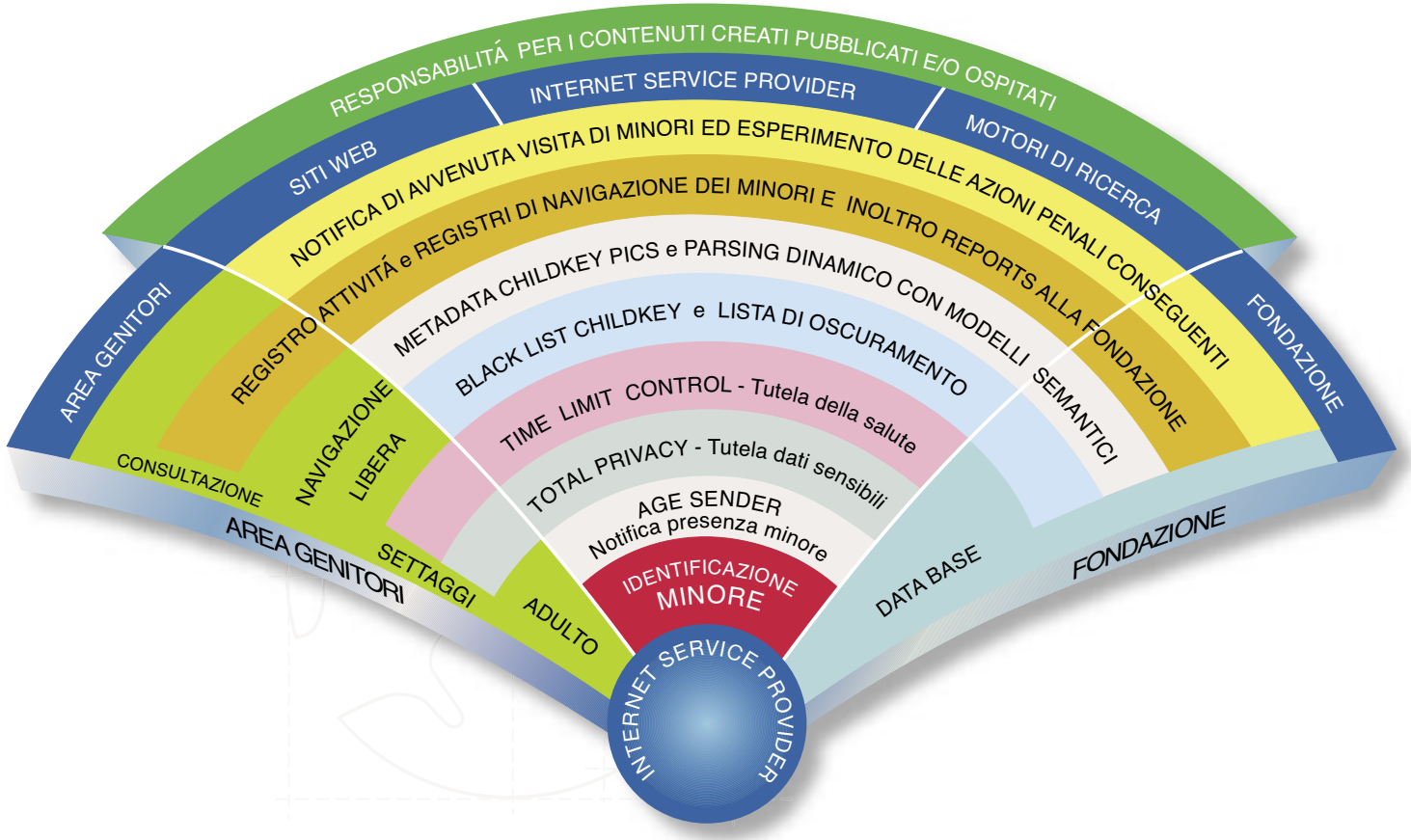


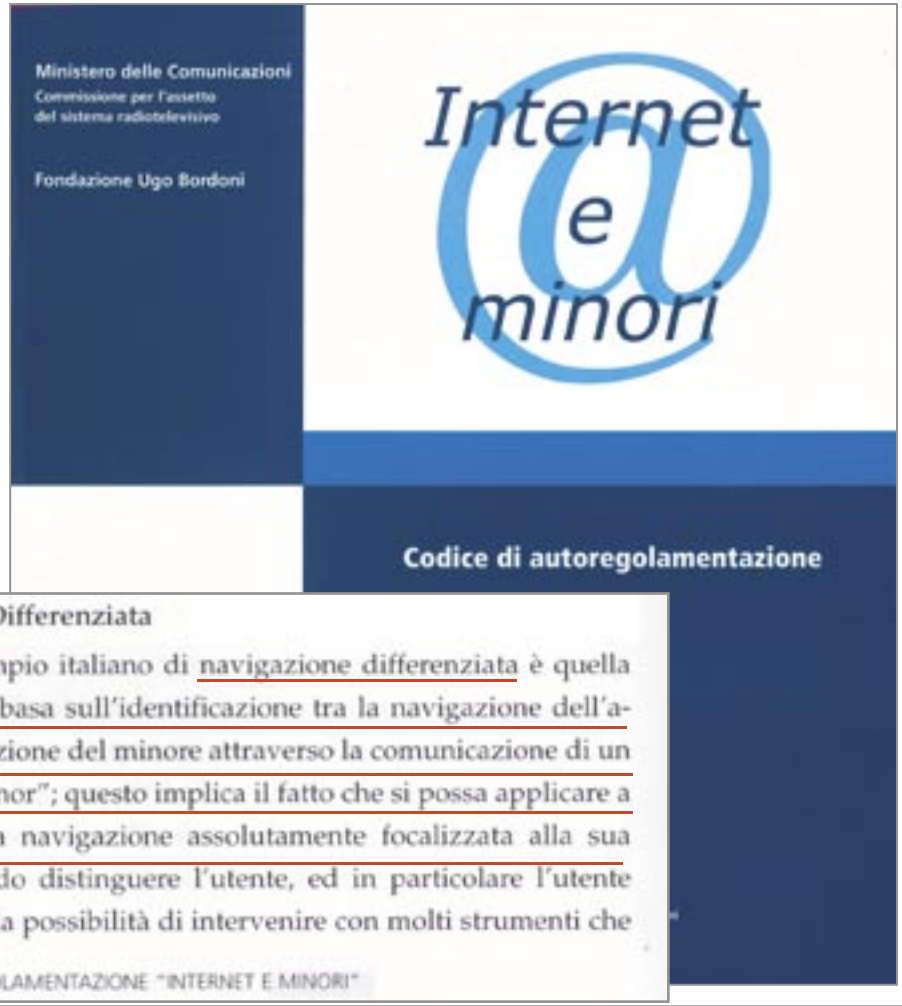

DWS - DIFFERENTIETED WEB SURFING
INTERNET SOCIAL RESPONSABILITY
EUROPEAN COUNTRIES
SCHOOL
TEACHERS
STUDENTS
OTHERS
ChildKey
Childkey password
DWS - DIFFERENTIETED WEB SURGING MODULE
Key student
1 CHILDKEY
Minor Identification
2 TIME LIMIT CONTROL
Health Protection
3 TOTAL PRIVACY
Antiallurement Protection
4 AGE SENDER
Minor presence notification
5 FILTERING
Metadata check
Metadata incongruosly check
Semantic check
Mime type check
White & black list
PUBLIC PHASE
CONNECTION INTERNET SERVICE PROVIDER
www request
tag minor (for minors only)
html page 1 2 3
YES
content OK ?
1 2
NO
3
COURT OF LAW
COGNIZANT OF OFFENCE
CONTENT PROVIDER AND WEB SITES
JOINT AND SEVERAL LIABILITY
PENAL ACTION
OFFENCE DATA REPORT
MINOR RIGHTS VIOLATION
SAFETY WORLD WIDE WEB FOUNDATION
CONTENT PROVIDER
CONTENTS HOSTED/HOUSED WEB SITES
1 CERTIFIED WITH METADATA CHILDKEY VISIBLE AND NOT VISIBLE TO MINOR
2 WITHOUT METADATA CHILDKEY AND VISIBLE TO MINOR
3 INTENTIONAL OFFENCE ZONE
WITH OUT METADATA CHILDKEY AND NOT VISIBLE TO MINOR
ALL OVER THE WORLD

POSTULATI DELLA NAVIGAZIONE DIFFERENZIATA



MAPPA CONCETTUALE DELLA NAVIGAZIONE DIFFERENZIATA





❑ Navigazione Differenziata

Un altro esempio italiano di navigazione differenziata è quella ChildKey che si basa sull'identificazione tra la navigazione dell'adulto e la navigazione del minore attraverso la comunicazione di un codice "age = minor"; questo implica il fatto che si possa applicare a quest'ultimo una navigazione assolutamente focalizzata alla sua sicurezza. Potendo distinguere l'utente, ed in particolare l'utente minore, l'ISP ha la possibilità di intervenire con molti strumenti che

88 CODICE DI AUTOREGOLAMENTAZIONE "INTERNET E MINORI"

consentono al minore di navigare in tutta sicurezza ed al genitore di poter intervenire sulla navigazione.Accompagnando il minore durante la navigazione è possibile attivare moduli di sicurezza e di controllo che non consentono ad "agenti esterni" di infiltrarsi nella Rete e disturbare la navigazione del minore.

La navigazione differenziata fornita dalla tecnologia ChildKey è l'unica al mondo che consente di avvisare i siti visitati della presenza del minore.

89 SOTTOGRUPPO "TECNICO-INFORMATICO"

Codice di Autoregolamentazione Internet@ Minori

Premessa

Considerato che:

a) la presenza dei contenuti illeciti o nocivi per i minori che accedono alla rete telematica è divenuta sempre più pervasiva;

b) il diritto del minore a uno sviluppo equilibrato è riconosciuto dall'ordinamento giuridico nazionale e internazionale (basta ricordare gli articoli della Costituzione che riguardano, direttamente o indirettamente l'infanzia e la gioventù e la Convenzione Internazionale sui Diritti del Fanciullo, adottata a New York dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989, e ratificata ai sensi della legge 27 maggio 1991, n. 176, che impone a tutti i soggetti pubblici e privati, così come alle famiglie, di collaborare per predisporre le condizioni perché i minori possano vivere una vita autonoma nella società, nello spirito di pace, dignità, tolleranza, libertà, eguaglianza, solidarietà, e che fa divieto di sottoporlo a interferenze arbitrarie o illegali nella sua privacy e comunque a forme di violenza, abuso mentale, sfruttamento);

c) la funzione educativa, che compete innanzitutto alla famiglia, può essere agevolata da un corretto utilizzo delle risorse presenti sulla rete telematica al fine di aiutare i minori a conoscere progressivamente la vita e ad affrontarne i problemi ed i pericoli;

d) il minore è un cittadino soggetto di diritti e deve essere protetto da contenuti illeciti o dannosi che possano nuocere alla sua integrità psichica e morale;

e) sussiste l'esigenza di bilanciare i diversi diritti fondamentali eventualmente contrapposti: la tutela dei minori, il diritto all'informazione e la libertà di espressione dei minori e di tutti gli altri individui;

f) appare necessario provvedere alla tutela generalizzata del minore nell'ambito dell'uso sicuro delle tecnologie della società dell'informazione e delle comunicazioni elettroniche.

Tutto ciò premesso e considerato, appare opportuno attuare uno scrupoloso rispetto della normativa nazionale ed internazionale vigente a tutela dei minori, ma anche l'adozione di un Codice di autoregolamentazione in materia (nel seguito indicato anche come "il Codice").

Finalità

Fermo restando il rispetto delle norme vigenti a tutela dei minori, il Codice si pone dunque i seguenti obiettivi e finalità:

a) aiutare gli adulti, i minori e le famiglie a un uso corretto e consapevole della rete telematica, tenendo conto delle esigenze del minore;

b) predisporre apposite tutele atte a prevenire il pericolo che il minore venga in contatto con contenuti illeciti o dannosi per la sua crescita;

c) offrire, nel rispetto della normativa nazionale ed internazionale, un accesso paritario e promuovere un accesso sicuro per il minore alle risorse di rete;

d) tutelare il diritto del minore alla riservatezza ed al corretto trattamento dei propri dati personali;

e) assicurare, nel rispetto dell'ordinamento vigente, una collaborazione piena alle autorità competenti nella prevenzione, nel contrasto e nella repressione della criminalità informatica ed in particolare nella lotta contro lo sfruttamento della prostituzione, la pornografia ed il turismo sessuale in danno di minori, attuati tramite l'utilizzo della rete telematica;

f) agevolare, nel rispetto dell'art. 9 del Decreto legislativo 9 aprila 2003 n.70 - Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, la tutela del minore nei confronti delle informazioni commerciali non sollecitate o che sfruttino la debolezza del minore, ovvero secondo quanto previsto all'art. 130 del Decreto legislativo 30 giugno 2003, n. 196, nei confronti delle comunicazioni indesiderate;

g) diffondere presso gli operatori e le famiglie il contenuto del Codice di autoregolamentazione.

VISTE E CONSIDERATE ALTRESI' LE NORME NAZIONALI ED INTERNAZIONALI DI RIFERIMENTO E CIOE':

VISTI gli articoli 2, 3, 21, sesto comma, 31, secondo comma e 32 della Costituzione;

CONSIDERATA la Convenzione Internazionale sui Diritti del Fanciullo, adottata a New York dall'Assemblea Generale delle Nazioni Unite il 20 novembre 1989 e ratificata ai sensi della legge 27 maggio 1991, n. 176, ed in particolare la lettera e) dell'art. 17 che testualmente prevede che gli Stati "favoriscono l'elaborazione di principi direttivi appropriati destinati a proteggere il fanciullo dalle informazioni e dai materiali che nuocciono al suo benessere in considerazione delle disposizioni degli articoli 13 e 18" e che tale obbligo deve essere realizzato tutelando la libertà di espressione del minore (articolo 13) e l'obbligo degli Stati di garantire ai genitori di poter svolgere congiuntamente il loro diritto/dovere di proteggere e educare i figli (articolo 18);

CONSIDERATA la Convenzione europea sull'esercizio dei diritti dei bambini, adottata a Strasburgo il 25 gennaio 1996 e ratificata ai sensi della legge 20 marzo 2003, n. 77;

VISTA la Legge 28 agosto 1997, n. 285 "Disposizioni per la promozione di diritti e di opportunità per l'infanzia e l'adolescenza";

CONSIDERATA la Direttiva 2002/58/CEE 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;

VISTO il decreto legislativo 30 giugno 2003, n 196 "Codice in materia di protezione dei dati personali", in particolare l'art. 50, dal titolo "Notizie o immagini relative ai minori" e l'art. 130, dal titolo "Comunicazioni indesiderate";

VISTO il Decreto legislativo 15 gennaio 1992, n. 50 - Attuazione della direttiva n. 85/577/CEE in materia di contratti negoziati fuori dei locali commerciali;

VISTO il Decreto legislativo 22 maggio 1999, n 185- Attuazione della direttiva 97/7/CE relativa alla protezione dei consumatori in materia di contratti a distanza;

VISTO il Decreto legislativo 9 aprile 2003, n.70 - Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno, in particolare gli Articoli:

- Art. 9 (Comunicazione commerciale non sollecitata);
- Art. 14 (Responsabilità nell'attività di semplice trasporto - Mere conduit);
- Art. 15 (Responsabilità nell'attività di memorizzazione temporanea - caching);
- Art. 16 (Responsabilità nell'attività di memorizzazione di informazioni - hosting);
- Art. 17 (Assenza dell'obbligo generale di sorveglianza);
- Art. 18 (Codici di condotta);

CONSIDERATO il Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione COM (96) 483;

CONSIDERATA la Comunicazione della Commissione delle Comunità europee del 16 ottobre 1996, relativa alle informazioni di contenuto illegale e nocivo su Internet;

VISTA l'adozione da parte della Commissione il 25 gennaio 1999 della decisione n. 276/1999/CE sul piano d'azione comunitario pluriennale per promuovere l'uso sicuro di Internet attraverso la lotta alle informazioni di contenuto illegale e nocivo diffuse attraverso le reti globali. Ed in particolare le linee d'azione indicate dalla Commissione:

1. creare un ambiente più sicuro;
2. creare una rete europea di hot-line che consenta ai consumatori di denunciare eventuali sospetti di pornografia infantile;
3. incoraggiare l'autoregolamentazione e i codici di condotta;
4. elaborare sistemi di filtraggio e di codificazione;
5. dimostrare i benefici dei sistemi di filtraggio, quali ad esempio PICS (Platform for Internet Content Selection), e di codificazione su base volontaria, quali ad esempio ICRA (Internet Content Rating Association);
6. facilitare l'intesa a livello internazionale sui sistemi di codificazione;
7. Incoraggiare le azioni di sensibilizzazione;
8. preparare il terreno alle azioni di sensibilizzazione;
9. incoraggiare la realizzazione di azioni di sensibilizzazione su vasta scala;
10. realizzare azioni di sostegno;
11. valutarne le implicazioni giuridiche;
12. coordinarne l'attuazione con iniziative internazionali analoghe;
13. valutarne l'impatto con le misure comunitarie;

VISTA altresì la decisione n. 1151/2003/CE del Parlamento europeo e del Consiglio, del 16 giugno 2003, che modifica la decisione precedente n. 276/1999/CE e che in particolare adotta un nuovo Piano pluriennale d'azione comunitario per promuovere l'uso sicuro di Internet estendendone la durata a 6 anni, fino al 31 dicembre 2004;

CONSIDERATA la Raccomandazione del Consiglio della UE riguardante la protezione dei minori e della dignità umana (2001/C 213/03);

VISTO il Parere del Comitato economico e sociale dell'Unione Europea sul "Programma di protezione dei minori su Internet" del 28 novembre 2001;

VISTA la Direttiva del Presidente del Consiglio dei Ministri - Dipartimento per l'Innovazione e le Tecnologie sulla sicurezza nelle P.A. del 16 gennaio 2002 "Sicurezza Informatica e delle Telecomunicazioni nelle Pubbliche Amministrazioni Statali";

VISTO il Decreto Interministeriale 24 luglio 2002 relativo alla istituzione del Comitato tecnico nazionale sulla sicurezza informatica e delle telecomunicazioni nelle pubbliche amministrazioni;

VISTA la legge 3 agosto 1998, n. 269 " Norme contro lo sfruttamento della prostituzione, della pornografia, del turismo sessuale in danno di minori, quali nuove forme di riduzione in schiavitù; In particolare, il terzo comma dell'art. 600-ter Codice penale;

VISTA la Convenzione del Consiglio D'Europa sulla Cyber-criminalità, aperta alla sottoscrizione a Budapest il 23 novembre 2001;

VISTO il Decreto Legislativo n. 259 del 1 agosto 2003 recante il "Codice delle comunicazioni elettroniche";

1 Definizioni

1.1 Aderente
Il soggetto che svolge attività imprenditoriale su Internet, anche a titolo non direttamente oneroso per Clienti ed Utenti, e che aderisce al Codice direttamente o per il tramite delle Associazioni firmatarie.

1.2 Cliente
Il soggetto giuridico che stipula un contratto con l'Aderente.

1.3 Utente
Il soggetto, anche diverso dal Cliente, che utilizza i servizi forniti dall'Aderente.

1.4 Access provider
Il soggetto che offre al pubblico e nell'ambito della propria attività imprenditoriale servizi di accesso ad Internet.

1.5 Hosting/housing provider
Il soggetto che offre al pubblico spazi raggiungibili dall'esterno (shared/dedicated hosting provider) o la possibilità di collegare computer di proprietà del Cliente alla rete Internet (housing provider).

1.6 Content provider
Il soggetto che, direttamente o indirettamente, mette a disposizione del pubblico, con qualsiasi mezzo o protocollo tecnico, dati, informazioni e programmi.

1.7 Gestore dell'Internet Point
Il soggetto che mette a disposizione del pubblico locali e strumenti, non ad uso esclusivo, che consentono l'accesso ai servizi della rete Internet.

1.8 Servizi di navigazione differenziata
Servizi di accesso ad Internet che, sulla base di criteri indicati dall'Aderente ai sensi del successivo art. 3.2, circoscrivono o escludono l'accesso a determinati contenuti.

1.9 Accesso Condizionato
Modalità di accesso a contenuti, altrimenti non disponibili all'Utente, mediante procedure e/o strumenti di tipo logico o fisico (ad es. codice identificativo di utente, password, smart card, ecc.).

1.10 Marchio "Internet@minori"
Logotipo che testimonia l'adesione al Codice del soggetto che svolge attività imprenditoriale su Internet e ne attesta la conformità dei comportamenti agli impegni assunti.

2 Ambito e modalità di applicazione

2.1 Adesione
Il Codice, promosso dalla Associazioni firmatarie, si applica a tutti gli Aderenti che lo sottoscrivono direttamente o attraverso le Associazioni medesime.
L'Aderente potrà pubblicare, sui propri servizi e nelle comunicazioni commerciali, la dicitura "Aderente al Codice di autoregolamentazione Internet@minori" oltre al relativo logo che viene concesso in licenza d'uso gratuito e a tempo indeterminato fino all'eventuale revoca, secondo quanto disposto all'art. 6.

2.2 Obblighi conseguenti all'adesione
L'adesione volontaria al presente Codice di autoregolamentazione implica inderogabilmente:
– l'accettazione integrale dei contenuti del Codice stesso e in particolare l'accettazione delle attività di vigilanza e delle sanzioni ivi previste;
– l'adattamento delle condizioni contrattuali di prestazione dei servizi alle disposizioni del presente Codice.

2.3 Recesso
L'adesione al Codice ed ai suoi aggiornamenti periodici è a tempo indeterminato. L'eventuale recesso dell'Aderente dovrà essere comunicato secondo le modalità fissate dal Regolamento di Organizzazione di cui al successivo punto 6.2.

3 Strumenti per la tutela del minore

3.1 Informazione alle Famiglie e agli Educatori
L'Aderente pubblica nella pagina Internet iniziale (home page) dei propri servizi un riferimento "TUTELA DEI MINORI", chiaramente visibile, che rimanda ad apposite pagine web con le quali fornire informazioni sulle corrette modalità per un utilizzo sicuro della rete Internet, sull'esistenza degli strumenti più utilizzati per la tutela dei minori e sulle modalità di segnalazione al Comitato di Garanzia di cui all'art. 6 delle violazioni del Codice. Il contenuto minimo delle pagine web verrà definito dal Comitato di Garanzia.

3.2 Servizi di *navigazione differenziata*
L'Aderente offrirà, secondo le tecnologie disponibili, alle Famiglie, agli Educatori, alle Scuole, alle Biblioteche e alle Aggregazioni giovanili Servizi di navigazione differenziata che dovranno essere chiaramente identificati come tali, ovvero indirizzerà il Cliente e gli Utenti verso altri fornitori di Servizi di navigazione differenziata. Nel rispetto del principio di non discriminazione, tali servizi non potranno impedire l'accesso ai contenuti sicuri offerti dai Content provider aderenti.

3.3 Classificazione dei contenuti
Il Content Provider aderente potrà applicare i sistemi di classificazione ai contenuti che riterrà opportuno subordinare ad Accesso condizionato.

3.4 *Identificatori d'età*
L'Aderente potrà utilizzare Sistemi di individuazione dell'età dell'Utente, a condizione che, nel rispetto delle norme sul trattamento dei dati personali, ne venga tutelata e garantita la massima riservatezza, sicurezza e dignità.
In particolare, tali sistemi non dovranno consentire di risalire all'identità, al domicilio, all'indirizzo di posta elettronica, all'eventuale pseudonimo ("alias" o "nick name"), all'indirizzo Internet (numero IP) del minore e non dovranno comunque permettere a terzi di raggiungerlo direttamente o indirettamente.

3.5 Profilazione e trattamenti occulti
Nel rispetto del Codice in materia di protezione dei dati personali (decreto legislativo 30 giugno 2003, n. 196), l'Aderente non esegue alcuna profilazione dell'Utente minore né alcun trattamento dei suoi dati personali senza la previa autorizzazione espressa, a seguito di informativa chiara e trasparente sulla tipologia delle profilazioni che l'Aderente medesimo intende effettuare e sull'uso che di tali informazioni intende fare, da parte di chi esercita la potestà genitoriale.

3.6 Custodia di password

L'Aderente custodisce le password di accesso ai servizi assegnate agli Utenti con adeguate misure di sicurezza. L'Aderente si impegna a fornire all'Utente la possibilità di cambiare la password.

3.7 Anonimato protetto

L'Aderente potrà consentire agli Utenti di utilizzare i propri servizi in modo da apparire totalmente anonimi.
In ogni caso, l'Aderente dovrà essere effettivamente informato della reale identità personale del soggetto cui viene concesso di fruire dell'anonimizzazione. All'interno dell'informazione di cui all'art. 3.1 l'Aderente dovrà altresì avvertire preventivamente gli Utenti della possibilità che elaborazioni non autorizzate, effettuate abusivamente da terze parti all'insaputa dell'Aderente, possano comunque consentire di risalire alla loro identità.

3.8 Identificazione dell'Utente

L'Aderente eroga i propri servizi solo ed esclusivamente a Utenti identificati direttamente o identificabili tramite elementi univoci anche se indiretti.

3.9 Prestazione di servizi fiduciari

L'Aderente che offre servizi in via fiduciaria (ad esempio registrazione di un nome a dominio per conto di un Cliente che vuole rimanere ignoto) è obbligato a identificare in modo certo il Cliente che richiede tali servizi, serbando la massima riservatezza.

3.10 Gestione dei dati utili alla tutela dei minori

3.10.1 Individuazione dei dati

L'accesso alla rete Internet richiede l'assegnazione permanente o temporanea all'Utente di un indirizzo di rete (indirizzo IP). Nei limiti imposti dalla normativa vigente, l'Aderente conserva, come dati utili:

a) i registri di assegnazione degli indirizzi IP;
b) il numero IP utilizzato per l'accesso alle eventuali funzioni di pubblicazione dei contenuti.

Nel caso di assegnazione temporanea dell'indirizzo IP, il relativo registro conterrà: data e ora di inizio e cessazione dell'assegnazione, numero di IP assegnato temporaneamente ed eventuale numero telefonico utilizzato (se disponibile).

3.10.2 Modalità e tempi di conservazione dei dati

L'Aderente conserva i dati di cui al punto 3.10.1 con modalità che ne garantiscano una ragionevole attendibilità e non ripudiabilità, comunque nel rispetto delle disposizioni vigenti in materia.
I dati medesimi vengono custoditi per sei mesi, salva la scelta individuale di conservarli per periodi maggiori, senza comunque eccedere i limiti temporali indicati dalla normativa vigente.

3.10.3 Modalità di comunicazione dei dati

3.10.3.1 All'Autorità giudiziaria

L'Aderente, eseguirà quanto richiesto nel provvedimento dell'Autorità giudiziaria documentando per iscritto le operazioni compiute.

3.10.3.2 Al Cliente

Secondo quanto previsto dalle norme sul trattamento dei dati personali (D.lgs. 196/2003), l'Aderente fornirà al Cliente solo ed esclusivamente le informazioni che lo riguardano e comunque a fronte di richiesta scritta e identificazione certa del richiedente.

3.11 Contrasto alla pedopornografia on-line

L'Aderente, nel rispetto delle normative vigenti in materia di trattamento dei dati personali, si impegna a conservare il numero IP utilizzato dall'Utente per l'accesso alle funzioni di pubblicazione dei contenuti, anche se ospitati gratuitamente.
L'Aderente pone in essere tutte le iniziative atte a realizzare la collaborazione con le autorità competenti, e in particolare con il Servizio della Polizia Postale e delle Comunicazioni, al fine di rendere identificabili gli assegnatari delle risorse di rete utilizzate per la pubblicazione dei contenuti ospitati presso i propri server, così come risultanti dai relativi contratti o documenti equipollenti, entro e non oltre le tre giorni lavorativi successivi al ricevimento del provvedimento dell'autorità richiedente.

4 Responsabilità

4.1 Access Provider

L'Aderente che offre servizi di accesso ad Internet dovrà verificare direttamente (p.e. tramite l'avvenuta sottoscrizione di un contratto) o indirettamente (almeno tramite CLI-Calling Line Identifier o metodi analoghi) l'accesso alla rete.
Nei contratti di accesso ad Internet l'Aderente inserisce clausole che responsabilizzano il Cliente anche per l'uso dei servizi concessi a terzi.

4.2 Housing/hosting provider

L'Aderente che offre servizi di housing e hosting dedicato dovrà identificare con ragionevole certezza il proprio Cliente che ha il controllo degli apparati oggetto di tali servizi. Nel caso di servizi di hosting condiviso l'Aderente è tenuto a conservare i dati di cui al punto b) dell'art. 3.10

4.3 Content Provider

L'Aderente che offre direttamente contenuti tramite qualsiasi metodo o protocollo di comunicazione, è tenuto a identificare in modo chiaro, ricorrendo eventualmente alle metodologie indicate all'art. 3.3, la natura e i contenuti della comunicazione stessa, adoperandosi per adeguare o rimuovere il contenuto su segnalazione del Comitato di Garanzia, e comunque delle Autorità Competenti.

4.4 Gestore dell'Internet Point

L'Aderente che offre servizi di accesso al pubblico come "Internet Point" o simili deve fornire strumenti adeguati per la navigazione dei minori ed identificare, direttamente o indirettamente, l'utilizzatore dei servizi medesimi.

5 La vigilanza sulla corretta applicazione del Codice è affidata al Comitato di cui al successivo art. 6.
In un'ottica di armonizzazione e di verifica degli sviluppi tecnologici e normativi il Comitato di Garanzia suggerisce eventuali aggiornamenti e modifiche del presente Codice.

6.1 Costituzione

La corretta, imparziale e trasparente applicazione del Codice è affidata ad un apposito Comitato di Garanzia (in seguito indicato anche come il "Comitato") costituito da undici componenti effettivi, esperti in materia, nominati con Decreto del Ministro delle Comunicazioni ed individuati come segue:

– quattro componenti in rappresentanza degli Aderenti designati dalle Associazioni di categoria firmatarie del presente Codice;
– quattro componenti in rappresentanza del Ministero delle Comunicazioni e della Presidenza del Consiglio dei Ministri Dipartimento dell'Innovazione e delle Tecnologie;
– tre componenti scelti dal Ministro delle comunicazioni in rappresentanza delle Associazioni per la tutela dei minori e del Consiglio Nazionale degli Utenti. In sede di prima nomina tali ultimi componenti saranno scelti tra i partecipanti al Gruppo di lavoro Internet@Minori istituito al Ministero delle Comunicazioni.

Con il medesimo Decreto del Ministro delle Comunicazioni viene altresì designato il Presidente del Comitato, scelto tra i componenti effettivi.
Il Ministero delle comunicazioni assicura la Segreteria per le attività di supporto al Comitato.
Con i medesimi criteri e modalità sono nominati anche undici componenti supplenti.
I componenti ed il Presidente nominati durano in carica tre anni.

6.2 Funzionamento

Le regole di funzionamento del Comitato e della Segreteria sono definite da un apposito Regolamento di Organizzazione adottato di comune accordo dai componenti del Comitato medesimo entro 30 giorni dal suo insediamento.
Nel medesimo Regolamento verranno indicate le modalità di realizzazione dell'apposito sito web dedicato al Codice.

6.3 Poteri

Il Comitato controlla che l'Aderente possieda tutti i requisiti e abbia assunto tutti i comportamenti previsti dal Codice, segnalando agli interessati eventuali inottemperanze al Codice medesimo.
Nel caso di accertate inottemperanze da parte degli Aderenti si applicheranno le sanzioni di cui al successivo art. 7.

6.4 Tempi di attuazione del Codice

Il Comitato di Garanzia individuerà i tempi per rendere effettivi gli obblighi di cui al presente Codice, che comunque entreranno in vigore entro e non oltre i sei mesi successivi alla firma dello stesso.

6.5 Decadenza dei componenti

Il Comitato di Garanzia definisce nel Regolamento di Organizzazione le ragioni che determinano la decadenza dei componenti del Comitato.

6.6 Rimborsi

Le Associazioni firmatarie del presente Codice si impegnano a segnalare, entro i trenta giorni successivi all'approvazione del presente Codice, l'Associazione , tra quelle firmatarie, che garantirà il rimborso delle spese sostenute, e documentate, dai rappresentanti delle Associazioni per la tutela dei minori per la loro partecipazione alle sedute del Comitato di Garanzia, secondo le modalità che saranno stabilite dal Regolamento di organizzazione del Comitato medesimo. Tali spese saranno suddivise tra tutte le Associazioni firmatarie. Il limite massimo annuo complessivo di tali spese è fissato in 8.000 Euro. Saranno ricercate altre forme di finanziamento e sostegno anche da parte di Enti istituzionali per l'eventuale svolgimento di attività di studio, promozione, ricerca e comunicazione anche in relazione alla campagna d'informazione che sarà auspicabilmente effettuata sul tema della tutela dei minori in rete.

7.1 Procedura per l'irrogazione dei provvedimenti disciplinari

7.1.1 Attivazione del procedimento

Chiunque ritenga fondatamente che sia intervenuta da parte dell'Aderente una violazione degli obblighi definiti all'art. 3, può segnalare al Comitato di Garanzia tale violazione inviando una comunicazione alla Segreteria del Comitato medesimo secondo le indicazioni dell'art. 3.1.
Per attivare la segnalazione dovrà essere compilato l'apposito modulo guidato, contenuto nelle pagine web informative, indicando:

– le sue generalità;
– i suoi recapiti (Indirizzo completo e numero di telefono, nonché, eventualmente, numero di fax ed e-mail);
– descrizione dettagliata della violazione della norma del Codice e degli elementi di responsabilità dell'Aderente riscontrati;

All'invio della segnalazione "telematica" di cui sopra, verrà attribuito un Numero di Protocollo che l'interessato dovrà indicare nella lettera di conferma (contenete gli stessi elementi informativi) da inviare per posta, tramite Raccomandata A.R., alla Segreteria del Comitato Tale segnalazione "telematica
La Segreteria procede ad una classificazione e registrazione delle segnalazioni ricevute ed accompagnate dalla relativa conferma postale.
I dati trasmessi verranno trattati secondo le norme sulla tutela dei dati personali.

7.1.2 Comunicazione di apertura del procedimento

La Segreteria, esaminate le segnalazioni pervenute, entro una settimana dal ricevimento della lettera raccomandata di conferma comunica all'Aderente l'apertura del procedimento di autodisciplina nei suoi confronti e le contestazioni oggetto della segnalazione. Vengono considerate inammissibili le segnalazioni prive dei requisiti di cui al punto 7.1.1.

7.1.3 Richiesta di documentazione

L'Aderente che riceve una comunicazione di apertura di un procedimento di autodisciplina nei suoi confronti, può trasmettere alla Segreteria, entro quindici giorni dalla comunicazione, la documentazione che ritiene utile per chiarire la sua posizione.

7.1.4 Audizione dell'Aderente

L'Aderente al quale sia stata comunicata l'apertura di un procedimento di autodisciplina, può richiedere un'audizione al Comitato negli stessi tempi previsti per l'invio di documentazione. L'audizione sarà effettuata in occasione della prima riunione del Comitato, che informerà l'interessato con un preavviso non inferiore a dieci giorni.

7.1.5 Decisione

Il Comitato opera, di norma, per via telematica e la Segreteria predispone i verbali delle attività che vengono sottoposti all'approvazione dei singoli componenti. Il Comitato completa l'iter procedurale entro sessanta giorni dall'apertura del procedimento di autodisciplina. Le decisioni finali vengono prese a maggioranza dei due terzi (con approssimazione all'unità superiore). Le audizioni si svolgono nell'ambito di riunioni del Comitato valide, ai fini delle decisioni, solo se alla presenza di almeno i due terzi del numero dei componenti.
Gli esiti delle procedure di autodisciplina rimangono agli atti del Comitato e vengono conservati a cura della Segreteria che li trasmette alle parti interessate e ne cura la pubblicazione sull'apposito sito web previsto dal Regolamento di Organizzazione.

7.1.6 Esecuzione della decisione

L'Aderente dà seguito a quanto deciso dal Comitato tempestivamente e comunque non oltre i quindici giorni successivi alla comunicazione del provvedimento adottato. La mancata esecuzione di quanto previsto nella decisione comporta, a seguito della procedura prevista dall'art. 7, l'applicazione della revoca prolungata di cui al punto 7.2.3.2 seguente.

7.2 Individuazione dei provvedimenti disciplinari

7.2.1 Richiamo

Qualora il Comitato di Garanzia accerti, al termine del procedimento di cui al punto 7.1, la violazione di uno o più degli obblighi previsti dall'art. 3, invierà all'Aderente una comunicazione di richiamo, invitandolo ad ottemperare entro 15 giorni agli impegni sottoscritti con l'adesione al Codice.

7.2.2 Censura

Nel caso in cui l'Aderente non provveda, nei termini previsti, ad adeguarsi alle indicazioni contenute nella comunicazione di richiamo ovvero nel caso in cui la violazione sia di particolare gravità per quantità o rilevanza degli inadempimenti al Codice, il Comitato invia all'interessato una comunicazione di censura invitandolo ad ottemperare entro 15 giorni a quanto previsto nel provvedimento adottato.

7.2.3 Revoca dell'autorizzazione all'uso del marchio Internet@minori"

7.2.3.1 Revoca temporanea

Nel caso in cui l'Aderente non proveda, nei termini previsti, ad adeguarsi alle indicazioni contenute nella comunicazione di censura, il Comitato revocherà l'autorizzazione all'uso del marchio "Internet@minori". L'uso del marchio sarà nuovamente autorizzato dal Comitato una volta accertato su richiesta dell'Aderente l'adeguamento dei suoi comportamenti agli impegni assunti.

7.2.3.2 Revoca prolungata

Nel caso in cui, dopo un primo provvedimento di revoca temporanea, intervengano le condizioni per un secondo provvedimento di revoca, l'Aderente non potrà avanzare richiesta di riammissione all'uso del marchio Internet@Minori prima di un anno.

7.2.4 Pubblicazione dei provvedimenti di revoca

L'Aderente al quale sia stato revocato l'uso del marchio "Internet@minori" non potrà più utilizzare il marchio medesimo fino a che non sia stato nuovamente autorizzato o riammesso all'uso.
Tutti i provvedimenti di revoca saranno raccolti ed oggetto di pubblicazione secondo le indicazioni del Comitato di Garanzia.

Firmato a Roma il 19 novembre 2003 presso
il Ministero delle Comunicazioni