FONDAZIONE
SAFETY WORLD WIDE WEB
ONLUS

DIFFERENTIATED NAVIGATION

CHILDKEY TECHNOLOGY

The Foundation
Onlus Safety World Wide Web

Through a research activity, as a non-recognised association, initiated in 1998, a patented technology called "ChildKey" was developed for the protection of minors who surf the Internet. A method of supervising minor's access to Internet which allows, through the usage of a password mechanism, to know exactly the user's age who accesses the service thus allowing notifying his/her presence on the "Network" and filter the contents and further allowing controlling by the parents of all the surfing privileges.

Such Technology, especially the access of public "Tagged Age" on line, determined the need to notify the non-safe sites the visit by a minor, therefore creating the parameters of behaviour damaging to the minor's rights and legally prosecutable.

To achieve such objective and promote "ChildKey" technology an association is born on April 2000 in Brescia (Italy), the Onlus Safety World Wide Web Foundation.
The aim of the foundation is to introduce on Internet safeguard mechanisms and protection for the minors who surf it and to sensitise all of the subjects who operate on it (Providers, Search engines, Owners and Webmasters) and conform their behaviours to criteria of responsibilities according to the new information document of "the presence of minors" which the ChildKey Technology allows to send "On Line" without in any way coercing the liberty of expression.

The Onlus Safety World Wide Web Foundation, together with Dominique Lapierre Foundation, International Coordination of Association for Minors Protection, Centre for the Study and Research on Family and to the Gestweb S.p.a. of Brescia which has developed the technical design, promotes and publicises throughout the world the ChildKey Technology, believed to be the sole and efficient technical instrument for the protection of minors during Internet surfing.

Freedom of expression and protection of minors

Internet and world of Web in general represent an inestimable value of evolution in the spreading of information and the many possibilities of free communication on a planetary level. Any form of censorship and limitation on the possibility of exchanging information is to be retained damaging, anti-liberal and counterproductive to the development of this technology...
It is obvious however, that custom and technological revolution introduced by the Web, contain also risks which cannot be ignored or underestimated like indiscriminate diffusion of violent and pornographic contents. Such risks are especially felt by the parents a by those persons from which we demand the protection of minors (churches, parishes and various other organisations) which have difficulty to find a solution to the problems brought by the new media.

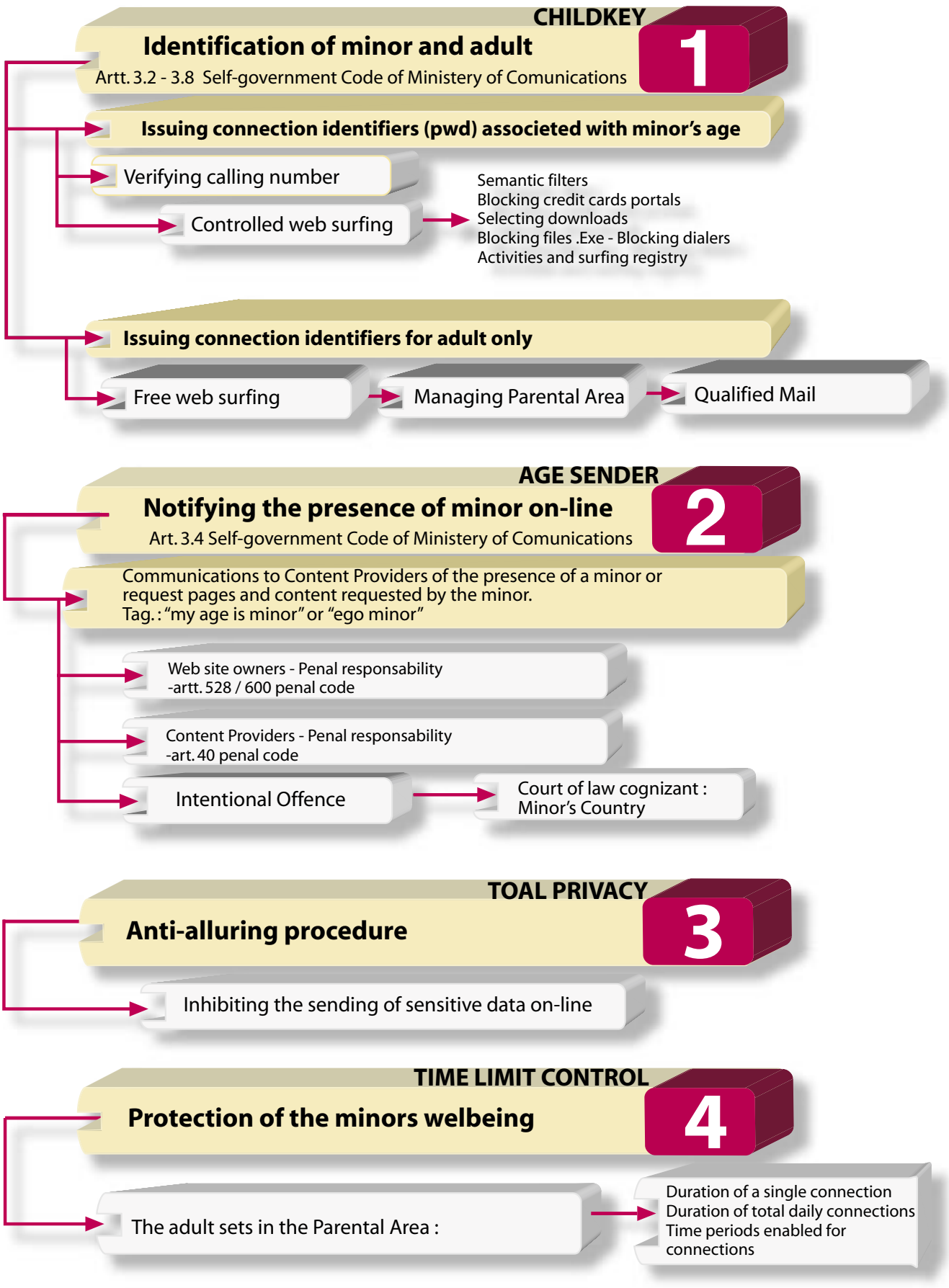
All technological system of protection currently

used aim at solving the problem "at the source", placing the surveillance at the end of the process of transmission of information, meaning at the moment in which this arrives at the user. This entails, in many cases, installation on a home computer of dedicated programmes which analyse and filter the incoming contents mainly comparing them with specific dictionaries included in the software.

There are also systems which don't require installation of software or hardware by the user but the principle is substantially the same: to obtain the filter, the surfing must pass through a site specialised which, at a distance, perform the same operations executed by systems installed at home.
The weak elements of these systems consist in the impossibility of understanding the presence of minors. None of them, however, is really secure and non-circumventable by savvier user on the handling of a computer.
The Foundation has offered itself to search and diffuse a solution capable of guaranteeing at the same time, on one end the freedom of expression on line on the other the protection of minors.
The ChildKey technology is believed to be capable of guaranteeing all this and above all to set the bases for a more assumption of responsibilities by the Web and by its operators for the protection of minors.

FONDAZIONE
SAFETY WORLD WIDE WEB
ONLUS

POSTULATED OF DIFFERENTIATED WEB-SURFING



EUROPEAN LEADERSHIP IN THE WORLD

Childkey Techonology was illustreted to the European Parlament in Strasburg in September 9, 2004.

Welcoming the Recommendations many times expressed by the European Union, Gestweb S.p.a. Company, together with Onlus Safety World Wide Web Foundation have elaborated, designed and created the ChildKey technology which represents the true and only system which satisfies and make their own all the postulates of the Differentiated Web-Surfing.
The architecture of the ChildKey technology is based on its ability to make a link between the requested web page and the age of the (tagged-age) user who requests it (Age Sender functions).

To do this is necessary that the user's profile is recognisable at the moment in which the connection to the web is made or, in any case, before surfing begins. Such recognition is made possible by an identifier of connection associated to the user's age that has to key-in and submit at connection.

The action of identification carried-out by the new ChildKey Network works in combination with Internet providers who have by contract signed on with the ChildKey service.

Such contract provides the use of ChildKey identifiers capable of providing a differentiated web-surfing, for adult and minor, based on an identifier of connection and issued to each family component.

When a connection identifier (password) is typed in and corresponds to that of a minor, the ChildKey authenticator routes the connection through an assisted surfing, activating Age Sender, Time Limit Control and Total Privacy, as well as, Parsing functions and Text Analysis.

With Age Sender, allows remote serves to recognize the age of the connected user (sole worldwide technology) therefore making providers of content and web hosts legally punishable.

Adapting themselves to the Childkey technology, web sites' managers, can easily "moralize" their work by applying on their web pages a simple declaration (metadata ChildKey) concerning visualization and non-visualization by minors of the content placed on the Web. It is the duty of the Safety World Wide Web Foundation to solicit for such declaration and verify that it is correctly executed.

A widespread use of this technology will modify the way Providers, Search Engines and online content suppliers operate, thus conforming to the criteria of their responsibilities towards minors as expected by society. Differentiated Web Surfing, a precaution in action, is the only measure of its kind available today and respecting the opinion of the Supreme Court of the Unites States n. 03-218 dated June 29, 2004.

The ChildKey technology has also been redesigned and integrated into KeyStudent, similar technology created specifically for schools, libraries and youth centers where the need to protect young web surfers is also a concern.

The technology designed provides the use of a software packet (KeyFamily) in the Provider's server which is capable of managing a high level of security to guarantee minor's Internet accesses while keeping a total transparency for an adult's surfing.

ADVANTAGES IN THE USE OF DIFFERENTIATED WEB-SURFING

1 It is utilised through a single Internet connection for the whole family, differentiating the access passwords for the various members according to age (one for each minor child registered).

2 It allows the minor identification even from the request for connection or however from the beginning of web-surfing.

3 It satisfies the safety need of families, allowing children to surf safely and preventing them access to sites with a coarse, obscene or violent content.

4 It informs the child that his/her web-surfing will be supervised and about his/her own privileges.

5 It also prevents the diffusion on the Web of sensitive information regarding minors and their families.

6 It permits to communicate the presence of minors to the whole "Web" informing the visited servers about the target of the minor presence that has requested the display of contents. The new computer science creates the pre-conditions for a penal awareness of all the subjects who take part and operate in the Net.

7 It allows preventing a minor from diffusing on line sensitive information regarding himself and his family (Anti- Alluring Function)

8 And enables parents to safeguard t he wellbeing of their children by determining the length of the single connections, the maximum length of daily connection, as well as connection times.

9 It permits parents to supervise the activity performed by the minor on line (Surfing Register and Activity Register).

10 It allows adults to determine – via Web-surfing privileges of every single minor within a family (Parents Area).

11 It does not require any hardware or software installation on the user's computer.

12 It allows the use of the Qualified Mail for a better protection towards the spam detrimental to the family rights.

13 Adults Web- surfing remains free and completely transparent to this technology.

14 It offers the provider the possibility of furnishing a service at value-added

15 In compliance with the objectives of Safety World Wide Web Foundation. It allows legal prosecution against those Providers indifferent to the legal aspects of diffusing pornographic material or unsuitable material to minors.

16 Safety World Wide Web e Web Foundation informs all the providers of the sites visited by minors about the existence of ChildKey technology and the changing of their own responsibilities.

17 Search Engines are enabled to understand when the "search" is requested by a minor, thus activating consequent and "obligatory" protection filters.

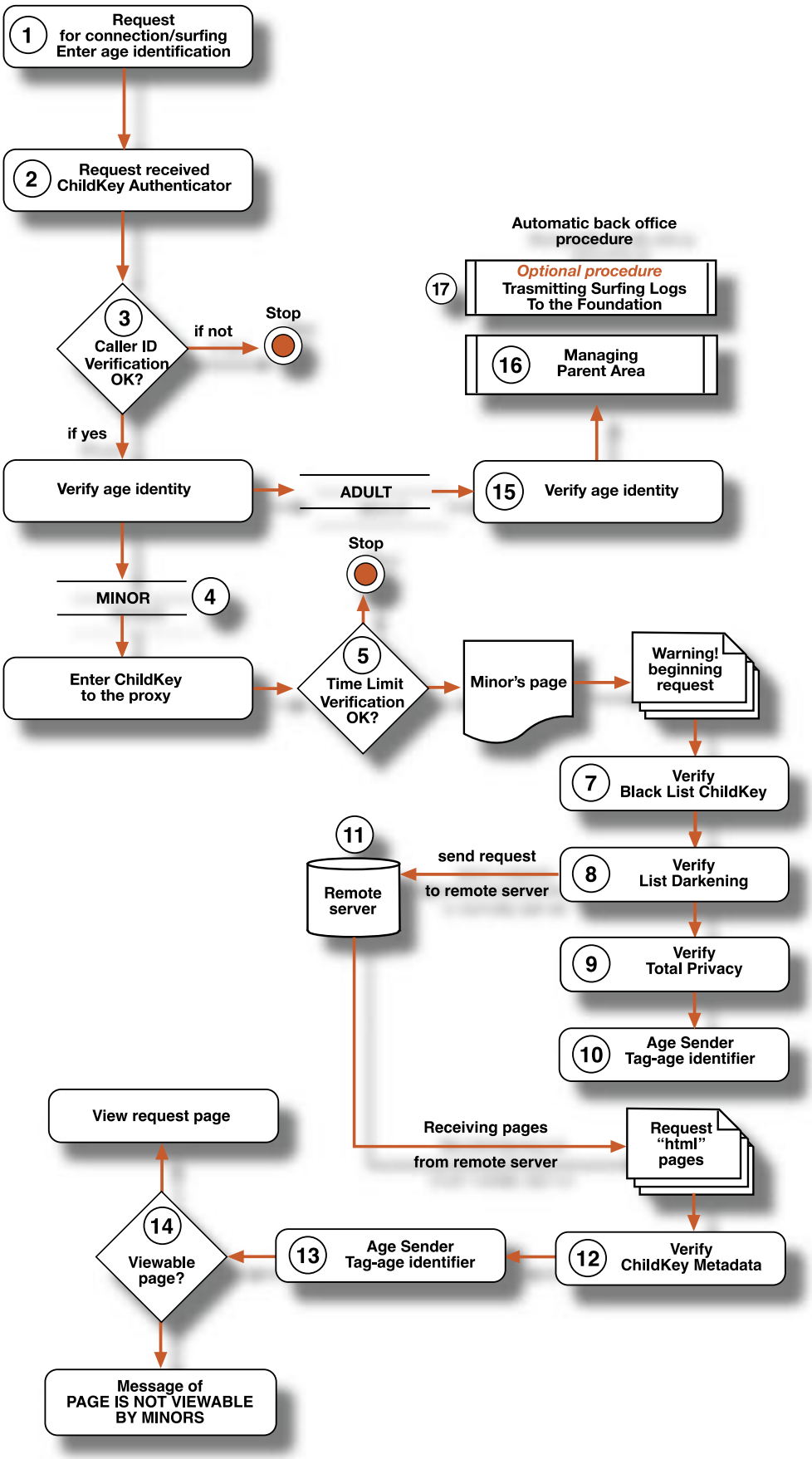
18 Authorities of every single State can contribute to compile the list of the sites to be blacked out containing all the sites with a content of offensive nature (paedophile-pornography, racism, etc.).

19 Content providers(Registrant) can self-certify the content of each html published page by requesting or freely adopting ChildKey metadata.

20 It is obligatory for end-users (sites) with contents unsuitable to minors.

21 Content providers become criminally responsible for what is diffused on line thanks to the notification of the minor presence(Age Sender).

WHAT HAPPENS WHEN YOU CONNECT AND SURF

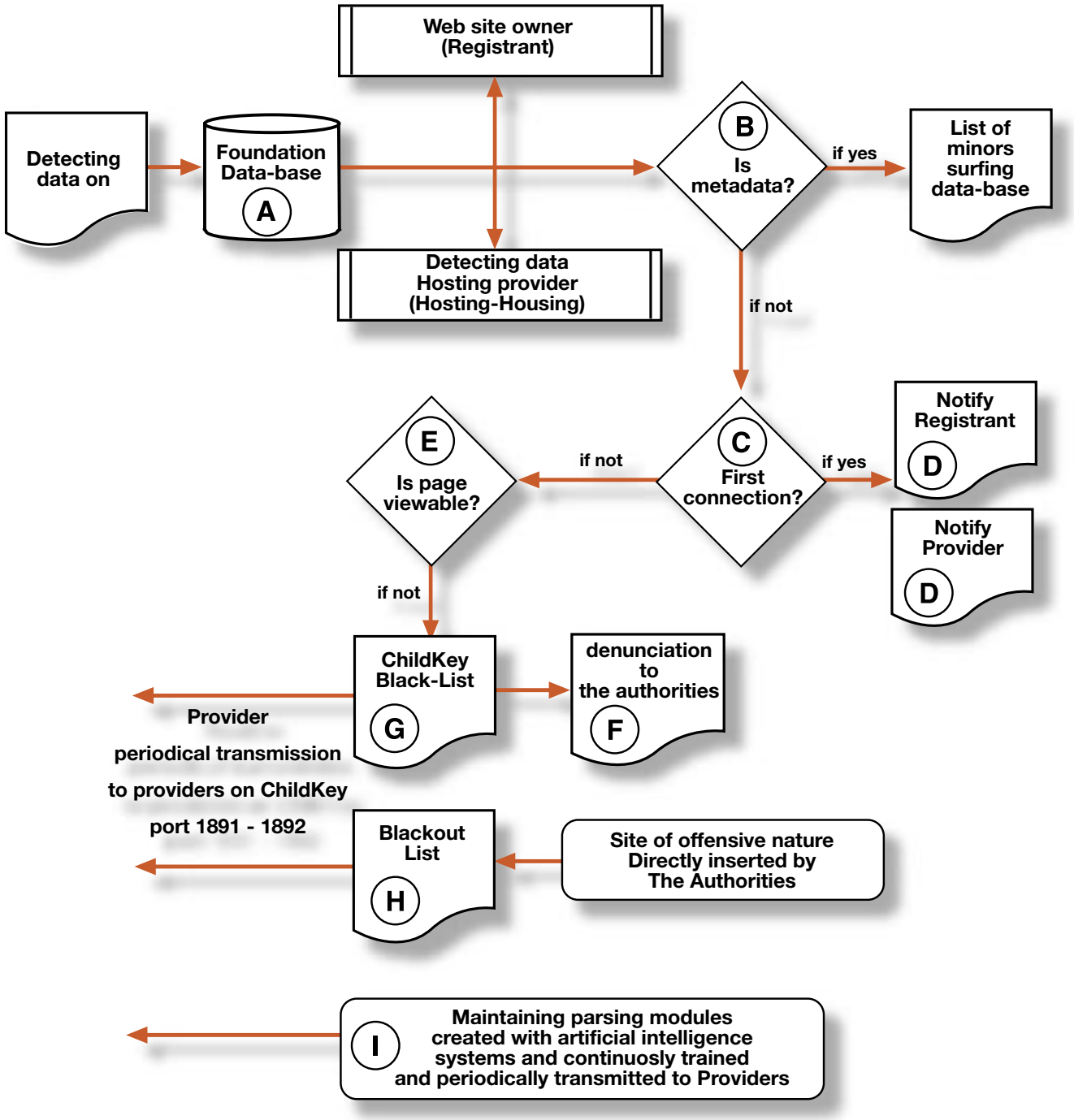


FLOW CHART DETAILS

Minor's identification and recognition	Phase pertinent to the Provider and its User. By sending the tag-age (ChildKey), the ChildKey is placed in condition of recognising the minor at the momenta connection is requested or, in case of cable connection, before surfing begins. • The ChildKey Provider issues as many connection identifiers associated with the age of as many family component.	1 2 3 4
Trasparency and information	After identification, the minor is informed, on the "Family Home Page", that the current connection is differentiated, of the set privileges and residual surfing time.	2
Adult Surfing at-will	There are no restrictions of adult surfing. There is an option of applying a Blackout List; this way the user would not be connecting to paedophile-pornographic sites.	15 16
Time Limit Control	Allows the adult to determine the duration of connection and enabled times and precisely: • Duration of a single continuous connection; • Maximum duration of daily total connections; • Times of the day enabled for connecting.	5
Parents Area	Allows the determining of surfing privileges of each individual minor and to visualise and verify: Privileges of configuration for the setting of surfing filters of each minor including Time Limit Control; Surfing Registries, surfing reports of each minor are available for verification via Web or they may be sent through e-mail and allows constant and detailed the minor's operations; Activity Registries, surfing reports of the entire family indicating date and duration of each daily connection.	16
ChildKey Black-List	List of web sites, previously notified, which have refused self-certification and considered harmful to the minor. The ChildKey Black-List is transmitted to the Providers.	7 G
Black out List	List of sites with offensive content (paedophile-pornographic) and directly added in data-base of the Foundation by the relevant Authorities. The Blackout List is also distributed to the providers.	8 H
Total Privacy	Block the alluring of minors by preventing the diffusion on-line of sensitive data regarding the family. It prevents that the Black-list is circumvented. It blocks the circumvention of the same or Parsing through the use of "cleaner" sites.	9 16
Content Self-certification	Insertion of a metadata in all visible html pages, either static or dynamic, allows the ChildKey Technology to discriminate among visible and non-visible contents for the minors.The adoption of metadata allows the standardisation and diffusion of the technology at no cost for all web masters and builders of Internet sites.	12 D E

FLOW CHART DETAILS

<table>
<tr><td rowspan="3">Age Sender
Notifies the
Presence of a minor
On-Line</td><td colspan="2">A phase which involves Provider and Internet
Consists of notifying the presence of a minor to the entire Internet through the use of an identifier recognisable by all and thus inserted in the public header of the request.
To each request for a page by the minor, the ChildKey Technology notifies to the server also the tag-age of the minor. Such function is carried out by the Age Sender module and it is patented.
The Provider will receive a communication as in example 2 modified by the Age Sender:</td><td rowspan="3">10</td></tr>
<tr><td>Example without 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</td><td>Example with 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</td></tr>
<tr><td colspan="2">Such function generates an information which produces repercussions in the field of crime creating the premises for criminal responsibilities by content suppliers and Providers that host them and Search Engines.</td></tr>
<tr><td>Dynamic Parsing Models with semantic intelligence</td><td colspan="2">Blocks the displaying of paedophiles and pornographic pages to the minor through the use of modules created and trained with artificial intelligence systems and constantly updated by the Foundation.
The interpretation of text content and other patented parameters allow the identification of 98% of harmful pages.</td><td>13
I</td></tr>
<tr><td>Sensor of the presence of a minor - Snasa ChildKey</td><td colspan="2">The use of Snasa ChildKey software allows Search Engines and Providers' servers to "understand" if the request of "html" pages is by a minor .</td><td>11
D</td></tr>
<tr><td>Issuing Qualified E-mail Boxes</td><td colspan="2">The use of qualifying suffixes before the @ as a demonstration directed to the net by the owner of a qualified e-mail box.</td><td></td></tr>
<tr><td>Automatic submitting Surfing reports (optional procedure)</td><td colspan="2">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.</td><td>17
A
D</td></tr>
</table>


Web site owner
(Registrant)
Detecting
data on
Foundation
Data-base
A
B
Is
metadata?
if yes
List of
minors
surfing
data-base
Detecting data
Hosting provider
(Hosting-Housing)
if not
E
Is page
viewable?
if not
C
First
connection?
if yes
Notify
Registrant
D
Notify
Provider
D
if not
ChildKey
Black-List
G
denunciation
to
the authorities
F
Provider
periodical transmission
to providers on ChildKey
port 1891 - 1892
Blackout
List
H
Site of offensive nature
Directly inserted by
The Authorities
I
Maintaining parsing modules
created with artificial intelligence
systems and continuosly trained
and periodically transmitted to Providers

FLOW CHART DETAILS

Reception of surfing reports	The Foundation data-base receives on ports 1891 and 1892 surfing reports by minors from all the Providers which utilise ChildKey technology. The reports do not contain personal data for the protection of Privacy of the minor.	17 A
Metadata ChildKey Verification	During this phase the technology verifies the presence of ChildKey Metadata. If positive, the site's html page is listed among those self-certified. The inserting of metadata on all visible html pages, either static or dynamic, allows the ChildKey Technology to discriminate among viewable and non-viewable page contents to the minors. The adoption of metadata, allows the standardisation of the technology and a diffusion at no cost to all web builders and webmasters of Internet sites. The failure to insert ChildKey metadata by the managers of sites visited by minors carries the inclusion of the site in the Black-List of sites not suited for minors compiled and updated by the Onlus Safety World Wide Web Foundation. The information regarding the presence of a minor carries the obligation of self-certification if the contents are not to be viewed by minors according to current Italian and European legislation. The use of Metadata is licensed free of charge and so the software and the automatic insertion of it if the site contains multiple pages. The licensing conditions provide that the self-certification be made based on European and Italian laws governing the protection of minors. How the ChildKey metadata is formulated: For sites viewable by minors: <meta name ="swww.childkey" content="childkey.green"> For sites not viewable by minors: <meta name ="swww.childkey" content="childkey.red"> NOTE: the ChildKey metadata certifies each individual Html page of the site and not the entire site. Therefore, a site may contain both, viewable and non-viewable pages by minors, maintaining even in the presence of the latter the navigational bars (as long as they are visible). The "green" metadata sites undergo Parsing anyway, just for safety measures.	B
Identification of Registrant and Provider	The Foundation provides, through an automatic technology, to identify, in the presence of a URL visited by a minor, the Registrant and Provider which hosts it.	D
Verification of Notification	During this phase there is a verification if the information on point E has been sent to the Registrant or Provider. If so and in the absence of a metadata certification we proceed the phase F.	C
Content verification	Through the use of Dynamic Parsing utilised by the ChildKey Technology, verification is done if an html page contents is non-viewable by minors. If so the URL is listed in the ChildKey Black-List (F) and proceed to a complaint-notification (H).	E
Parsing Semantic Models	The Foundation takes care of up-dating and training the Semantic Intelligence systems to obtain Models from which to extract dictionaries for the analysis of the html page's content. The Foundation takes care also for the use of other recognising methods. The updated dictionaries and software are transmitted to the Providers through ports 1891/1892.	I
Complaint notification	The Foundation is charged with formulating complaints-notifications in case of infringements of minors' rights who surf the Web. In such cases it furnishes all the necessary technical documentation.	F
ChildKey Black-List	A Black-List is compiled of sites not self-certified or with contents not suited for minors. Such Black-List is constantly monitored and updated and is distributed to providers through ports 1891/1892.	G 7
Black out List	The list of sites with offensive content is directly inserted in the Foundation data-base by the relevant Authorities. The Blackout list is distributed to Providers through ports 1891/1892	H 8

OBLIGATIONS OF THE FOUNDATION

An institutional obligation of the Safety World Wide Web is to operate and supervise in such a way that the rights of minors surfing the Web through ChildKey technology are not infringed or violated. In particular the Foundation classifies files and deals with the reports of the sites visited by minors which are periodically sent by Internet Service Providers who furnish the ChildKey service.

According to these data, the Foundation sends to all the persons responsible for the sites visited by those minors who have not yet self-certified the contents of their own web pages through the ChildKey metadata, an e-mail followed by a recorded delivery letter in which it informs them about the visitation of a minor and asks them to adapt their behaviour to the necessary criteria of responsibility.

Subsequently the Foundation compiles a Black list of sites at risk (that is not yet provided with ChildKey metadata and, after a close study, proved to be unsuitable to minors) and bounds itself to update it regularly.

The Foundation bounds itself to remove from the list those sites which in the meantime have adopted ChildKey metadata self-certifying correctly the contents of their pages.

The Black List is transmitted regularly to all the Internet Service Providers furnishing the ChildKey protection service that can use it in the analysis procedure of the web pages requested by minors.

The Foundation monitors, classifies and constantly informs Providers and Search Engines to supervise if their behaviour conforms to the responsibility criteria for minor's protection.

Schools and Youth Centres

The Foundation proposes and promotes ChildKey technology to be used in schools, libraries and other youth centres.

KeyStudent, a product of ChildKey technology is a registered integrated system, applied within the school network, which prevents the consultation of Internet pages with unsuitable contents, such as pornography and the installation of additional software on each PC is not required. Through an intuitive Web interface the supervisor will be able to determine web surfing privileges for each student.

Software diffusion in free licence

The Foundation proposes and promotes Snasa ChildKey Software- sense of minor presence- for Providers and Search Engines and promotes ChildKey metadata self-certification for all the sites requesting it, as well as SpiderCk to identify non self-certified pages lying on the servers of Contents Lenders.

Relations with Authorities and Blacked-out Lists

With the aim to fight paedophile, the Foundation allows every single State which makes a request, to insert directly in its data-base the sites with an offensive content. These sites form the Blacked-out List which is regularly transmitted to Providers. The connection is effected through a protected procedure (https) and is released by request and in accordance with the laws in force.

Relations with RIR (RIPE NCC - ARIN - APNIC)

The Foundation informs the three institutions which assign the IP for Internet end users by:

- sending to SIR the Blacked-out List with IP request for blacking out.

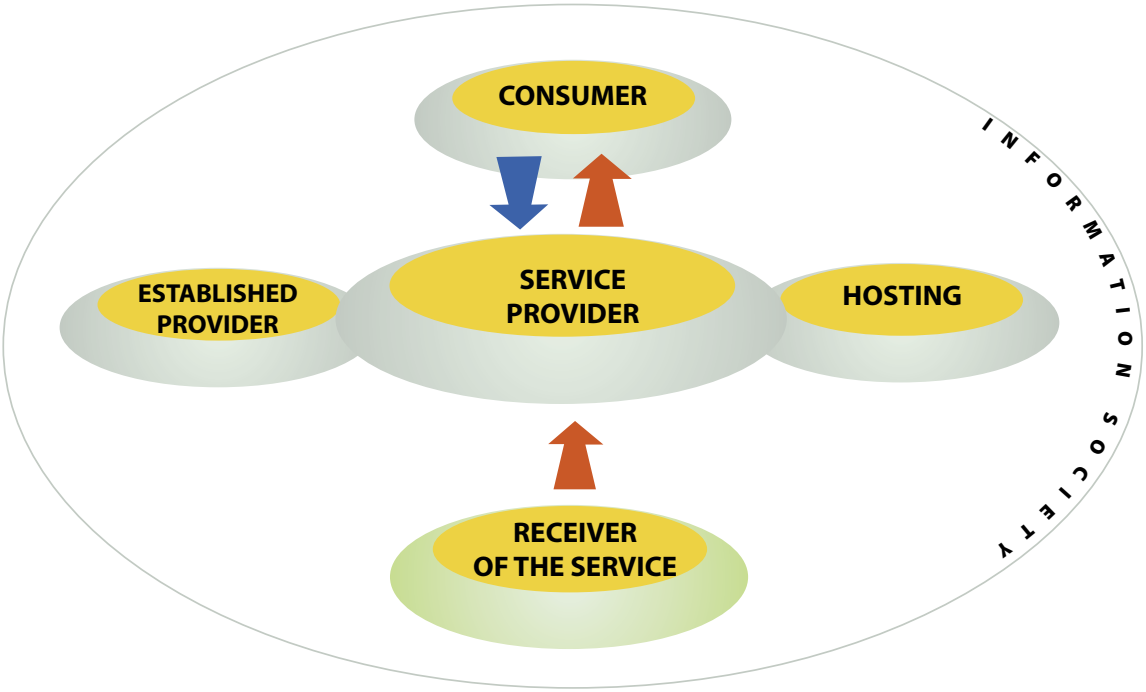
  These procedures, if accepted, would involve non visibility, at a world level, of all those sites which the Authorities of every single State have considered to be offensive by nature (paedophile-pornographic sites and others) and therefore non visible to minors and adults.
- sending to RIR a List of Inconsistencies from data of Registrant (site proprietor) and the real proprietor. Such list is the consequence of the notifications effected by the Foundation to the Registrant.

  It has also been verified that the data of certain Registrant do not correspond to real data therefore the notification has been unsuccessful.

  Such inconsistencies are reported to SIR.

THE NETWORK SUBJECTS

The network as seen by the Directive 2000/31/CE - June 8 - 2000



To fully understand the responsibility of each individual subject who operates on the Internet, it is appropriate to refer to the distinction made by the European Provisions through the Directive 2000/31/CE.
In such Directive the following subjects are identified:

Information Society:
The services according to art.1 comma 2 of the directive 98/34/ Ce, as modified in the directive 98/48/CE;

Provider:
The legal or physical person who providesa service to the information society;

Established Provider:
The provider who actually exercises and for an undetermined amount of time an economic activity through a fixed installation. With the advent of Differentiated Surfing, he presence and use of technical mediums and technologies necessary to perform a service do not constitute in itself the performer

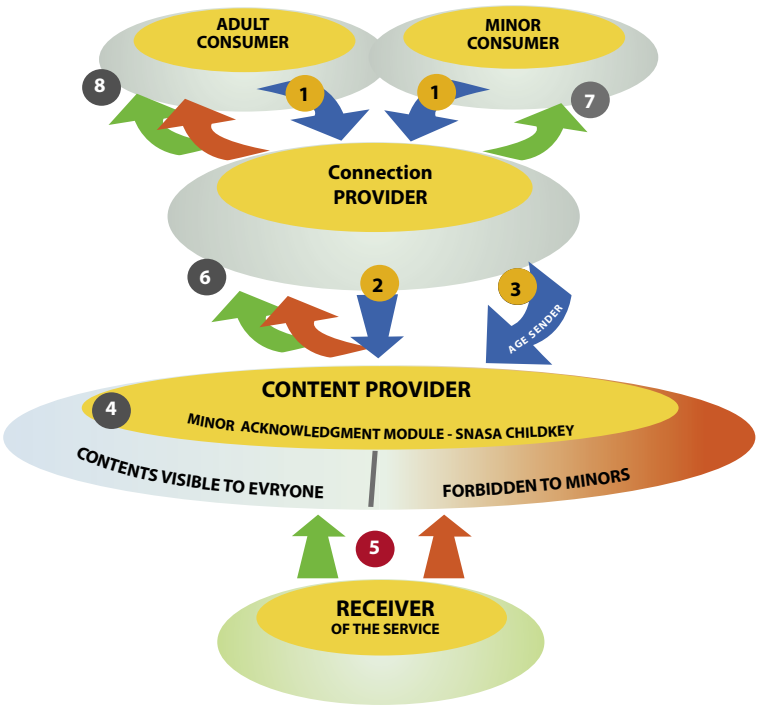
Hosting:
fulfilment of a service by the Information Society consisting of memorising information furnished by the receiver of the service at the request of the same receiver;

Receiver of the service:
The physical or legal person who, for professional the diagram on the following page reasons and non, utilises a service of the information society, especially for research or make information accessible;

Consumer:
any physical or legal person who acts with purposes which do not fall under commercial,business or professional activity.

With the advent of Differentiated Surfing such Network vision must be modified as in the diagram on the following page

THE NETWORK AS SEEN TODAY WITH DIFFERENTIATED NAVIGATION



On-line penal responsabilities

Today, thanks to the ChildKey technology and the advent of Differentiated Surfing, the Providers of Service are in a position of knowing if the person requesting a web page is a minor or adult.

Such information forces the Providers and Receivers of Service (Search engines, Web sites etc.) to adapt their behaviour to the criteria of responsibilities. This may be done through the use of ChildKey metadata for the sites and Snasa ChildKey (software which detects the presence of minors) both licensed free of charge by the Onlus safety Wide World web Foundation.

We believe that nowadays already exist, thanks to such information, the premises for applying the penal code for violating art. 40, 528 and 600 third and fourth.

Legal aspects: Responsabilities

The European Union and other Countries legislations have already disciplined various information crimes to combat the spreading on Internet of illegal information, pornography (especially child pornography), racial slurs and information which incite violence. The authors or suppliers of such contents may be called to answer in a court of law. Even the providers of service may be involved: being able to prove illegal access to a minor, in fact, there are proven details of uncontrolled access and therefore sufficient grounds for administrative or legal prosecutions.
According to the Italian Penal Code, the person or persons who displays on a public site, acquires, detains or places in circulation writings, drawings, images or other obscene acts of any kind is legally prosecutable (art. 528 p.c., whereby are considered obscene, acts or objects which, according to common sentiment, offend against decency.
The criminal acts may be committed also in an omissible manner, meaning doing nothing to avoid acts that can be construed as illegal actions.

In addition, as far as child pornography field is concerned, the Decision issued by the counsel of European Union on May 29 2000, provides that the member States examine appropriate steps apt at eliminating child pornography and steps to solicit Internet's service providers to:

- ✔ Eliminate from circulation all child pornography material of which they have been informed or come to know and widespread through such services
- ✔ Save all information regarding such traffic
- ✔ Install control systems to combat production, possession and diffusion of child pornography material
- ✔ Offer consultancy to the Authorities about child pornography of which they have been informed or come to know and diffused through their system

Adhering to the Convention on children rights, the Italian legislators has provided, through appropriate amendment of the penal code (law 269/98), norms regulating child protection against any form of exploitation and sexual violence to safeguard their physical, psychological, spiritual, moral and social development.

See art 600 third and fourth regarding paedophile and pornographic material.

CLASSIFICATION OF RESPONSABILITIES

1 RECEIVER OF THE SERVICE

The service receiver is surely the subject on which falls the obligation of self-certify and classify the contents published.
The failure to do so makes it responsible for the "diffusion of material offensive to the rights of minors to a minor"

2 CONTENT PROVIDER

The Provider (of contents) is capable of recognizing if the request for html pages is done by a minor.
This allows demanding from the Service Receiver the classification of contents.
In order to avoid responsibility of the P.C. (art.40) it will have to supply to:

1 memorisation of data to be diffused on-line either as Hosting or Housing (established provider) is done by the identified receiver of the service.

2 contractual clauses will be provided which impose to the service Receiver the classification or self-certification of the contents.

3 CONNECTION PROVIDER

The (connection) Provider doesn't
carry any particular responsibility.
We, however, believe that he has the
duty of offering a Differentiated surfing service to families, even by utilising third party (manager of differentiated surfing service)

1 2 3

Offence "event" Competence of a Judge Criminal proceedings

The Foundation takes on also the burden of formulating a complaint-reporting those who have started behaviours believed to contrary or have violated children rights by furnishing all necessary documentation to the Authorities.

Being an offence of "event" type, the natural Judge is the one in the Country where the images have been or attempted to be displayed.

Italy

As far as our country is concerned, there are three Bills being analysed to adopt Differentiated Surfing.

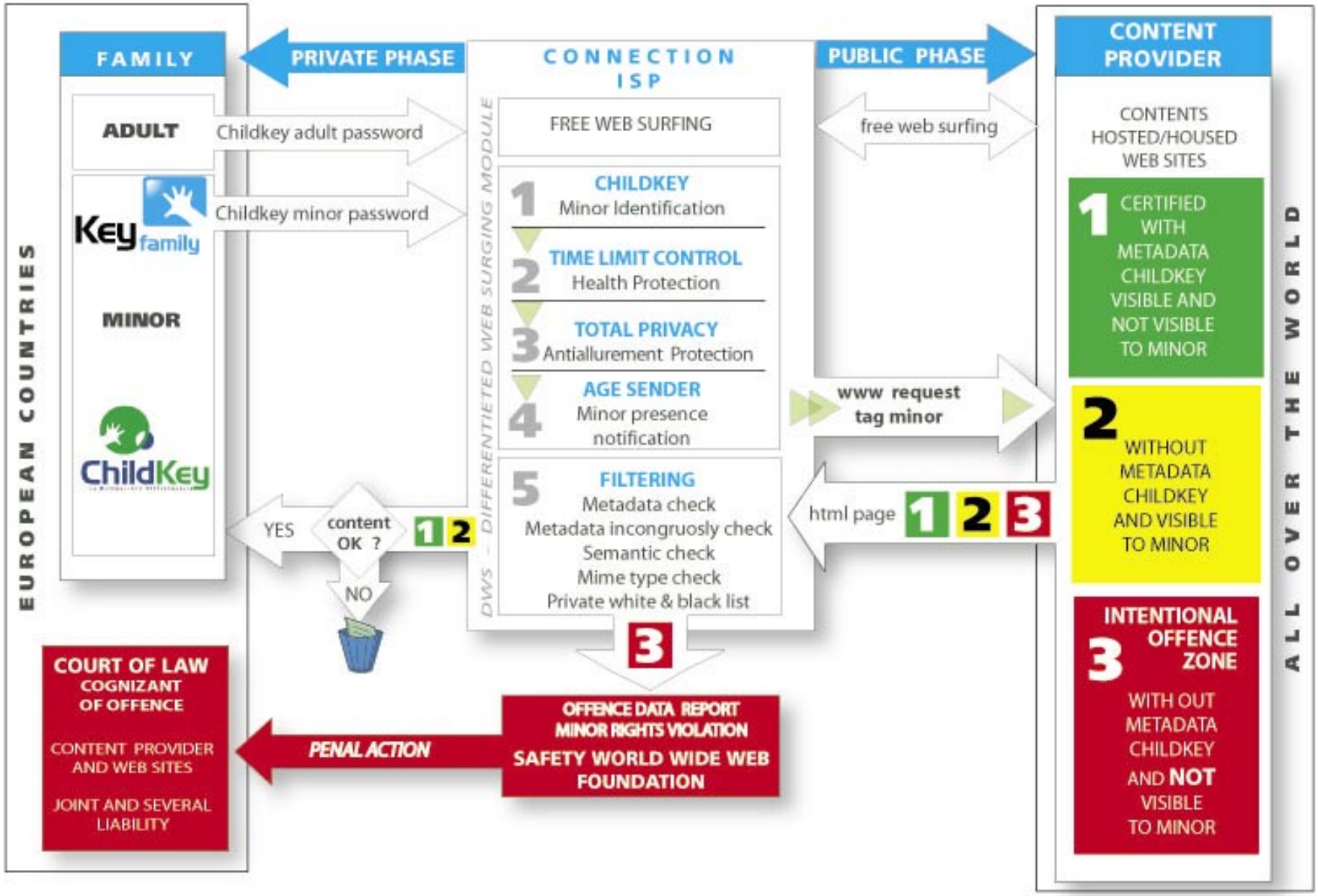
In particular the Bill presented by the representative Honourable Francesca Martini on October 8 2002 who has recognised that the ChildKey technology is capable of letting the Providers recognise a connected minor placing on them the responsibility , as in Art. 1, the obligation of equipping themselves of means apt at protecting the minors.

The Bill provides in Art. 3 the introduction of the Art 528 b of the P.C., severe penalties for providers and connection providers of Internet who don't abide by Art. 1.

A big success for the Onlus Safety Wide World Web Foundation and a big step forward for the protection of minors who surf the Internet.

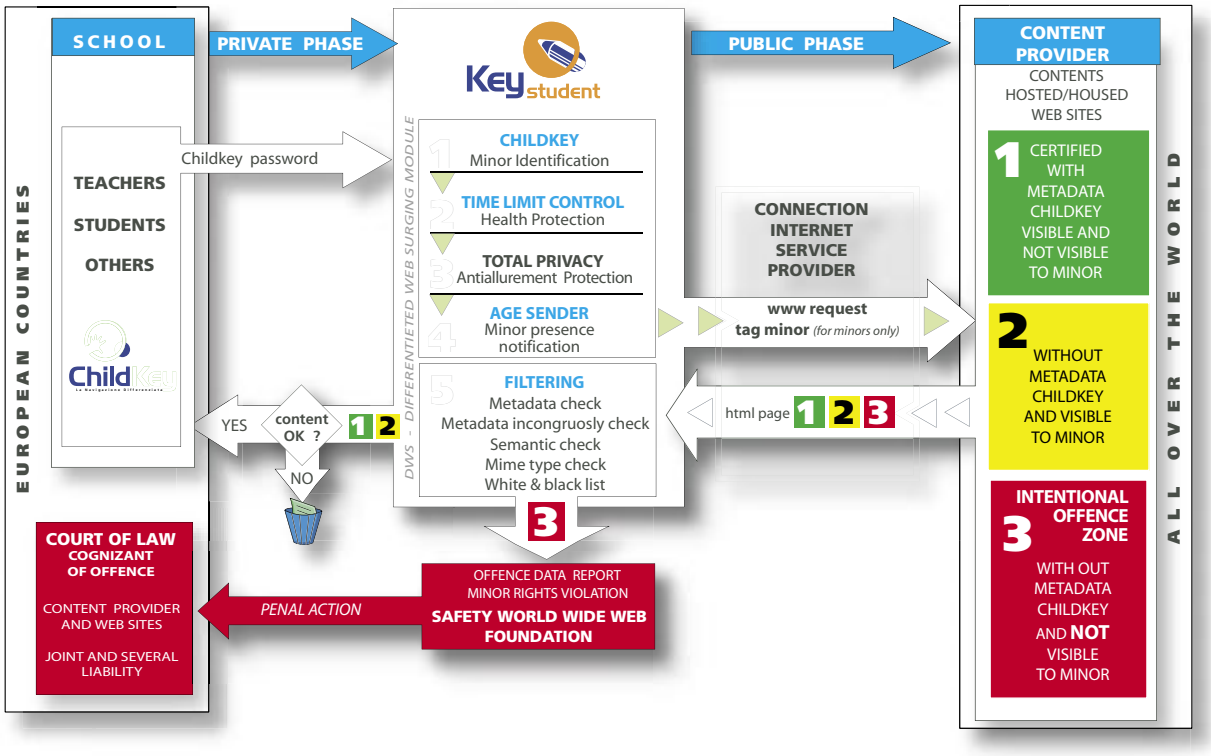
DWS - DIFFERENTIETED WEB SURFING

INTERNET SOCIAL RESPONSABILITY



DWS - DIFFERENTIETED WEB SURFING

INTERNET SOCIAL RESPONSABILITY



DWS - DIFFERENTIETED WEB SURFING

INTERNET SOCIAL RESPONSABILITY