



# Naar een **safer** internet

Aanbevelingen van  
de European Youth  
Protection Roundtable

**NICAM DOSSIER 5**

#### Colofon

#### Uitgever

Nederlands Instituut voor de Classificatie van Audiovisuele Media (NICAM)

Postbus 322

1200 AH Hilversum

Telefoon: 035-6460860

Email: [info@nicam.cc](mailto:info@nicam.cc)

[www.kijkwijzer.nl](http://www.kijkwijzer.nl)

#### Druk

Drukkerij Imprimo. Bussum

#### Ontwerp en opmaak

Jan Pieter Ekker

#### Copyright

Stichting Youth Protection Roundtable – Stifting Digitale Chancen / Stichting NICAM

#### Eindredactie

Marloes van Hoorn, Tiffany van Stormbroek

Bronvermelding is verplicht.

Vereenvoudiging voor eigen of intern gebruik is toegestaan.

Het originele rapport is te downloaden van: [www.kijkwijzer.nl](http://www.kijkwijzer.nl)

Hilversum 2009

# Naar een safer internet

Aanbevelingen van  
de European Youth  
Protection Roundtable

**NICAM DOSSIER 5**

## Voorwoord

Het NICAM krijgt regelmatig de vraag of Kijkwijzer ook op internet kan worden toegepast. Op dit moment is Kijkwijzer nog primair een classificatie- en informatiesysteem voor televisie, film en dvd producties. Conform de afspraken met de Nederlandse overheid. En voor games is er het van Kijkwijzer afgeleide Europese classificatiesysteem PEGI.

Maar het is evident dat de snelle ontwikkeling en de belangrijke rol van internet de vraag oproept hoe mogelijke schadelijke effecten van online activiteiten zo goed mogelijk voorkomen kunnen worden. Al enige tijd is het NICAM betrokken bij verschillende (inter)nationale internet overlegplatforms. Enkele jaren geleden werd op verzoek van het Ministerie van EZ een advies uitgebracht over de haalbaarheid en wenselijkheid van een Kijkwijzer toepassing voor internet. En onlangs is op verzoek van het Ministerie van Justitie een project afgerond dat tot doel had de classificaties geschikt te maken voor internet filtersoftware.

De afgelopen maanden heeft het NICAM deelgenomen aan Youth Protection Roundtable (YPRT). Een initiatief van het Safer Internet Plan van de Europese Commissie. Tijdens een aantal rondetafelgesprekken wisselden deskundigen best practices op het gebied van veilig internet voor jeugdigen uit. Deze bijeenkomsten hebben geleid tot een aantal aanbevelingen met het doel de jeugd op internet beter te beschermen tegen mogelijke risico's.

Wij publiceren de aanbevelingen in deze nieuwe uitgave in de reeks NICAM Dossiers, ter informatie en mogelijk inspiratie van alle (professionele) belanghebbenden en belangstellenden bij het vraagstuk 'safer internet'.

De publicatiereeks NICAM Dossiers heeft tot doel nieuwe onderzoeksinzichten en relevante informatie met betrekking tot de invloed van media onder de aandacht te brengen.



Wim Bekkers  
directeur

## Inhoudsopgave

Inleiding .....	7
<b>A</b> <b>Risico's bij het gebruik van internet door kinderen en jongeren .....</b>	<b>9</b>
A1 Risico's bij online content .....	10
A2 Risico's bij online contact .....	12
<b>B</b> <b>Beschikbare technologieën voor de bescherming van de jeugd .....</b>	<b>15</b>
B1 Filtersoftware .....	16
B2 Monitorsysteem .....	18
B3 Leeftijdsverificatie .....	19
B4 Overige technische middelen .....	19
<b>C</b> <b>Aanbevelingen voor de bescherming van de jeugd op internet .....</b>	<b>21</b>
C1 Verbetering van ondersteunende technologieën .....	22
C2 Verbetering van de bruikbaarheid van filtersoftware .....	22
C3 Verbetering van internettoepassingen .....	23
C4 Overeenstemming over beleid tussen providers en exploitanten .....	24
C5 Mediawijsheid .....	24
C6 Bewustwording .....	25
C7 Onderzoek .....	26
C8 Juridische regelgeving .....	26
<b>D</b> <b>Bronnen .....</b>	<b>27</b>
<b>E</b> <b>Overzicht zelfregulering .....</b>	<b>31</b>
E1 Zelfregulerende organisaties in Europa .....	32
E2 Instrumenten van zelfregulering in Europa .....	35
<b>F</b> <b>Overzicht van Europese wet- en regelgeving .....</b>	<b>41</b>
<b>G</b> <b>Deelnemers Youth Protection Roundtable .....</b>	<b>47</b>

## Inleiding

Deelnemen aan de informatiesamenleving is belangrijk voor mensen van alle leeftijden. Internet biedt enorm veel mogelijkheden: het heeft een positief effect op onderwijs, werk en economie. Vooral kinderen en jongeren kennen de toepassingen van internet goed. Ze hebben daar veel profijt van, maar zijn ook kwetsbaar. Er zijn namelijk risico's verbonden aan internet, vaak analoog aan risico's in de offline wereld. Met technologieën kunnen de gevaren van internet ingeperkt worden. Maar hoe goed de technologieën ook zijn, techniek alleen is nooit voldoende. De beste manier om de veiligheid van de jeugd te bevorderen is te zorgen voor *empowerment* en voorlichting. Hierdoor leert zij met de risico's om te gaan.

Deze aanbevelingen zijn ontwikkeld door de Youth Protection Roundtable in het kader van het Safer Internet Plan van de Europese Commissie. De Youth Protection Roundtable (YPRT) is opgericht in 2006 en bestaat uit technisch specialisten en experts op het gebied van jeugdwelzijn. Zij hebben nagedacht over de vraag hoe je technologie en voorlichting het best kunt inzetten om te zorgen dat jonge mensen – en in het geval van minderjarigen: de verantwoordelijke volwassenen – internet veilig gebruiken. De 32 leden uit 13 Europese landen hebben 30 maanden samengewerkt<sup>1</sup>. In deze periode zijn ze viermaal bijeengekomen. De stem van de jongeren zelf is gehoord in de zogenaamde Young Roundtable. Hierdoor heeft de YPRT inzicht gekregen in het gedrag van jongeren op internet. Op basis van de bijeenkomsten en de inzichten heeft de YPRT deze aanbevelingen opgesteld om de jeugd op internet beter te beschermen.

De Youth Protection Roundtable doet aanbevelingen voor technische maatregelen én voorlichting, die in zowel de publieke als de particuliere sector kunnen worden toegepast. De aanbevelingen zijn niet bindend en houden rekening met:

- het Verdrag inzake de Rechten van het Kind van de Verenigde Naties, 1989;
- artikel 10 van het Europees Verdrag voor de Rechten van de Mens, waarin waarborgen worden gegeven voor het fundamentele recht op vrijheid van meningsuiting en op uitwisseling van informatie en ideeën zonder tussenkomst van openbare instanties en ongeacht grenzen;
- de *Declaration on Human Rights and the Rule of Law in the Information Society* (verklaring inzake bescherming van mensenrechten in de informatiesamenleving), aangenomen door het Comité van Ministers op 13 mei 2005, op basis waarvan lidstaten zich verplichten juridische en praktische maatregelen te handhaven en verbeteren om censuur door overheden of particulieren te voorkomen;
- de *Declaration on Freedom of Communication* (verklaring inzake vrijheid van communicatie via internet) van het Comité van Ministers op 28 mei 2003;
- aanbeveling Rec(2007)11 van het Comité van Ministers aan lidstaten over bevordering van de vrijheid van meningsuiting en informatie in de nieuwe informatie- en communicatieomgeving;
- aanbeveling Rec(2007)16 van het Comité van Ministers over maatregelen ter bevordering van de waarde van internet als openbare dienst;
- aanbeveling CM/Rec(2008)6 van het Comité van Ministers aan lidstaten over maatregelen ter bevordering van het respect

<sup>1</sup> Zie blz. 48 voor een overzicht van alle deelnemende leden van de YPRT.

voor de vrijheid van meningsuiting en informatie met betrekking tot internetfilters (aangenomen door het Comité van Ministers op 26 maart 2008 op de 1022ste vergadering van de afgevaardigden van de ministers).

De YPRT- aanbevelingen bieden ondersteuning aan politieke besluitvorming en voor Internet service- en content providers, hard- en softwareontwikkelaars en mensen die voorlichting en training geven aan ouders, kinderen, docenten en zorgverleners.

### **De aanbevelingen voor technische ontwikkelingen:**

- geven providers en ontwikkelaars informatie over de risico's die kinderen en jongeren lopen bij gebruik van hun online services (hoofdstuk A);
- geven een overzicht van bestaande technologieën voor de bescherming van de jeugd (hoofdstuk B);
- beschrijven maatregelen voor efficiënte implementatie van deze technologieën (hoofdstukken C1-C4); en
- beschrijven algemene voorwaarden voor bescherming van de jeugd.

### **De aanbevelingen voor voorlichting en het gebruik van filtertechnologieën:**

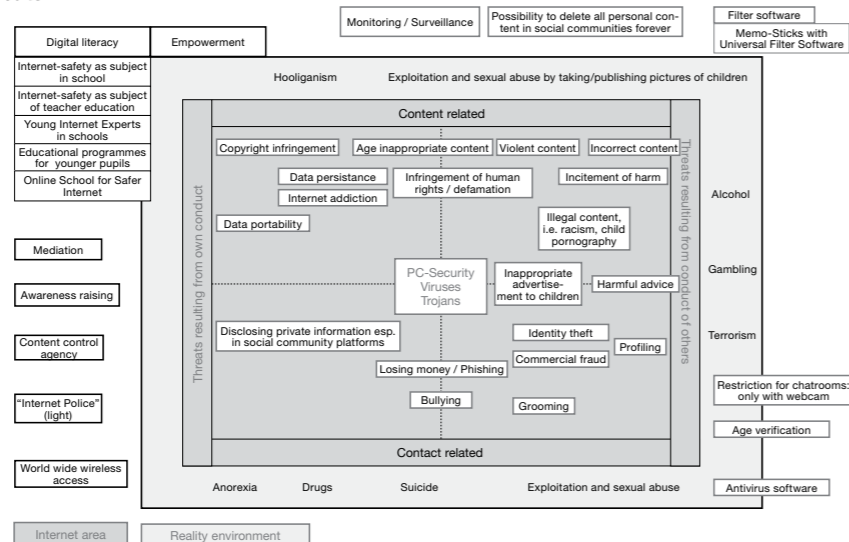
- geven pedagogische hulpverleners (docenten en zorgverleners) informatie over de relatie tussen specifieke online toepassingen of producten en de bijbehorende risico's (hoofdstuk A);
- beschrijven welke technologieën geschikt zijn voor bescherming van de jeugd op internet (hoofdstuk B);
- beschrijven waar aanvullende voorlichtingsmaatregelen nodig zijn voor een optimaal effect van deze technologieën op de bescherming van de jeugd (hoofdstuk C2-C7).



## A Risico's bij het gebruik van internet door kinderen en jongeren

De Youth Protection Roundtable heeft in kaart gebracht welke risico's internet met zich meebrengt en tegen welke gevaren de jeugd op internet zou moeten worden beschermd. De risico's zijn onderverdeeld in twee categorieën. Er zijn risico's die samenhangen met online content en risico's die samenhangen met online contact. Binnen deze categorieën kan er een verdeling gemaakt worden in risico's als gevolg van gedrag van de gebruiker zelf en risico's als gevolg van gedrag van anderen. Deze verdeling in soorten risico's is terug te vinden in onderstaande figuur, de matrix van risico's en bedreigingen. Sommige risico's blijken alleen te gelden voor specifieke leeftijdsgroepen. Deze kunnen alleen worden aangepakt met maatregelen die zijn afgestemd op de specifieke behoeften van die groep.

Matrix of risks and threats



### A1 Risico's bij online content

Bij online content is het belangrijk onderscheid te maken tussen illegale, schadelijke en ongeschikte content. Er is binnen Europa geen consensus over wat onder deze begrippen wordt verstaan. Toch zijn bepaalde typen content, zoals kinderpornografie, vrijwel overal ter wereld verboden.

#### 1.1 Content die ongeschikt is voor jonge kinderen

Internet biedt een schat aan informatie. Er is informatie te vinden over onderwerpen die voor iedereen interessant zijn, maar ook over onderwerpen die slechts voor specifieke gebruikers zijn bestemd. Niet alle content zou toegankelijk moeten zijn voor kinderen en jongeren. Daarom moet zorgvuldig worden bepaald welke content voor welke leeftijdsgroep geschikt is. Speciale aandacht is nodig voor content die niet illegaal is, maar wel ongeschikt voor jongere gebruikers, bijvoorbeeld pornografische content. Zeker wanneer jonge kinderen onbedoeld stuiten op deze content kan dit schadelijke

gevolgen hebben. Ongeschikte content kan om commerciële redenen worden geleverd, maar kan ook door gebruikers zelf worden gegenereerd. Toegang tot commerciële content is vaak beperkt tot besloten gebruikersgroepen. User-generated content daarentegen is meestal voor iedereen toegankelijk en behoeft daarom speciale aandacht. Veel kinderen en jongeren hebben toegang tot ongeschikte content. Tegenwoordig hebben velen onder hen immers een mobiele telefoon met multimediafunctionaliteit en internettoegang, en zij staan niet altijd onder toezicht van een volwassene. Door mobiele apparatuur kunnen kinderen bovendien altijd en overal hun eigen digitale content maken, en zo bijdragen aan de groeiende hoeveelheid user-generated content.

#### 1.2 Gewelddadige content

Ook gewelddadige content is niet voor elke leeftijd geschikt. Het effect van zulke content op de gebruiker hangt grotendeels af van diens leeftijd, internetconsumptie en sociale omgeving. Vooral jonge kinderen moeten worden beschermd tegen gewelddadige content op internet. Ook moeten zij beschermd worden tegen schadelijke content via andere media of in winkels. Kinderen en jongeren produceren en publiceren soms zelf gewelddadige content, zonder zich bewust te zijn van de schade die zij zo berokkenen.

#### 1.3 Illegale content (racisme, kinderpornografie)

Welk type content wordt geclassificeerd als illegaal, hangt af van nationale wetgeving. Sommige typen content, zoals kinderpornografie, zijn in de meeste landen verboden. Toch kunnen kinderen en jongeren, onbedoeld of opzettelijk, met illegale content in aanraking komen. Kinderen en jongeren kunnen ook slachtoffer zijn van illegale content doordat zij bijvoorbeeld het onderwerp zijn van pornografische foto's of films.

#### 1.4 Onjuiste content

Onjuiste content kan bijvoorbeeld worden aangetroffen in Wikipedia of in advertenties van niet-bestaande producten. Hoe groot het risico op confrontatie met deze content is, hangt af van andere gebruikers. Dit risico wordt vergroot door het groeiende aantal Web 2.0-toepassingen; de correctheid hiervan wordt hooguit door de gebruikers zelf gecontroleerd, niet door een redacteur. Ook tendentieuze content, content die opzettelijk is ontwikkeld om een bepaalde boodschap over te dragen, kan door onervaren jonge gebruikers voor waar worden aangenomen.

#### 1.5 Aanzetten tot kwaad

Er zijn veel websites die gebruikers ertoe aanzetten zichzelf kwaad te doen. Zo zijn er websites die zelfmoord, anorexia en sektarisme aanmoedigen. Met Web 2.0 en het groeiende aantal mogelijkheden voor publicatie van eigen content stijgt het risico op blootstelling aan zulke content. Vooral kinderen en jongeren zijn vaak niet in staat een realistische inschatting te maken van de risico's die zij lopen als ze de instructies op dergelijke websites opvolgen.

#### 1.6 Schending van mensenrechten/smaad

Door de anonimiteit van internet is het heel eenvoudig propaganda te verspreiden tegen bevolkingsgroepen of individuen. Bovendien gedragen mensen zich online anders dan in een directe confrontatie, waar zij de reactie van hun tegenstanders

of slachtoffers en de gevolgen van hun gedrag kunnen zien. Daarom is het risico van smaad en schending van mensenrechten op internet veel groter dan in de offline wereld. Deze content is vooral schadelijk voor kinderen en jongeren, omdat hun mening relatief makkelijk kan worden beïnvloed door misleidende informatie.

### 1.7 Ongeschikte advertenties en marketing

Kinderen lopen het risico advertenties en services te ontvangen of onder ogen te komen die niet voor hen geschikt zijn. Denk aan advertenties voor cosmetische chirurgie of vragen om deelname aan loterijen. Hoe meer persoonlijke gegevens kinderen op internet prijsgeven, zoals naam, leeftijd of geslacht, hoe meer kans zij op zulke advertenties en services lopen. Kinderen zijn zich vaak niet bewust van de consequenties die het invoeren van hun naam in een formulier of veld op internet heeft. Mobiele telefoons vormen een extra distributiekanaal voor advertenties.

### 1.8 Eeuwige ronddwalende gegevens

Eenmaal op internet gepubliceerde content kan zich snel verspreiden. Het is onmogelijk deze informatie achteraf volledig te verwijderen. Vooral kinderen en jongeren publiceren vaak teksten en foto's. Zij zijn zich meestal niet bewust van de korte- en langetermijengevolgen hiervan. Daarmee is het risico groot dat gegevens ongewenst blijven ronddwalen.

### 1.9 Overdraagbaarheid van gegevens

Gegevens die met opzet zijn opgeslagen op slechts één server of platform kunnen heel eenvoudig naar ontelbare andere servers worden overgezet. Dit gaat ten koste van de privacy, zonder dat gebruikers dit in de gaten hebben. Jongeren weten heel veel van de technische mogelijkheden van internet, maar de meeste overzien toch niet de gevolgen als hun privégegevens worden gecombineerd met andere gegevens over hen.

### 1.10 Inbreuk op het auteursrecht

Of gebruikers inbreuk maken op het auteursrecht, hebben zij vaak zelf in de hand. Maar bewuste inbreuk of niet, de inbreukpleger loopt het risico beboet te worden wegens fraude jegens de auteursgerechtigde.

## A2 Risico's bij online contact

### 2.1 Schadelijk advies

Op fora, blogs of andere platforms op internet kunnen gebruikers adviezen uitwisselen. Hier kunnen zij waardevolle steun vinden, maar ook eenvoudig contact leggen met onbekwame of zelfs gevaarlijke adviseurs. Kinderen en jongeren lopen meer risico schadelijk advies te krijgen op sociale netwerken of andere Web 2.0-toepassingen dan op andere websites.

### 2.2 Internetverslaving

Naarmate mensen langer online zijn, groeit het risico dat zij verslaafd raken aan internet. Vooral jongeren lopen het gevaar de computer niet meer te kunnen uitschakelen. Dit risico hangt daarom vooral samen met gedrag van de gebruiker.

### 2.3 Identiteitsdiefstal

Bij identiteitsdiefstal bemachtigt iemand de elektronische identiteit van een ander (bijvoorbeeld de gebruikersnaam en het wachtwoord) en maakt daarvan opzettelijk gebruik om fraude te plegen. Het risico op identiteitsdiefstal neemt toe: het aantal virtuele identiteiten groeit naarmate mensen meer online zijn en ook vaker gebruikmaken van op hen afgestemde services.

### 2.4 Phishing

Phishing is het vergaren van bankgegevens, vooral pin- en TAN-codes, om de bankrekening van anderen te plunderen. Jongeren lopen het meeste risico om een vervalste website niet te herkennen, en zodoende hun bankgegevens te bekend te maken.

### 2.5 Oplichterij

Er is sprake van oplichterij als personen goederen of diensten verkopen die na betaling niet in orde blijken of helemaal niet worden geleverd. Oplichterij kan ook het gevolg zijn van identiteitsdiefstal of phishing. Een andere vorm van oplichterij is de online verkoop van digitale services, bijvoorbeeld ringtones, tegen een onredelijke prijs. Dit is vaak gekoppeld aan een abonnement op de service, zonder dat de gebruiker dat beoogde. Kinderen en jongeren zijn zich vaak niet bewust van de consequenties van dergelijke contracten.

### 2.6 Grooming

Pedofielen gebruiken internet om in contact te komen met kinderen en jongeren. Ze houden hierbij geheim dat ze volwassen zijn. Ze baseren hun strategie vaak op het verlangen van kinderen naar vriendschap en vertrouwde. Op alle online platforms voor persoonlijk contact kan sprake zijn van grooming. De mobiele telefoon kan ook toegang geven tot bijvoorbeeld sociale netwerken. Kinderen zien mobiele telefoons als een deel van hun privéleven en zijn meestal alleen wanneer ze de telefoon gebruiken. Omdat er dan geen ouderlijk toezicht is, is het risico hierbij groter dat ze slachtoffer worden van grooming en gevaarlijke uitnodigingen.

### 2.7 Pesten

Pesten lijkt in allerlei vormen deel uit te maken van het leven van jonge mensen. Door de anonimiteit van internet is pesten eenvoudiger geworden. Kinderen en jongeren lopen niet alleen het risico om slachtoffer te worden van pesterijen maar ook om zelf te gaan pesten. Daarom hangt pesten samen met zowel gedrag van gebruiker zelf als gedrag van anderen. Hoewel het publiceren van bijvoorbeeld smadelijke foto's onderdeel kan zijn van pesten (online content), is het fenomeen toch vooral gerelateerd aan online contact.

Ook bij pesten spelen multifunctionele mobiele telefoons vaak een grote rol. Er worden bijvoorbeeld lasterlijke foto's mee gemaakt, met de bedoeling om te pesten. Deze foto's worden vervolgens op internet gezet of via MMS naar anderen gestuurd. Doordat zo veel kinderen en jongeren een mobiele telefoon met digitale camera hebben, is de kans groot dat deze telefoons pesten vereenvoudigen.



## 2.8 **Onthulling van persoonlijke gegevens**

Gebruikers die willen deelnemen aan een sociaal netwerk, worden uitgenodigd een profiel aan te maken. Daarin staan de persoonlijke gegevens waarmee zij zich binnen het netwerk presenteren. Ook in chatrooms en fora kunnen gebruikers privégegevens, zoals hun adres en telefoonnummer, onthullen aan anderen. Vooral jonge mensen kunnen de gevolgen van openbaarmaking van persoonlijke informatie niet overzien. Ze zijn zich er vaak niet van bewust dat een chatroom geen privé- maar een openbare ruimte is.

## 2.9 **Persoonsgegevens op sociale netwerksites**

Gebruikers maken steeds meer profielen van zichzelf aan, op verschillende platforms. Hierdoor neemt het risico toe dat persoonlijke gegevens van verschillende platforms worden samengevoegd of worden gecombineerd met gegevens die elders zijn ingevuld, bijvoorbeeld op stemsites of bij loterijen. Door deze gecombineerde gegevens kunnen gebruikers direct worden benaderd met mogelijk ongewenste content, services of advertenties. Gegevens kunnen worden verkregen van de website waarop de persoonlijke gegevens openlijk worden weergegeven. Gevaarlijker is het als gebruikersprofielen geheel of gedeeltelijk uit de database van de website worden gehaald en door de platformeigenaar worden verkocht aan derden.

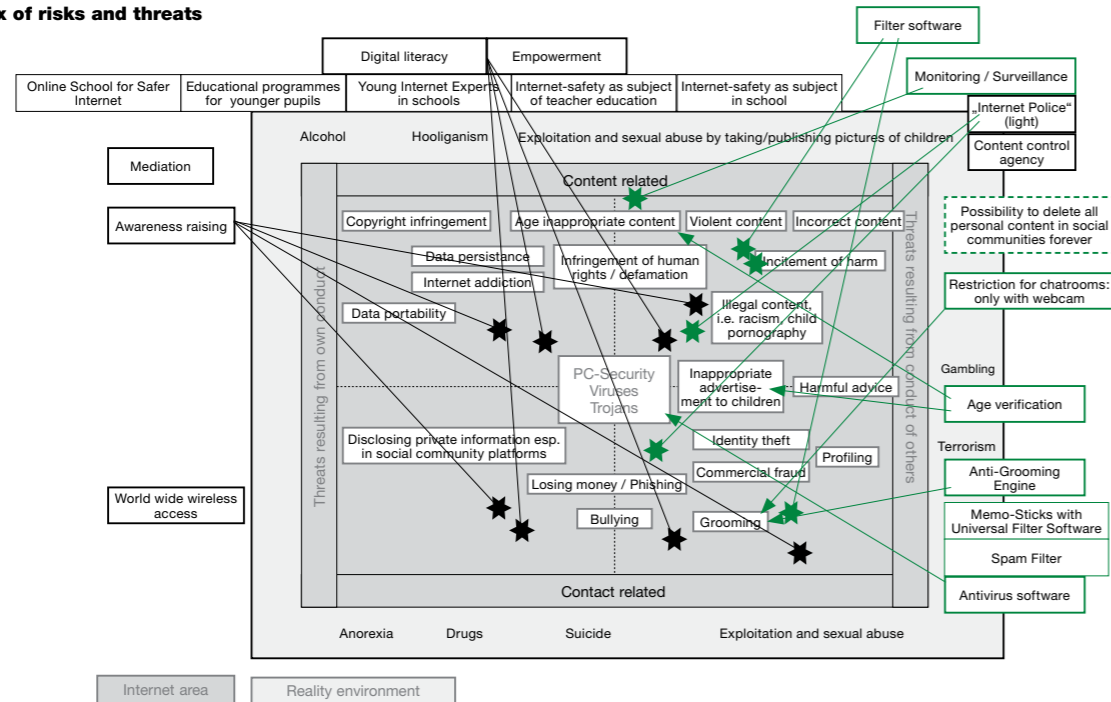


## B Beschikbare technologieën voor de bescherming van de jeugd

Er zijn verschillende technische middelen beschikbaar om de risico's aan te pakken die voortvloeien uit het gebruik van internet door kinderen en jongeren. De YPRT heeft recente bevindingen over de effectiviteit van deze middelen beoordeeld. In twee rondes werd de effectiviteit ingeschat, besproken en gevalideerd. Hierdoor werd een hoge mate van overeenstemming bereikt. De YPRT kwam tot de conclusie dat technische middelen pas echt effectief zijn als ze worden aangevuld met empowerment door mediawijsheid.

In de matrix met risico's en gevaren ziet u op welke gebieden deze technologieën effectief kunnen zijn.

Matrix of risks and threats



### B1 Filtersoftware

#### 1.1 Beschrijving en werkwijze

Met filtersoftware kan data worden geselecteerd en gefilterd. Dit elektronische middel kan kinderen en jongeren beschermen tegen illegale en potentieel schadelijke content. Men dient er echter rekening mee te houden dat jongeren technisch zeer bedreven zijn en veel filters eenvoudig kunnen omzeilen. Filterprogramma's gebruiken lijsten van geclassificeerde content of analyseren de content van websites via semantische en statistische methoden. Content kan via allerlei methoden worden geclassificeerd: er zijn zogenaemde *black lists* en *white lists*. (In Nederland is *MyBee*<sup>2</sup> een goed voorbeeld van

een white list methode, noot red.). Deze zijn opgesteld door de content provider, bijvoorbeeld via het ICRA-labelsysteem. Ook kunnen classificaties gecheckt worden door onafhankelijke organisaties, bijvoorbeeld het NICAM als beheerder van PEGI. Een andere manier om te classificeren is automatische analyse van content. Dit gebeurt bijvoorbeeld bij trefwoord-blokkering. De meeste filterprogramma's combineren verschillende manieren.<sup>3</sup>

Volgens de SIP-benchmark<sup>4</sup> kan er op verschillende niveaus worden gefilterd. Filtersoftware kan worden geïnstalleerd op de pc van de eindgebruiker, op een lokale server, bij de internetserviceprovider en elders op internet, bijvoorbeeld als internetfilterservice op een proxyserver.

Voor effectieve filtering is een combinatie van verschillende methoden vereist. De software kan de volgende methoden gebruiken:

- URL's blokkeren die staan vermeld op de black list die de provider heeft geleverd (lokale controle van black lists) of op de black list die te vinden is op de site van de provider (externe controle van black lists);
- URL's blokkeren die *niet* staan vermeld op de white list van de provider (lokale of externe controle van white lists);
- URL's blokkeren die één of meer trefwoorden bevatten die de gebruiker op de black list heeft geplaatst;
- content blokkeren die één of meer trefwoorden bevat die de gebruiker op de black list heeft geplaatst;
- delen van content wissen die overeenkomen met trefwoorden die de ouder of verzorger van het kind op de black list heeft geplaatst;
- URL's blokkeren met een ICRA-label dat de gebruiker op de black list heeft geplaatst (externe ICRA-controle);
- pagina's blokkeren met een ICRA-label dat de gebruiker op de black list heeft geplaatst (lokale ICRA-controle);
- specifieke applicaties uitschakelen (eventueel voor een bepaalde tijd);
- specifieke applicaties uitschakelen buiten het tijdslot dat de gebruiker heeft ingesteld;
- specifieke poorten uitschakelen.

Het filterproces heeft een aantal neveneffecten waarmee men rekening dient te houden. Zo kan de vrijheid van meningsuiting in het geding komen. Ook kan het leiden tot onbedoelde censuur. Daarnaast kan het gebeuren dat informatie onrecht wordt gefilterd, wat ten koste kan gaan van de kwaliteit en service.

#### 1.2 Effectiviteit

Filtersoftware wordt gezien als een effectief middel om de jeugd op internet te beschermen. Hoe concreter een type content of een type online gedrag kan worden gedefinieerd, hoe groter de kans dat het door filtersoftware wordt gedetecteerd. Naar schatting blokkeert filtersoftware ongeveer de helft van alle websites met *gewelddadige content* en *content die ongeschikt is voor jonge kinderen*. Bij *illegale content* is filtersoftware effectiever. Wat illegaal is, is namelijk makkelijker te definiëren. Om dezelfde reden – definitie van content – is filtersoftware niet effectief als het gaat om *onjuiste content*. De effectiviteit van filtersoftware op dit gebied wordt tamelijk gering geacht. De contenttypen *ongeschikte advertenties en*

2 Bron: [www.mybee.nl](http://www.mybee.nl)

3 Bron: [www.lusi.lu/index.php?id=16&L=1](http://www.lusi.lu/index.php?id=16&L=1)

4 Bron: Deloitte: [www.sip-bench.eu/Reports2007/SIP%20Bench%202007%20-%20Synthesis%20Report.pdf](http://www.sip-bench.eu/Reports2007/SIP%20Bench%202007%20-%20Synthesis%20Report.pdf)

*marketing* en *aanzetten tot kwaad* kunnen goed worden gedefinieerd. Daarom kan filtersoftware ze in bijna een derde van alle gevallen detecteren als content die moet worden geblokkeerd. Het is een grotere uitdaging om *schadelijk advies* te detecteren. Dit wordt vaak verstrekt in direct contact tussen gebruikers. Ook *grooming* wordt onvoldoende gedetecteerd door filtersoftware; naar schatting van de experts in een vijfde van de gevallen. Het risico van *onthulling van persoonlijke informatie*, dat zich ook vaker voordoet wanneer mensen online met elkaar in contact komen, kan volgens de experts van de YPRT slechts in een tiende van de gevallen worden aangepakt door filtersoftware. Risico's verbonden aan gedrag van de gebruiker zelf, zoals *inbreuk op het auteursrecht* en *internetverslaving*, kunnen slechts in beperkte mate worden aangepakt met filtersoftware. Ook bij risico's verbonden aan gedrag van andere gebruikers, zoals *identiteitsdiefstal* en *pesten* en bij risico's die verbonden zijn aan zowel eigen gedrag als gedrag van anderen, bijvoorbeeld bij *schending van mensenrechten/smaad*, biedt filtersoftware weinig soelaas; naar schatting in slechts een tiende van de gevallen. Volgens de experts kan filtersoftware een zesde van alle gevallen van *oplichterij* en *phishing* aanpakken. De effectiviteit lijkt lager te zijn bij *profilering op sociale netwerksites*.

## B2 Monitorsysteem

### 2.1 Beschrijving en werkwijze

Ook met een monitorsysteem kan veilig internetgebruik worden bevorderd. Met dit instrument wordt systematisch gezocht naar content en gebruikersactiviteiten, die vervolgens worden ingedeeld,<sup>5</sup> bijvoorbeeld in 'schadelijk' en 'onschadelijk'. Vervolgens rapporteert het systeem de resultaten aan een ouder, opvoeder of leerkracht. Onder 'monitoren' verstaan we het automatisch controleren van het proces van een gebruiker met systemen en services in een online omgeving<sup>6</sup>. De ouder, leerkracht of opvoeder kan aangeven of de content achteraf gefilterd moet worden. Met een monitorsysteem kunnen bijvoorbeeld chatsessies, blogteksten en het uploaden en uitwisselen van foto's worden beoordeeld. Technisch is het mogelijk monitoring te installeren bij de internetserviceprovider of bij de operator. Er zijn monitorsystemen die ongewenste online content detecteren.<sup>7</sup>

### 2.2 Effectiviteit

Door content en communicatie op internet te monitoren kan de inhoud tot op zekere hoogte worden beoordeeld. Er kan op verschillende momenten worden gemonitord: tijdens het opslaan en hosten van content, maar ook op het moment dat de gebruiker de content wil benaderen. Het wordt verondersteld dat de effectiviteit van monitoren hoger is dan die van filtersoftware op zichzelf. Dit omdat bij monitoren het besluit om online content uit te schakelen en *online gedrag te filteren* pas wordt genomen na aanvullende beoordeling. Monitoren is het effectiefst – in meer dan de helft van alle gevallen – bij *content die ongeschikt is voor jonge kinderen*. De effectiviteit bij *gewelddadige* en *illegale content* en bij *aanzetten*

<sup>5</sup> Bron: [Wikipedia de.wikipedia.org/wiki/Webmonitoring](https://de.wikipedia.org/wiki/Webmonitoring)

<sup>6</sup> Bron: [SiteScope193.138.212.37/SiteScope/docs/SiteScopeTerms.htm](https://SiteScope193.138.212.37/SiteScope/docs/SiteScopeTerms.htm)

<sup>7</sup> PEGI Online is een voorbeeld van een dergelijke systeem. Het ondertekenen van een PEGI Online Safety Code is verplicht voor het verkrijgen van het PEGI Online-label. Zie voor meer info [www.pegionline.eu](http://www.pegionline.eu)

*tot kwaad* is slechts iets lager: twee vijfde van alle gevallen wordt hiermee aangepakt. In naar schatting een derde van alle gevallen worden via monitoring *schadelijk advies*, *schending van mensenrechten/smaad*, *ongeschikte advertenties* en *marketing* en *grooming* gedetecteerd. Naar schatting wordt meer dan een kwart van alle *phishing*-aanvallen door monitoring gedetecteerd, en ook meer dan een derde van alle gevallen van *pesten*. Bij *onjuiste content*, *inbreuk op het auteursrecht*, *oplichterij*, *identiteitsdiefstal* en *onthulling van persoonlijke informatie* wordt de effectiviteit echter geschat op slechts 20 procent. De effectiviteit van monitoring bij *internetverslaving* wordt tamelijk klein geacht; zij is slechts effectief in een van de zes gevallen. Monitoring scoort weer wat hoger dan filtersoftware bij *eeuwig ronddwalende gegevens*, *overdraagbaarheid van gegevens* en *persoonsgegevens op sociale netwerksites*. Toch is de mate van effectiviteit voor alle drie minder dan 10 procent.

## B3 Leeftijdsverificatie

### 3.1 Beschrijving en werkwijze

Leeftijdsverificatie speelt een belangrijke rol bij het beperken van de toegang van minderjarigen tot specifieke content of tot platforms die contactmogelijkheden bieden. Er bestaan verschillende systemen om de leeftijd van internetgebruikers te verifiëren en ervoor te zorgen dat zij content en services aangeboden krijgen die voor hen geschikt zijn. Leeftijdsverificatie kan buiten internet plaatsvinden. Hiervoor identificeert de gebruiker zich eenmalig. Geavanceerde systemen voor identificatie en leeftijdsverificatie zijn gebaseerd op de combinatie van een token (kaart of stick) en kennis (pincode of wachtwoord). Alleen als iemand over beide beschikt, kan hij aantonen dat hij de wettige eigenaar is van de identiteit en dus bewijzen dat hij tot een bepaalde leeftijdsgroep behoort. Dit type technische leeftijdsverificatie kan erg effectief zijn. Hiervoor is wel specifieke technische apparatuur (bijvoorbeeld een kaartlezer) en bijbehorende juridische regelgeving vereist. Op dit moment staat de wetgeving in veel Europese landen leeftijdsverificatie van volwassenen het toe om minderjarigen toegang tot content voor volwassenen te weigeren. Er zijn slechts enkele concepten voor leeftijdsverificatie van minderjarigen. België kent bijvoorbeeld de Kids-ID, die redelijk goed kan garanderen dat alleen minderjarigen toegang hebben tot speciale internetgebieden, zoals chatrooms voor kinderen.

### 3.2 Effectiviteit

Aangezien met leeftijdsverificatie de toegang tot specifieke content of gebieden van internet kan worden beperkt, is het vanzelfsprekend dat leeftijdsverificatie effectiever is bij *content die ongeschikt is voor jonge kinderen* (bijna de helft van alle gevallen) en *gewelddadige content* dan bij andere risicovolle content. Bij *illegale content* en *ongeschikte advertenties* en *marketing* is leeftijdsverificatie naar verwachting effectief in een vijfde tot een kwart van de gevallen. Leeftijdsverificatie zou, naar men aanneemt, in slechts een van de zeven gevallen van *grooming* kunnen belemmeren. Ook *aanzetten tot kwaad* kan door deze technologie niet goed worden aangepakt. Leeftijdsverificatie is weinig effectief tegen risico's als *schadelijk advies*, *phishing* en *oplichterij*. Aangenomen wordt dat zij bij alle andere risico's bijna even ineffectief is.

## B4 Overige technische middelen

Er zijn naast leeftijdsverificatie nog andere middelen die specifiek zijn voor speciale risico's. Met een *tijdslot* kan het com-

putergebruik worden beperkt tot een vaste tijdsduur, waarna het apparaat automatisch wordt uitgeschakeld. Een tijdslot is niet specifiek ontwikkeld voor het bestrijden van *internetverslaving*, maar kan hierbij erg nuttig zijn. De experts schatten in dat met tijdcontrole de helft van de gevallen van internetverslaving kan worden aangepakt. *Automatische verificatieprocessen*, waaronder ook leeftijdsverificatie valt, hebben meestal betrekking op iets wat de persoon bezit, zoals een identiteitskaart; iets wat de persoon weet, zoals een pincode of wachtwoord; of iets wat de persoon doet, zoals een vingerafdruk plaatsen. Verificatieprocessen die moeten voldoen aan hoge vereisten zijn vaak gebaseerd op asymmetrische cryptografie, zoals digitale handtekeningen. Volgens de experts kunnen automatische verificatieprocessen meer dan een derde van de gevallen van *identiteitsdiefstal* voorkomen. *Antiphishingsoftware* is een speciaal type filtersoftware dat is ontwikkeld om gevallen van *phishing* te detecteren en verhinderen. De meningen over de effectiviteit ervan zijn verdeeld: sommige experts vinden deze software erg effectief (twee derde van alle gevallen), terwijl andere menen dat de software in niet meer dan een kwart van de gevallen effectief is.

*Digitale-watermerktechnologie*<sup>8</sup> kan een oplossing zijn om *inbreuk op het auteursrecht* te voorkomen. Onder watermerktechnologie verstaan we hier: de implementatie van een stuk code in digitale content. Om te detecteren waar de content zich bevindt, of waar naartoe deze is gekopieerd of verspreid, is daarnaast een programma nodig dat het watermerk kan herkennen. Naar schatting zou in een kwart van de gevallen inbreuk op het auteursrecht kunnen worden voorkomen met watermerktechnologie. Soms is het waardevol dat niet mogen worden veranderd of als ze op een ander systeem moeten kunnen worden overgezet. Toch kan dit problemen opleveren voor gebruikers. Niet iedereen wil dat alle persoonlijke gegevens permanent ergens zijn opgeslagen en altijd kunnen worden opgevraagd. Zoals hiervoor beschreven, zijn bijna alle bekende technische middelen ontoereikend als het gaat om de risico's van 'ongewenste' gegevenspersistentie en overdraagbaarheid van gegevens. *Codering* kan een middel zijn om ongewenste *overdraagbaarheid van gegevens* te voorkomen. Hierbij worden gegevens omgezet in een ander format. De gecodeerde gegevens moeten worden gedecodeerd voor ze kunnen worden overgezet op een ander systeem, om bijvoorbeeld te worden samengevoegd met andere gegevens. De experts schatten dat met codering ongewenste gegevensoverdracht in ongeveer de helft van de gevallen kan worden voorkomen. In een kwart van alle gevallen kan het instellen van een *vervaldatum* voor alle door *user-generated content* het risico van *eeuwig rondwalende gegevens* enigszins verminderen. Ook een niet te verwijderen tag met een vervaldatum zou dit risico omlaag kunnen brengen. In een zogenoemde *antigrooming-engine*<sup>9</sup> worden verschillende methoden gecombineerd om ongewoon gedrag te detecteren en *grooming* in chatrooms te voorkomen. De engine werkt vanuit een database met profielen van gedrag van echte groomers en echte kinderen. Deze profielen worden ontwikkeld op basis van een analyse van de communicatie. Er wordt vooral gekeken naar woordkeuze, interpunctie, zinslengte, typesnelheid en agressieniveau. Aan de hand van deze profielen, die regelmatig worden bijgewerkt, kan de engine een groomer detecteren. Als hier aanwijzingen voor zijn, wordt de verantwoordelijke volwassene gealarmeerd via sms, e-mail of een waarschuwingsvenster op de pc. Dit middel wordt verondersteld effectief te zijn in ongeveer twee vijfde van alle gevallen. Dit betekent dat het waarschijnlijk even effectief is tegen grooming als monitoring.

<sup>8</sup> Bron: [www.copyrightinfo.eu](http://www.copyrightinfo.eu)

<sup>9</sup> Bron: [www.crispthinking.com](http://www.crispthinking.com)



## C Aanbevelingen voor de bescherming van de jeugd op internet

De aanbevelingen van de Youth Protection Roundtable (YPRT) voor betere bescherming van de jeugd op internet zijn bedoeld voor politieke besluitvorming en voor Internetserviceproviders, hard- en softwareontwikkelaars en mensen die voorlichting en training geven aan ouders, kinderen, docenten en zorgverleners. De aanbevelingen zijn niet bindend. Ze zijn ondergebracht in verschillende categorieën, elk van belang voor verschillende belanghebbenden.

### C1 Verbetering van ondersteunende technologieën

Bestaande technologieën voor veilig internetgebruik – bijvoorbeeld filtersoftware, databases en identificatie- en verificatiesystemen – worden vaak niet optimaal ingezet om de jeugd te beschermen. Er moet dus meer van de technische mogelijkheden gebruik worden gemaakt. Dit kan worden bereikt door technische verbeteringen, maar ook door betere samenwerking tussen de verschillende belanghebbenden, zoals internetserviceproviders, softwareontwikkelaars, onderzoekers en regelgevende instanties.

De Youth Protection Roundtable moedigt technische verbeteringen en betere samenwerking aan. Zij adviseert de volgende verbeteringen:

- regelmatig updaten van *black lists* en *white lists*;
- implementeren van bestaande lijsten die zijn goedgekeurd door nationale overheden en die in het betreffende land zijn geïmplementeerd, zoals de zogenoemde BPJM-module in Duitsland. Om misbruik van deze lijsten te voorkomen worden ze nooit openbaar gemaakt;
- verbeteren van de onderlinge uitwisselbaarheid van classificatiesystemen;
- bevorderen van classificaties door gebruikers, opgeslagen in een database die alle belanghebbenden mogen gebruiken voor een goed doel;
- zorgen voor correcte rapportage van filteractiviteiten in logboeken;
- verbeteren van de bruikbaarheid van logboeken (door softwareondersteunde analyse van logboeken);
- verbeteren van intelligente software/kunstmatige intelligentie;
- verbeteren van filtersoftware, zodat die in alle browsers goed werkt;
- verbeteren van ondersteunende technologieën, zodat die op alle apparaten met toegang tot internet (pc, mobiele telefoon, spelsysteem enzovoort) goed werken.

### C2 Verbetering van de bruikbaarheid van filtersoftware

Hoe effectief filtersoftware is, hangt grotendeels af van de gebruiker: is hij in staat het programma te installeren, te configureren en aan te passen aan zijn behoeften? De Youth Protection Roundtable stelt daarom voor de bruikbaarheid van filtersoftware te verbeteren. Dit kan worden bereikt met het:

- vooraf installeren van filtersoftware op apparatuur die wordt gebruikt voor internettoegang (pc, spelsysteem of mobiel apparaat) of levering van deze software als onderdeel van een service. De software is bij voorkeur standaard ingeschakeld: opt-out in plaats van opt-in;
- voorkomen van conflicten met andere software (bijvoorbeeld antivirussoftware);

- voorkomen dat filtersoftware omzeild kan worden op het apparaat van de eindgebruiker (bijvoorbeeld via spelfouten, andere talen en alternatieve browsers of netwerken);
- zorgen voor heldere installatie- en updateprocedures;
- zorgen voor begrijpelijke dialoogvensters met uitleg/begeleiding;
- zorgen voor volledig transparante en begrijpelijke filters;
- informeren over de filterprocessen, vooral over:
  - het feit dat filtersoftware op de computer wordt geïnstalleerd;
  - de basis waarop de filtersoftware werkt (bijvoorbeeld een black of white list met URL's of woorden);
  - de filtercriteria;
  - de reden dat specifieke content is gefilterd;
  - de geschatte effectiviteit van filtersoftware bij de verschillende soorten content en communicatie;
  - de manier waarop blokkades en filtering ongedaan gemaakt kunnen worden;
  - de plaats waar klachten over onjuiste blokkade van content kunnen worden gerapporteerd.
- zorgen voor een gebruikersvriendelijk filter met informatie over de manier waarop gebruikers het kunnen aanpassen aan hun behoeften en die van hun kinderen;
- bieden van een optie om filterinstellingen te importeren en exporteren, zodat ouders en docenten deze makkelijker kunnen delen;
- tegemoetkomen aan de vraag om consistente, transparante en begrijpelijke filterprocedures, en vooral inconsistente filterresultaten vermijden.

### C3 Verbetering van internettoepassingen

Mediawijsheid is de sleutel tot veilig gebruik van internettoepassingen. Daarom is voorlichting cruciaal. Technologie kan hierbij een ondersteunende rol spelen door ervoor te zorgen dat de gebruiker zich continu bewust is van zijn gedrag: gebruikt hij internet verantwoord en vermijdt hij onveilig of ongepast gedrag? De aanbevelingen zijn als volgt:

- zorgen dat gebruikersprofielen alleen zichtbaar zijn voor bekenden, tenzij gebruikers expliciet aangeven dat iedereen hun profiel mag zien;
- steunen van gebruikers bij wachtwoordbeheer, bijvoorbeeld met een controlevraag;
- bieden van een optie om tags te verwijderen van content in het profiel van de gebruiker;
- toevoegen van een knop waarmee schadelijke content kan worden gemeld, bij voorkeur rechtstreeks aan hotlines en hulplijnen, op alle sites met user-generated content;
- waarschuwen via pop-up of mouse-over wanneer persoonlijke gegevens worden ingevoerd;
- waarschuwen via pop-up of mouse-over over inbreuk op mensenrechten/smaad, bijvoorbeeld bij het uploaden van foto's;
- automatisch verwijderen van content na de vervaldatum die de gebruiker heeft ingesteld;
- toevoegen van een knop waarmee de gebruiker zijn gegevens kan verwijderen, op alle sites waar gebruikers persoonlijke gegevens invoeren. Eenmaal gepubliceerde content kan nooit helemaal worden verwijderd;
- koppelen van een vervaldatumtag aan user-generated content, zodat deze altijd wordt verwijderd, ook wanneer de informatie wordt gekopieerd;

- bieden van technische ondersteuning om ongewenst kopiëren van online gepubliceerde teksten en foto's te voorkomen;
- bieden van een optie om vóór het uploaden gps-gegevens te verwijderen uit foto's, zodat onbedoelde onthulling van plaatsgegevens wordt vermeden;
- zorgen dat passieve gps-localisatieservices alleen met toestemming van de eigenaar mogen worden aangeboden aan derden;
- aangeven of de communicatie op internet openbaar of privé verloopt;
- gebruiken van woordfilters bij rechtstreekse communicatie tussen gebruikers op plaatsen waar kinderen rechtstreeks worden benaderd (forums, e-cards);
- bieden van een optie voor ouders om het internetgebruik – tijd, gedrag en communicatie – van hun kinderen in de gaten te houden. De privacy van de kinderen moet hierbij worden gerespecteerd;
- bieden van een optie om persoonlijke gegevens te coderen;
- bieden van digitale opsporingsmogelijkheden (*footprints*) voor gegevens van gebruikers die bezwaar hebben tegen opslag en gebruik hiervan;
- zorgen dat woordfilters de tekstbeschrijving voor advertentiebanneren kunnen lezen;
- zorgen voor betrokkenheid bij de ontwikkeling en invoering van veiligheidsmaatregelen.

#### C4 Overeenstemming over beleid tussen providers en exploitanten

De Youth Protection Roundtable stimuleert internet-serviceproviders beleid te voeren dat gericht is op veilig gebruik van internet door kinderen en jongeren. Dit beleid moet worden afgestemd op hun diensten en worden uitgevoerd binnen hun financiële, technische en organisatorische mogelijkheden. De YPRT adviseert:

beleid en procedures voor de afhandeling van gemelde overtredingen, vooral voor het bepalen van de snelheid waarmee een service wordt uitgeschakeld of content wordt gefilterd;

- beleid voor eenvoudig traceren en afhandelen van klachten van gebruikers;
- beleid voor menselijke tussenkomst overal waar gebruikers online en rechtstreeks met elkaar communiceren;
- beleid voor het reguleren van zoekopdrachten (wanneer bijvoorbeeld in een zoekmachine gezocht wordt op 'anorexia', kunnen bovenaan in de zoekresultaten beter sites verschijnen met informatie over hulpverlening in plaats van 'proanasesites');
- beleid voor samenwerking met welzijns- en hulporganisaties;
- beleid voor samenwerking tussen hotlines, politie en providers;
- beleid voor opslaan, kopiëren en verspreiden van gebruikersgegevens;
- beleid voor advertenties;
- overeenstemming over de vraag of op het hiervoor genoemde beleid intern wordt toegezien of door een onafhankelijke instantie.

#### C5 Mediawijsheid

De Youth Protection Roundtable wil mediawijsheid verbeteren, zowel van kinderen en jongeren als van degenen die voor hen verantwoordelijk zijn. Onder mediawijsheid verstaan wij kennis van digitale media, kennis van technologieën die de

jeugd kunnen beschermen en het vermogen om van beide te profiteren. In dit informatietijdperk wordt *empowerment* gezien als het belangrijkste beschermingsschild voor kinderen en jongeren. De Youth Protection Roundtable pleit daarom voor het:

- vergroten van kennis van technische applicaties voor internettoegang (met speciale aandacht voor nieuwe gebieden, bijvoorbeeld mobiele toegang);
- vergroten van kennis van ondersteunende technologieën en hulpmiddelen;
- vergroten van bekendheid van hotlines en hulplijnen voor het melden van illegale of schadelijke content;
- geven van voorlichting over kritisch omgaan met content;
- geven van voorlichting over privacy- en gegevensbescherming;
- oprichten van een online school voor veiliger internet (website en online lespakket), in nauwe samenwerking met bestaande online initiatieven;
- trainen van jonge internetexperts op scholen en instellingen voor maatschappelijk werk;
- invoeren van internetveiligheid als vak op school en vakoverstijgende behandeling van veilig internetgebruik;
- ontwikkelen van bemiddeling tussen slachtoffers en daders van pesterijen;
- geven van voorlichting over digitaal burgerschap: gebruikmaken van technologie op een autonome en verantwoordelijke manier;
- promoten van veilig internetgebruik als onderdeel van de opleiding voor docenten en maatschappelijk werkers;
- trainen van mediators en moderators;
- trainen van professionals op scholen en andere professionals die met kinderen en jongeren werken;
- bieden van hulp aan schoolhoofden bij het opzetten van een veiligheidsconcept op school en bij het verbeteren van veiligheid, privacy, gegevensbeveiliging en mediawijsheid;
- opstellen van huisregels voor het gebruik van digitale media in onderwijsinstellingen en openbare gelegenheden voor internettoegang. Jongeren kunnen helpen bij het opstellen van de regels;
- ontwikkelen van materiaal om mediawijsheid te verbeteren, in nauwe samenwerking met bestaande aanbieders;
- stimuleren van kinder- en jongerenactiviteiten die te maken hebben met veiliger internetgebruik, bijvoorbeeld door wedstrijden te organiseren en hen te betrekken bij de ontwikkeling van materiaal.

#### C6 Bewustwording

Voor de *empowerment* is bewustwording cruciaal. Daarom moeten mensen attent worden gemaakt op zowel de risico's als de kansen die internet biedt. De Youth Protection Roundtable benadrukt de positieve effecten van internetgebruik op de ontwikkeling van jonge mensen. Bij het creëren van meer bewustzijn moet ingezet worden op alle groepen in de samenleving, ongeacht leeftijd, geslacht en etnische achtergrond. De aanbevelingen van de YPRT zijn:

- benadrukken van de positieve effecten die internetgebruik heeft op de ontwikkeling van jonge mensen;
- organiseren van informatiedagen voor jongeren, zoals de Safer Internet Day;
- ontwikkelen van gedrukt en online materiaal speciaal voor:
  - kinderen en jongeren,
  - volwassenen die zorg dragen voor minderjarigen,

- internetserviceproviders,
- contentproviders,
- providers van sociale netwerken,
- organiseren van bewustwordingscampagnes voor jongeren;
- vergroten van kennis over de mogelijkheid misbruik te rapporteren aan hotlines en helplijnen;
- trainingen in mediawijsheid.

## **C7 Onderzoek**

Onderzoek vormt de basis voor het ontwikkelen van technische hulpmiddelen en voorlichtingsprogramma's. Daarom raadt de YPRT het volgende aan:

- steun van kwantitatief en kwalitatief onderzoek naar het online gedrag van kinderen en jongeren;
- promotie van beschikbaar onderzoek en steun voor pan-Europese uitwisseling van onderzoeksresultaten op het gebied van mediagebruik door kinderen en jongeren;
- steun van onderzoek dat bestudeert hoe kinderen en jongeren zich aan media aanpassen;
- evaluatie van het gebruik van digitale media.

## **C8 Juridische regelgeving**

De Youth Protection Roundtable stelt voor over te gaan tot harmonisering en concretisering van bestaande wetten en regels. Hierbij moet rekening worden gehouden met de verschillen in nationale wetten en culturen. Zij is voorstander van het:

- harmoniseren en concretiseren van regelgeving voor het recht user-generated content en profielen op socialenetwerksites te verwijderen;
- harmoniseren en concretiseren van regelgeving voor het recht op privacy,
- harmoniseren en concretiseren van regelgeving voor de vervolging van online overtredders;
- harmoniseren en concretiseren van de wettelijke definitie van 'illegale content' en 'voor kinderen schadelijke content'.

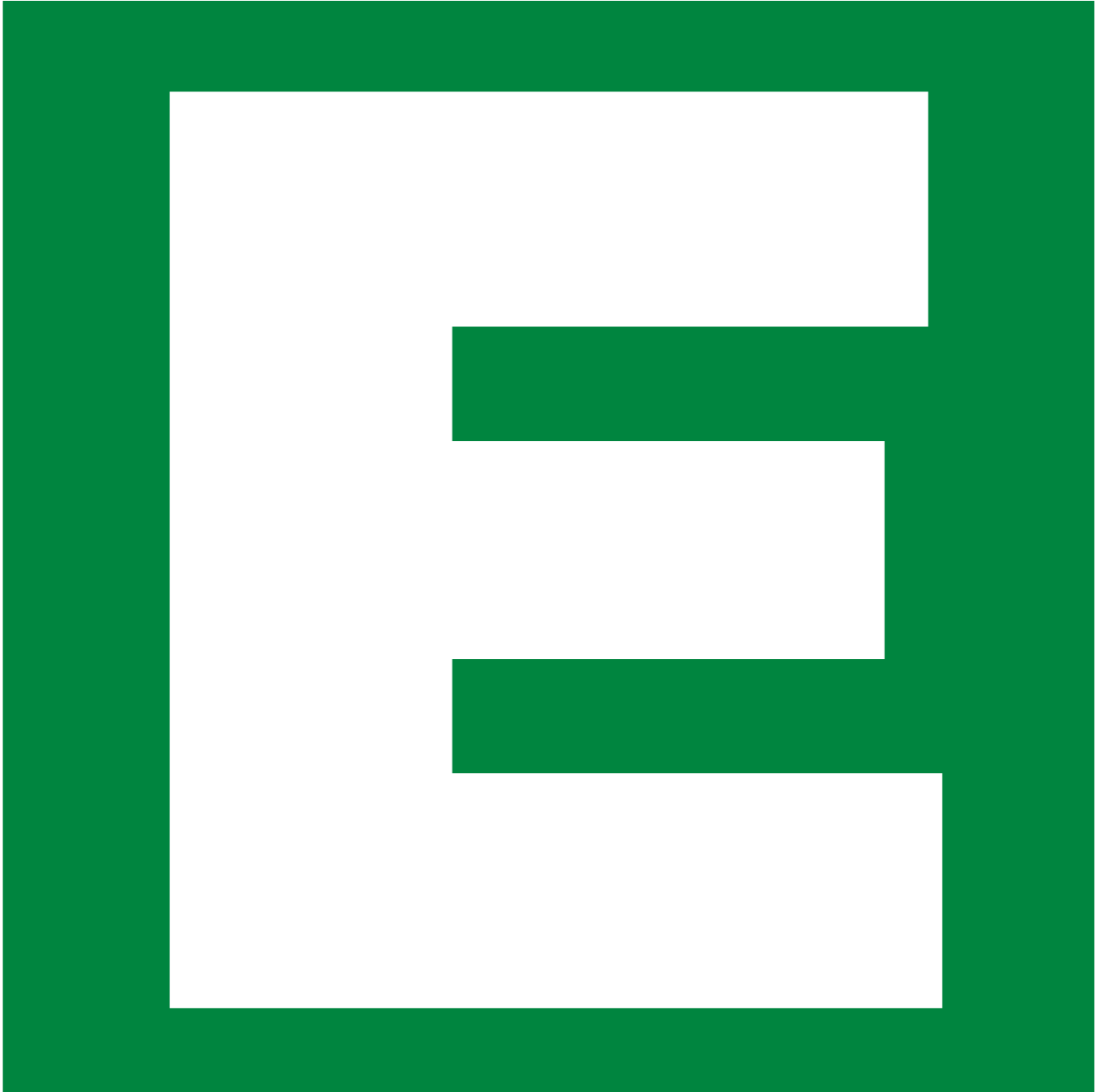


**D****Bronnen**

- Code for the ChatCheck Badge by the Association of Danish Internet Media (2007)
- Comparing Children's Online Activities and Risks across Europe. A Preliminary Report Comparing Findings for Poland, Portugal and UK, June 2007
- Crisp Thinking Group Ltd. (2005). Anti-Grooming Engine™. Retrieved January 21, 2009 from <http://www.crispthinking.com/anti-grooming-engine.htm>
- ENISA - Children on virtual worlds – What parents should know, September 2008
- ENISA - Photo Sharing, Wikis, Social Networks –Web 2.0 and Malware 2.0, EU Agency issues Position Paper on security for the next generation web, December 2008
- ENISA Position Paper No.1: Security Issues and Recommendations for Online Social Networks, October 2007
- ENISA - Technology-induced challenges in Privacy & Data Protection in Europe, October 2008
- Euro Media Literacy: Charter for Media Literacy (2005)
- EurActiv.com (2008). Web 2.0: New opportunities, new risks. Retrieved September 4, 2008 from <http://www.euractiv.com/en/infosociety/web-20-new-opportunities-new-risks/article-171600>
- Eurobarometer (2006). Eurobarometer on Safer Internet: quantitative surveys 2005-2006. Retrieved January 27, 2009 from [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm)
- Eurobarometer (2007). Eurobarometer on Safer Internet for Children: qualitative study 2007. Retrieved January 21, 2009 from [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm)
- Flash Eurobarometer survey (2008). Towards a Safer Use of the Internet for children in the EU - a parents' perspective. Retrieved January 27, 2009 from [http://ec.europa.eu/information\\_society/activities/sip/eurobarometer/index\\_en.htm](http://ec.europa.eu/information_society/activities/sip/eurobarometer/index_en.htm)
- Institute for Public Policy Research (ippr): Behind the Screen, the hidden life of youth online, March 2008- 10-20
- Internet Filters, a Public Policy Report by the Brennan Center for Justice, 2006
- JFF – Institut für Medienpädagogik in Forschung und Praxis. Untersuchung der Akzeptanz des Jugendmedienschutzes aus der Perspektive von Eltern, Jugendlichen und pädagogischen Fachkräften. Eigenständige Teilstudie des JFF zur Analyse des Jugendmedienschutzesystems, München, August 2007
- Luxembourg Safer Internet Helpline Project 2006, para.1, Definition von Filtersoftware [Electronic version]. Retrieved January 21, 2009 from <http://www.lusi.lu/index.php?id=16&L=1>
- Media Literacy – An Alternative to censorship by the Free Expression Policy Project, 2003
- Mercury Interactive Corporation (2004). SiteScope User's Guide, Version 7.9.5.0. para. 14, Monitoring. Retrieved January 21, 2009 from <http://mon15ny450.doubleclick.net/SiteScope/docs/SiteScopeTerms.htm>
- Niedersächsische Landesmedienanstalt. Helmut Volpers (Hrsg.). Funktionsweise des Internets und sein Gefährdungspotenzial für Kinder und Jugendliche. Ein Handbuch zur Medienkompetenzvermittlung. NLMBand 17, 2004
- Ofcom. Social Networking. A quantitative and qualitative research report into attitudes, behaviours and use, April 2008
- Paris Agenda or 12 Recommendations for Media Education, Paris, UNESCO, 21-22 June 2007

- Photopatrol (2007). Mehr Schutz und Erfolg für Ihre Bilder durch digitale Signaturen. Retrieved January 21, 2009 from [http://www.photopatrol.eu/fileadmin/templates/Hilfe\\_Texte/Informationen\\_ueber\\_Photopatrol\\_Download\\_-\\_V.1.pdf](http://www.photopatrol.eu/fileadmin/templates/Hilfe_Texte/Informationen_ueber_Photopatrol_Download_-_V.1.pdf)
- Protecting Children Using the Internet – Opinion by the European and Social Committee, May 2008
- Public consultation of the European Commission in regard to Age Verification, Cross Media Rating and Classification, Online Social Networking, July 2008
- Recommendation CM/Rec (2008) 6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters (May 2008)
- Resolution on Children's Online Privacy (30th International Conference of Data Protection and Privacy Commissioners – Strasbourg), October 17, 2008
- Resolution on Privacy Protection in Social Network Services (30th International Conference of Data Protection and Privacy Commissioners – Strasbourg), October 17, 2008
- Safer Children in a Digital World – The report of the Byron Review, March 2008
- Schulen ans Netz e.V. IT works. Jugendmedienschutz Filterlösungen im schulischen Umfeld, Bonn 2005
- SIP Benchmark Synthesis Report 2007 Edition by Deloitte Enterprise Risk Services, December 2007
- SIP Benchmark Synthesis Report 2008 Edition by Deloitte Enterprise Risk Services, November 2008
- Good practice guidance for the providers of social networking and other user interactive services 2008, March 2008
- Good Practice Guidance for Moderation of Interactive Services for Children, December 2005
- Good practice guidance for search service providers and advice to the public on how to search safely, December 2005
- Good Practice Models and Guidance for the Internet Industry On: Chat Services, Instant Messaging, Webbased Services, January 2003
- United Nations Convention on the Rights of the Child signed 1989
- Universität Leipzig. Medienkonvergenz Monitoring Report 2008, Jugendliche in konvergierenden Medienwelten
- Wikipedia Encyclopaedia (2009). Webmonitoring. Retrieved January 21, 2009 from <http://de.wikipedia.org/wiki/Webmonitoring>





## E Overzicht zelfregulering

### E1 Zelfregulerende organisaties in Europa

Name of organisation	Type of organisation	Geographical scope	Content-related scope	URL
Austrian E-Commerce Trust Mark	Association	Austria	web	<a href="http://www.guetezeichen.at/">http://www.guetezeichen.at/</a>
Internet Ombudsmann	Association	Austria	web	<a href="http://www.ombudsmann.at/">http://www.ombudsmann.at/</a>
Asociace provozovatelů mobilních sítí	Association of Mobile Network Operators	Czech Republic	mobile	<a href="http://www.apms.cz/Default.aspx?ModuleId=379&amp;ID=156">http://www.apms.cz/Default.aspx?ModuleId=379&amp;ID=156</a>
Sdružení pro internetovou reklamu v ČR, z.s.p.o. (SPIR)	Association of Internet advertising	Czech Republic	web	<a href="http://www.spir.cz">http://www.spir.cz</a>
Association of eCommerce	Association	Czech Republic	web	<a href="http://www.certifikovany-obchod.cz/o-apek-certifikaci">http://www.certifikovany-obchod.cz/o-apek-certifikaci</a>
Media Council for Children and Young People	Association	Denmark	movies	<a href="http://www.medieraadet.dk/">http://www.medieraadet.dk/</a>
European Internet Coregulation Network	Association	Europe	web	<a href="http://network.foruminternet.org/">http://network.foruminternet.org/</a>
Interactive Software Federation of Europe (ISFE)	Association of Companies	Europe	interactive software	<a href="http://www.isfe-eu.org/">http://www.isfe-eu.org/</a>
Freiwillige Selbstkontrolle Multi-media Diensteanbieter e.V.	Association of Companies	Germany	web	<a href="http://www.fsm.de">www.fsm.de</a>
Freiwillige Selbstkontrolle Fernsehen e.V.	Association of Companies	Germany	TV	<a href="http://www.fsf.de">www.fsf.de</a>
Spitzenorganisation der Filmwirtschaft e.V.	Association of Companies	Germany	movies	<a href="http://www.spio.de">www.spio.de</a>
Unterhaltungssoftware Selbstkontrolle	Association of Companies	Germany	interactive software	<a href="http://www.usk.de">www.usk.de</a>
Deutscher Presserat	Association of Companies	Germany	all media	<a href="http://www.presserat.de/">http://www.presserat.de/</a>
Deutscher Werberat	Association of Companies	Germany	advertisement	<a href="http://www.werberat.de/">http://www.werberat.de/</a>
Freiwillige Selbstkontrolle Telefonmehrwertdienste e.V.	Association of Companies	Germany		<a href="http://www.fst-ev.org/">http://www.fst-ev.org/</a>

Name of organisation	Type of organisation	Geographical scope	Content-related scope	URL
Beschwerdestelle / Deutschland sicher im Netz	Working group of Association of Companies	Germany	web	<a href="http://www.eco.de/servlet/PB/menu/1020202_11/index.html">http://www.eco.de/servlet/PB/menu/1020202_11/index.html</a>
ICRA Deutschland	Association of Companies	Germany	web	<a href="http://www.eco.de/servlet/PB/menu/1211767_11/index.html">http://www.eco.de/servlet/PB/menu/1211767_11/index.html</a>
Kommission für Jugendmedienschutz	Authority	Germany	all media	<a href="http://www.kjm-online.de/public/kjm/">http://www.kjm-online.de/public/kjm/</a>
Bundesprüfstelle für jugendgefährdende Medien	Federal Authority	Germany	all media	<a href="http://www.bundespruefstelle.de/">http://www.bundespruefstelle.de/</a>
Freiwillige Selbstkontrolle der Chatbetreiber	Association of Companies	Germany	web	<a href="http://www.fsm.de/de/Chat">http://www.fsm.de/de/Chat</a>
Automaten-Selbst-Kontrolle (ASK)	Association	Germany	interactive software	<a href="http://www.automaten-selbstkontrolle.de">http://www.automaten-selbstkontrolle.de</a>
Arbeitsgemeinschaft der Landesmedienanstalten (ALM)	Association	Germany	all media	<a href="http://www.alm.de">http://www.alm.de</a>
Greek Self-Regulating Organisation for Internet Content - SAFENET	NGO	Greece	web	<a href="http://www.safenet.org.gr/">http://www.safenet.org.gr/</a>
National Committee of Users (CNU)	Association	Italy	all media	<a href="http://www.agcom.it/cnu/">http://www.agcom.it/cnu/</a>
ADUC - Associazione per i Diritti degli Utenti e Consumatori	Association for the Rights of Consumers	Italy	all media	<a href="http://www.aduc.it/">http://www.aduc.it/</a>
Netherlands Institute for the Classification of Audio-visual Media	Association of Companies	Netherlands	all media	<a href="http://www.kijkwijzer.nl/">http://www.kijkwijzer.nl/</a>
ECP.NL	Public-private not for profit organisation	Netherlands		<a href="http://www.ecp.nl/">http://www.ecp.nl/</a>
Stichting Reclame Code (SRC)	Advertising Code Foundation	Netherlands	advertisement	<a href="http://www.reclamecode.nl/">http://www.reclamecode.nl/</a>
Rada Reklamy (Advertising Council)	Polish Advertising Industry	Poland	advertisement	<a href="http://www.radareklamy.org">http://www.radareklamy.org</a>
hotline Spletno oko	Non-profit project (Internet)	Slovenia	web	<a href="https://www.spletno-oko.si/">https://www.spletno-oko.si/</a>

Name of organisation	Type of organisation	Geographical scope	Content-related scope	URL
Slovenian Consumers' Association	Non-profit organisation (Consumers' rights using Internet, mobile phones and computers)	Slovenia	all media	<a href="http://www.zps.si/">http://www.zps.si/</a>
APEK (Post and Electronic Communications Agency of the Republic of Slovenia)	Independent Regulatory Body (electronic communications and postal market)	Slovenia	all media	<a href="http://www.apek.si/">http://www.apek.si/</a>
Association Vita Activa	Association	Slovenia	all media	<a href="http://www.drustvo-vitaactiva.si/401.html">http://www.drustvo-vitaactiva.si/401.html</a>
Slovenian Advertising Chamber	Non-profit association of legal and physical persons (companies and individuals) regulation of media advertising	Slovenia	advertisement	<a href="http://www.soz.si/">http://www.soz.si/</a>
Asociación Española de Distribuidores y Editores de Software de Entretenimiento	Spanish Association of Editors and Wholesalers of Entertainment Software	Spain	interactive software	<a href="http://www.adese.es">http://www.adese.es</a>
Asociación para la Autoregulación de la Comunicación Comercial "Autocontrol"	Spanish advertising self-regulation organisation	Spain	advertisement	<a href="http://www.autocontrol.es/lación de">http://www.autocontrol.es/lación de</a>
Agencia de Calidad de Internet	Internet Quality Agency	Spain	web	<a href="http://www.iqua.net">http://www.iqua.net</a>
Internet Watch Foundation	Charity	UK	web	<a href="http://www.iwf.org.uk/">http://www.iwf.org.uk/</a>
OFCOM - Office of Communication	Public regulation Authority	UK	all media	<a href="http://www.ofcom.org.uk/about/csg/ofcom_board/code/">http://www.ofcom.org.uk/about/csg/ofcom_board/code/</a>
Home Office Task Force on Child Protection on the Internet	Task Force	UK	web	<a href="http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce">http://police.homeoffice.gov.uk/operational-policing/crime-disorder/child-protection-taskforce</a>
Family Online Safety Institute	Association	UK	web	<a href="http://www.fosi.org/icra">http://www.fosi.org/icra</a>

## E2 Instrumenten van zelfregulering in Europa

Name of instrument	Type of document	Geographical scope	Content-related scope	URL
Spam code of conduct of ISPA	Code of Conduct	Austria	web	<a href="http://www.ispa.at/downloads/ISPA_COC_spam_english.pdf">http://www.ispa.at/downloads/ISPA_COC_spam_english.pdf</a>
Journalists' Code of Conduct	Code of Conduct	Cyprus	journalistic ethics	<a href="http://www.mmc2000.net/docs/leggi/CYPRUS.pdf">http://www.mmc2000.net/docs/leggi/CYPRUS.pdf</a>
Kodex Etického Nákupu Vodafonu	Code of ethical purchase	Czech Republic	mobile	<a href="http://www.vodafone.cz/pdf/kodex_cz.pdf">http://www.vodafone.cz/pdf/kodex_cz.pdf</a>
Etický kodex o užívání veřejných informacních služeb pro šíření sázkových služeb	Code of Conduct	Czech Republic	gambling	<a href="http://web01.sazka.cz/LoterieAHry/docDetail.aspx?docid=19015601&amp;doctype=ART&amp;cpi=1&amp;highlight=etick_%20kodex">http://web01.sazka.cz/LoterieAHry/docDetail.aspx?docid=19015601&amp;doctype=ART&amp;cpi=1&amp;highlight=etick_%20kodex</a>
Evropská Asociace Státních Loterií A Toto Společností	Code of Conduct	Czech Republic	web	<a href="http://www.sazka.cz/o-nas/vice-osazka/zakony/kodex.php">http://www.sazka.cz/o-nas/vice-osazka/zakony/kodex.php</a>
Code for the ChatCheck Badge	Code of Conduct	Denmark	web	<a href="http://www.fdim.dk/?pageid=52">http://www.fdim.dk/?pageid=52</a>
European Framework for Safer Mobile Use by Younger Teenagers and Children	Framework	Europe	mobile	<a href="http://www.gsmworld.com/gsm europe/documents/eur.pdf">http://www.gsmworld.com/gsm europe/documents/eur.pdf</a>
Rec. on measures to promote the freedom of expression and information with regard to Internet filters	Recommendations	Europe	web	<a href="http://www.coe.int/">http://www.coe.int/</a>
Journalists' Code of Conduct	Code of Conduct	Europe	all media	<a href="http://www.presswise.org.uk">http://www.presswise.org.uk</a>
ISPA Code of Conduct	Code of Conduct	Europe	journalistic ethics	<a href="http://www.ispa.org.za/code/code_of_conduct.shtml">http://www.ispa.org.za/code/code_of_conduct.shtml</a>
Code of Conduct for search engines / Verhaltenssubkodex für Suchmaschinenanbieter der FSM	Sub - Code of Conduct	Germany	web	<a href="http://www.fsm.de/en/SubCoC_Search_Engines">http://www.fsm.de/en/SubCoC_Search_Engines</a>
Code of Conduct of Mobile Phone Service Providers in Germany for the Protection of Minors Using Mobile Phones	Sub - Code of Conduct	Germany	mobile	<a href="http://www.fsm.de/en/Subcode_of_Conduct_mobile">http://www.fsm.de/en/Subcode_of_Conduct_mobile</a>

Name of instrument	Type of document	Geographical scope	Content-related scope	URL
Code of Conduct of Chat Providers in the FSM	Sub - Code of Conduct	Germany	web	<a href="http://www.fsm.de/inhalt.doc/Sub-Code_Chat.pdf">http://www.fsm.de/inhalt.doc/Sub-Code_Chat.pdf</a>
NICAMs regulations for film, DVD, TV and Mobile Operators	Sub - Statutes	Netherlands	all media	<a href="http://www.kijkwijzer.nl/">http://www.kijkwijzer.nl/</a>
Richtlijn voor chatrooms	Guidelines	Netherlands	web	<a href="http://www.chatinfo.nl/">http://www.chatinfo.nl/</a>
Dutch Advertising Code	Code	Netherlands	advertisement	<a href="http://www.reclamecodecommissie.nl/bijlagen/dutch_advertising_code.pdf">http://www.reclamecodecommissie.nl/bijlagen/dutch_advertising_code.pdf</a>
Code of Ethics in Advertising	Code of Conduct	Poland	advertisement	<a href="http://www.radareklamy.pl/img_in//PLIKI/Kodeks%20Etyki%20Reklamy%20Eng.pdf">http://www.radareklamy.pl/img_in//PLIKI/Kodeks%20Etyki%20Reklamy%20Eng.pdf</a>
Slovenian Code of Advertising Practice	Code of Conduct	Slovenia	advertisement	<a href="http://www.soz.si/oglasevalsko_razsodisce/slovenski_oglasevalski_kodeks/">http://www.soz.si/oglasevalsko_razsodisce/slovenski_oglasevalski_kodeks/</a>
Internet Service Providers' Association Code of Conduct	Code of Conduct	South Africa	web	<a href="http://www.ispa.org.za/code/code_of_conduct.shtml">http://www.ispa.org.za/code/code_of_conduct.shtml</a>
Convenio Marco De Colaboración Para La Promoción Del Uso Seguro De Internet Por La Infancia Y La Juventud	Agreement	Spain	web	not digitally available
Código de autorregulación de la publicidad de alimentos dirigida a menores, prevención de la obesidad y salud	Food advertising for children and obesity prevention selfregulation code	Spain	advertisement	<a href="http://www.fiab.es/datos/1/PAOS_1676.pdf">http://www.fiab.es/datos/1/PAOS_1676.pdf</a>
Código de conducta de la industria europea del software interactivo relativo a la clasificación por edades, el etiquetado, la promoción y la publicidad de productos de software interactivo.	Code of Conduct	Spain	interactive software	<a href="http://www.adese.es/web/criterios_autoregulacion.asp">http://www.adese.es/web/criterios_autoregulacion.asp</a>
Código de Conducta Publicitaria	Code of Conduct	Spain	journalistic ethics	<a href="http://www.autocontrol.es/pdfs/Cod_conducta_publicitaria.pdf">http://www.autocontrol.es/pdfs/Cod_conducta_publicitaria.pdf</a>

Name of instrument	Type of document	Geographical scope	Content-related scope	URL
Código Ético de Comercio Electrónico y Publicidad Interactiva	Code of Conduct	Spain	web	<a href="http://www.confianzaonline.org/codigoetico/codigoetico.php">http://www.confianzaonline.org/codigoetico/codigoetico.php</a>
Código Deontológico para Publicidad Infantil de la Asociación Española de Fabricantes de Juguetes, y Unión de Consumidores de España	Consumers Code of Ethics	Spain	advertisement	<a href="http://www.aefj.es/template.php?id=91">http://www.aefj.es/template.php?id=91</a>
Código de Autorregulación sobre contenidos televisivos e infancia.	Self-regulation code on TV content for children	Spain	TV	<a href="http://www.tvinfancia.es/Textos/CodigoAutorregulacion/Codigo.htm">http://www.tvinfancia.es/Textos/CodigoAutorregulacion/Codigo.htm</a>
Convenio de Autorregulación para promover el buen uso de Internet en España	Self-regulation code for the promotion of an appropriate use of Internet in Spain	Spain	web	<a href="http://www.aui.es/./biblio/documentos/legislacion/proteccion_menores/convenio/tex_conv.htm">http://www.aui.es/./biblio/documentos/legislacion/proteccion_menores/convenio/tex_conv.htm</a>
Código deontológico de la Agencia de Calidad de Internet	Internet Quality Agency Code of Ethics	Spain	web	<a href="http://www.iqua.net/Codigos_de_conducta/Codigo_de_conducta/?go=WWW6aWP3clUyUj7fiM3LUP2TC+M0m3NphIdSA2vOCAqmvvV3BpkG0o8">http://www.iqua.net/Codigos_de_conducta/Codigo_de_conducta/?go=WWW6aWP3clUyUj7fiM3LUP2TC+M0m3NphIdSA2vOCAqmvvV3BpkG0o8</a>
Convenio Marco De Colaboración Para La Seguridad Del Menor	Committment	Spain		
Code of Practice for the selfregulation of new forms of content on mobiles	Code of Practice	UK	mobile	<a href="http://www.mobilebroadbandgroup.com/content-code.pdf">http://www.mobilebroadbandgroup.com/content-code.pdf</a>
Self-regulatory Code for the responsible selling of mobile telephony	Code of Practice	UK	mobile	<a href="http://www.mobilebroadbandgroup.com/documents/mbg_cop_sm_250707_f.pdf">http://www.mobilebroadbandgroup.com/documents/mbg_cop_sm_250707_f.pdf</a>
Industry Code of Practice for the use of mobile phone technology to provide passive location services in the UK	Code of Practice	UK	mobile	<a href="http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf">http://www.mobilebroadbandgroup.com/documents/UKCoP_location_servs_210706v_pub_clean.pdf</a>
Good Practice Guidance for the Moderation of Interactive Services for Children	Guidelines	UK	web	<a href="http://police.homeoffice.gov.uk/newsandpublications/publication/operational-policing/moderation-document-final.pdf?view=Binary">http://police.homeoffice.gov.uk/newsandpublications/publication/operational-policing/moderation-document-final.pdf?view=Binary</a>

Name of instrument	Type of document	Geographical scope	Content-related scope	URL
Good practice guidance for search service providers and advice to the public on how to search safely	Guidelines	UK	web	<a href="http://police.homeoffice.gov.uk/newsand-publications/publication/operational-policing/search-and-advice-public.pdf?view=Binary">http://police.homeoffice.gov.uk/newsand-publications/publication/operational-policing/search-and-advice-public.pdf?view=Binary</a>
Promoting Internet Safety Through Public Awareness Campaigns Guidance for Using Real Life Examples Involving Children or Young People	Guidelines	UK	web	<a href="http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/RealLifeExamples.pdf?view=Binary">http://police.homeoffice.gov.uk/news-and-publications/publication/operational-policing/RealLifeExamples.pdf?view=Binary</a>
Good Practice Models and Guidance for the Internet Industry On: Chat Services, Instant Messaging, Webbased Services	Guidelines	UK	web	<a href="http://police.homeoffice.gov.uk/newsand-publications/publication/operational-policing/ho_model.pdf?view=Binary">http://police.homeoffice.gov.uk/newsand-publications/publication/operational-policing/ho_model.pdf?view=Binary</a>
Television Advertising of Food and Drink Products to Children	Code	UK	advertisement	<a href="http://www.ofcom.org.uk/consult/condocs/foodads_new/statement/">http://www.ofcom.org.uk/consult/condocs/foodads_new/statement/</a>
BCAP Spread Betting Advertising Rules and BCAP Radio Advertising Code	Code	UK	advertisement	<a href="http://www.cap.org.uk/NR/rdonlyres/6C6CECA6-CCCB-44B7-A146-460D2726BC48/0/BCAP-Spread-BettingRadioAdvertising-Rules.pdf">http://www.cap.org.uk/NR/rdonlyres/6C6CECA6-CCCB-44B7-A146-460D2726BC48/0/BCAP-Spread-BettingRadioAdvertising-Rules.pdf</a>
BCAP Rules on the Scheduling of Advertising	Rules	UK	advertisement	<a href="http://www.asa.org.uk/NR/rdonlyres/7F763788-6A51-4A73-B35B-C60346FD5F6C/0/BCAPRulesontheSchedulingofTelevisionAdvertisements_20080108.pdf">http://www.asa.org.uk/NR/rdonlyres/7F763788-6A51-4A73-B35B-C60346FD5F6C/0/BCAPRulesontheSchedulingofTelevisionAdvertisements_20080108.pdf</a>
Advertising Standards Code for Text Services	Code	UK		<a href="http://www.asa.org.uk/NR/rdonlyres/3B4358E5-85CC-40EE-A2DD-EE883BBABB6E/0/BCAP-CodeforTextServices_20080108.pdf">http://www.asa.org.uk/NR/rdonlyres/3B4358E5-85CC-40EE-A2DD-EE883BBABB6E/0/BCAP-CodeforTextServices_20080108.pdf</a>
BCAP Guidance to Broadcasters on the Regulation of Interactive Television Services	Guidelines	UK	TV	<a href="http://www.asa.org.uk/NR/rdonlyres/D41345A2-31B5-4149-879B-69A08A64879C/0/BCAP_Guidance_on_Interactive_TV.pdf">http://www.asa.org.uk/NR/rdonlyres/D41345A2-31B5-4149-879B-69A08A64879C/0/BCAP_Guidance_on_Interactive_TV.pdf</a>

Name of instrument	Type of document	Geographical scope	Content-related scope	URL
BCAP Advertising Guidance Notes	Notes to Guidelines	UK	advertisement	<a href="http://www.clearcast.co.uk/clearcast/notes_of_guidance/Appendix+3+Guidelines+for+Superimposed+Text+from+BCAP+Guidance+on+Text+and+Subtitling+in+Television.htm">http://www.clearcast.co.uk/clearcast/notes_of_guidance/Appendix+3+Guidelines+for+Superimposed+Text+from+BCAP+Guidance+on+Text+and+Subtitling+in+Television.htm</a>
Good practice guidance for the providers of social networking and other user interactive services 2008	Guidance	UK	web	<a href="http://police.homeoffice.gov.uk/">http://police.homeoffice.gov.uk/</a>
Editors' Code of Practice	Code of Practice	UK	journalistic ethics	<a href="http://www.pcc.org.uk/">http://www.pcc.org.uk/</a>
CAP and BCAP Gambling Advertising Rules and BCAP Spread Betting Rules	Rules	UK	web	<a href="http://www.cap.org.uk/NR/rdonlyres/8C9D2140-EE00-424F-9E67-CE1914B3DA71/0/FINAL-CAPBCAPGamblingRules.pdf">http://www.cap.org.uk/NR/rdonlyres/8C9D2140-EE00-424F-9E67-CE1914B3DA71/0/FINAL-CAPBCAPGamblingRules.pdf</a>



## Overzicht van Europese wet- en regelgeving

EU Member States	Youth Protection / Youth Media Protection	Source
Austria	Pornografiegesetz	<a href="http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR12058546/NOR12058546.pdf">http://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR12058546/NOR12058546.pdf</a>
	9 different youth protection laws (including youth media protection) of the Federal States	<a href="http://www.bmwfj.gv.at/BMWA/Schwerpunkte/Jugend/Jugendschutz/default.htm">http://www.bmwfj.gv.at/BMWA/Schwerpunkte/Jugend/Jugendschutz/default.htm</a>
	Anti-Stalkinggesetz § 107a Strafgesetzbuch. Tatbestand der "beharrlichen Verfolgung"	<a href="http://www.ris.bka.gv.at/GeltendeFassung.wxe?QueryID=Bundesnormen&amp;Gesetzesnummer=10002296">http://www.ris.bka.gv.at/GeltendeFassung.wxe?QueryID=Bundesnormen&amp;Gesetzesnummer=10002296</a>
Belgium	Belgian Penal Code Articles 380 till 383	<a href="http://www.stopchildporno.be/index.php?pid=13">http://www.stopchildporno.be/index.php?pid=13</a>
Bulgaria	Child protection Act from 03.04.2003	<a href="http://www.sacp.government.bg/index_en.htm">http://www.sacp.government.bg/index_en.htm</a>
Cyprus		<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxwecyp.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxwecyp.htm</a>
Czech Republic	Act No. 359/1999 Coll., on the socio-legal protection of children, as amended (Act No. 501/2004 Coll., comes into effect 1.1.2006)	<a href="http://www.czso.cz/csu/cizinci.nsf/engogender_odkazy-links_with_legislative">http://www.czso.cz/csu/cizinci.nsf/engogender_odkazy-links_with_legislative</a>
	Act No. 94/1963 on family	<a href="http://mujweb.cz/www/vaske/rodina.htm">http://mujweb.cz/www/vaske/rodina.htm</a>
	Act No. 108/2006 on social services	<a href="http://www.ilo.org/dyn/natlex/natlex_browse.details?p_lang=en&amp;p_country=CZE&amp;p_classification=15.05&amp;p_origin=COUNTRY&amp;p_sortby=SORTBY_COUNTRY">http://www.ilo.org/dyn/natlex/natlex_browse.details?p_lang=en&amp;p_country=CZE&amp;p_classification=15.05&amp;p_origin=COUNTRY&amp;p_sortby=SORTBY_COUNTRY</a>
	Act No. 218/2003 on legal responsibility of youth and judiciary in cases of youth	<a href="http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN012622.pdf">http://unpan1.un.org/intradoc/groups/public/documents/NISPAcee/UNPAN012622.pdf</a>
	Act No. 140/1961 Criminal law § 205a "Receiving of child pornography" § 205b "Misuse of children for pornography production"	<a href="http://web.mvcr.cz/archiv2008/prevence/priority/kszd/english.html">http://web.mvcr.cz/archiv2008/prevence/priority/kszd/english.html</a>
	Act No. 500/2004 Administrative law	<a href="http://www.nssoud.cz/default.aspx?cls=art&amp;art_id=1">http://www.nssoud.cz/default.aspx?cls=art&amp;art_id=1</a>
Denmark	The Marketing Practices Act No. 1389 of 21 December 2005, latest amended in 2007	<a href="http://www.forbrug.dk/english/dco/lawsandacts/marketing-practises-act/">http://www.forbrug.dk/english/dco/lawsandacts/marketing-practises-act/</a>
	Radio and Television Broadcasting Act No. 338 of 11 April 2007	<a href="http://www.kum.dk/sw4507.asp">http://www.kum.dk/sw4507.asp</a>
Estonia	Youth Work Act	<a href="http://www.hm.ee/index.php?148615">http://www.hm.ee/index.php?148615</a>
	Juvenile Sanctions Act	<a href="http://www.hm.ee/index.php?149399">http://www.hm.ee/index.php?149399</a>
	Hobby Schools Act	<a href="http://www.hm.ee/index.php?149396">http://www.hm.ee/index.php?149396</a>

EU Member States	Youth Protection / Youth Media Protection	Source
Finland	Child Welfare Act from 05.08.1983	<a href="http://www.finlex.fi/pdf/saadkaan/E9830683.PDF">http://www.finlex.fi/pdf/saadkaan/E9830683.PDF</a>
	Act on the Classification of Audiovisual Programmes (L775/2000) from 25.08.2000	<a href="http://www.vet.fi/english/lait_kuvaohjelmien_tarkastaminen.php">http://www.vet.fi/english/lait_kuvaohjelmien_tarkastaminen.php</a>
	Finish Government's Child and Youth Policy Programme 2007–2011 (Finish Ministry of Education)	<a href="http://www.minedu.fi/OPM/Julkaisut/2007/Lapsija_nuorisopolitiikan_kehittamisohjelma_2007-2011?lang=en">http://www.minedu.fi/OPM/Julkaisut/2007/Lapsija_nuorisopolitiikan_kehittamisohjelma_2007-2011?lang=en</a>
France	Penal code	<a href="http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm">http://www.legifrance.gouv.fr/html/codes_traduits/code_penal_textan.htm</a>
	separate bills regarding youth protection for different media. No specific regulation for youth media protection	<a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a>
Germany	Youth Protection Act (2002)	<a href="http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse.did=12862.html">http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse.did=12862.html</a>
	Interstate Treaty for the Protection of Minors from Harmful Content in the Media (2003)	<a href="http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse.did=12862.html">http://www.bmfsfj.de/bmfsfj/generator/Kategorien/Service/themenlotse.did=12862.html</a>
Greece	LAW NO. 1729 Combat against the spread of drugs, protection of youth and other provisions	<a href="http://www.unodc.org/en/showDocument.do?documentUid=446&amp;node=docs&amp;country=GRE&amp;cmd=add">http://www.unodc.org/en/showDocument.do?documentUid=446&amp;node=docs&amp;country=GRE&amp;cmd=add</a>
	Penal Code	<a href="http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/CsaGreece.pdf">http://www.interpol.int/Public/Children/SexualAbuse/NationalLaws/CsaGreece.pdf</a>
	separate bill for youth protection from the National Radio and TV Council	No source
	General information on legal regulation	<a href="http://www.kep.gov.gr/portal/page/portal/MyNewPortal?lng=us">http://www.kep.gov.gr/portal/page/portal/MyNewPortal?lng=us</a> <a href="http://old.mfa.gr/english/greece/today/media/internet.html">http://old.mfa.gr/english/greece/today/media/internet.html</a>
Hungary	Act I of 1996 on Radio and Television Broadcasting (Media Act)	<a href="http://www.helsinki.hu/docs/Act%20I%20of%201996.pdf">http://www.helsinki.hu/docs/Act%20I%20of%201996.pdf</a>
Ireland	Criminal Justice Act 2008	<a href="http://www.baillii.org/cgi-bin/markup.cgi?doc=/ie/legis/num_act/2008/a0708.html&amp;query=Youth+Media+Protection&amp;method=all">http://www.baillii.org/cgi-bin/markup.cgi?doc=/ie/legis/num_act/2008/a0708.html&amp;query=Youth+Media+Protection&amp;method=all</a>
Italy	Codice del consumo (D.lgs. 206/2005)	<a href="http://www.altalex.com/index.php?idstr=39&amp;idnot=33366">http://www.altalex.com/index.php?idstr=39&amp;idnot=33366</a>
	Gentiloni's decree (against online pedo-pornographic materials through a blocking filter on the basis of a national black list provided by LEA to ISP (Italian Ministry of Communication)	<a href="http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0707/it3.htm">http://www.saferinternet.org/ww/en/pub/insafe/news/articles/0707/it3.htm</a> <a href="http://www.comunicazioni.it/361-381.html">http://www.comunicazioni.it/361-381.html</a> <a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxweita.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxweita.htm</a>

EU Member States	Youth Protection / Youth Media Protection	Source
Italy	Bill on video games	<a href="http://www.comunicazioni.it/binary/min_comunicazioni/news_eng/Parliamentary%20Bill%20on%20Regulations%20for%20the%20Protection%20of%20Children%20in%20Film%20Viewing%20and%20Use%20of%20Videogames.pdf">http://www.comunicazioni.it/binary/min_comunicazioni/news_eng/Parliamentary%20Bill%20on%20Regulations%20for%20the%20Protection%20of%20Children%20in%20Film%20Viewing%20and%20Use%20of%20Videogames.pdf</a>
	Personal Data Protection Code, Legislative Decree no. 196 dated 30 June 2003	<a href="http://www.garanteprivacy.it/garante/document?ID=1219452">http://www.garanteprivacy.it/garante/document?ID=1219452</a>
	Legislative Decree No. 345 Of 4 August 1999 Implementing The Directive No. 94/33 EC On The Protection Of Young People At Work	<a href="http://www.ilo.org/dyn/natlex/docs/WEBTEXT/54507/65185/E99ITA01.htm">http://www.ilo.org/dyn/natlex/docs/WEBTEXT/54507/65185/E99ITA01.htm</a>
	bill 6 February 2006, n. 38 against pedo-pornography and child sex abuse (the bill affords also online aspect of these issues),	<a href="http://www.edri.org/edrigram/number5.1/italy_blocking">http://www.edri.org/edrigram/number5.1/italy_blocking</a>
	bill 3 august 1998 n. 269 against child prostitution, child pornography and sexual tourism	
	bill 15 February 1996 n. 66 on sex violence against children	
Latvia	Children's Rights Protection Law	<a href="http://www.humanrights.lv/doc/latlik/bern.htm">http://www.humanrights.lv/doc/latlik/bern.htm</a>
	Advertising Law (20.12.1999)	<a href="http://www.kp.gov.lv/uploaded_files/ENG/E_likumR.pdf">http://www.kp.gov.lv/uploaded_files/ENG/E_likumR.pdf</a>
	Youth Law	<a href="http://www.bm.gov.lv/eng/regulatory_enactment/regulatory_enactment/?doc=10753">http://www.bm.gov.lv/eng/regulatory_enactment/regulatory_enactment/?doc=10753</a>
Lithuania	Law On Fundamentals Of Protection Of The Rights Of The Child	<a href="http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/359.HTM">http://www.litlex.lt/Litlex/Eng/Frames/Laws/Documents/359.HTM</a>
Luxembourg	Loi sur la liberté d'expression dans les medias (Juni 2004): Chapitre V/Section 5: De la protection des mineurs	<a href="http://www.legilux.public.lu/leg/textescoordonnes/compilation/recueil_lois_speciales/MEDIAS.pdf">http://www.legilux.public.lu/leg/textescoordonnes/compilation/recueil_lois_speciales/MEDIAS.pdf</a>
Malta	Criminal Code	<a href="http://docs.justice.gov.mt/lom/legislation/english/leg/vol_1/chapt9.pdf">http://docs.justice.gov.mt/lom/legislation/english/leg/vol_1/chapt9.pdf</a>
	Electronic Commerce Act: Article 25.1.i	<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxwemal.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxwemal.htm</a>
	Broadcasting Code for the Protection of Minors (Sept.2001) (350.05: subsidiary legislation on broadcasting act)	<a href="http://docs.justice.gov.mt/lom/Legislation/English/SubLeg/350/05.pdf">http://docs.justice.gov.mt/lom/Legislation/English/SubLeg/350/05.pdf</a>

EU Member States	Youth Protection / Youth Media Protection	Source
Netherlands	Dutch Media Act	<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediaact.pdf">http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediaact.pdf</a>
	The Media Decree	<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediadecree.pdf">http://www.lexadin.nl/wlg/legis/nofr/eur/arch/ned/mediadecree.pdf</a>
	Dutch Advertising Code: B: Code for advertising directed at children or young people (Article 5 and 6)	<a href="http://www.reclamecode.nl/bijlagen/dutch_advertising_code.pdf">http://www.reclamecode.nl/bijlagen/dutch_advertising_code.pdf</a>
	Criminal Code; Article 240a	<a href="http://www.thefuturegroup.org/youwillbecaught/law_Netherlands.html">http://www.thefuturegroup.org/youwillbecaught/law_Netherlands.html</a>
Poland	Polish Penal Code 202	<a href="http://www.internationalresourcecentre.org/missingkids/servlet/PageServlet?LanguageCountry=en_X2&amp;PagelD=3428">http://www.internationalresourcecentre.org/missingkids/servlet/PageServlet?LanguageCountry=en_X2&amp;PagelD=3428</a> <a href="http://www.era.int/domains/corpus-juris/public_pdf/polish_penal_code2.pdf">http://www.era.int/domains/corpus-juris/public_pdf/polish_penal_code2.pdf</a>
Portugal		<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxwepor.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxwepor.htm</a>
Romania		<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxwerom.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxwerom.htm</a>
Slovakia		<a href="http://www.lexadin.nl/wlg/legis/nofr/eur/lxweslw.htm">http://www.lexadin.nl/wlg/legis/nofr/eur/lxweslw.htm</a>
Slovenia	Constitution of the Republic of Slovenia; Article 56	<a href="http://www.up-rs.si/up-rs/uprs-eng.nsfdokumentiweb/063E5907BE5B679CC1256FB20037658C?OpenDocument">http://www.up-rs.si/up-rs/uprs-eng.nsfdokumentiweb/063E5907BE5B679CC1256FB20037658C?OpenDocument</a>
	Public Media Act	<a href="http://www.mk.gov.si/si/postopki/mediji/vpis_v_register_tujih_dopisnikov_in_dopisnistev/navodila_eng/?type=98">http://www.mk.gov.si/si/postopki/mediji/vpis_v_register_tujih_dopisnikov_in_dopisnistev/navodila_eng/?type=98</a>
Spain	Ley Organica 1/1996 de 15/1/96	<a href="http://vlex.com/vid/ley-organica-codigo-penal-126987">http://vlex.com/vid/ley-organica-codigo-penal-126987</a>
Sweden	The Children's Ombudsman Act	<a href="http://www.bo.se/adfinity.aspx?pageid=86">http://www.bo.se/adfinity.aspx?pageid=86</a>
United Kingdom	Protection of Children Act 1978 (England and Wales)	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>
	Sex Offences Act 2003 (SOA 2003)	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>
	Civic Government (Scotland) Act, 1982	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>
	Obscene Publications Act 1959 & 1964	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>
	Police and Justice Act 2006 (Section 39 and Schedule 11)	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>
	Public Order Act 1986	<a href="http://www.iwf.org.uk/police/page.22.htm">http://www.iwf.org.uk/police/page.22.htm</a>



## Europese regelgeving

### Youth Protection / Youth Media Protection

	Source
Framework decision on combating the sexual exploitation of children and child pornography	<a href="http://europa.eu/scadplus/leg/en/lvb/l33138.htm">http://europa.eu/scadplus/leg/en/lvb/l33138.htm</a>
Green Paper: Protection of minors and human dignity in audiovisual and information services (from 1996)	<a href="http://europa.eu/scadplus/leg/en/lvb/l24030b.htm">http://europa.eu/scadplus/leg/en/lvb/l24030b.htm</a>
Cybercrime Convention from 23.11.2001 (Council of Europe)	<a href="http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&amp;CL=ENG">http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&amp;CL=ENG</a>
Stockholm Agenda for Action regarding child pornography from 1996	<a href="http://www.ilo.org/public/english/comp/child/standards/resolution/stockholm.htm">http://www.ilo.org/public/english/comp/child/standards/resolution/stockholm.htm</a>
Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual abuse, signed on the 25th October 2007	<a href="http://www.nspcc.org.uk/Inform/policyandpublicaffairs/Europe/Briefings/councilofeurope_wdf51232.pdf">http://www.nspcc.org.uk/Inform/policyandpublicaffairs/Europe/Briefings/councilofeurope_wdf51232.pdf</a>
Communication (COM (2000) 890): Creating a safer information society by improving the security of information infrastructures and combating computer-related crime	<a href="http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML">http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52000DC0890:EN:HTML</a>
Council Decision of 29 May 2000 to combat child pornography on the Internet.	<a href="http://europa.eu/scadplus/leg/en/lvb/l33116.htm">http://europa.eu/scadplus/leg/en/lvb/l33116.htm</a>
Joint action to combat trafficking in human beings and sexual exploitation of children	<a href="http://europa.eu/scadplus/leg/en/lvb/l33072.htm">http://europa.eu/scadplus/leg/en/lvb/l33072.htm</a>
Communication on Illegal and Harmful Content on the Internet (1996)	<a href="http://www.copacommission.org/meetings/hearing3/eu.test.pdf">http://www.copacommission.org/meetings/hearing3/eu.test.pdf</a>
UN Convention on the Rights of the Child	<a href="http://www.unicef.org/crc/">http://www.unicef.org/crc/</a>
Charter of Fundamental Rights (2000)	<a href="http://europa.eu/scadplus/leg/en/lvb/l33501.htm">http://europa.eu/scadplus/leg/en/lvb/l33501.htm</a>
Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography	<a href="http://europa.eu/scadplus/leg/en/lvb/l33138.htm">http://europa.eu/scadplus/leg/en/lvb/l33138.htm</a>
Television without Frontiers Directive (03.10.1989)	<a href="http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1989L01989L0552-19970730-en.pdf">http://eur-lex.europa.eu/LexUriServ/site/en/consleg/1989L01989L0552-19970730-en.pdf</a>
Audiovisual Media Services Directive (11 December 2007)	<a href="http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0065:EN:NOT">http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32007L0065:EN:NOT</a>



**G****Deelnemers Youth Protection Roundtable**

ADICONSUM – Associazione italiana difesa consumatori e ambiente, Italy, Nicola Fabiano  
AOL, Germany, Per Christiansen  
AOL, UK, Camille de Stempel  
Arbeitskreis Neue Erziehung e. V., Germany, Gundel Hessemer  
BAGFW – Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege, Germany, Michael Sommer  
Citizens Online, UK, John Fisher  
Comenius Foundation for Child Development, Poland, Janusz Lukasiak  
D.O.M. Datenverarbeitung GmbH, Germany, Alfred Jakob  
Deutscher Kinderschutzbund –Bundesverband e.V., Germany, Ekkehard Mutschler  
Extreme Media Solutions Ltd., Greece, Veronica Samara  
FOSI – Family Online Safety Institute, UK, David Miles  
Le Forum des droits sur l'internet, France, Laurent Baup  
F-Secure, Germany, Bernd Erlbeck  
FSM – Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V., Germany, Martin Drechsler  
Fundacja Dzieci Niczyje, Poland, Agnieszka Wrzesien  
ICRAdeutschland.de GbR, Germany, Alexandra Koch  
ISFE – Interactive Software Federation of Europe, Belgium, Patrice Chazerand  
Internet ABC e. V., Germany, Antje vom Berg  
Johannisches Sozialwerk e. V., Germany, Alexander Romahn  
Jugendschutz.net, Germany, Mark Bootz  
Landeszentrale für Medien und Kommunikation Rheinland-Pfalz – Klicksafe.de, Germany, Dr. Joachim Kind  
Mannerheim League for Child Welfare, Finland, Sanna Harakkamäki  
Microsoft, EMEA, Rita Balogh  
NCH, UK, John Carr  
NICAM – Nederlands Instituut voor de Classificatie van Audiovisual Media, Netherlands, Tiffany van Stormbroek  
ÖIAT – Österreichisches Institut für Angewandte Telekommunikation, Austria, Barbara Buchegger  
Pegasus GmbH, Germany, Michael Beer  
Protegeles, Spain, José Luis Zatarain  
Safer Internet Institute, z.s.p.o, Czech Republic, Dr. Zdenek Zalis  
Save the Children, Italy, Maria Elisa Marzotti  
SurfControl, UK,  
University of Ljubljana, Faculty of Social Sciences, Slovenia, Tanja Sterk

Dit project is gecoördineerd door **Stiftung Digitale Chancen**

**Managing Director**

**Jutta Croll**

Fasanenstraße 3

10623 Berlin

Tel.: ++49-30-43727730

Fax: ++49-30-43727739

email: jcroll@digitale-chancen.de

**Project Manager**

**Katharina Kunze**

Fasanenstraße 3

10623 Berlin

Tel.: ++49-30-43727740

Fax: ++49-30-43727739

email: kunze@yppt.eu

Dit project valt binnen the Safer Internet Programme of the European Commission

Gefinancierd door de Europese Commissie



