Filteren van kinderporno op internet

Een verkenning van technieken en reguleringen in binnen- en buitenland

W.Ph. Stol
H.W.K. Kaspersen
J. Kerstens
E.R. Leukfeldt
A.R. Lodder

26 mei 2008

Deze studie is uitgevoerd in opdracht van het WODC, ministerie van Justitie.

Deze uitgave zal tevens verschijnen in de reeks Veiligheidsstudies van Boom Juridische Uitgevers te Den Haag.

Exemplaren kunnen worden besteld bij:
Boom distributiecentrum te Meppel
Tel. 0522-23 75 55
Fax 0522-25 38 64
E-mail bdc@bdc.boom.nl

Filteren van kinderporno op internet

Een verkenning van technieken en reguleringen in binnen- en buitenland

Noordelijke Hogeschool Leeuwarden
Lectoraat Integrale Veiligheid

Vrije Universiteit
Instituut voor Informatica en Recht

W.Ph. Stol
H.W.K. Kaspersen
J. Kerstens
E.R. Leukfeldt
A.R. Lodder

CyREN – Cybersafety Research and Education Network

2008

Inhoudsopgave

Voorwoord

In de samenleving heerst bezorgdheid over de verspreiding van kinderpornografie via internet. De Tweede Kamer heeft daarom aan de minister van Justitie gevraagd om maatregelen te nemen. Niet alleen gaat het daarbij om opsporing, de Kamer vraagt nadrukkelijk ook om technologische maatregelen in de vorm van filteren en blokkeren van kinderpornografie.

De maatschappelijke bezorgdheid is terecht in die zin dat we uit eerder onderzoek weten dat internet in belangrijke mate bijdraagt aan de verspreiding van kinderpornografie en dat internet met zich meebrengt dat mensen eerder dan voorheen de grenzen van het toelaatbare opzoeken – en overschrijden. We weten echter nog niet veel over filteren als instrument tegen kinderpornografie op internet. Daarover gaat dit rapport.

Filteren kan vanuit verschillende invalshoeken worden benaderd. Het gaat om een technisch middel (hoofdstuk 2) dat wordt gebruikt in een juridische context (hoofdstuk 3). Daarnaast zijn er reeds ervaringen in andere landen opgedaan. Daarbij is de vraag aan de orde met welke partijen het filteren kan worden geregeld en wat daarbij de mogelijkheden zijn voor zelfregulering (hoofdstuk 4). De Nederlandse situatie rond filteren en kinderporno nemen we onder de loep in hoofdstuk 5 en in hoofdstuk 6 geven we daarvan een juridische analyse. In het slothoofdstuk presenteren we de conclusies, beantwoorden we de onderzoeksvragen en schetsen we aan de hand van vier scenario's hoe het verder zou kunnen gaan met het filteren van kinderporno op internet. Voor wie snel kennis wil nemen van de hoofdlijnen uit dit onderzoek, is er de leesvervangende samenvatting.

Dit onderzoek is een samenwerking tussen de Noordelijke Hogeschool Leeuwarden (Lectoraat Integrale Veiligheid) en de Vrije Universiteit (Instituut voor Informatica en Recht). Een onderzoek als dit kan alleen tot stand komen dankzij de medewerking van velen. Het onderzoek werd begeleid door een commissie bestaande uit: prof. mr. R.V. De Mulder (EUR – Faculteit der Rechtsgeleerdheid, voorzitter), de heer S. van de Geer (ministerie van Justitie, directie Rechtshandhaving en Criminaliteitsbestrijding), drs. M. Kruissink (ministerie van Justitie, WODC), mw. mr. M.J.C. Spoormaker (Arrondissementsrechtbank Rotterdam), en de heer C.S. Groeneveld (KLPD). Wij zijn hen zeer dankbaar voor de enthousiaste en deskundige begeleiding. We zijn Stefaan Pleysier (KATHO, dept. IPSOC – Expertisecentrum Maatschappelijke Veiligheid) zeer erkentelijk voor zijn commentaar op het manuscript. Uiteraard blijft de uiteindelijke tekst onze verantwoordelijkheid. Verder zijn we alle respondenten en andere personen die ons van informatie voorzagen zeer dankbaar voor hun inbreng.

Het filteren van kinderpornografie is volop in discussie en de technische, juridische en organisatorische ontwikkelingen gaan snel, zowel nationaal als internationaal. In dat verband zij vermeld dat de informatievergaring voor dit onderzoek is gestopt op 1 mei 2008.

mei 2008

Wouter Stol
Rik Kaspersen
Joyce Kerstens
Rutger Leukfeldt
Arno Lodder

Samenvatting

In de eerste helft van 2006 nam de Tweede Kamer een motie aan waarin zij de minister van Justitie verzoekt 'om de verdere uitbouw en toepassing van de technische mogelijkheden tot het blokkeren, filteren en afsluiten van kinderpornografisch materiaal op internet en andere media te bevorderen en de Kamer daarover nader te berichten'. Die motie was de aanleiding tot dit onderzoek dat een verkenning biedt van de technische en juridische mogelijkheden om kinderpornografisch materiaal op internet te filteren en te blokkeren.

Onderzoeksvragen en methoden
De hoofdvraag van dit onderzoek luidt: wat zijn de technische mogelijkheden om informatie op internet te filteren en te blokkeren en op welke gronden kunnen deze mogelijkheden gelegitimeerd worden? Deze hoofdvraag is uitgewerkt in vijf groepen onderzoeksvragen:

1. Technische mogelijkheden:
   a. Welke technische mogelijkheden (*tools*) zijn er om kinderpornografisch materiaal op internet te filteren en blokkeren?
   b. Welke ervaringen zijn met die tools opgedaan? Welke praktische problemen zijn verbonden aan de toepassing van die tools, zoals beschikbaarheid, onderhoudbaarheid, installatie, effecten op snelheid en capaciteit van het internetverkeer?
   c. Is de toepassing van die tools effectief, haalbaar en duurzaam?

2. Juridische context:
   a. Welke juridische mogelijkheden zijn er om kinderpornografisch materiaal op internet middels filteren en blokkeren te verhinderen?
   b. Bestaan er juridische belemmeringen en knelpunten en op welke wijze kan daarvoor een oplossing worden gevonden?

3. Zelfregulering:
   a. In hoeverre kan 'zelfregulering' (d.w.z. gedragsregulering zonder wettelijke dwang) door internetproviders een effectieve en duurzame wijze zijn om kinderpornografisch materiaal op internet te filteren en blokkeren?
   b. Welke mogelijkheden heeft de overheid voor 'gecontroleerde zelfregulering'?
   c. Welke ervaringen zijn in relatie tot internet met 'zelfregulering' opgedaan?

4. Buitenland:
   a. Hoe wordt in het buitenland getracht kinderpornografisch materiaal op het internet te filteren en blokkeren?
   b. Welke technische middelen worden hiertoe aangewend?
   c. Hoe is het filteren en blokkeren juridisch ingebed?
   d. Wat voor praktijkervaringen heeft men met het filteren/blokkeren opgedaan (met aandacht voor effectiviteit, haalbaarheid en duurzaamheid)?
   e. Zijn de buitenlandse ervaringen te vertalen naar de Nederlandse situatie?

5. Technische doorontwikkeling:
   a. Is het zinnig om de bestaande technische mogelijkheden verder uit te bouwen?
   b. Zo ja, welk type applicaties zou dan gebouwd moeten worden?
   c. Zo ja, wie zou dergelijke applicaties moeten bouwen?
   d. Is er een rol voor de overheid bij het ontwikkelen van dergelijke applicaties?

De twee centrale onderzoeksmethoden zijn: een deskresearch (literatuur, documenten, media, websites) en semi-gestructureerde interviews met deskundigen en betrokkenen. Omdat in Nederland nog weinig ervaring is opgedaan met het filteren van internetinformatie, zijn ervaringen in het buitenland in het onderzoek betrokken. Daarnaast heeft het onderzoeksteam zich ter plaatse een oordeel gevormd van de werkwijze van het KLPD bij de samenstelling en het onderhoud van de zogenoemde blacklist.

In dit onderzoek zijn technische, recherche- of handhavingstactische en juridische kennis over het tegenhouden van kinderporno op internet met elkaar verbonden. Het leggen van dwarsverbanden tussen de tijdens het onderzoek verkregen informaties, hebben we niet bewaard tot de analysefase aan het einde van het onderzoek, maar is van meet af aan ingebouwd in het onderzoeksproces. Op die manier konden bijvoorbeeld juristen reageren op door technici geopperde technische mogelijkheden en tekortkomingen en konden opsporingsdeskundigen reageren op standpunten van ISP's.

Filtertechnieken

Om kinderpornografisch materiaal op internet te kunnen filteren en te blokkeren is inzicht nodig in hoe de verspreiding van dit materiaal precies verloopt. Exacte cijfers over de omvang en de route waarlangs de verspreiding verloopt, zijn echter niet bekend. Uit ander onderzoek en statistisch materiaal is wel af te leiden via welke soorten internetverkeer kinderpornografisch materiaal wordt verspreid: websites, P2P-netwerken, virtuele harde schijven, nieuwsgroepen en chatboxen. Van de P2P-netwerken is bekend dat zij op substantiële wijze bijdragen aan de verspreiding van kinderporno en vermoed wordt dat deze verspreidingswijze in de toekomst de grootste rol zal spelen. Omdat onbekend is hoeveel kinderporno via welke van de genoemde internetvoorzieningen wordt verspreid, kan in dit onderzoek geen uitspraak worden gedaan over het effect van het filteren en blokkeren van bepaalde internetonderdelen op de totale verspreiding van kinderporno.

Filters werken op basis van lijsten met adressen en/of codes die geblokkeerd moeten worden (blacklist filtering) of op basis van algemene criteria waarmee het filterprogramma vaststelt of bepaalde informatie wel of niet kan worden doorgelaten (dynamic filtering). Dynamic filtering leidt tot relatief veel *overblocking*. Voor zover bekend wordt in Europa voor het filteren van kinderpornografie enkel gebruik gemaakt van door mensen samengestelde blokkeerlijsten.

Het blokkeren op basis van een blacklist kan met IP-adressen, domeinnamen, URL's, of hashcodes. Blokkeren op IP-adres is niet geschikt, want te grofmazig (alle informatie op het niveau van een IP-adres wordt dan geblokkeerd). In Nederland wordt geblokkeerd op basis van domeinnamen. Dit is relatief eenvoudig en goedkoop, maar niet zo precies en vrij eenvoudig te omzeilen. Het tegenovergestelde geldt voor het blokkeren op URL of hashcode. Deze methode vergt echter substantiële technische investeringen, omdat alle internetverkeer inhoudelijk moet worden gecontroleerd. Een technische oplossing voor dit laatste probleem is een tweetrapsfiltermethode waarbij uit alle verkeer (bijvoorbeeld op IP-adres) eerst een verdachte informatiestroom wordt gefilterd, waarna alleen dit verkeer (bijvoorbeeld op basis van URL's) nader inhoudelijk wordt gecontroleerd.

Filteren kan op verschillende plaatsen: op de computer van de internetter, in zoekmachines, op de centrale server van een organisatie, op de server(s) van de ISP's of op landelijk niveau. Dit laatste is binnen Europa niet aan de orde. Filteren op gebruikers- en organisatieniveau stuit niet op technische of praktische bezwaren. Het op ISP-niveau filteren van chatkanalen, P2P-netwerken, MMS- en webcamverkeer is technisch gezien aanzienlijk lastiger dan het filteren van websites op het internet. Bovendien kan daarbij niet altijd op basis van blokkeerlijsten worden gewerkt. Dergelijke verbindingen lopen namelijk langs minder gestructureerde wegen.

Het is technisch onmogelijk een filter te maken dat 100 procent kinderporno tegenhoudt en tegelijk alle legale informatie doorlaat. Daar komt bij dat het informatieaanbod op internet voortdurend verandert. Wat nu terecht wordt gefilterd, kan over enkele momenten ten onrechte zijn. Wie met een filter een serieuze drempel tegen kinderporno wil opwerpen, moet dan ook reëel gesproken[1] een bepaalde mate van structurele *overblocking* accepteren.

Juridische context

De strafbaarstelling van kinderpornografie in art. 240b Sr richtte zich eerst alleen tegen misbruik van jeugdigen. Onder invloed van internationale ontwikkelingen is ook in Nederland het besef doorgedrongen dat het minstens zo belangrijk is dat kinderen worden beschermd tegen gedrag dat kan worden gebruikt hen aan te moedigen of te verleiden tot deelname aan seksueel verkeer, of tegen gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.

Internationaal gezien zijn inspanningen verricht om te komen tot harmonisatie van kinderpornostrafbepalingen. Hoewel deze inspanningen niet zonder resultaat zijn gebleven, blijven belangrijke verschillen tussen landen bestaan. Zo is virtuele kinderpornografie niet in alle landen strafbaar. Ook wordt niet overal de leeftijdsgrens van 18 jaar gehanteerd. Hierdoor kan de situatie ontstaan dat zelfs met landen waarmee Nederland een rechtshulpverdrag heeft, toch niet tegen alle in Nederland strafbaar gestelde verschijningsvormen van kinderporno kan worden opgetreden. Nederland is bevoegd internetverkeer met kinderporno tegen te houden, wanneer de gevolgen van het strafbare feit zich binnen de Nederlandse rechtsorde manifesteren. Dat geldt ook voor andere landen. Daardoor kan de situatie ontstaan dat beeldmateriaal dat hier rechtmatig in het (internet-)verkeer kan worden gebracht, door andere landen als strafbaar wordt tegengehouden. Het omgekeerde kan ook het geval zijn.

Het toepassen van filteren of blokkeren van internetverkeer houdt in dat kennis wordt genomen van de inhoud van bepaalde verkeersstromen. De vertrouwelijkheid van dit verkeer wordt gewaarborgd door art. 8 EVRM en de corresponderende bepalingen van de Nederlandse Grondwet. Dat houdt in dat blokkering door of namens de overheid plaats dient te vinden op basis van een formeelwettelijke bevoegdheid. Blokkering van kinderporno door ISP's behoeft de toestemming van de abonnees.

Internetproviders zijn op grond van Europese regelgeving niet aansprakelijk voor gegevensverkeer dat zij niet zelf initiëren of inhoudelijk beïnvloeden. Zij hoeven niet na te gaan of zij strafbare of inbreukmakende informatie hosten, maar zij dienen wel in actie te komen indien zij wetenschap hebben van het strafbare of onrechtmatige karakter van de informatie.

De huidige wet voorziet in art. 125o Sv op het ontoegankelijk maken van opgeslagen gegevens. Voor art. 54a Sr geldt dat onduidelijk is waartoe de bevoegdheid precies strekt en in welke gevallen die bevoegdheid toepassing kan vinden. In het verlengde hiervan is een aanvulling en herziening van zowel art. 125o Sv als art. 54a Sr in onderlinge samenhang gewenst. Uitgangspunt dient immers te zijn dat de wet een bevoegdheid verschaft tot het (doen) verwijderen van bepaalde informatie uit de systemen van internetproviders en individuele internetgebruikers. Deze bevoegdheid dient ook te strekken tot het blokkeren van de informatiestromen waarmee kinderporno wordt aangeboden.

Beperkingen van het grondrecht van de vrijheid van meningsuiting dienen door de formele wet te worden gesteld. Alle maatregelen om te kunnen filteren en blokkeren gaan gepaard met een bepaalde mate van overblocking. Het blokkeren door of namens de overheid, zo de wet daartoe een bevoegdheid zou geven, verplicht tot een zorgvuldige keuze van het aan te wenden instrument en een permanente verificatie of de maatregel aan zijn doel beant-

[1] Theoretisch maar niet reëel is de optie dat men alle items op de blokkeerlijst voortdurend door deskundigen op hun juistheid laat controleren.

woordt. Dit om te voorkomen dat toepassing van de maatregel in strijd komt met art. 10 EVRM en art. 7 GW.

Buitenlandse ontwikkelingen

Het blokkeren van informatieaanbod op internet gebeurt in minstens veertig landen. Verkend is hoe in een aantal westerse en niet-westerse landen het filteren en blokkeren van informatie op internet wordt aangepakt. In dit onderzoek is vooral gekeken naar de situatie in Noorwegen, Zweden en Engeland. De situatie in Noorwegen is extra belicht, omdat het Noorse initiatief tot het blokkeren van websites met kinderpornografische inhoud via UPC naar Nederland is gebracht. Daarnaast worden de Verenigde Staten kort belicht en wat de niet-westerse landen betreft is – meer ter illustratie – gekeken naar Saoedi-Arabië, Iran en China.

In Europa zijn twee filtermodellen in gebruik: het Scandinavische (Noorwegen en Zweden) en het Engelse model. Het Scandinavische model is organisatorisch gezien gebaseerd op een in eerste aanleg vrijwillige publiek-private samenwerking tussen met name de politie en de ISP's en technologisch gezien op het blokkeren van domeinen. Het Engelse model is organisatorisch gezien gebaseerd op zelfregulering door commerciële ISP's ondersteund door de ngo IWF en technisch gezien op het blokkeren van URL's. Het Engelse model is vergeleken met het Scandinavische model ingewikkelder en duurder, maar daarnaast ook fijnmaziger. In Noorwegen en Zweden is het uiteindelijke doel van het filteren ambitieus geformuleerd: het terugbrengen van het aantal misbruikte kinderen. In Engeland is het hoofddoel: voorkomen dat onschuldige internetters ongewild in aanraking komen met kinderpornografie. Óf er onschuldige internetters zijn die op webpagina's (daarop zijn de filters gericht) ongewild in aanraking komen met kinderpornografisch materiaal is overigens een goed bewaard geheim.

De Verenigde Staten nemen een bijzondere positie in. De heersende *First Amendment*-doctrine biedt aan de Amerikaanse overheid weinig mogelijkheden voor het filteren en blokkeren van kinderpornografisch materiaal op internet. Bij het filteren en blokkeren door particulieren speelt dit niet. Er zijn dan ook tal van bedrijven die filters maken en aanbieden. Uit onderzoek blijkt echter dat de prestaties van deze filters matig zijn.

Saoedi-Arabië, Iran en China laten zien dat het mogelijk is te filteren op nationaal niveau. Een nationale filterstructuur omvat technologie, wetgeving en controleorganisaties. China lijkt hierin het meest effectief, maar dit land accepteert een aanzienlijke mate van overblocking. Een wereldwijd overzicht van internetfiltering laat zien dat filtersystemen niet waterdicht te krijgen zijn, omdat filterende overheden de strategieën die gebruikers ontwikkelen om de filters te omzeilen niet kunnen bijhouden.

Concrete, meetbare doelstellingen om kinderpornografie op internet te filteren en te blokkeren ontbreken veelal. Veel genoemde doelstellingen zijn: het tegengaan van seksueel misbruik van kinderen, het onaantrekkelijk maken van het commercieel aanbieden van kinderporno en het beschermen van argeloze gebruikers tegen kinderporno op internet. Er zijn geen studies gedaan naar de maatschappelijke effectiviteit van filteren en blokkeren van kinderpornografisch materiaal op internet. Wie onder welke omstandigheden op het filter stuiten en wat dat tot gevolg heeft, is onbekend. De grond voor toepassing van filteren en blokkeren van kinderpornografisch materiaal wordt dan ook voornamelijk gevonden de verwachting dat de maatregel effectief is.

In de westerse landen is zelfregulering een terugkerend en essentieel onderdeel van filteren en blokkeren van kinderpornografie op internet. Meestal zien we dan wel overheidsbemoeienis op de achtergrond, niet zelden in de vorm van het richting ISP's dreigen met wetgeving. In Noorwegen en Zweden houdt de overheid de blacklist bij en voeren ISP's het filteren uit. In Engeland is ook het bijhouden van de blacklist een particuliere aangelegenheid (IWF). Verder zien we ook zelfregulering bij internetters (ouders) en LAN-beheerders. Zij gebruiken

filters die weer worden ontwikkeld door andere private partijen: commerciële bedrijven. Die zien hier een markt. In de VS heeft de wetgever openbare scholen en bibliotheken de plicht opgelegd om maatregelen te nemen tegen kinderpornografie op internet, in Noorwegen zijn werkgevers en leidinggevenden wettelijk verplicht om maatregelen te nemen om te voorkomen dat werknemers kinderporno kunnen downloaden. Alles met elkaar lijkt het dat filteren van kinderporno duurzaam kan worden geregeld via zelfregulering, zij het dat de eerder gemaakte opmerkingen over de effectiviteit van filteren ook dan van toepassing zijn.

Nederlandse situatie

In Nederland wordt een levendige politiek-maatschappelijke discussie gevoerd over de wijze waarop de verspreiding van kinderporno op internet kan worden tegengegaan. De discussie beweegt zich tussen twee polariteiten, waarbij enerzijds de gevaren van internetcensuur worden benadrukt en anderzijds de noodzaak van een daadkrachtig optreden waarin elke maatregel lijkt te zijn gerechtvaardigd. Ook de huidige regering wil een daad stellen in de bestrijding van kinderporno en daarmee gehoor geven aan de morele verontwaardiging in de samenleving. Aangezien er, zoals gezegd, geen onderzoek beschikbaar is naar de effectiviteit van filteren en blokkeren, is de huidige inzet van filters door of namens de Nederlandse overheid niet gebaseerd op onderbouwde kennis omtrent de effectiviteit van deze maatregel.

Op dit moment kunnen websites met kinderpornografisch materiaal die in Nederland zijn gehost door de hosting provider fysiek worden verwijderd. Websites met kinderporno die worden gehost in landen waarmee Nederland een rechtshulpverdrag heeft, kunnen in het kader van een juridische samenwerking door de desbetreffende autoriteiten worden verwijderd. Voor websites die in landen zijn gehost waarmee Nederland geen rechtshulpverdrag heeft, is dit niet mogelijk. Een optie die dan overblijft is het blokkeren van sites. Het KLPD heeft hiertoe in navolging van en analoog aan de wijze van blokkeren in Noorwegen een eerste stap gezet.

Uit dit onderzoek blijkt dat de inhoud en de wijze van samenstelling van de blacklist van het KLPD op basis waarvan ISP's kinderpornosites blokkeren een aantal onvolkomenheden bevat. De lijst heeft betrekking op circa 100 websites, terwijl de totale omvang van kinderpornosites die vallen binnen de reikwijdte van art. 240b Sr hier vermoedelijk een veelvoud van is. Bovendien bevat de lijst websites die (inmiddels) niet meer bestaan of die (inmiddels) geen kinderporno meer bevatten. Ook komen sites op de lijst voor die in Nederland worden gehost en wordt een belangrijk deel van de vermelde sites gehost in landen waarmee Nederland een rechtshulpverdrag heeft (vooral de VS). Voor het beheer van de lijst zijn door het KLPD geen procedures vastgelegd en zijn geen toetsbare criteria geformuleerd op basis waarvan tot toevoeging aan de lijst wordt besloten. Het onderhoud van de lijst is onvoldoende frequent.

De vereiste tijdsinvestering voor het actualiseren van de blacklist vormt, gezien de (opsporings)taak van het KLPD, een onevenredig grote aanslag op de beschikbare tijd van de rechercheurs. Mede in het kader van het debat over kerntaken van de politieorganisatie is het dan ook de vraag of het opstellen en bijhouden van een blacklist niet aan andere partijen moet worden overgelaten.

Juridische analyse filterpraktijk Nederland

Het KLPD sluit convenanten met internetproviders die ertoe strekken dat een ISP domeinen blokkeert die door het KLPD zijn aangemerkt als kinderpornografisch en daarom door het KLPD op een blokkeerlijst zijn geplaatst. De ISP verplicht zich de lijst van het KLPD te gebruiken en leidt de internetgebruiker niet naar het gevraagde domein maar naar een zogenoemde stoppagina. Het KLPD vrijwaart de ISP voor aanspraken van derden vanwege de op instructie van het KLPD toegepaste blokkering.

Het KLPD gaat met private partijen convenanten aan ter uitvoering van een veronderstelde publiekrechtelijke taak, namelijk de daadwerkelijke handhaving van de rechtsorde. Aangezien het filteren en blokkeren van internetverkeer een inbreuk maakt op het grondrecht van vertrouwelijke informatie, zoals geregeld in art. 13 GW en art. 8 EVRM, behoeft een dergelijke maatregel een formeelwettelijke grondslag. Zo de wet al in een dergelijke bevoegdheid zou voorzien – art. 54a Sr en art. 125o Sv zijn hierop niet toegesneden – komt deze niet toe aan de politie en aan het KLPD als onderdeel daarvan. Artikel 2 Polw biedt evenmin een grondslag voor het (doen) filteren en blokkeren van internetverkeer. Deze convenanten vormen daarom een onaanvaardbare doorkruising van publiekrechtelijke bevoegdheden en daarmee van publiekrechtelijke waarborgen. Deze convenanten zijn daarom in de Nederlandse rechtsleer niet rechtsgeldig. Vanuit het oogpunt van rechtstatelijkheid is het niet aanvaardbaar dat de overheid zich bedient van instrumenten zonder deugdelijke juridische grondslag ter bereiking van een overigens legitiem doel. Indien de wetgever voornemens is om het blokkeren van kinderporno als een politietaak aan te wijzen, dan dient te worden voorzien in specifieke wettelijke bevoegdheden.

Scenario's

Om aan te geven op welke mogelijke manieren de verspreiding van kinderporno op internet in de nabije toekomst kan worden tegengegaan, schetsen we vier scenario's. Deze scenario's bevinden zich binnen het spectrum van spontane zelfregulering tot aan een door de overheid gecontroleerd internetverkeer.

In het eerste scenario steekt de overheid haar energie in kerntaken en laat zij het ontwikkelen, beheren en invoeren van filters tegen kinderporno over aan particuliere bedrijven, ideële organisaties en internetgebruikers. Ontwikkelingen in het buitenland laten zien dat er een groeiende (commerciële) markt is van aanbieders van allerhande filters. Door uit te gaan van marktwerking blijft de overheid buiten de discussie van internetcensuur, bovendien zijn er geen juridische complicaties.

In het tweede scenario stimuleert en faciliteert de overheid de ontwikkeling van filters, zonder zelf uitvoerende taken op zich te nemen. In dit scenario heeft de overheid tot op zekere hoogte de regie in handen en is er op onderdelen sprake van een publiek-private samenwerking (PPS).

In het derde scenario neemt de overheid wel uitvoerende taken op zich. In een PPS stelt de politie een blokkeerlijst ter beschikking aan marktpartijen die deze gebruiken bij het ontwikkelen van kinderpornofilters. De politie stelt protocollen op voor het beheren van de bestanden die onder haar verantwoordelijkheid vallen. Tevens zorgt zij voor volledige transparantie in de criteria op basis waarvan de betreffende lijst is samengesteld.

In het vierde scenario stelt de overheid het invoeren van kinderpornofilters verplicht op basis van formele wetgeving. Zij verplicht ISP's om filters te installeren waarmee websites met kinderporno kunnen worden geblokkeerd. Een variant hierop is dat de overheid bepaalde personen of organisaties de verplichting oplegt maatregelen te nemen tegen de verspreiding van kinderporno op internet. De overheid regelt dan niet voor zichzelf de bevoegdheid om te filteren, maar verplicht bijvoorbeeld werkgevers of openbare bibliotheken om maatregelen te nemen.

Summary

During the first half of 2006 the Lower House passed a motion in which it requested the Minister of Justice 'to promote the further development and use of the technical possibilities to block, filter and to cut off child pornographic material from the internet and other media and to further inform the House about this'. That motion was the reason for this research that offers an investigation of the technical and legal possibilities to filter and block child pornographic material on the internet.

Research questions and methods
The main question of this research is: What are the technical possibilities of filtering and blocking information on the internet and on what grounds can these possibilities be legitimized? This main question has been worked out in five groups of research questions:

1. Technical possibilities:
    a. Which technical possibilities (tools) are available for filtering and blocking child pornography on the internet?
    b. What experience has been acquired with those tools? What practical problems are connected to the application of those tools, such as the availability of those tools, ability to maintain, installation, effects on speed and capacity of internet traffic?
    c. Is the application of those tools effective, feasible and sustainable?

2. Legal context
    a. What legal possibilities are available for using filtering and blocking to prevent child pornography on the internet?
    b. Are there any legal impediments and/or bottlenecks and how can a solution to these be found?

3. Self-regulation:
    a. How can self-regulation (i.e. regulation of behaviour without legal duress) by internet providers be an effective and long-term way to filter and block child pornographic material on the internet?
    b. Which possibilities are available for the government for 'controlled self-regulation'?
    c. In relation to the internet what has the experience of 'self-regulation' been?

4. Abroad:
    a. In other countries, how have they attempted to filter and block child pornographic material on the internet?
    b. What are the technical means that are being used?
    c. How are the filtering and blocking legally embedded?
    d. What is the practical experience that has been acquired with filtering and blocking (with respect to effectiveness, feasibility and sustainability?
    e. Can the foreign experience be translated to the Dutch situation?

5. Further technical developments
    a. Does it make sense to expand the existing possibilities?
    b. If yes, what type of applications should be built?
    c. If yes, who should be building those applications?
    d. Is there a role for the government in the development of such applications?

The two main methods of research are: desk research (literature, documents, media websites) and semi-structured interviews with experts and those involved. Because in the Netherlands there is still little experience with filtering information from internet, experience from abroad is involved in the research. Furthermore the research team on the scene has formed an opinion about the procedures being used by the *KLPD* (*Korps Landelijke Politiediensten* / National Police Services Agency) putting together and maintaining the so-called blacklist.

In this research the technical investigation of the maintenance strategy and the legal knowledge about the prevention of child pornography on internet are linked together.

We did not save putting together the connections between the information acquired during the research for the phase of analysis at the end of the research but it has been part of the research process right from the beginning.

In that way jurists, for instance, were able to react to technical possibilities and shortcomings proposed by technicians and investigation specialists were able to react to ISP's standpoints.

Filter techniques

In order to be able to filter and block child pornography on internet there should be an understanding exactly how this material is being spread. Exact figures about the size and the routes along which the distribution takes, however are unknown. From other research and statistical material can be deducted through which kinds of internet traffic child pornography is being spread: Websites, P2P networks, virtual hard disks, newsgroups and chat boxes. It is known that P2P networks substantially contribute to the spread of child pornography and it is suspected that this way of spreading child pornography around will play the biggest role in the future. Because it is unknown how much child pornography is being spread through which internet facilities, this research is unable to judge the effects of filtering and blocking certain parts of internet on the total spread of child pornography.

Filters work on the basis of lists with addresses and/or codes that have to be blocked (blacklist filtering) or on the basis of general criteria by which the filter program determines if certain information can or cannot be allowed to pass through (dynamic filtering). Dynamic filtering leads relatively to a lot of *overblocking*. As far as it is known in Europe only use is being made of block lists put together by people for filtering child pornography.

Blocking on the basis of a blacklist can be done with IP addresses, domain names, URLs or hash codes. Blocking on the basis of an IP address is not suitable because it is not precise enough. In the Netherlands blocking on the basis of domain names is being done at this time. This is relatively easy and cheap but not as precise and quite easy to get around. The opposite applies to blocking on the basis of the URL or the hash code. However this method requires substantial technical investments because all internet traffic has to be controlled with respect to content. A technical solution for the latter problem is a two-stage filter method in which from all traffica suspected data flow is filtered first (for example on the basis of IP addresses), after which just this traffic (for example on the basis of the URLs) is checked for content.

Filtering can be done in different places: on the computer of the person using the internet, in search engines, in the central server of an organisation, in the server(s) of the ISPs or on a national level. The latter is not under discussion in Europe. Filtering on the level of individual users and organisations does not meet technical or legal difficulties. Filtering on the ISP level of chat channels, P2P networks, MMS and webcam traffic is much more difficult to filter than websites on internet. Moreover it cannot always be done on the basis of block lists since such connections usually run through less structured channels.

Technically it is impossible to manufacture a filter that stops child pornography 100 percent and at the same time lets all legal information through. On top of which the informa-

tion that is being put on the internet is changing continually. What rightfully is being filtered now in a few moments could be wrongful. Whoever wants to put up a serious barrier against child pornography, realistically spoken[2] has to accept a certain amount of structural *over-blocking.*

Legal context

The penalization of child pornography in art. 240 Sr was first aimed at abuse of youngsters. Also in the Netherlands under the influence of international developments, the realisation has gotten through that it is at least as important that youngsters are being protected from behaviour that can be used to encourage or tempt them to participate in sexual intercourse or against behaviour that can become a part of a subculture that encourages sexual abuse of youngsters.

Internationally considered there have been efforts to harmonize legislation on child pornography. Although these efforts have not been without results major differences between countries continue to exist. Virtual child pornography for example is not punishable in all countries. Also the age limit of 18 years old does not apply everywhere. Because of this a situation can exist where even with countries that the Netherlands has a treaty with for legal cooperation it is not possible to act against all the manifestations of child pornography. The Netherlands has the authority to block child pornography when the consequences of the criminal offence manifest themselves within the Dutch rule of law. That also applies to other countries as well. Because of this the situation can arise that visual material that is being put on (internet) traffic lawfully here will be stopped by other countries as liable to punishment. The opposite can also be the case.

The application of filtering or blocking of internet traffic means that the content of certain flows of traffic will become known. The confidentiality of this traffic is guaranteed by art. 8 EVRM and the corresponding provisions of the Dutch Constitution. That means that blocking should be done by or in name of the government on the basis of a formal statutory authority. Blocking child pornography through ISPs needs the approval of the subscribers.

Based on European rules, internet providers are not responsible for the traffic of data that they did not initiate or influence with respect to content. They do not have to verify whether or not they host punishable information or information that violates the law, but they are supposed to act in case they have knowledge of the punishable or unlawful character of the information.

In art 125o Sv the present law provides the legal authorities with the power to make stored data inaccessible. For art. 54a Sr (another article with respect to removing data from a suspected persons computer) holds that it is not clear to where the jurisdiction exactly extends and in which cases that jurisdiction can apply. In a continuation of this an addition and a revision of art. 125o Sv as well as 54a Sr for a mutual cohesion is desired. The starting point after all should be that the law gives the permission to remove or to have removed certain information from the systems of internet providers and individual users of internet. This should also extend to the blocking of the flow of information by which child pornography has been offered.

Limitations of the basic law of freedom of speech need to be set by formal law. All the rules enabling filtering and blocking are coupled to a certain amount of overblocking. Blocking by or on behalf of the government, provided the law would give authority to that, binds one to a careful choice of the instruments to be used and a continuous verification whether the measure serves its purpose. This is to prevent that application of the rule is in violation with art. 10 EVRM and art. 7 GW.

[2] Theoretical but not realistic is the option that people have all the items on the block list checked for their correctness by experts all the time.

International developments

Blocking of the supply of information on the internet happens in at least forty countries. How filtering and blocking have been dealt with in a number of western and non-western countries has been investigated.

During this research the situation in Norway, Sweden and England has been looked at in particular. The situation in Norway has been extra emphasized because the Norwegian initiative to block websites with child pornographic content has been brought through UPC to the Netherlands. Furthermore the United States is briefly discussed and as far as the non-western countries is concerned – more as an illustration – Saudi-Arabia, Iran and China have also been looked at.

In Europe two filter models are used: the Scandinavian (Norway and Sweden) and the English model. The Scandinavian one is organisationally spoken in the first instance based on a voluntary public-private cooperation between the police and the ISPs in particular and technologically spoken on the blocking of domains. The English model organisationally spoken is based on self-regulation by commercial ISPs supported by the NGO IWF and technically spoken is based on the blocking of URLs.

The English model compared to the Scandinavian model is more complicated and more expensive but in addition it is also of a more intricate structure. In Norway and Sweden the ultimate goal of filtering is ambitiously formulated: reduce the number of abused children. In England the chief purpose is: to prevent innocent users of internet unintentionally from getting in contact with child pornography. If there are any internet users that are unwillingly getting in contact with web pages (the filters are aimed at those) with child pornographic material however is a very well kept secret.

The United States take a special position. The prevailing First Amendment doctrine offers the American government few possibilities for filtering and blocking of child pornographic material on the internet. This doctrine does not play a role with respect to filtering and blocking by private citizens. There are a number of companies that manufacture and offer filters. Research however shows that the performance of these filters is mediocre.

Saudi-Arabia, Iran and China show that it is possible to filter on a national level. A national filter structure includes technology, law and monitoring organisations.

China seems to be the most effective, but this country accepts a high degree of over-blocking. A worldwide survey of internet filtering shows that filtering governments are not able to get those systems watertight, because governments cannot keep up with the strategies that are being developed by users to avoid these filters.

Concrete, measurable aims in order to filter and block child pornography are often lacking. The aims frequently mentioned are: preventing sexual abuse of children, making the sale of child pornography unattractive and protecting unsuspecting internet users from child pornography. No studies have been done about the social effectiveness of filtering and blocking child pornographic material on the internet. Who, whatever the circumstances, encounters a filter and what that results in is unknown. The argument for using filters and blocking child pornographic material would then also be based mainly on the expectation that the measure is effective.

In Western countries self-regulation is a reoccurring and essential part of filtering and blocking child pornography on the internet. Mostly we then see government intervention in the background, not infrequently threatening ISPs with legislation. In Norway and Sweden the authorities keep up the blacklist and the ISPs carry out the filtering. In England the upkeep of the blacklist is done by a private business (IWF – Internet Watch Foundation). In addition we also see self-regulation by internet users (parents) and LAN administrators. They use filters that again are developed by other private parties: commercial businesses that see a market in this. In the US the legislature has charged the public schools and libraries with the duty to

take measures against child pornography on the internet; in Norway employers and management are legally obliged to take measures to prevent employees from downloading child pornography. Altogether it seems that filtering of child pornography can be regulated by means of self-regulation, provided the observations made earlier about the effectiveness of filtering are then also applicable.

The situation in the Netherlands

In the Netherlands a lively political-social discussion has taken place concerning the manner in which the spread of child pornography on the internet can be prevented. The discussion moves between two polarities, by which on one hand the dangers of internet censure is emphasised and on the other side the need for a clamp down in which every measure seems to be justified. Also the present government wants to act to combat child pornography and with that answer the moral indignation of society. Since there is, as already stated, no research available about the effectiveness of filtering and blocking, the present application of filters by or on behalve of the Dutch government is not based upon well-founded knowledge about the effectiveness of this measure.

At this moment websites containing pornographic material that are hosted in the Netherlands are physically removed by the hosting provider. Websites with child pornography that are hosted in countries with which the Netherlands has a legal cooperation treaty can under the terms of a legal cooperation be removed by the appropriate authorities. For websites that are hosted in countries with which the Netherlands has no legal cooperation treaty this is not possible. The one option that remains is to block the sites. The *KLPD* has taken the first step for this purpose following and analogous to Norway's way of blocking.

From this study has been found that the contents and the manner of compilation of the *KLPD*'s blacklist on the basis with which the ISP's block child pornography sites contain a number of inadequacies. The list has connection with about 100 websites, while the total number of child porno sites that fall within the range of art. 240b Sr probably is a multiple of this. Moreover the list contains websites that (by now) do not exist anymore or that (by now) do not contain child pornography anymore. Also sites appear on the list that are hosted in the Netherlands and an important portion of the stated sites are hosted in countries with which the Netherlands has a legal cooperation treaty (especially the US). No procedures have been established for the management of the list by the *KLPD* and no verifiable criteria have been formulated on the basis from which additions to the list are decided. The upkeep of the list is not frequent enough.

The required time investment for the realisation of the blacklist forms, considering the (investigation) task of the *KLPD*, a disproportionately large demand on the detectives' available time. Also in the framework of the debate about the core responsibilities of the police is it then also the question whether or not the set up and the upkeep of a blacklist should be left to other parties.

Legal analysis of the practise of filtering in the Netherlands

The *KLPD* makes agreements with internet providers to the extent that an ISP blocks domains that the *KLPD* considers child pornographic and therefore are placed on a blocking list by the *KLPD*. The ISP is obliged to use the *KLPD*'s list and does not direct the internet user to the requested domain but to a so-called stop page. The *KLPD* protects the ISP from third-party claims because of the instruction of the applied blocking by the *KLPD*.

The *KLPD* implements convents with private parties of a presupposed public duty, namely the actual maintenance of the rule of law. Since the filtering and blocking of internet traffic infringe on the constitutional right of confidential information, as regulated in art. 13 GW and art. 8 EVRM, these require a similar measure for a formal legal basis. So if the law

in a similar competence would provide this – article 54a Sr and art. 125o Sv are not geared to this – this does not depend on the police or the *KLPD* as a part of that. Art. 2 Polw provides just as little basis for filtering and blocking internet traffic. These agreements form therefore an unacceptable thwarting of public law authority and with this public safeguards. These agreements are therefore not legally valid. From the point of view of the constitutional law it is not acceptable that the authorities make use of instruments without sound legal basis in order to reach an otherwise legitimate goal. If the legislature's intention is to designate the blocking of child pornography as a duty of the police, then this should be provided in specific legal jurisdiction.

Scenarios

In order to indicate which possible ways the spread of child pornography on the internet in the near future can be prevented, we give a rough sketch of four scenarios. These scenarios are within the spectrum of spontaneous self-regulation up to internet traffic controlled by the government.

In the first scenario the government puts all its energy in core responsibilities and it leaves the development, management and operation of filters to private companies, non-commercial organisations and internet users. Developments abroad show that there is a growing (commercial) market of suppliers of all sorts of filters. By starting with the free market the government stays out of the discussion about internet censure, moreover there are no legal complications.

In the second scenario the government stimulates and facilitates the development of filters without taking on the executory duties itself. In this scenario the government up to a certain point itself has control and partially one can speak of a public-private cooperation (PPC).

In the third scenario the government takes care of the implementation of some of the tasks itself. In a PPC the police put a block list at the disposal of the market sectors that use those to develop child pornography filters. The police draw up protocol rules for managing the files that fall under their responsibility. They also take care of full transparency in the criteria on which the basis of the particular list has been put together.

In the fourth scenario the government makes the implementation of child pornography filter mandatory based on formal legislation. It requires ISPs to install filters with which websites with child pornography can be blocked. A variation on this is that the government forces certain persons or organisations to take action against the spreading of child pornography on internet. The government itself in this case does not the authority to filter, but forces employers or public libraries to take action.

HOOFDSTUK 1

Inleiding en verantwoording

1.1 Aanleiding tot dit onderzoek

Internet biedt mensen communicatie- en handelingsmogelijkheden die zij daarvoor niet hadden. Zij maken daarvan volop gebruik, ook voor criminele doeleinden. Het gebruik van internet bij het plegen van delicten is al lang niet meer nieuw (Akdeniz, 1996; Duncan, 1997, Durkin 1997, Van Eecke, 1997, Boerstra, 1997; Grabowsky, 1999). Tegelijk wordt bij herhaling geconstateerd dat politie en justitie de ontwikkelingen maar moeizaam kunnen bijbenen. Groot probleem is gebrek aan kennis over wat zich op internet precies afspeelt met betrekking tot criminaliteit en hoe dat kan worden opgespoord (Stol e.a., 1999; PWC, 2001; LPDO, 2003; Griffith, 2005; Lünnemann e.a., 2006; Van der Hulst en Neven, 2008).

Een van de prioriteiten bij politie en justitie in de bestrijding van internetgerelateerde criminaliteit, ook in veel andere landen, is het tegengaan van kinderpornografie. Dat is in Nederland vooral hoog op de agenda gekomen met de Zandvoortse kinderpornozaak in de zomer van 1998 (Stol e.a., 1999). De inspanningen tegen kinderpornografie hebben effect gehad op de werkwijze van de aanbieders. Was het materiaal medio jaren negentig in Nederland niet zelden te vinden op eenvoudig benaderbare websites, gaandeweg is het aanbod verschoven naar de minder gemakkelijk door politie en justitie te controleren delen van het internet (van websites, naar nieuwsgroepen, afgesloten domeinen, en peer-to-peer omgevingen). De wijze waarop commerciële aanbieders hun materiaal bij potentiële kopers onder de aandacht brengen, beweegt ook: van 'reclame' op openbare portalen van gesloten websites naar mail in nieuwsgroepen en spamberichten (Stol, 2004). Repressieve maatregelen hebben aldus effect gehad op de wijze waarop kinderporno wordt aangeboden. We kunnen ook zeggen: aanbieders bewegen mee met de maatregelen van politie en justitie en verrichten hun activiteiten nu op plaatsen op internet waar zij minder eenvoudig zijn te traceren. Dit betekent dat de opsporing van aanbieders van kinderporno er niet eenvoudiger op is geworden. Mede daardoor richt de aandacht zich op preventiemogelijkheden.

In een debat over de aanpak van kinderpornografie, eerste helft 2006, nam de Tweede Kamer een motie aan waarin zij de minister van Justitie verzoekt 'om de verdere uitbouw en toepassing van de technische mogelijkheden tot het blokkeren, filteren of afsluiten van kinderpornografisch materiaal op internet en andere media te bevorderen en de Kamer daarover nader te berichten' (TK, 2006:12). Die motie was de aanleiding tot dit onderzoek. Vanuit het perspectief van criminaliteitsbestrijding hebben we het dan over technische maatregelen ter voorkoming van criminaliteit, een aanpak die valt binnen wat de politie noemt het 'tegenhouden' van criminaliteit en waaraan zij de voorkeur geeft boven opsporing achteraf (PO, 2003). Aan die invalshoek is in dit onderzoek het juridische perspectief toegevoegd omdat juridische haalbaarheid een belangrijke voorwaarde is voor het kunnen realiseren van technische maatregelen tegen criminaliteit.

1.2 Onderwerp en doel van onderzoek

Dit onderzoek gaat over het met technische hulpmiddelen filteren van kinderpornografisch materiaal op internet, met aandacht voor zowel de mogelijkheden als de beperkingen van deze vorm van technopreventie. Onder filteren verstaan we het hele proces van selecteren en tegenhouden van informatie, inclusief het gebruik van technische hulpmiddelen daarbij. De uitkomst van filteren is dat bepaalde (de meeste) informatie verder ongemoeid wordt gelaten en dat bepaalde, door de filterende instanties als ongewenst beschouwde informatie wordt geblokkeerd. Hoewel in theorie kan worden gefilterd zonder te blokkeren (alle informatie is 'ok' en wordt doorgelaten) is het in de praktijk zo dat filteren blokkeren impliceert. Immers, de aanleiding om te gaan filteren is steeds de vaststelling dat bepaalde informatie ongewenst is.

'Blokkeren' klinkt vrij definitief, maar een van de vragen is hoe *effectief* een blokkade is. Hoe beter het lukt om bepaalde informatie voor internetters onbereikbaar te maken, hoe effectiever de blokkade is. Effectiviteit heeft te maken met hoe eenvoudig een blokkade is te omzeilen. Ook kent effectiviteit een tijdsperspectief. We spreken van *duurzaam* effectief blokkeren wanneer de tegengehouden informatie niet vroeg of laat alsnog weer via andere informatiekanalen beschikbaar komt, bijvoorbeeld omdat de aanbieder de informatie verplaatst naar een andere, wel bereikbare internetlocatie. Daarmee komen we aan de *haalbaarheid* van het blokkeren. Een bepaald filterproces is haalbaar indien het geen onevenredige inspanningen vergt of geen onredelijke gevolgen heeft.

Dit onderzoek gaat over het blokkeren van kinderpornografie. Kinderpornografie is volgens de Nederlandse wet: 'een afbeelding – of een gegevensdrager, bevattende een afbeelding – van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken' (art. 240b Wetboek van Strafrecht (Sr)) .

Het maatschappelijke doel van dit onderzoek is het leveren van een bijdrage aan de bestrijding van kinderpornografie. Het dichterbij gelegen doel is het verschaffen van inzicht in de praktische mogelijkheden en belemmeringen, zowel technisch als juridisch, om kinderpornografisch materiaal op internet te blokkeren. Niet toevallig voegen we het woord 'praktische' toe. Het onderzoek dient niet alleen technische en juridische mogelijkheden te identificeren maar ook inzicht te geven in de praktische waarde ervan in termen van duurzaamheid en haalbaarheid.

1.3 Zelfregulering en regie

De partijen die een rol kunnen spelen bij het filteren van kinderpornografie zijn de wetgever, politie en justitie en de private partijen die het internet in stand houden of daarvan gebruik maken. Ieder van deze partijen heeft eigen mogelijkheden en verplichtingen. De mogelijkheden van de overheid om bij wijze van preventieve maatregel in te grijpen in internetverkeer vinden grenzen in de vrijheid van meningsuiting en in het grondwettelijk censuurverbod. Als het aankomt op preventie kan ook een beroep worden gedaan op eigen verantwoordelijkheden van de overige bij het functioneren het internet betrokken partijen. Dat is niet nieuw. Zie bijvoorbeeld de oproep in 1999 van de Engelse Metropolitan Police aan de gezamenlijke Britse internet-providers om (kinder)pornografisch materiaal te weren (Grabowsky, 1999).

Aandacht verdient de vraag welke mogelijkheden de overheid heeft in relatie tot zelfregulering. Aan de socioloog Elias (1939) danken we de uitdrukking 'automatische zelfbewaking van de driften' – die in zijn ogen het gevolg is van de opvoeding en niet van overheidsoptreden. De socioloog Foucault (1975) stelt daar tegenover dat mensen zich fatsoenlijk gedragen als gevolg van een continue disciplinering door de overheid. De waarheid ligt vermoedelijk ergens in het midden.

In het veiligheidsdomein vinden we 'regie' als hedendaags alternatief voor harde wettelijke dwang enerzijds en 'hopen dat het vanzelf goed komt' anderzijds. Zo komen we van zelfregulering terecht bij veiligheidsregie. Het begrip zelfregulering vatten we breed op. Het omvat niet alleen 'spontane zelfregulering' (Wat gebeurt er als de overheid afwacht?) maar ook, en vooral, de mogelijkheden voor de overheid om middels 'regie' invloed uit te oefenen op het doen en laten van betrokken partijen, speciaal de ISP's. We spreken dan van 'gecontroleerde zelfregulering'. Regie betreft dan alle beïnvloedingsmogelijkheden anders dan wettelijke maatregelen of aansturing via een gezagsrelatie.

1.4 Onderzoeksvragen

Filteren van informatie op internet is allereerst een technisch vraagstuk. Aan de orde is dan hoe het filteren kan worden gerealiseerd. Direct daarop volgt de vraag wat de wettelijke mo-

gelijkheden en beperkingen zijn. Immers, niet alles wat kan is toegestaan. Een volgende kwestie is wie het filteren uitvoert. We komen dan aan vraagstukken op het vlak van regie en zelfregulering. In Nederland is met filteren nog niet veel ervaring opgedaan. Daarom kijken we ook nadrukkelijk naar ervaringen in het buitenland. Tot slot is de vraag of en zo ja hoe Nederland verder moet met het filteren van kinderpornografisch materiaal op internet. De zojuist gestelde vragen hebben we voor dit onderzoek als volgt uitgewerkt:

1. Technische mogelijkheden:
   a. Welke technische mogelijkheden (*tools*) zijn er om kinderpornografisch materiaal op internet te filteren en te blokkeren?
   b. Welke ervaringen zijn met die tools opgedaan? Welke praktische problemen zijn verbonden aan de toepassing van die tools, zoals beschikbaarheid, onderhoudbaarheid, installatie, effecten op snelheid en capaciteit van het internetverkeer?
   c. Is de toepassing van die tools effectief, haalbaar en duurzaam?

2. Juridische context:
   a. Welke juridische mogelijkheden zijn er om kinderpornografisch materiaal op internet middels filteren en blokkeren te verhinderen?
   b. Bestaan er juridische belemmeringen en knelpunten en op welke wijze kan daarvoor een oplossing worden gevonden?

3. Zelfregulering:
   a. In hoeverre kan 'zelfregulering' (d.w.z. gedragsregulering zonder wettelijke dwang) door internetproviders een effectieve en duurzame wijze zijn om kinderpornografisch materiaal op internet te filteren en blokkeren?
   b. Welke mogelijkheden heeft de overheid voor 'gecontroleerde zelfregulering'?
   c. Welke ervaringen zijn in relatie tot internet met 'zelfregulering' opgedaan?

4. Buitenland:
   a. Hoe wordt in het buitenland getracht kinderpornografisch materiaal op het internet te filteren en blokkeren?
   b. Welke technische middelen worden hiertoe aangewend?
   c. Hoe is het filteren en blokkeren juridisch ingebed?
   d. Wat voor praktijkervaringen heeft men met het filteren/blokkeren opgedaan (met aandacht voor effectiviteit, haalbaarheid en duurzaamheid)?
   e. Zijn de buitenlandse ervaringen te vertalen naar de Nederlandse situatie?

5. Technische doorontwikkeling:
   a. Is het zinnig om de bestaande technische mogelijkheden verder uit te bouwen?
   b. Zo ja, welk type applicaties zou dan gebouwd moeten worden?
   c. Zo ja, wie zou dergelijke applicaties moeten bouwen?
   d. Is er een rol voor de overheid bij het ontwikkelen van dergelijke applicaties?

1.5 Methodische verantwoording

Onderzoeksmethoden
De twee centrale methoden van onderzoek zijn het uitvoeren van een deskresearch (literatuur, documenten, media, websites) en het houden van semi-gestructureerde interviews. Beide methoden worden gebruikt voor alle onderzoeksvragen en ze zijn beide zowel gericht op informatie uit Nederland als het buitenland. Hierna lichten we beide methoden toe.

Voor de deskresearch hebben we onder meer gebruik gemaakt van (online) bibliotheken zoals de mediatheek van de Politie Academie en de digitale databank ScienceDirect (www.sciencedirect.com), kennis omtrent documenten bij onze respondenten, de newsportal van LexisNexis (inhoud van een groot aantal dagbladen) en open bronnen via internet.

Bij ieder interview is gebruik gemaakt van een interviewprotocol, waarvoor de onderzoeksvragen als leidraad golden. Kennis over technische en juridische oplossingen die naar voren kwamen uit een interview hebben we steeds meegenomen naar de volgende te interviewen persoon. Ook hebben we deze nieuwe kennis teruggekoppeld naar personen die we reeds geïnterviewd hadden, zodat de betreffende personen hierop konden reageren. Voor de interviews zijn personen benaderd vanuit het KLPD (technici, rechercheurs en beleidsmakers) het Nederlands Forensisch Instituut (NFI), Internet Service Providers (zowel juristen als technici), het particuliere Meldpunt Kinderporno op Internet en commerciële beveiligingsbureaus op het gebied van ICT.

Aanvullend op de twee centrale methoden verrichtten we tweemaal een schouw van de door de politie gehanteerde blacklist. We bekeken een selectie van de in de lijst opgenomen sites. Het doel hiervan was om te zien of de inhoud van de sites op de blacklist dusdanig is dat gesproken kan worden over strafbaarheid in de zin van artikel 240b Sr. Ook is bekeken in hoeverre de huidige blokkeermethode, te weten op domeinniveau, mogelijk leidt tot het blokkeren van niet strafbare inhoud (zie hoofdstuk 2 voor uitleg over blokkeren op domeinniveau en overblocking). Tot slot is tijdens de schouws gekeken naar de herkomst van de sites. Immers, sites met een onmiskenbaar onrechtmatige inhoud die in Nederland zijn gehost, kunnen na melding aan de betreffende internetprovider direct uit de lucht worden gehaald. Hetzelfde geldt, zij het via een omweg, voor sites die in landen zijn gehost waarmee Nederland een justitieel samenwerkingsverband heeft (op basis van een rechtshulpverdrag of het Cybercrimeverdrag van de Raad van Europa[3]). Naast de onderzoekers waren tijdens de eerste schouw rechercheurs van het KLPD en medewerkers van het genoemde Meldpunt Kinderporno op Internet aanwezig. De tweede schouw werd uitgevoerd door een van de onderzoekers en een rechercheur van het KLPD.

We selecteerden de eerste keer uit de lijst van 110 sites steekproefsgewijs een serie van 36 en de tweede keer uit de lijst van 103 een serie van 34 sites.[4] We selecteerden beide keren elke derde site op de lijst. Een medewerker van het KLPD toonde ons de betreffende sites, die we vervolgens beoordeelden aan de hand van een protocol (bijlage III).

Een andere aanvulling op dit onderzoek betreft een presentatie die voor ons werd gehouden door het bedrijf Comsenso over haar filterinstrument.

Aparte aandacht verdient het verkrijgen van informatie over de situatie in het buitenland. Eerdere ervaringen met het benaderen van respondenten bij politie- en opsporingsdiensten in het buitenland leren ons dat daarvan niet veel moet worden verwacht, ook niet als zij via vertrouwde (politie)kanalen worden benaderd. Dat ondervonden we in een onderzoek naar criminaliteit in cyberspace (Stol e.a., 1999) en in een onderzoek naar het gebruik van forensische databases (Stol e.a., 2005). De meeste informatie kregen we eertijds nog via persoonlijke

[3] Door Nederland ondertekend in 2001, geratificeerd in 2006 en inwerking getreden in 2007.
[4] In paragraaf 5.4, waar we de uitkomsten van de schouw presenteren, staan ook de met deze steekproeven gerealiseerde betrouwbaarheidsmarges.

contacten in het wetenschappelijke veld. Voor informatie over de situatie in het buitenland maakten we in onderhavig onderzoek derhalve gebruik van open bronnen via internet, overheidsdocumenten, literatuur en persoonlijke contacten met (politie)wetenschappers en andere sleutelpersonen uit Noorwegen, Denemarken, Duitsland, België, Frankrijk, Italië, Turkije en de Verenigde Staten. Via hen zochten we met name naar informatie over de mate van filteren in hun land en naar eerder onderzoek naar (de effectiviteit van) internetfilters. Tevens spraken we lopende het onderzoek over dit onderwerp met vertegenwoordigers van het International Centre for Missing and Exploited Children te Brussel (www.icmec.org); met verschillende deelnemers aan de Egyptian Internet Safety Conference te Cairo op 25 en 26 maart 2008 en met enkele deelnemers aan de zogenoemde octopus-conferentie op 1 en 2 april 2008 te Straatsburg. Een van de onderzoekers (Stol) leest Noors, Deens en Zweeds, zodat we ons voor de situatie in die landen steeds hebben kunnen baseren op de oorspronkelijke geschriften in de betreffende taal.

Onderzoeksstrategie

In dit onderzoek zijn technische, recherche- of handhavingstactische en juridische kennis over het tegenhouden van kinderporno op internet met elkaar verbonden. Het leggen van dwarsverbanden tussen de tijdens het onderzoek verkregen informatie (bijvoorbeeld informatie over technische mogelijkheden en informatie over juridische beperkingen), hebben we niet bewaard tot de analysefase aan het einde van het onderzoek, maar zijn van meet af aan ingebouwd in het onderzoeksproces. Dit hebben we gedaan door de gedane bevindingen direct en expliciet op te nemen in de aandachtspuntenlijst voor het lopende deskresearch en de nog komende interviews. Als een respondent bijvoorbeeld een instrument of *tool* noemde dat kan dienen om kinderporno te blokkeren, dan namen we de (technische en juridische) grondslagen van dat instrument op als aandachtspunt in de deskresearch en als gespreksonderwerp voor de nog te houden interviews. Op die manier konden bijvoorbeeld juristen reageren op door technici geopperde technische mogelijkheden en tekortkomingen, konden opsporingsdeskundigen reageren op visies van ISP's, et cetera. In verband met deze onderzoeksstrategie, hebben we standaard aan de respondenten gevraagd of we hen naderhand nog aanvullende vragen mochten voorleggen.

Overeenkomstig deze strategie is niet geheel op voorhand vastgelegd welke sleutelfiguren geïnterviewd zouden worden. In totaal hebben we 25 personen geïnterviewd (zie bijlage II). In de voorbereiding van dit onderzoek hebben we een lijst opgesteld met 15 sleutelfiguren uit verschillende organisaties. De overige interviews zijn gehouden door het hanteren van de zogenaamde sneeuwbalmethode. Daarvoor hebben we aan iedere geïnterviewde de vraag gesteld welke andere sleutelfiguren we zouden moeten benaderen voor dit onderzoek.

HOOFDSTUK 2

Filtertechnieken

In dit hoofdstuk bespreken we de technische mogelijkheden om kinderporno op internet te filteren en te blokkeren. We presenteren eerst enkele technische begrippen (paragraaf 2.1). Daarna gaan we in op de manieren waarop kinderporno op internet verspreid en aangeboden wordt (2.2). Dat is van belang om te weten hoe er gefilterd en geblokkeerd zou kunnen worden. Daarna bespreken we de verschillende filtermogelijkheden (2.3). We besluiten het hoofdstuk met een samenvatting (2.4). Een verklarende (technische) begrippenlijst staat achter in dit rapport.

2.1 Digitale verspreiding van kinderporno

Vormen van verspreiding

Om kinderporno op internet te filteren en te blokkeren is het van belang om te weten hoe de verspreiding op internet precies verloopt. Staat de meeste kinderporno op gemakkelijk te bereiken websites of is het alleen te vinden op verborgen plaatsen op internet? Cijfers over de mate en route van verspreiding zijn echter niet bekend. Wat we wel weten is het aantal keer dat kinderporno is *gemeld* bij het particuliere Meldpunt Kinderporno op Internet en via welke route die gemelde kinderporno werd verspreid. Uit de jaarverslagen van het meldpunt blijkt in ieder geval dat kinderporno op verschillende manieren wordt verspreid.

In 2006 betrof 65,2 procent van de meldingen kinderporno via spam; 25,4 procent via websites en 4,8 procent via P2P-systemen (tabel 2.1). De meeste meldingen (90,6%) hebben betrekking op websites en spam. Spam bevat vaak links naar websites en nieuwsgroepen waar de kinderporno zich bevindt. In de jaren 2002-2005 is het beeld niet wezenlijk anders, zij het dat in 2006 ten opzichte van 2002 wat meer de nadruk ligt op verspreiding via spam.

Tabel 2.1: Meldingen over kinderporno bij het particuliere Meldpunt Kinderporno op Internet

Verspreidingswijze	2002		2003		2004		2005		2006	
	Meld.	KP*	Meld.	KP*	Meld.	KP*	Meld.	KP*	Meld.	KP*
Websites	2.506	1.592	2.018	1.090	2.321	1.195	2.121	803	1.715	670
Spam	2.565	-	3.100	567	3.153	1.999	5.271	2.378	4.401	1.982
Nieuwsgroepen	212	73	151	104	88	62	61	35	124	30
Peer-2-peer **	479	-	439	-	368	-	291	-	326	-
Chat **	69	-	52	-	79	-	92	-	154	-
Overige **	32	-	37	-	12	-	38	-	32	-

Bron: MKI, 2003, 2004, 2005, 2006, 2007.

* Meldingen die volgens het meldpunt kinderpornografie betreffen.

** Meldingen aangaande deze categorieën worden niet door het meldpunt gecontroleerd.

Uit deze cijfers mogen we niet concluderen dat kinderporno overwegend via websites en spam wordt verspreid. Het gaat immers om *gemelde* kinderporno. De conclusie moet eerder zijn dat vooral kinderporno op websites en via spam aanleiding is voor internetters om een melding te doen.

Uit tabel 2.1 en eerder onderzoek naar kinderpornografie op internet (Stol e.a., 1999; Stol, 2004; Oosterink en Van Eijk, 2006; Schell e.a., 2007) kunnen we afleiden via welke onderdelen van internet kinderporno in ieder geval wordt verspreid:

- *Spam*. Ongevraagde en veelal ook ongewenste e-mail.
- *Website*. Een verzameling samenhangende webpagina's die op het internet te bereiken zijn. Dit kunnen zowel openbaar toegankelijke als gesloten websites zijn (waarvoor bijvoorbeeld eerst betaald moet worden).
- *Peer-to-peer netwerk*. Netwerk dat onderlinge uitwisseling tussen twee of meer partijen mogelijk maakt, zoals Kazaa, eDonkey LimeWire en Gnutella. Bestanden die worden uitgewisseld staan niet op centrale servers maar op de computers van de gebruikers zelf. Dit in tegenstelling tot normale websites, waarbij de gebruiker contact heeft met de centrale server waarop de website gehost wordt. Volgens respondenten vindt via P2P-netwerken op substantiële schaal verspreiding plaats van kinderpornografie. Ook de NFI-onderzoekers Oosterink en Van Eijk (2006) komen tot die conclusie. De P2P-programma's gaan volgens Schell e.a. (2007) in de toekomst zelfs de grootste rol spelen in de distributie van kinderporno, met name door de via die weg te realiseren anonimiteit en de mogelijkheden van het versleutelen van bestanden.
- *Virtuele harde schijven*. Een opslagmiddel dat zich niet lokaal onder direct handbereik van de gebruiker bevindt, maar op afstand (een e-mail account kan ook dienen als virtuele harde schijf). Er zijn op dit moment geen aanwijzingen dat dergelijke accounts door kinderpornoverzamelaars gebruikt worden. Dit kan echter komen doordat hiernaar geen structureel zaakonderzoek wordt gedaan (Oosterink en Van Eijk, 2006). Ook politierespondenten wijzen op de mogelijkheid dat kinderporno via virtuele harde schijven wordt verspreid.
- *Nieuwsgroepen*. Een wereldwijd netwerk van servers dat als doel heeft om berichten te verspreiden onder de gebruikers (ook bekend als Usenet). De berichten blijven gedurende een bepaalde tijd toegankelijk voor de nieuwsgroepbezoekers.
- *Chat*. Een protocol dat het snel achter elkaar plaatsen van berichten van twee of meerdere gebruikers mogelijk maakt ('chatten'). Het IRC-protocol (Internet Relay Chat) is het meest gebruikte protocol om te chatten. Andere chat-technologieën zijn Instant Messaging, ICQ of Windows Live Messenger.

We weten dan wel niet precies welk aandeel van de kinderporno op internet wordt verspreid via welke route, we weten wel dat de wijze waarop de verspreiding loopt aan verandering onderhevig is, deels omdat er voortdurend nieuwe technische mogelijkheden ontstaan (Deibert e.a., 2008) en deels omdat de aanbieders van kinderporno reageren op repressieve maatregelen (Stol, 2004). Zo gezien is te verwachten dat het effectief filteren van kinderpornografie in de loop der jaren steeds ingewikkelder wordt.

Globaal overzicht van blokkeermogelijkheden

We geven hier eerst een globaal overzicht van de blokkeermogelijkheden. In paragraaf 2.3 gaan we meer in detail op deze materie in.

Een eerste vereiste voor het blokkeren van kinderpornografisch materiaal is dat het niet versleuteld of gecomprimeerd is of op andere wijze onherkenbaar gemaakt. Om te kunnen blokkeren moet men (of een softwareprogramma) immers kunnen zien of het bestand kinderpornografie bevat. De enige praktische mogelijkheid om versleuteld of gecomprimeerd kinderpornografisch materiaal te blokkeren is om al het versleutelde of gecomprimeerde materiaal te blokkeren. Maar waterdicht is dat ook weer niet want dan rest nog het probleem dat niet alle versleutelde bestanden als zodanig te herkennen zijn. Wil men iedere mogelijkheid op verspreiden van kinderpornografie uitsluiten, dan dienen dus *alle* bestanden te worden geblokkeerd. Daarmee zien we direct de beperking van filters: er is uiteindelijk altijd een omweg, want men kan nu eenmaal niet alles blokkeren. Met slim filteren kan men wel die omweg zo moeilijk mogelijk maken.

Verkeer van websites kan worden geblokkeerd op verschillende manieren. Een website, en dus alle informatie die op die site staat, kan aan de hand van bepaalde kenmerken (bijvoorbeeld het IP-adres of de domeinnaam) worden tegengehouden. Verderop bespreken we methoden daarvoor. Om niet de hele website maar alleen bepaalde content (bijvoorbeeld één plaatje) tegen te houden moet er gebruik worden gemaakt van Deep Packet Inspection (DPI). Bij deze methode wordt er gekeken in de informatiepakketjes die tussen de gebruiker en de webserver worden verstuurd.

Ook het blokkeren van content afkomstig uit een P2P-netwerk vergt DPI. De verstuurde content is nu niet van een website afkomstig maar van (de computer van) een internetter. In dat geval vereist blokkeren dat men eerst bepaalt welk verkeer afkomstig is van P2P-systemen (dat is technisch mogelijk) en vervolgens wat er in de verstuurde pakketjes zit. Bevat een pakketje content die niet mag worden doorgelaten, bijvoorbeeld omdat het gaat om bekende kinderpornoafbeeldingen, dan kan die worden geblokkeerd.

Voor het blokkeren van content afkomstig van een virtuele harde schijf, geldt hetzelfde als voor het blokkeren bij P2P-netwerken: het blokkeren van bepaalde content is mogelijk met behulp van DPI.

Het blokkeren van kinderpornografisch materiaal afkomstig uit nieuwsgroepen is ook mogelijk. Een Internet Service Provider (ISP) kan de nieuwsgroep van een nieuwsgroepenserver die hij niet zelf host eenvoudigweg niet accepteren en dus niet doorgeven aan zijn abonnees. Dat gebeurt op dit moment ook al.

Het blokkeren van de uitwisseling van kinderpornografisch materiaal via de chat is relatief lastig. Een chatkanaal kan door internetters zelf geopend worden. Er zal een constante controle op chatkanalen moeten zijn om effectief te kunnen blokkeren. Een mogelijkheid is om een chatkanaal te blokkeren indien in de naam van het betreffende kanaal bepaalde sleutelwoorden voorkomen.

De aanbieders van kinderpornografie

Volgens verschillende van onze respondenten zijn er twee verschillende groepen aanbieders van kinderpornografisch materiaal: een commerciële groep en een groep 'liefhebbers'. De commerciële groep ziet de handel in kinderpornografisch materiaal als een nieuwe manier om geld te verdienen. Nieuwe klanten worden bijvoorbeeld geworven door het versturen van spam of nieuwgroepberichten en er moet betaald worden met een creditkaart.

De tweede groep, de 'liefhebber', is doorgaans niet uit op geld. Deze groep wil nieuw materiaal krijgen. Journalist Van Kleef (2004) beschrijft in een artikel in de Nieuwe Revu de virtuele wereld van deze pedofielen. De strekking van dit artikel komt overeen met wat experts ons tijdens de interviews hebben gezegd over het via internet verkrijgen van toegang tot een groep met 'liefhebbers'. De teksten in de kaders zijn afkomstig van Van Kleef.

Stap 1: de aanbieder vinden:

De eerste stap om kinderporno te verkrijgen is het vinden van de aanbieder. Dit is echter lastiger dan het in eerste instantie lijkt.

Maar wie niet weet waar hij kinderporno moet zoeken, vindt nog geen foto van een blote peuter op het strand. Zoekmachine Google levert 6,8 miljoen hits op de term childporn maar al die links verwijzen gewoon naar legale pornowebsites waar de modellen niet onder de 18 zijn.

De gemiddelde surfer komt dus niet zo maar terecht bij kinderporno. Wie echter op de juiste plaats de juiste vraag stelt komt uiteindelijk wel in de hoek terecht waar kinderporno verspreid wordt.

In de chatroom van Free Spirits treffen we Nestor en die heeft een tip: "Ik heb gehoord dat op de Alex BBS wel eens zulke foto's staan. Meer weet ik niet." Alex is een digitaal prikbord waar links naar gratis sexsites worden uitgewisseld. Illegale porno zit er op het eerste gezicht niet bij. We besluiten zelf een bericht te plaatsen. We schrijven dat we kinderporno zoeken en vermelden een hotmailadres. Een uur later zit de mailbox stampvol.

Stap 2: anoniem en ontraceerbaar surfen
Eenmaal doorverwezen naar een website met kinderporno moet er een aantal veiligheidsmaatregelen worden genomen om ervoor te zorgen dat de aanbieder en de andere gebruikers van de website niet het risico lopen om gepakt te worden doordat de nieuwe klant door de politie getraceerd kan worden. Indien de nieuwe klant de politie naar het netwerk leidt zijn immers ook de andere gebruikers in gevaar.

Ontraceerbaar surfen is mogelijk, maar er is een hoop voor nodig. We moeten een firewall gebruiken, software installeren die het geheugen van de computer kan wissen en ons ip-nummer versleutelen.

Stap 3: binnentreden in een groep
Indien de voorzorgsmaatregelen getroffen zijn, kan er contact worden gezocht met een aanbieder van kinderporno.

Twipsy mailt een webadres en schrijft dat we in moeten loggen met een bepaalde code. We klikken op de link die naar het online prikbord -"or all your questions about this nice hobby!"- verwijst. Er verschijnt een inlogvenster. We typen de code in die we van Twipsy hebben gekregen. Een paar seconden later verschijnt een andere webpagina. Welcome at K-Book staat bovenaan. Enjoy your stay!

Stap 4: klimmen in de hiërarchie
Eenmaal aangekomen in een groep 'kinderpornoliefhebbers' moet eerst het vertrouwen van de overige leden in de groep gewonnen worden. De hiërarchie binnen de groep blijkt belangrijk. Leden van de groep die grote hoeveelheden nieuw materiaal op het netwerk zetten, worden volgens het artikel vereerd als helden.

Is dit nu een kinderporno-walhalla? vragen wij. "Wacht af," raadt Sirax aan. "De chat is het belangrijkst hier. Zorg dat je wat vrienden maakt. Verspreid je nestgeur. Dan komt alles goed." (…) Hier selecteert Twipsy en de rest wie ze doorsluizen naar een niveau hoger. Daar vind je betere foto's en films.

Op de vraag waarom, ondanks alle veiligheidsmaatregelen, er de afgelopen maanden vele arrestaties van pedofielen geweest zijn antwoord een lid de groep: "*Die zaten in een hele andere tak van sport. Die hadden zich aangemeld bij commerciële kinderpornowebsites. Ze betaalden met hun creditcard. Ja, dan vraag je om politie aan de deur.*"

Resumerend
We kennen verschillende *manieren waarop* kinderporno verspreid wordt, we weten echter niet in *welke mate* het gebeurt. Ook weten we niet hoe de verhoudingen liggen tussen de verschillende wijzen van verspreiden. We kunnen dus niet aangeven wat filteren en blokkeren van bepaalde verspreidingsmanieren voor effect heeft op de totale verspreiding van kinder-

porno. In de volgende paragrafen bespreken we uitsluitend die verspreidingsvormen waarbij filteren en blokkeren technisch haalbaar is.

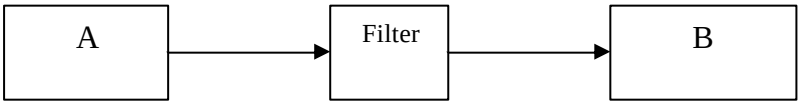
Er zijn globaal gesproken twee soorten aanbieders van kinderporno. Er is een commerciële groep die geld wil verdienen en er is een groep liefhebbers die hun eigen collectie wil uitbreiden.

2.2 Technische methoden om te blokkeren

Inleiding

Blokkeren is het tegenhouden van bepaalde content. Dit kan zowel een gehele website of nieuwsgroep zijn of alleen een bepaalde afbeelding. Om te kunnen blokkeren moet er *altijd* gefilterd worden. De informatiestroom moet immers bekeken worden om te kunnen beslissen welke informatie wel en welke niet mag worden doorgegeven. Het filter is feitelijk een digitale *tool* voor het selectief doorlaten van informatie. Het filter wordt geplaatst op een bepaalde informatieroute (zie figuur 2.2). Het filter bevat software met – door mensen bepaalde – beslissingsregels aan de hand waarvan het verkeer wordt beoordeeld en al dan niet wordt doorgelaten. Daarbij kan logisch gesproken worden geselecteerd op 'statuskenmerken', zoals afzender van bepaalde content (alle informatie afkomstig van een bepaald domein of IP-adres wordt niet doorgelaten) of op de inhoud van de content (bepaalde sleutelwoorden of afbeeldingen).

Figuur 2.2: Een filter op de informatieroute van A naar B



Hierna bespreken we verschillende blokkeringsmethoden. Van elke methode beschrijven we de werking en de belangrijkste begrippen. Ook kijken we naar de effectiviteit van de verschillende methoden. We hebben het dan over de technische haalbaarheid, de duurzaamheid en de mogelijkheden om het filter of de blokkade te omzeilen. Tenslotte geven we aan of de methode momenteel in gebruik is en in welke landen. Voor technische details verwijzen we naar de vakliteratuur (Clayton, 2005; Consumer Reports, 2005; Deshmukh en Rajagopalan, 2005; Edelman, 2003; Greenfield e.a., 2001; Fleck e.a., 1996; Jones en Rehg, 1998; Kranich, 2004; Resnick e.a., 2004; Shih e.a., 2007; Schell e.a., 2007; Wang e.a., 1998; Yang e.a., 2004; Yoo, 2004; Zeng e.a., 2004; Zittrain en Edelman, 2002).

Door de ontwikkeling van de 3G-standaard voor mobiele telefoons, waardoor gebruikers ook breedband internet kunnen gebruiken op hun telefoon, beperkt de toegang tot kinderpornografisch materiaal op internet zich niet langer tot alleen de computergebruikers. Het is nu immers ook mogelijk om websites op een mobiele telefoon te bekijken en afbeeldingen te downloaden. Technisch gezien is er echter geen verschil tussen internet op een computer en op een 3G mobiele telefoon. De technische mogelijkheden om kinderpornografisch materiaal te blokkeren blijven daarom ook dezelfde. De technische methoden die we verderop in dit hoofdstuk bespreken gelden daarom steeds voor zowel computergebruikers als 3G mobiele telefoongebruikers.

Blokkeren op IP-adres

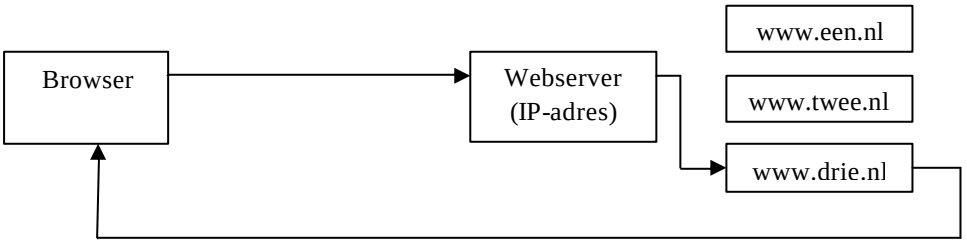
Algemene beschrijving. De meest grofmazige methode om content op internet te blokkeren is het blokkeren van IP-adressen. Een IP-adres (IP staat voor Internet Protocol) is een unieke code voor een machine die is aangesloten op internet. Zo heeft elke computer die gebruikt wordt om op internet te surfen een unieke code, maar ook de server waarop de website gehost wordt, heeft zo'n code. Op deze manier kunnen computers elkaar vinden en met elkaar communiceren.

Het IP-adres is vergelijkbaar met een telefoonnummer en bestaat uit vier groepen getallen die gescheiden worden door een punt. Bijvoorbeeld 123.123.123.123. We beperken ons hier tot de huidige, vierde versie: IPv4. Op dit moment is dit het meest gebruikte Internet Protocol. Maar doordat binnen IPv4 de IP-adressen op raken is IPv6 ontwikkeld. Deze versie zorgt ervoor dat er meer IP-adressen gebruikt kunnen worden. De komende jaren echter zal IPv4 nog door verreweg de meeste internetters worden gebruikt.

IP-adres: 123.123.123.123

Onder andere door het tekort aan IP-adressen zijn er methoden ontwikkeld waardoor één IP-adres meerdere websites kan herbergen. Het toekennen van meerdere domeinennamen aan één IP-adres kan onder andere door het gebruik van een 'shared web hosting service' of een 'virtual hosting service'. Bij een dergelijke vorm van hosting kunnen meerdere websites via één webserver zijn verbonden met het internet. Behalve dat men op deze wijze zuiniger omspringt met IP-adressen is deze vorm van hosting goedkoper omdat men immers met verschillende gebruikers één IP-adres deelt. Elke website heeft in dat geval een eigen stukje van de server in gebruik dat gescheiden is van de andere websites. Indien een internetter een bepaalde website opvraagt dan stelt zijn webbrowser een request aan het IP-adres. In de request staat naast het IP-adres extra informatie, zoals de domeinnaam en de URL. De webserver bepaalt dan welke website getoond moet worden (figuur 2.3).

Figuur 2.3 Meerdere domeinnamen op één IP-adres



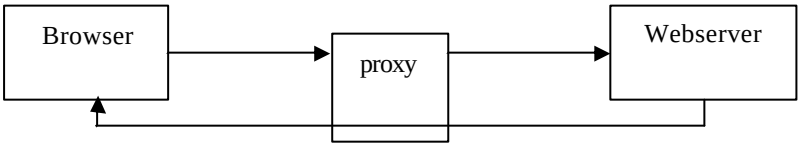
Om op basis van een IP-adres te kunnen blokkeren zal er een lijst moeten worden aangemaakt met IP-adressen die niet bezocht mogen worden. Deze lijst wordt gekoppeld aan een zogenoemde proxy: een computer waar al het internetverkeer doorheen moet voordat het bij de webserver en dus de internetgebruiker aankomt (zie figuur 2.4).

Een webserver is een computerprogramma dat van de browser van de internetter verzoeken ontvangt en vervolgens documenten naar de internetter terugstuurt. Het kan zijn dat voor de webserver een eigen computer ingericht is, in dat geval kan die computer met 'webserver' worden aangeduid. In figuur 2.4 zien we dat de webbrowser via een proxy (zie hierna)

een website aanvraagt bij de webserver. Op deze webserver staat de website die aangevraagd is. De webserver geeft vervolgens de website door aan de webbrowser.

Een proxy kan vergeleken worden met een tussenpersoon. Het is een machine die staat tussen de computer van de gebruiker en de computer waarmee gecommuniceerd wordt. Een proxy kan door een ISP in het netwerk geïmplementeerd worden. Al het verkeer van de gebruikers van die ISP dat het netwerk opgaat, loopt dan door de proxy. Een proxy kan verschillende doelen hebben, bijvoorbeeld om het internetverkeer te versnellen (een zogenaamde web proxy). Dit werd met name in de beginperiode van het internet gebruikt. De proxy heeft namelijk een geheugen. Indien iemand een internetpagina oproept, onthoudt de proxy de pagina en zodra een andere gebruiker dezelfde pagina oproept hoeft er geen contact meer te worden gelegd met de webserver die de pagina host. De pagina kan direct uit het geheugen van de proxy worden gehaald. Door de huidige grote snelheden van internet wordt deze methode tegenwoordig bijna niet meer gebruikt. Een andere mogelijkheid om een proxy toe te passen is om verkeer te filteren. De proxy bevat dan een filterprogramma dat bijvoorbeeld bepaalde, vooraf in een lijst opgenomen IP-adressen blokkeert. Het gaat hier om een zogenoemde transparante proxy: deze proxy is voor de gebruiker onzichtbaar. Voor effectief filteren is uiteraard noodzakelijk dat de proxy dwingend is opgenomen in de communicatieketen.

Figuur 2.4. Blokkeren op IP-adres



Effectiviteit. Blokkeren op IP-adres is een technisch vrij simpele methode maar zorgt voor een aanzienlijk risico op overblocking (Clayton, 2005). Overblocking is een technisch begrip en betekent dat men door de gekozen methode verkeer tegenhoudt dat men niet wilde tegenhouden. Uit onderzoek blijkt dat 87,3 procent van de actieve .org-, .com- en .net-domeinnamen hun eigen IP-adres met één of meer andere domeinnamen deelt (Edelman, 2003) (vgl. figuur 2.3). Meer dan tweederde (69,8%) van de actieve domeinnamen deelt zelfs het eigen IP-adres met meer dan 50 andere domeinnamen.

Domeinnamen hebben dus niet allemaal een uniek IP-adres, alhoewel dit voor de gebruiker niet altijd zichtbaar is. Verder zijn de verschillende domeinen die op één IP-adres staan vaak niet homogeen. Er zijn bijvoorbeeld IP-adressen met domeinen die zowel seksuele content als niet seksuele content bevatten (Edelman, 2003).

Bovenstaande illustreert de complicaties met betrekking tot het blokkeren van sites op IP-adres. Door de grote hoeveelheid verschillende domeinnamen die gebruik maken van hetzelfde IP-adres en de verschillen in onderwerp van de domeinen is er dus bijna altijd sprake van overblocking. Websites zonder kinderpornografisch materiaal worden dan ten onrechte ook geblokkeerd.

Een manier om de proxy van een bepaalde ISP te omzeilen is om te kiezen voor een andere ISP – een ISP die niet blokkeert, eventueel een ISP in het buitenland. Deze route om het blokkeren te omzeilen kan worden tegengegaan door te blokkeren aan de landsgrenzen.

Gebruik. Voor zover ons bekend, wordt het blokkeren van IP-adressen niet als filtermethode gebruikt.

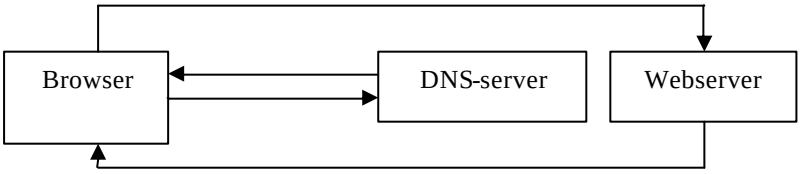
Blokkeren op domeinnaam

Algemene beschrijving. Blokkeren van websites op domeinnaam is specifieker dan blokkeren op IP-adres. Een IP-adres kan immers meerdere domeinnamen omvatten. Een domeinnaam is een eenvoudig te onthouden naam die in eerste instantie verwijst naar een IP-adres. Een voorbeeld van een domeinnaam is 'www.kinderporno.nl'. Verwijst een domeinnaam naar een machine waarop meerdere domeinen zijn gehuisvest (bijvoorbeeld behalve www.kinderporno.nl ook www.youngmodels.nl en www.preteens.nl) dan sluist de server de internetter op grond van de domeinnaam (www.kinderporno.nl) door naar dat domein binnen de server. Zie ook figuur 2.3.

Domeinnaam behorende bij het IP-adres 123.123.123.123: www.kinderporno.nl

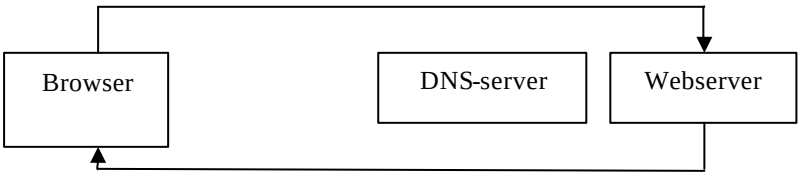
Domeinnamen zijn bedacht omdat de cijferreeksen van het IP-adres voor mensen moeilijk te onthouden zijn. Het omzetten van een domeinnaam naar een IP-adres gebeurt door een DNS-server (Domain Name Server). Zodra een internetter middels de webbrowser op zijn computer een domeinnaam aanvraagt, maakt de browser contact met de DNS-server van de Internet Service Provider (ISP). De DNS-server zoekt dan het IP-adres bij de opgegeven domeinnaam. Het IP-adres wordt teruggezonden aan de webbrowser en deze kan contact maken met het IP-adres op de webserver waarop de website gehost wordt (zie figuur 2.5).

Figuur 2.5. Het opvragen van een webpagina middels een domeinnaam



Indien een gebruiker het IP-adres van de te bezoeken website weet en dat in zijn browser intikt wordt er overigens geen gebruik van een DNS-server gemaakt. De browser maakt dan direct contact met de webserver die de website host. In figuur 2.6 staat dit schematisch weergegeven.

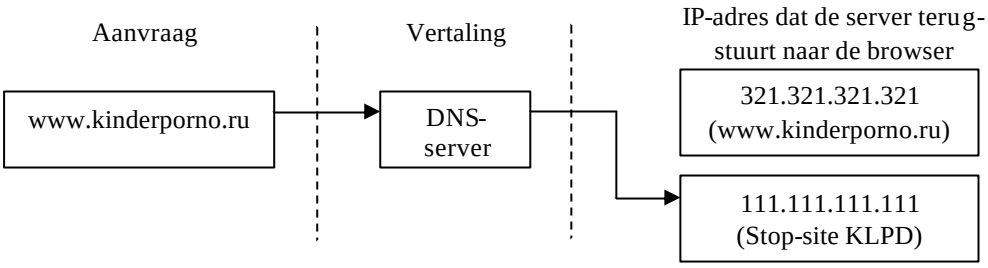
Figuur 2.6. Het opvragen van een webpagina middels een IP-adres



De meeste mensen maken echter gebruik van de gemakkelijk te onthouden domeinnamen en laten de vertaling naar IP-adres over aan de DNS-server. Indien aan de hand van een domeinnaam een website wordt opgevraagd, moet het verkeer door de DNS-server van de ISP. In de DNS-server kan de koppeling tussen de domeinnaam en het IP-adres aangepast worden. Indien iemand een IP-adres van een site opvraagt die op de zwarte lijst staat, stuurt de DNS-

server niet het IP-adres van de betreffende website maar een andere IP-adres (in Nederland krijgt de aanvrager een 'stoppagina' te zien waarop staat dat op de aangevraagde pagina strafbare content staat). In figuur 2.7 staat het verkeerd toewijzen van een IP-adres aan een domeinnaam schematisch weergegeven.

Figuur 2.7 . Verkeerd toewijzen van een IP-adres aan een domeinnaam



We zien dat de website 'www.kinderporno.ru' wordt aangevraagd. De gebruiker heeft in zijn webbrowser deze domeinnaam ingetypt en wordt verbonden met de DNS-server van zijn ISP. De DNS-server moet de domeinnaam nu vertalen in een IP-adres en deze teruggeven aan de webbrowser. Oorspronkelijk was het domein 'www.kinderporno.ru' gekoppeld aan het (fictieve) IP-adres 321.321.321.321. Maar omdat op dit IP-adres kinderporno staat is in de DNS-server de domeinnaam gekoppeld aan het IP-adres van de 'stoppagina' van het Korps Landelijke Politiediensten (KLPD): 111.111.111.111. De DNS-server geeft nu het IP-adres 111.111.111.111 terug aan de webbrowser. De webbrowser haalt vervolgens van het internet die pagina (vgl. figuur 2.5). De gebruiker die de pagina www.kinderporno.ru aanvroeg krijgt nu niet de gewenste site, maar de stoppagina van het KLPD.

Effectiviteit. Deze methode is vrij gemakkelijk en relatief goedkoop te implementeren. Er hoeven geen aanpassing bij de gebruiker en geen grote aanpassingen bij de ISP te worden gedaan. Bij de effectiviteit van deze methode zijn enkele opmerkingen te maken.

Ten eerste is het vrij eenvoudig om te veranderen van DNS-server. Wanneer een internetter een DNS-server gebruikt die wel steeds het gevraagde IP-adres toewijst, kan de gebruiker alsnog op de geblokkeerde sites komen. De gebruiker kan zo'n DNS-server vinden door te switchen van ISP (mits de betreffende ISP de sites niet blokkeert), maar er zijn ook bedrijven die commercieel een DNS-server aanbieden. Ten slotte is het voor de gevorderde internetter mogelijk om zelf een DNS-server te maken (die minder gevorderde internetters dan weer kunnen overnemen).

Ten tweede kan een internetter de geblokkeerde pagina nog steeds bereiken door het oorspronkelijke IP-adres in te typen. In dat geval loopt het verkeer immers niet door de DNS-server (figuur 2.6). De internetter kan via die route ook specifieke pagina's opvragen, bijvoorbeeld '321.321.321.321/index.htm'. Het IP-adres 321.321.321.321 zorgt ervoor dat de internetter langs de DNS-server meteen contact heeft met de gewenste webserver; het toevoegsel 'index.htm' maakt dat de internetter van de webserver de gewenste pagina krijgt.

Ten derde is er, net als bij blokkeren op IP-adres, sprake van overblocking. Er worden nu dan wel geen hele machines, maar wel hele domeinen geblokkeerd.

Gebruik. Het blokkeren op domeinniveau middels het aanbrengen van wijzigingen in de DNS-server wordt in verschillende Europese landen gebruikt, waaronder Noorwegen, Zweden, Denemarken en Nederland (zie hoofdstuk 4 en 5).

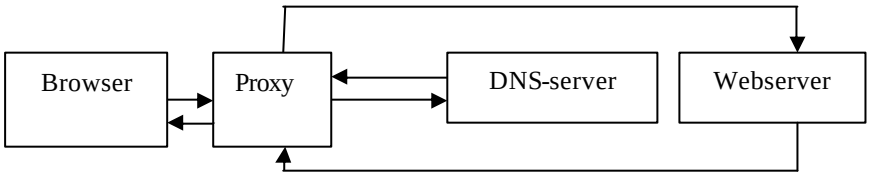
Blokkeren op URL

Algemene beschrijving. Een URL (Uniform Resource Locator) is een verwijzing naar een specifiek bestand of gegeven op een machine. Bijvoorbeeld een webpagina, databasegegeven of e-mailadres. Een URL bestaat uit meerdere delen, te weten 'de naam van de machine' en 'een aantal directory-paden of filenamen die op die machine zitten'. Bijvoorbeeld: www.kinderporno.nl/index.html. De naam van de machine is dan: www.kinderporno.nl en het directorypad is dan index.html.

Twee voorbeelden van een URL: Een bestand op het IP-adres 123.123.123.123: www. kinderporno.nl/index.htm Een afbeelding op het IP-adres 123.123.123.123: www.kinderporno.nl/index/afbeelding.jpg

Het blokkeren op URL is de meest fijnmazige methode. Er wordt immers niet alleen naar het domein gekeken maar ook naar het specifieke bestand of gegeven binnen dat domein. Op die manier kan bijvoorbeeld alleen een plaatje op een website of een deel van een website worden geblokkeerd. Voor het blokkeren op URL is het gebruik van een proxy vereist. Al het verkeer dat naar de webserver gaat moet via de proxy. Aan de proxy kan dan een lijst met specifieke URL's gekoppeld worden die niet mogen worden doorgelaten. Een schematische voorstelling staat in figuur 2.8.

Figuur 2.8. Blokkeren op URL



Effectiviteit. Deze methode is fijnmazig, er worden specifieke URL's geblokkeerd en er is zodoende geen sprake van overblocking (tenzij fouten worden gemaakt). Het blokkeren van URL's is duurder dan het blokkeren van domeinen. Dit komt mede door het verplichte gebruik van proxies (Clayton, 2003).

Doordat al het netwerkverkeer door de proxy moet, neemt de snelheid van het netwerk af. Daarnaast werkt deze methode niet met beveiligde verbindingen. Een beveiligde verbinding, bijvoorbeeld met een bank, komt alleen tot stand als de verbinding tussen de gebruiker en de host niet omgeleid wordt. Doordat het verkeer door de proxy gaat, wordt het wel omgeleid en komt de verbinding niet tot stand.

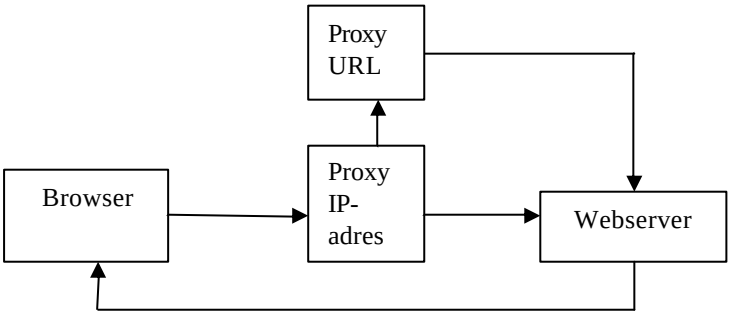
Gebruik. Deze methode, waarbij het internetverkeer door een of meerdere proxies wordt geleid, is in verschillende landen in gebruik, bijvoorbeeld in Saoedi-Arabië. De regering heeft een 'Internet Service Unit' die het netwerkverkeer binnen Saoedi-Arabië verbindt met de rest van de wereld (Zittrain en Edelman, 2002; zie ook paragraaf 4.5). De structuur van internet is daar dus zodanig dat het onmogelijk is om het internet anders dan via proxies te benaderen. Er is een blacklist gekoppeld aan de proxies en zodra een domein of URL wordt opgevraagd die op de blacklist staat, krijgt de gebruiker een site te zien waarop staat dat de toegang tot de site verboden is.

Engeland maakt op een andere manier gebruik van proxies. Het grootste verschil met Saoedi-Arabië is dat niet al het verkeer op de landsgrenzen door een proxy wordt geleid. In Engeland kunnen de afzonderlijke ISP's een filtermethode invoeren. British Telecom was de

eerste die websites op een dergelijke manier blokkeerde. Het bedrijf gebruikt daarvoor het filter Cleanfeed (Hunter, 2004). Dit stuurt niet al het internetverkeer door een proxy, maar alleen het 'verdachte' verkeer. Op deze wijze worden de hierboven genoemde nadelen (vertraging en problemen met beveiligde verbindingen) tot op zekere hoogte opgevangen.

De informatie over de exacte werking van het Cleanfeed-filter is niet vrijgegeven (Clayton, 2005), onze uitleg kan daarom op detailniveau fouten bevatten. De eerste stap in de werking van het filter is de controle van het aangevraagde poortnummer en IP-adres. Aan het poortnummer in de aanvraag kan worden afgeleid om wat voor soort internetverkeer het gaat. Bijvoorbeeld om e-mailverkeer of om een webpagina. Indien het IP-adres in de aanvraag niet op de zwarte lijst staat of als het niet gaat om het opvragen van een webpagina, maar om het versturen van een e-mail dan mag dit verkeer door naar de webserver waarom gevraagd wordt. Indien het IP-adres wel op de zwarte lijst voorkomt, wordt het doorgestuurd naar een proxy. In deze proxy wordt gekeken of de aangevraagde URL op de zwarte lijst staat. Is dit het geval, dan krijgt de aanvrager in zijn browser 'page unavailable' te zien. Staat de aangevraagde URL niet op de zwarte lijst dan mag het verkeer door naar de webserver waarop de URL staat. De lijst met IP-adressen en URL's die Cleanfeed blokkeert, wordt aangeleverd door de Internet Watch Foundation (IWF) (Clayton, 2005). De IWF is vergelijkbaar met het particuliere Meldpunt Kinderporno op Internet in Nederland. Een schematische voorstelling van het Cleanfeed filter staat in figuur 2.9.

Figuur 2.9. Blokkeren met het Cleanfeed filter



De Cleanfeed methode is dan wel niet vrijgegeven, het basisprincipe (eerst op hoofdlijnen verdacht verkeer selecteren en vervolgens alleen dat verkeer nader op URL-niveau controleren) zien we ook op andere plaatsen terug. Er zijn commerciële bedrijven die dergelijke filtertechnieken aanbieden. Zo'n methode werkt bijvoorbeeld als volgt:

1 IP-adressen achterhalen die behoren bij de URL's die op de zwarte lijst staan (een zogenaamde reverse lookup). Dat zijn dan 'verdachte IP-adressen'.
2 Verdachte IP-adressen die een internetter aanvraagt worden niet direct naar de betreffende server geleid maar eerst naar een proxy van de ISP.
3 In deze proxy worden de verdachte aanvragen bekeken op URL-niveau. Indien er een match is tussen de aangevraagde URL en de URL op de blacklist dan wordt de pagina geblokkeerd. Indien de URL niet op de lijst voorkomt dan mag het verkeer alsnog door naar de server die de betreffende website host.

Afbeelding (m.b.v. Deep Packet Inspection – DPI)

Algemene beschrijving. Bij het blokkeren van afbeeldingen moet op dezelfde wijze gebruik gemaakt worden van proxies als bij het blokkeren van URL's. Al het internetverkeer moet

door een proxy worden geleid. In de proxy wordt nu niet naar de URL's gekeken maar naar de afbeeldingen die worden opgevraagd (zie ook figuur 2.8). Dit kan alleen middels een methode die Deep Packet Inspection (DPI) heet. Bij DPI wordt niet alleen *naar* de pakketjes gekeken die verstuurd worden (zoals bij het blokkeren op IP-adres, domeinnaam en URL wel gebeurd), maar wordt er ook *in* de pakketjes gekeken.

De afbeeldingen worden bekeken aan de hand van hun hashcodes. Een afbeelding is opgebouwd uit pixels, deze pixels kunnen worden omgezet in een code die uniek is voor die afbeelding: de hashcode. Een hashcode is een 'digitale handtekening' van een databestand zoals een afbeelding.

Aan de proxy wordt een lijst gekoppeld met alle hashcodes van afbeeldingen waarvan bekend is dat het kinderporno is.

Bij het blokkeren van afbeeldingen in P2P-systemen moet altijd gebruik gemaakt worden van Deep Packet Inspection. De ISP moet bepalen of het verkeer van de gebruiker afkomstig is van een P2P-netwerk. Vervolgens kan de afbeelding bekeken worden. De hashcode van de afbeelding en de hashcodes uit de databank (de blacklist) worden vergeleken. Indien een afbeelding voorkomt in de databank wordt de betreffende afbeelding niet doorgelaten.

Effectiviteit. Het blokkeren van afbeeldingen aan de hand van hashcodes is zeer fijnmazig. Er is geen sprake van overblocking. Volgens de experts die wij gesproken hebben vertraagd deze methode het internetverkeer dermate dat het op grote schaal praktisch niet uitvoerbaar is.

Daarnaast is het eenvoudig om een hashcode van een afbeelding te veranderen. Er hoeft immers maar één pixel in de afbeelding anders te zijn om de hashcode te wijzigen. De gewijzigde afbeelding wordt dan niet geblokkeerd.

Gebruik. Voor zover bekend wordt deze methode niet gebruikt op ISP-niveau. Technisch gezien speelt in dat verband een rol dat het tot (aanzienlijke) vertraging in het verkeer leidt indien alle passerende informatie met DPI zou moeten worden gecontroleerd, of dat grote investeringen in apparatuur moeten worden gedaan om die vertraging te voorkomen. Wel wordt de methode (bijvoorbeeld in Zweden, zie paragraaf 4.3) gebruikt voor het blokkeren van kinderporno op het niveau van een lokaal netwerk, bijvoorbeeld het netwerk van een bedrijf of overheidsinstelling. Op dat niveau speelt het genoemde bezwaar minder omdat men dan te maken heeft met kleinere informatiestromen.

Blokkeren op basis van algemene criteria (dynamisch blokkeren)

In de vorige subparagrafen was er sprake van het blokkeren van websites of content op internet door het gebruik van een blacklist of zwarte lijst. Op deze lijst staat de website of de content die geblokkeerd dient te worden (bijvoorbeeld het IP-adres van de website of de hashcode van een afbeelding). Een nieuwe website of nieuwe afbeelding die nog niet op de zwarte lijst staat, wordt dus niet geblokkeerd. Er bestaan echter filtertechnieken om content te blokkeren die nog niet eerder bekend was. Men maakt dan gebruik van algemene criteria, zoals trefwoorden, op grond waarvan wordt bepaald of content dient te worden geblokkeerd. Dit heet ook wel dynamisch blokkeren (Haselton, 2007).

De kritiek op deze manier van blokkeren is groot, omdat vaak onduidelijk is welke reguliere dan wel nuttige informatie eveneens wordt geblokkeerd. Filtertechnieken kunnen twee soorten fouten maken: legale websites tegenhouden (valse positieven) en illegale websites doorlaten (valse negatieven) (Deshmukh, 2005). Er zijn verschillende studies waarin de effectiviteit is onderzocht van filters die zijn gebaseerd op algemene criteria. Daaruit blijkt dat geen van dergelijke filters een 100 procent hit-rate heeft. Kranich (2004) concludeert dat filters die werken met algemene criteria driekwart van het beoogde materiaal blokkeren. Een kwart van het te blokkeren materiaal wordt doorgelaten. We spreken dan van underblocking of valse negatieven. Naast underblocking – niet alle beoogde informatie wordt daadwerkelijk

tegengehouden – is er volgens Kranich ook altijd sprake van overblocking: in 20 procent van de gevallen wordt informatie tegengehouden zonder dat dat de bedoeling was. Bij dynamisch blokkeren wordt, aldus Kranich, altijd een deel van de te blokkeren informatie ten onrechte doorgelaten (vals-negatieven) èn ten onrechte tegengehouden (vals-positieven). Dit komt ook in andere studies naar voren (Greenfield e.a., 2001; Resnick e.a., 2004; Richardson, 2002). In deze studies varieert het percentage underblocking (valse negatieven) tussen 10 en 50 procent en het percentage overblocking (valse positieven) tussen de 1 en 50 procent. Overigens hebben filters met weinig *overblocking* doorgaans veel *underblocking*, en andersom (zie ook paragraaf 4.5).

Websites kunnen geblokkeerd worden aan de hand van bepaalde sleutelwoorden of zinsneden die op die website voorkomen. Van te voren moet er een lijst worden opgesteld met sleutelwoorden waarop geblokkeerd wordt. Om effectief te zijn, moet al het internetverkeer bekeken worden. Het gebruik van een proxy is daarom noodzakelijk. De proxy wordt op eenzelfde manier geïmplementeerd als bij het blokkeren op URL, zie figuur 2.8. Bij het blokkeren op URL wordt het verkeer bekeken in de proxy zodra de browser contact maakt met het internet. Bij het blokkeren op basis van algemene criteria moet eerst de gevraagde content worden opgehaald van de webserver. In de proxy wordt vervolgens de content beoordeeld aan de hand van de algemene criteria. Komt de content door deze screening, dan wordt hij doorgezonden naar de browser van de internetter (figuur 2.8).

Overblocking komt snel voor bij deze vorm van blokkeren. Voorbeelden van websites die onterecht werden tegengehouden zijn sites over seksuele voorlichting, borstkanker en minister Borst. Overigens kan een tekst als plaatje worden opgenomen waardoor hij niet meer als tekst te traceren is (Shih e.a., 2007).

Blokkeren op alleen sleutelwoorden zorgt voor veel overblocking. De methode is daarom doorontwikkeld: er bestaan filtertechnieken die niet alleen naar de sleutelwoorden kijken maar ook naar de context waarin de sleutelwoorden staan (Deshmukh, 2005). Een site waarin het woord ‘borst’ in combinatie met ‘minister’ voorkomt wordt dan bijvoorbeeld wel doorgelaten, maar een site met de combinatie ‘borst’ en ‘pornoster’ niet. Ook kan aan sleutelwoorden een waarde worden gegeven. Komt de waarde van de totale webpagina boven een bepaalde grens dan wordt de pagina geblokkeerd.

Nieuwsgroepen kunnen technisch gesproken ook op grond van algemene criteria geblokkeerd worden. In feite geldt hier dan eenzelfde methodiek als bij het blokkeren van websites. Aan de hand van bepaalde sleutelwoorden of combinaties daarvan kan een nieuwsgroep worden geblokkeerd. Daarbij kan zowel worden gekeken naar de naam van de nieuwsgroep als naar de inhoud van de berichten (dat laatste zoals spamfilters werken bij e-mail – alleen zijn e-mails niet openbaar). De inhoud van nieuwsgroepberichten kan worden beoordeeld aan de hand van teksten en de daarbij opgenomen afbeeldingen. Of nieuwsgroepen ook werkelijk op een dergelijke wijze worden gefilterd en geblokkeerd, is ons niet bekend geworden.

Het blokkeren van chatkanalen is lastiger. Websites en nieuwsgroepen werken in principe altijd op dezelfde poort (de toegang tot de computer), hetgeen helpt bij het lokaliseren en identificeren van dit soort verkeer. Bij chatkanalen is dit niet zo. Theoretisch gezien kunnen chatkanalen wel geblokkeerd worden aan de hand van bepaalde sleutelwoorden die voorkomen in de naam van het chatkanaal.

Ook bij zoekmachines (zoals Google) kan gefilterd worden aan de hand van sleutelwoorden. Bepaalde zoekresultaten worden dan weggelaten, waardoor de betreffende websites lastiger te vinden zijn. Google biedt zelf al een gefilterde zoekmachine aan: Google SafeSearch. Bepaalde websites worden niet getoond in de lijst met zoekresultaten. Bij deze techniek worden websites bekeken op sleutelwoorden en zinsneden en wordt gekeken naar bepaalde URL’s. In Engeland maakt Google gebruik van de lijst met URL’s die de Internet

Watch Foundation aanlevert. De URL's die op die lijst staan worden niet getoond in de onderzoekresultaten.

Het weglaten van bepaalde zoekresultaten aan de hand van sleutelwoorden, zoals beschreven bij het blokkeren in zoekmachines, is ook toepasbaar op P2P-systemen.

Er zijn methoden ontwikkeld om met algemene criteria afbeeldingen te classificeren als toelaatbaar of niet toelaatbaar. Via DPI wordt de afbeelding bekeken aan de hand van de pixels waaruit zij is opgebouwd. Bij filteren op basis van algemene criteria wordt gekeken naar bijvoorbeeld de kleur, de textuur en vorm (Shih e.a., 2007). Er is een aantal methoden ontwikkeld om pornografisch materiaal te detecteren:

- Fleck ontwikkelde een methode om naakte mensen te detecteren (Fleck e.a., 1996). Deze methode maakt gebruik van een 'skin filter' en een 'human figure grouper'.
- Anderen (Jones en Regh, 1998; Zeng, 2004) ontwikkelden een statistisch kleurmodel om onderscheid te maken tussen huid en non-huid.
- Yang (2004) analyseerde de 'human body trunk' om pornografisch materiaal te identificeren. Eerst wordt gekeken of er veel huidpixels aanwezig zijn. Vervolgens wordt gekeken naar de vorm van deze plekken.
- Yoo (2004) ontwikkelde een methode waarbij afbeeldingen vergeleken worden met afbeeldingen uit twee databanken. In de eerste databank staan afbeeldingen die gekenmerkt zijn als 'niet toelaatbaar'. In de tweede databank staan afbeeldingen die gekenmerkt zijn als 'toelaatbaar'. Uit de twee databanken worden de tien meest gelijkende afbeeldingen gezocht. Als de meeste van deze tien plaatjes uit de databank met niet toelaatbare content komen dan wordt de originele afbeelding geclassificeerd als niet toelaatbaar.
- Wang e.a. (1998) ontwikkelde het Wavelet Image Pornography Elemination systeem (WIPE). Dit is een systeem dat afbeeldingen classificeert als geschikt of ongeschikt. Het maakt gebruik van: icon-filter, graph-photo detector, color histogram filter, texture filter, en een shape matching algorithm.

Moeilijkheden bij het classificeren van afbeeldingen is de selectie van goed vergelijkingsmateriaal en het vaststellen van randvoorwaarden om een afbeelding als verdacht aan te merken. De bovenstaande methodes zijn bedoeld om pornografisch materiaal tegen te houden. Voor bekend is er op dit moment geen methode in gebruik die speciaal kinderpornografische afbeeldingen blokkeert.

Blacklists op basis van dynamische technieken

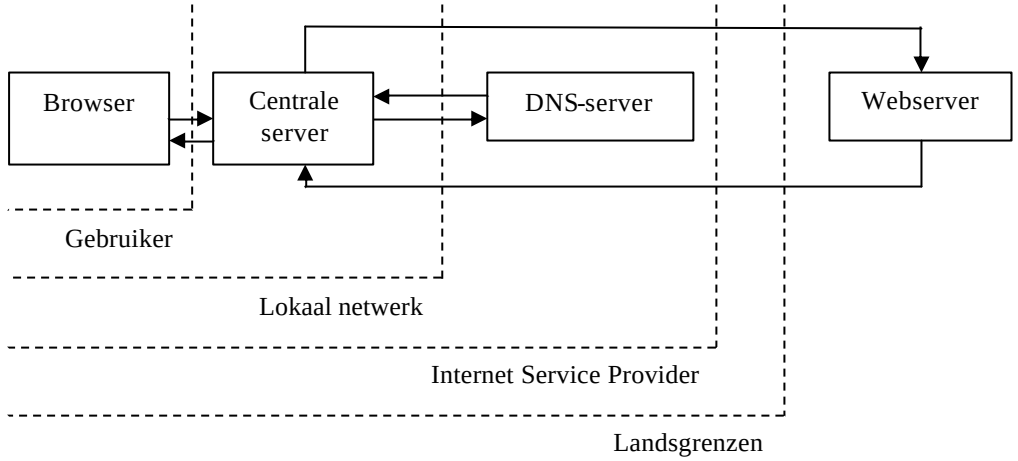
In het voorgaande stelden we twee blokkeervormen naast elkaar: blokkeren met een blacklist ('blacklist filtering') en blokkeren op basis van algemene criteria ('dynamic filtering'). Van oudsher is een groot verschil tussen die twee dat bij *blacklist filtering* de te filteren informatie van tevoren door mensen is beoordeeld terwijl dat bij *dynamic filtering* niet het geval is. Bij die laatste methode wordt de te filteren informatie door een softwareprogramma gedetecteerd middels een combinatie van zoekcriteria (een bepaald algoritme). Op grond van dat verschil is te verwachten dat de accuratesse van *blacklist filtering* aanzienlijk groter is (en de mate van overblocking dus aanzienlijk geringer) dan die van *dynamic filtering.*

Haselton (2007) merkt op dat het tussen 1995 en 2002 gebruikelijk was dat bedrijven die filters maakten, zich erop lieten voorstaan dat alle sites op hun blacklist door hun medewerkers waren beoordeeld (*human review).* Tegenwoordig worden blacklists echter ook automatisch samengesteld: een zoekrobot van het bedrijf zoekt op basis van bepaalde criteria naar sites die kennelijk behoren tot een te filteren categorie. De aldus gevonden sites worden dan op de blacklist geplaatst (*automated review).* Zo ontstaat in feite een blacklist die is samengesteld op basis van *dynamic filtering*. Het onderscheid in accuratesse tussen *blacklist filtering* en *dynamic filtering* vervalt op die manier.

2.3 Beheersgebieden

Naast de verschillende technische mogelijkheden om te filteren en blokkeren zijn er verschillende plaatsen waar het filter kan worden geïmplementeerd. Er kan gefilterd worden aan de landsgrenzen, bij de verschillende internetaanbieders, bij lokale netwerken en bij de gebruikers (figuur 2.10). In de volgende paragrafen bespreken we deze verschillende plaatsen van implementatie.

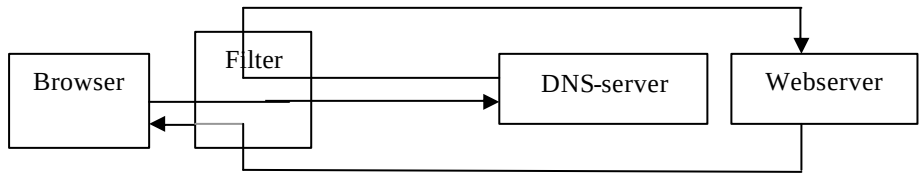
Figuur 2.10. Implementatiemogelijkheden filter



Gebruikersniveau

Gebruikers kunnen zelf speciaal ontwikkelde softwarepakketten op hun pc installeren, waardoor ze geen toegang hebben tot sites met een ongewenste of strafbare content. Verschillende van dergelijke pakketten zijn reeds voorhanden. Een computerprogramma op de computer van de gebruiker bekijkt of de gebruiker de website die opgevraagd wordt door de webbrowser, wel of niet mag zien. Er wordt dan gefilterd voordat er een verbinding met internet is (zie figuur 2.11). Er kan bijvoorbeeld gewerkt worden met een witte lijst, dat is een lijst met websites die de internetter (vaak een kind) *wel* mag opvragen, of met een zwarte lijst, een lijst met sites die internetter *niet* mag opvragen (Schell e.a., 2007). Een zwakte bij dergelijke filters is dat ze door de internetters (ook de wat oudere kinderen) vaak gemakkelijk te omzeilen zijn. Ook kan een gebruiker ervoor kiezen het filter uit te zetten. Daar staat tegenover dat de gebruiker zelf sites aan de blacklist kan toevoegen, en dus een filter op maat kan maken.

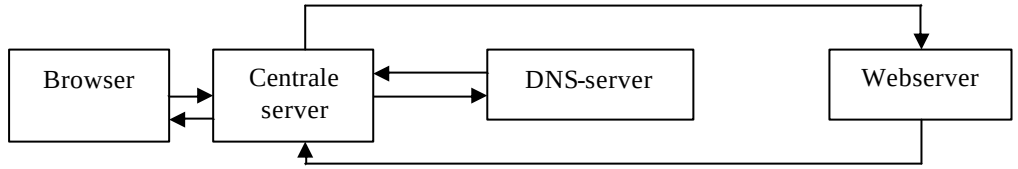
Figuur 2.11. Implementatie op gebruikersniveau



LAN-niveau

Een tweede mogelijkheid is het blokkeren bij lokale netwerken, ook wel een 'Local Area Network' genoemd, afgekort LAN (figuur 2.12). Een LAN is een groep computers die rechtstreeks, of via een gedeeld medium met elkaar verbonden zijn. LAN's worden vaak opgezet op locaties waar veel computers in één ruimte of gebouw aanwezig zijn en waar een snelle overdracht van informatie tussen verschillende computers nodig is. In deze groep vallen bijvoorbeeld bedrijven, scholen en bibliotheken. Via het LAN heeft een computer toegang tot andere bronnen die aan het netwerk zijn gekoppeld, zoals andere computers, printers en eventueel andere netwerken zoals het internet. In de meeste gevallen gaat bij dergelijke verbinding tussen een LAN en het internet het internetverkeer eerst door een centrale server en kan daar gefilterd worden. In principe werkt de centrale server dan als een proxy (zie ook figuur 2.8). De lokale netwerkbeheerder kan zelf bepalen of op IP-adres, domeinnaam of URL wordt gefilterd. Een verschil met de implementatie bij de gebruiker is dat niet de individuele gebruiker, maar de netwerkbeheerder kan bepalen of het filter gebruikt wordt of niet.

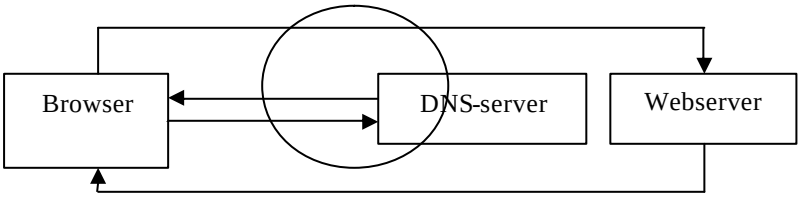
Figuur 2.12. Implementatie op LAN-niveau



Vanuit de ISP

De ISP's kunnen al het verkeer van hun klanten filteren. De lijnen die binnen de cirkel in figuur 2.13 vallen, zijn plaatsen waar implementatie kan plaatsvinden. Het gaat dan om blokkeren van domeinnamen in de DNS-server (figuur 2.5 en 2.7), of om blokkeren op IP-adres of URL middels de implementatie van een proxy tussen de browser en de webserver (figuur 2.4 en 2.8). Filters die door de ISP's worden geïmplementeerd, kunnen niet door de internetter worden uitgeschakeld.

Figuur 2.13. Implementatie bij de ISP



Landsgrenzen

Het blokkeren aan de landsgrenzen is de ingrijpendste manier van blokkeren. Al het internetverkeer van alle gebruikers in Nederland moet dan gefilterd worden. Dat kan door het plaatsen van proxies tussen de nationale internet backbone en de digitale wereld daarbuiten.

Saoedi-Arabië blokkeert op een dergelijke manier. Al het internetverkeer komt door een serie proxies waar de opgevraagde URL's vergeleken worden met de URL's op een zwarte lijst (Zittrain en Edelman, 2002). China blokkeert ook aan de landgrenzen, maar het Chinese filter werkt op verschillende niveaus. Het is niet bekend hoe de filtersystemen precies werken; er wordt niet alleen geblokkeerd aan de landsgrenzen, ook blokkeren ISP's sites (ONI 2005).

2.4 Samenvatting

Kinderporno kan op internet via verschillende wegen verspreid worden. Bekende wegen zijn websites, P2P-systemen, virtuele harde schijven, nieuwsgroepen en chatboxen. Onbekend is in welke mate dit gebeurt en welke van de wegen meer of juist minder voor de verspreiding van kinderporno worden gebruikt. We weten wel dat de wijze waarop de verspreiding loopt aan verandering onderhevig is, deels vanwege nieuwe technische mogelijkheden en deels als reactie op repressieve maatregelen zoals filteren. Te voorzien valt daardoor dat effectief filteren van kinderpornografie gaandeweg ingewikkelder wordt.

Naast verschillende verspreidingswijzen bestaan er, aldus onze respondenten, op hoofdlijnen twee verschillende groepen aanbieders van kinderpornografisch materiaal op internet: de commerciële groep die uit is op geld en de 'liefhebbers' die nieuwe kinderporno willen verkrijgen.

Om te kunnen blokkeren is vereist dat men het kinderpornografische materiaal als zodanig herkent, het gezochte materiaal moet dan dus niet onherkenbaar zijn gemaakt door bijvoorbeeld versleuteling of comprimering. Voor het overige kan het blokkeren van kinderporno op internet technisch gezien op een aantal manieren. Er kan geblokkeerd worden op IP-adres, domeinnaam, of URL, of middels DPI op de hashcode of andere unieke kenmerken (classificatie) van een afbeelding. Ook kan er aan de hand van bepaalde sleutelwoorden of zinsneden geblokkeerd worden. In figuur 2.14 staan de verschillende verspreidingswijzen en de manieren waarop blokkeren technisch mogelijk is.

Figuur 2.14. Verspreidingswijzen van kinderporno en manieren om te blokkeren

Verspreidingsvorm / **Blokkeermethode**	Websites	P2P	Nieuws-groep	Chat
Tekst	X	X	X	X
Tekst dynamisch	X		X	
Afbeelding (classificatie)	X	X	X	
IP-adres	X			
Domein	X			
URL	X			
Afbeelding hash	X	X	X	

Deze methoden verschillen in fijnmazigheid en daarmee in de kans op overblocking. De fijnmazigheid van de blokkeermethoden staat globaal samengevat in figuur 2.15.

Er zijn verschillende plaatsen van implementatie van een filter mogelijk. Dit kan bij de gebruiker zijn, bij een LAN-netwerk (bijvoorbeeld een netwerk van een universiteit of werkgever), bij een ISP of aan de landsgrenzen.

Filters werken ofwel op basis van een vaste lijst met te blokkeren informatie (*blacklist filtering*), ofwel op basis van een softwareprogramma dat aan de hand van bepaalde criteria (een bepaald algoritme) bepaalt of de door een internetter opgevraagde informatie wel of niet kan worden doorgelaten (*dynamic filtering*), ofwel op basis van een combinatie van die twee technieken. Blacklists van filterbedrijven worden tegenwoordig vaak automatisch samengesteld met gebruik van zoekrobots die werken op basis van *dynamic filtering* technieken.

Figuur 2.15. Blokkeermethoden en fijnmazigheid

Fijnmazigheid / **Blokkeermethode**	Grofmazig						Fijnmazig
Tekst		X					
Tekst dynamisch			X				
Afbeelding (classificatie)	X						
IP-adres				X			
Domein					X		
URL						X	
Afbeelding hash							X

HOOFDSTUK 3

Juridische context

In dit hoofdstuk zijn enkele juridische onderwerpen bijeengeplaatst die verband houden met het filteren en blokkeren van kinderporno. Waar elders in deze studie nodig wordt naar onderstaande beschouwingen terugverwezen. In hoofdstuk 6 wordt een juridische analyse gegeven van de huidige afspraken tussen KLPD en enkele providers met betrekking tot het filteren/blokkeren van internetverkeer.

3.1. Strafrechtelijke definitie van kinderporno

Een twintigtal jaren geleden werd tegen kinderpornografie opgetreden op basis van de niet specifieke zedelijkheidsartikelen 240 en 242 Sr. Bij de bestrijding van pornografie speelde vooral het bestanddeel 'aanstotelijk voor de zeden' een centrale rol. De Hoge Raad overwoog in het Deep Throat-arrest[5] dat er 'bezwaarlijk kan worden gesproken' van aanstotelijkheid voor de zeden ten opzichte van de toeschouwers van de filmvertoning met een dergelijk karakter. 'Immers ten aanzien van die personen mag worden aangenomen dat zij het aanschouwen van de betrokken film, in weerwil van bedoeld karakter, juist hebben gewild en derhalve aan de inhoud dier film geen aanstoot zullen nemen.' Het gevolg van deze overweging van de Hoge Raad was dat er alleen aanleiding zou zijn voor een veroordeling wegens verspreiding van dergelijk materiaal indien sprake was van een ongewenste confrontatie.

Figuur 3.1: Artikel 240b (oud) Wetboek van Strafrecht i.w.tr. 21 mei 1986

Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft degene die een afbeelding - of een informatiedrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van zestien jaar nog niet heeft bereikt, is betrokken, hetzij verspreidt of openlijk tentoonstelt, hetzij om verspreid of openlijk tentoongesteld te worden, vervaardigt, invoert, doorvoert, uitvoert of in voorraad heeft.

In het kader van een algemene herziening van de zedelijkheidswetgeving kwam de Commissie Melai in 1980 met een aantal voorstellen. In verband met kinderpornografie was het de bedoeling om artikel 240 Sr aan te vullen. Het daartoe ingediende wetsvoorstel kwam nagenoeg overeenkwam met de voorstellen van de Commissie Melai.[6] Ook nu was het idee dat bij kinderpornografie met een verbod op ongewenste confrontatie kon worden volstaan. De wetgever zou opvattingen van degenen die van dergelijk materiaal kennis wensen te nemen moeten te respecteren en niet ondergeschikt dienen te maken aan een eigen inhoudelijke beoordeling.[7] Al snel kwam er echter kritiek, vooral van het vrouwelijk deel van het maatschappelijk veld. Pornografie zou niet alleen schadelijk zijn, maar vooral beledigend en discriminerend. In juli 1984 deed de Amsterdamse politie invallen bij seksshops ter inbeslagneming van kinderpornografisch materiaal. Uit het buitenland werd gemeld dat vanuit Nederland aanzienlijke

[5] HR 28 november 1978, *NJ* 1979, 93.

[6] De Commissie Melai – officieel de Adviescommissie Herziening Zedelijkheidswetgeving – is ingesteld in 1970. In 1980 kwam zij met liberale voorstellen en met name het voorstel tot gedeeltelijke decriminalisering van seks met en door minderjarigen deed veel stof opwaaien.

[7] *Kamerstukken II*, 1979/80, 15 836, nr. 6.

hoeveelheden kinderpornografie werden geëxporteerd (NLR, 2002).[8] Op de golven van de maatschappelijke verontwaardiging werd alsnog een wetswijziging doorgevoerd. Met de Wet van 3 juli 1985 werd een nieuw artikel 240b Sr werd ingevoerd dat onder meer het verspreiden van kinderpornografie verbiedt (figuur 3.1).

Het artikel kent een bestanddeel dat voordien niet in de wet voorkwam: seksuele gedraging.[9] Op andere plaatsen in de wet vindt men de 'ontuchtige handeling' en 'ontucht'. De Commissie Melai stelde het meer neutrale begrip 'seksuele handeling' voor (Adviescommissie, 1980). Als goed compromis werd uiteindelijk gekozen voor het begrip 'seksuele gedraging'.[10] De werkgroep kinderpornografie bakende dit begrip als volgt af door kinderpornografie te omschrijven als: 'een afbeelding van iemand die kennelijk de leeftijd van zestien jaren nog niet heeft bereikt, al dan niet alleen, in een zodanige houding dat daarmee kennelijk het opwekken van een seksuele prikkeling wordt beoogd.' (De Wit, 1986) De Hoge Raad heeft deze definitie overgenomen in zijn arrest over de fotograaf D.H. Mader.[11] Deze beslissing ondervond kritiek van een deel van de Tweede Kamer, omdat hierdoor de begrenzing van strafbare afbeeldingen ruimer werd getrokken dan naar het oordeel van de Kamer geboden was.[12]

Figuur 3.2: Artikel 240b (oud) Wetboek van Strafrecht i.w.tr. 1 februari 1996

1. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding - of een gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van zestien jaren nog niet heeft bereikt, is betrokken, verspreidt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert of in voorraad heeft. 2. Niet strafbaar is degene, die dergelijke afbeelding in voorraad heeft waarvan het vaststaat dat hij deze voor een wetenschappelijk, educatief of therapeutisch doel gebruikt. 3. Met een gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid een gewoonte maakt.

Als tekortkomingen van artikel 240b Sr ter andere zijde werden ervaren het lage strafmaximum in verhouding met hogere strafmaxima voor ontucht en het vereiste van het oogmerk verspreiding of openlijke tentoonstelling, hetgeen een voor het Openbaar Ministerie bij vervolging een zware bewijslast impliceerde. Op 26 januari 1990 ondertekende Nederland de VN-Conventie inzake de Rechten van het Kind.[13] Artikel 34 van deze conventie bepaalt dat de deelnemende staten zich ertoe verbinden 'het kind te beschermen tegen alle vormen van seksuele exploitatie en seksueel misbruik'. De hieruit voortvloeiende verdragsverplichting strekt tot de bestrijding van alle vormen van kinderpornografie waarbij een seksuele handeling met een kind wordt afgebeeld. Dit laatste feit gevoegd bij de kritiek van de Kamer op het

[8] Een onderzoek van de werkgroep kinderpornografie (ingesteld in 1985 mede na aanleiding van de berichten uit het buitenland) bevestigt dit. Zie (de Wit, 1986).

[9] J.L. van der Neut, 'Kinderpornografie, de situatie in Nederland.' *Delikt en Delinkwent*, februari 2000 nr. 2, p.108-149.

[10] Opmerkelijk is dat de Kamer zich in 2008 bij de behandeling van het initiatief wetsvoorstel Waalkens over seks met dieren weer voorstander betoond van 'ontuchtige handelingen' teneinde uit te sluiten dat kunstmatige inseminatie onder de voorgestelde strafbepaling zou vallen (TK 2007-2008, 31 009, nr. 9).

[11] HR 6 maart 1990, *NJ* 1990, 667.

[12] *Kamerstukken II* 1994/95, 23 682, nr. 5.

[13] Ratificatie door Nederland op 6 februari 1990 (http://www.unhchr.ch/html/menu2/6/crc/treaties/status-crc.htm), Trb. 1995, 92.

bestaande artikel was aanleiding voor de ingrijpende wijziging van artikel 240b bij Wet van 13 november 1995 (figuur 3.2).[14]

De strafbedreiging werd verhoogd naar vier jaar of geldboete van de vijfde categorie. Hierdoor werd de afschrikkende werking vergroot en beter aangesloten bij de ernst van de strafbaar gestelde gedragingen.[15] Bovendien werd door de verhoging van het strafmaximum de toepassing van dwangmiddelen zoals voorlopige hechtenis, huiszoeking en strafrechtelijk financieel onderzoek mogelijk.[16] Nieuw is ook de verbreding van de ratio van artikel 240b Sr. Van een seksuele gedraging kan worden gesteld 'dat het gaat om een gedraging, die – als ze wordt vastgelegd – schadelijk is voor de jeugdige, òf omdat het tot die gedraging brengen al schadelijk is, òf vanwege de publicatie ervan'.[17]

De kern is dus niet dat de afgebeelde houding van een jeugdige een seksuele prikkeling teweeg kan brengen. Als dat het criterium zou zijn – aldus annotator 't Hart bij een arrest van de Hoge Raad uit 1990 – is nauwelijks meer af te grenzen wat strafbaar is en wat niet. Mensen kunnen immers door van alles opgewonden raken.[18] In algemene zin strekt het gewijzigde artikel 240b Sr tot de bescherming van jeugdigen tegen seksuele exploitatie.[19] Het schadelijke – en dus strafbare karakter – van de afbeelding kan ook zijn gelegen in bijkomende factoren, zoals de context waarin het kind op de foto is afgebeeld of de context waarin de foto is aangetroffen.[20]

De Handleiding van het College van Procureurs-generaal van 1996 onderscheidt kinderpornografische afbeeldingen in twee categorieën. De eerste groep is een weergave van seksuele gedragingen die elders in de strafwet strafbaar gesteld zijn, maar nu afgebeeld in verband met een kind. De tweede groep betreft afbeeldingen waarop alleen een kind te zien is. Een vragenlijst helpt om te bepalen of er sprake is van een seksuele gedraging of een 'normale' afbeelding.[21]

Het oude artikel 240b Sr verlangt de aanwezigheid van een specifiek oogmerk met betrekking tot het in voorraad hebben: 'hetzij om verspreid of openlijk tentoongesteld te worden'. Dit zinsdeel is met de wetswijziging vervallen. De Kamerstukken geven twee argumenten voor deze wijziging. De praktijk geeft aan dit oogmerk moeilijk te bewijzen is. Maar of dit specifieke oogmerk nu wel of niet aanwezig is, in beide gevallen wordt door de dader voortgebouwd op het seksueel misbruik van kinderen.[22] Het opnemen van dit specifieke oogmerk in de delictsomschrijving levert daarom geen bijdrage aan het doel van artikel 240b Sr. Het gevolg van het vervallen van dit bestanddeel is, dat ook het als privépersoon in voorraad hebben van kinderpornografie voortaan strafbaar is.[23] De minister voelde zich daarom geroepen tot de volgende uitleg: 'Ik heb schriftelijk en mondeling betoogd dat het begrip 'in voorraad hebben' een externe connotatie heeft en niet dezelfde betekenis heeft als 'in bezit hebben'.

---

[14] Niet besproken wordt hier de wijziging van artikel 240b Sr door de Wet Computercriminaliteit (Stb. 1993, 33) waarbij het bestanddeel 'informatiedrager' werd aangepast op het begrippenkader van die wet en werd vervangen door 'gegevensdrager'.

[15] *Kamerstukken II* 1994/95, 23 682, nr. 5.

[16] De overtreding van artikel 240b Sr valt dan binnen het bereik van de zogenaamde 'Pluk ze'-wetgeving met als doel voordeelsontneming.

[17] *Kamerstukken II* 1994/95, 23 682, nr. 5.

[18] HR 6 maart 1990, *NJ* 1990, 667.

[19] *Kamerstukken II* 1994/95, 23 682, nr. 5. Dit ook in aansluiting op artikel 34 VN-Conventie inzake de Rechten van het Kind.

[20] *Kamerstukken II* 1994/95, 23 682, nr. 5 en *Kamerstukken I* 1994/95, 23 682, nr. 250b.

[21] College van procureurs-generaal, 'Handleiding voor de opsporing en vervolging van kinderpornografie (artikel 240b Sr)', *Staatscourant* 1996, 216, 11.

[22] *Kamerstukken II* 1994/95, 23 682

[23] D. van der Linden, 'Wetsvoorstel 23 682, Privé-bezit naaktfoto's kinderen strafbaar'. *Nederlands Juristenblad*, 9 december 1994, p. 1518 e.v.

(…) 'In voorraad' wijst op pluraliteit.'[24] De Hoge Raad laat zich later door deze opvatting niet in de war brengen. Aangezien in het tweede lid sprake is 'een afbeelding' (enkelvoud) kan 'in voorraad hebben' niet anders worden uitgelegd dan ook betrekking hebbend op een enkel exemplaar van een afbeelding, ook indien bedoeld voor eigen gebruik.[25]

Het tweede lid van artikel 240b Sr geeft de toegelaten uitzonderingen: gebruik van kinderpornografie voor een wetenschappelijk, educatief of therapeutisch doel. Vanuit de Kamer werd nog voorgesteld om ook artistieke uitingen rond kinderseksualiteit buiten de strafwet te houden. Het amendement werd afgewezen, want: 'Iedereen kan op een gegeven moment wel zeggen, dat iets kunst is.'[26]

Met de wijziging van artikel 240b Sr in 1996 was het maatschappelijke en dus ook het politieke debat nog niet afgelopen. In 1996 wordt Marc Dutroux gearresteerd en in 2004 begint het proces tegen hem en zijn handlangers. Hij wordt onder meer verdacht van ontvoering, verkrachting en moord. De meeste van zijn slachtoffers zijn minderjarige meisjes. In België, maar ook in Nederland veroorzaakt dit proces grote beroering. Tijdens het Wereldcongres tegen commerciële seksuele exploitatie van kinderen gehouden in Stockholm in 1996 committeert Nederland zich aan het opstellen van een Nationaal Actieprogramma voor het jaar 2000.

Op 15 juli 1998 komt het Tv-programma NOVA met het bericht dat een internationaal kinderpornonetwerk jonge peuters heeft misbruikt en de beelden daarvan op internet heeft gezet. De centrale figuur in deze zaak was een in Zandvoort woonachtige computerhandelaar. NOVA kreeg deze informatie van de Belgische werkgroep Morkhoven, een pressiegroep tegen kinderpornografie.[27] De Zandvoortse kinderpornozaak ging een belangrijke rol spelen in de discussie over kinderpornografie op internet (Stol, 1999). Immers, ook na inbeslagname van het materiaal door de politie bleef (en blijft) dit materiaal op internet beschikbaar. In de maatschappij en in de politiek wordt men zich meer en meer bewust van de implicaties van het vrije verkeer op internet. Over de toepasbaarheid van artikel 240b Sr in de elektronische omgeving werd al eerder geconcludeerd dat de delictsomschrijving zich daartegen niet verzet (De Roos, 1996). Als onderdeel van de ratio van artikel 240b Sr ziet men niet alleen dat de strafbaarstelling zich richt tegen het seksuele misbruik van kinderen, maar ook tegen het ontstaan van een markt die de verspreiding van kinderpornografie bevordert. Aangezien in geval van 'in voorraad hebben' van zelf vervaardigde kinderpornografie voor eigen gebruik de bescherming van een concreet jeugdig slachtoffer niet aan de orde behoeft te zijn, is voorstelbaar dat in dergelijke gevallen geen vervolging plaats vindt.[28]

De maatschappelijke discussie over kinderpornografie, de politieke discussie over de zedelijkheidswetgeving, de relevante internationale verdragen en gesignaleerde problemen uit

---

[24] *Kamerstukken I* 1994/95, 23 682, nr. 250b.

[25] HR 21 april 1998, *NJ* 1998, 782.

[26] Handelingen Tweede Kamer 6 april 1995; een discussie over de grens tussen kunst en kinderporno deed zich recentelijk nog voor in België naar aanleiding van het tentoonstellen van de Fenomenale Feminatheek van schrijver Louis Paul Boon, welke tentoonstelling werd geannuleerd omdat de collectie kinderpornografisch materiaal zou bevatten (bv. www.nieuwsblad.be, 29 februari 2008)

[27] Deze pressiegroep raakte later zelf in opspraak omdat haar oprichter Marcel Vervloesem handelde in strijd met de kinderpornowetgeving en daarvoor uiteindelijk werd veroordeeld tot vier jaar gevangenisstraf (bv. www.demorgen.be, www.gva.be, 6 februari 2008).

[28] *Kamerstukken II* 2000/01, 27 745, nr. 6. Voor een andere benadering door het OM, zie Rechtbank Zutphen 24 januari 2008, LJN:BC2954. Een minderjarige jongen heeft pornografische foto-opnames gemaakt van zijn minderjarige vriendin. De Kinderrechter constateert dat de foto's voldoen aan de criteria van artikel 240b Sr, maar aangezien zij in de privésfeer zijn gemaakt - voor privédoeleinden in een affectieve en seksuele relatie, waarbij geen sprake was seksueel misbruik - is het maken van de foto's niet strafbaar. De kinderrechter ontslaat de verdachte minderjarige van rechtsvervolging. Dit vonnis is qua strekking begrijpelijk, qua motivering echter onjuist. Aangezien de delictsomschrijving van artikel 240b Sr hier vervuld is, had de rechter de verdachte moeten veroordelen, in dit geval zonder oplegging van straf. In het andere geval had de rechter de door de verdediging aangevoerde feiten mogen verstaan als een beroep op het ontbreken van de materiële wederrechtelijkheid.

de rechtspraktijk vormden de aanleiding tot de meest recente wetswijziging van artikel 240b Sr in 2002 (figuur 3.3). De basis van het wetsvoorstel werd gevormd door de nota van 19 juli 1999 inzake de bestrijding van seksueel misbruik van en seksueel geweld tegen kinderen.[29]

[29] *Kamerstukken II* 1998/99, 26 690, nr. 1 en 2.

Figuur 3.3: Artikel 240b Wetboek van Strafrecht i.w.tr. 1 oktober 2002

1. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding – of gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar betrokken, verspreidt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert of in bezit heeft. 2. Met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of gewoonte maakt.

De leeftijdsgrens is opgetrokken van zestien naar achttien jaar, in overeenstemming met internationale verdragen. De Memorie van Toelichting wijst op het Verdrag inzake de Rechten van het Kind, het Wereldcongres tegen seksuele exploitatie van kinderen in Stockholm en het ILO-verdrag betreffende het verbod op en de onmiddellijke actie voor de uitbanning van de ergste vormen van kinderarbeid (NLR, 2002). Artikel 2 van het eerste verdrag bepaalt dat het begrip 'kind' van toepassing is op alle personen jonger dan achttien jaar.

In 1993 werden voor het eerst zorgen uitgesproken – ook nu afkomstig uit feministische kring - over de mogelijkheden om zgn. virtuele (kinder-)pornografische afbeeldingen te vervaardigen (Gerstendörfer, 1993). De minister erkende in 1995: 'dit materiaal kan een werkelijke seksuele gedraging nabootsen. Het valt naar de letter onder het bereik van artikel 240b Sr. Nu daarbij geen reëel persoon is betrokken, zal vervolging naar mijn oordeel achterwege moeten blijven.'[30] Dit oordeel sluit aan bij de opvatting dat aan de afbeelding alleen geen zekerheid kan worden ontleend dat het afgebeelde ook daadwerkelijk heeft plaatsgevonden.[31] De kabinetsnota van 1999 wijst erop dat de strafbaarstelling van artikel 240b Sr zijn rechtvaardiging niet alleen vindt in de bescherming van echte kinderen tegen seksueel misbruik maar ook 'in het voorkomen van schade als gevolg van het in omloop brengen van beeldmateriaal dat seksueel misbruik suggereert'.[32] Moderne technieken bieden de mogelijkheid tot vervaardiging van ogenschijnlijk echte kinderpornografie. Het zou ongewenst zijn om voor strafbaarheid in ieder concreet geval te moeten vaststellen dat de afbeelding een werkelijk bestaand kind weergeeft.[33] Ondanks deze bezwaren is virtuele kinderpornografie toch onder de werking van artikel 240b Sr gebracht. Het Openbaar Ministerie en de Tweede Kamer[34] drongen er op aan om strafbaarstelling van virtuele kinderpornografie te onderzoeken. Nederland heeft zich verplicht tot strafbaarstelling door ondertekening van het Cybercrimeverdrag van de Raad van Europa[35] en een soortgelijke verplichting vloeit voort uit het kaderbesluit van de Raad van de Europese Unie ter bestrijding van seksuele uitbuiting van kinderen en van kinderpornografie.

Het bestanddeel 'in voorraad' hebben in artikel 240b Sr wordt vervangen door 'in bezit' hebben. De wetstekst wordt daarmee aangepast aan de uitleg van de Hoge Raad.[36] Als bijkomend argument wordt gegeven dat de bezitter van kinderpornografie aan het eind van de

[30] *Kamerstukken II* 1994/95, 23 682, nr. 5.
[31] *Handelingen II* 25 oktober 1984.
[32] *Kamerstukken II* 1998/99, 26 690, nr. 2.
[33] *Kamerstukken II* 2000/01, 27 745, nr. 3.
[34] *Kamerstukken II* 1999/2000, 26 690, nr. 7.
[35] Dit verdrag is door Nederland ondertekend in 2001, geratificeerd in 2006 en inwerking getreden in 2007. Met name artikel 9 uit dit verdrag is relevant.
[36] HR 28 april 1998, *NJ* 1998, 782.

verspreidingslijn kan zitten, het aanbod kan bevorderen en zelf ook weer verspreider kan zijn.[37]

Bij amendement werd voorgesteld om de excepties van het tweede lid van artikel 240b (oud) Sr te laten vervallen. Indien dergelijke situaties zich zouden aandienen, kan met succes een beroep op het ontbreken van de materiële wederrechtelijkheid worden gedaan. Het handhaven van de excepties in de wetstekst zou sommige personen aanleiding kunnen geven verzamelingen van kinderpornografie aan te leggen onder het mom van een wetenschappelijk, educatief of therapeutisch doel. Over de strafbaarheid van het bezit van kinderpornografie mag geen twijfel bestaan.[38]

Vanaf de jaren tachtig zijn verschillende argumenten aangevoerd die de strafbaarstelling van kinderpornografie rechtvaardigden. Aanvankelijk was er alleen aandacht voor het aanstootgevende karakter en de morele verwerpelijkheid van de uiting. Samengevat komt de ratio van artikel 240b Sr erop neer dat jeugdigen beschermd moeten worden tegen gedrag dat kan worden gebruikt om hen aan te moedigen of te verleiden deel te nemen aan seksueel verkeer, of tegen gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.[39]

In Nederland wordt de bestrijding van kinderpornografie vooral gefundeerd op de begunstigingsgedachte: door de consument van kinderpornografie te vervolgen (en te bestraffen) wordt degene getroffen die het misbruik van kinderen voor (dergelijke) commerciële doeleinden in stand houdt en bevordert.

3.2 Internationale harmonisatie van strafwetgeving

Hierboven is reeds aangegeven dat de wetgever artikel 240b Sr heeft aangepast aan de geldende internationale verdragen en afspraken. De belangrijkste rechtsbron is hier artikel 9 van het Cybercrimeverdrag. Dit verdrag stelt een aantal gedragingen strafbaar die zich in een elektronische omgeving kunnen voordoen. Diezelfde gedragingen kan men soms ook in niet-elektronische omgevingen aantreffen. Het ligt voor de hand in die gevallen een technologieneutrale implementatie te kiezen, zodat de betreffende strafbepalingen in beide situaties toepassing kunnen vinden. Het verdrag verplicht de verdragsstaten tot strafbaarstelling van de volgende gedragingen genoemd in figuur 3.4:

Het vierde lid van artikel 9 staat de verdragsstaten toe delen van artikel 9 te implementeren. Nederland heeft het verdrag geratificeerd zonder gebruik te maken van enige reserveringsmogelijkheid en heeft zich derhalve verplicht tot een volledige implementatie. Niet alle verdragsstaten kennen dezelfde benadering. Geconstateerd moet overigens worden dat de huidige versie van artikel 240b Sr twee zij het minieme verschillen met de verdragstekst laat zien. Het eerste lid onder letter d verplicht de verdragsstaat tevens strafbaar te stellen degene die zichzelf of iemand anders de beschikking over kinderpornografisch materiaal verwerft. In artikel 240b Sr ontbreekt dat bestanddeel en ontstaat eerst strafrechtelijke aansprakelijkheid in geval van bezit. Hoewel het logische gevolg van het 'zich verwerven' meestal het gaan 'bezitten' zal zijn, dekken beide begrippen elkaar niet volledig.

[37] *Kamerstukken II* 2001/02, 27 745, nr. 6.
[38] *Kamerstukken II* 2001/02, 27 745, nr. 12.
[39] Zie o.a. *Kamerstukken I* 2001/02, 27 745, nr. 299b en Aanwijzing kinderpornografie (artikel 240b Sr) *Staatscourant*, 2007, 162.

Figuur 3.4: Cybercrime verdrag, Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

Het tweede lid van artikel 9 van het Cybercrimeverdrag[40] spreekt van *realistic images* waartoe de strafbaarstelling zich dient uit te strekken, ook al betreft het geen afbeelding/opname van een echt kind als slachtoffer. Het Explanatory Memorandum bij artikel 9 van het Cybercrimeverdrag beschrijft in *para* 101 virtuele kinderporno als 'images although "realistic", do not in fact involve a real child engaged in sexually explicit conduct. The latter scenario includes pictures that are altered, such as morphed images of natural persons, or even generated entirely by the computer.' Daartoe is in artikel 240b Sr het bestanddeel 'betrokken' aangevuld tot 'schijnbaar is betrokken'.

De Aanwijzing Kinderpornografie van het College van Procureurs-generaal (zie ook paragraaf 3.3) noemt hier op de voet van de wetsgeschiedenis[41] als criterium: realistische, niet van echt te onderscheiden afbeeldingen. Terecht merkt de Aanwijzing op dat er (te) weinig jurisprudentie bestaat over hoe dit criterium toepassing kan vinden, dit met name – zoals gesteld in de Aanwijzing - met het oog op de beschermwaardigheid van kinderen tegen beeldmateriaal dat seksueel misbruik suggereert, tegen gedrag dat kinderen kan aanmoedigen of verleiden deel te nemen aan seksueel gedrag, of gedrag dat deel uit kan maken van een subcultuur die seksueel misbruik van kinderen bevordert. Deze belangen vorderen dat eerder een brede dan een beperkte uitleg wordt gehanteerd met betrekking tot de duiding van virtuele kinderporno. Ook het gebruik van 'niet van echt te onderscheiden' kinderpornografische afbeeldingen kan immers deze negatieve gevolgen in het leven roepen. De mate waarin dergelijke afbeeldingen door minderjarigen of door anderen die met dit materiaal worden geconfronteerd als 'realistisch en niet van echt te onderscheiden' wordt ervaren is toch primair een subjectieve ervaring die zich moeilijk in objectieve criteria laat vangen. Recent heeft als eerste de rechtbank van Den Bosch zich over de strafbaarheid van 'virtuele kinderporno' gebogen. De rechtbank con-

[40] Trb. 2007, 10. De Engelse en Franse tekst zijn geplaatst in Trb. 2002, 18.
[41] TK 2001-2002, 27745, nr. 3 p. 4 en 27745, nr. 6, p. 8-9.

stateert dat een onder verdachte aangetroffen filmpje afbeeldingen bevat van een minderjarig meisje dat met een volwassen man betrokken is in een seksuele gedraging. De afgebeelde personen zijn geen fysiek bestaande personen, het filmpje is een animatie. Voor volwassenen is het gebeurde op het filmpje volgens de rechtbank weliswaar van echt te onderscheiden, maar niet voor het gemiddelde kind, op welke doelgroep het filmpje qua inrichting kennelijk gericht is. Aangezien de Aanwijzing een dergelijke grond voor strafbaarstelling van kinderporno aanvoert – de zinsnede wordt in het vonnis letterlijk overgenomen – acht de rechtbank de verdachte strafbaar.[42]

De beslissing van de rechtbank houdt niet in, dat iedere 'virtuele' kinderpornografische afbeelding onder artikel 240b Sr kan worden gebracht, als er maar de verwachting is dat deze afbeeldingen voor een bepaalde groep personen 'realistisch' dan wel 'niet van echt te onderscheiden' zijn. De rechtbank houdt rekening met de context van de afbeeldingen: het gewraakte filmpje richt zich kennelijk op een doelgroep van jeugdigen. De rechtbank vraagt zich vervolgens af in hoeverre deze beelden voor het gemiddelde kind realistisch zijn. Wat precies onder het gemiddelde kind moet worden verstaan blijft in het midden. Van het kind in kwestie mag men verwachten dat het enerzijds nog niet de leeftijd heeft om te kunnen onderscheiden tussen echt en animaties. Dat stelt een bovengrens aan de leeftijd. Aan de andere kant moet het kind kunnen begrijpen wat de betreffende afbeeldingen voorstellen, impliceren of suggereren. Dat stelt een leeftijdsgrens aan de onderzijde. Of en hoeveel ruimte er tussen beide leeftijdsgrenzen bestaat is ter bepaling aan deskundigen. De rechtbank geeft dat verder niet aan. Duidelijk is wel dat met deze beslissing nog geen sluitende set van criteria is verkregen voor de afgrenzing van de strafbaarheid van virtuele kinderporno.

Al zijn de partijen rond de hierboven genoemde internationale overeenkomsten het eens dat de strafbaarheid zich ook tot virtuele kinderporno behoort uit te strekken, dezelfde verdragsteksten laten tevens zien dat er niet onaanzienlijke interpretatie- en implementatieverschillen kunnen optreden met betrekking tot de duiding van strafbare kinderporno en daarmee samenhangende gedragingen. Binnen de Europese Unie zijn deze verschillen klein door de implementatie van het betreffende Kaderbesluit 2004/68/JHA.[43] Daar buiten kunnen sterk afwijkende opvattingen worden gehanteerd. Partijen bij het Cybercrimeverdrag die (nog) geen deel uitmaken van de Europese Unie (bijvoorbeeld Noorwegen) hebben de vrijheid om met hun nationale wetgeving verdergaande strafbaarstellingen te voorzien dan het Cybercrimeverdrag eist, mits de nationale wet niet in strijd komt met de tekst en de bedoeling van het verdrag. Een ander voorbeeld van een verdragspartij is de Verenigde Staten, die handelingen met virtuele kinderporno, zoals verwoord door het tweede lid van artikel 9, niet strafbaar stellen.[44]

In dit rapport wordt in hoofdstuk 4 nader ingegaan op de situatie in verschillende landen, waaruit in ieder geval duidelijk wordt dat er landen zijn die strengere criteria kennen voor strafbaarheid van kinderporno dan Nederland, maar ook landen die minder strenge criteria stellen. Bij de internationale vergelijking van maatregelen tegen kinderporno moet rekening worden gehouden met verschillen in nationale wetgeving. Voor filtering/blokkering betekent dat aanbod van kinderpornografie uit landen waarmee wel rechtshulpverdragen bestaan, maar waar die kinderpornografie niet als strafbaar geldt, in Nederland toch moet worden tegengehouden, terwijl omgekeerd legaal aanbod vanuit Nederland in andere landen als strafbaar materiaal zal worden tegengehouden. Verdere internationale harmonisatie wetgeving op het gebied van kinderpornografie en versterking van de internationale samenwerking is hier geboden.

---

[42] Rechtbank 's Hertogenbosch, 4 februari 2008, LCN: BC3225.
[43] OJ L 13 d.d. 20 januari 2004, 13.
[44] Een verbod op virtuele kinderporno verdraagt zich niet met het *First Amendment* (Freedom of Speech), zie Supreme Court, 16 april 2002, Ashcroft v. Free Speech Coalition (198 F.3d 1083).

3.3 Kinderporno volgens de Aanwijzing van het College van Procureurs-generaal

De Aanwijzing kinderpornografie van het College van Procureurs-generaal[45] bevat een summiere samenvatting van de wetshistorie van artikel 240b Sr, met name van de wijzigingen in verband met de laatste wetswijziging. Bijlage 1 van de Aanwijzing bevat een toelichting op de voor de opsporingspraktijk bepalende delictsbestanddelen van artikel 240b Sr, terwijl bijlage 2 criteria geeft om te bepalen of sprake is van een seksuele gedraging in de zin van hetzelfde artikel. Achtereenvolgens worden deze onderdelen hierna besproken. In figuur 3.5 is opgenomen hoe de ratio van art. 240b Sr in de Aanwijzing is samengevat.

Figuur 3.5: Aanwijzing van het College van Procureurs-generaal, 30 juli 2007

a. Een jeugdige in een situatie wordt gebracht waarin hij/zij wordt gebruikt voor het op beeldmateriaal vastleggen van een seksuele gedraging in de zin van artikel 240b WvSr waarbij hij/zij alleen of met een ander/anderen is betrokken;

   Hierbij zij aangetekend, dat als seksuele gedraging onder omstandigheden ook het aannemen van een uitdagende houding door het kind worden beschouwd, bijvoorbeeld indien het brengen van het kind in die houding schadelijk moet worden geacht. Op zich is het afbeelden van geheel of gedeeltelijk ontbloot kind, niet noodzakelijk een seksuele gedraging.[46] De context waarin het kind wordt afgebeeld kan echter van zodanige onnatuurlijke aard zijn dat het brengen van de jeugdige in die onnatuurlijke ambiance een seksuele connotatie krijgt die als schadelijk voor het kind moet worden aangemerkt. Het bestanddeel 'seksuele gedraging' impliceert niet dat tenminste twee deelnemers moeten zijn afgebeeld.[47]

b. Beeldmateriaal dat onder het bereik van artikel 240b WvSr valt, na vervaardiging (verder) wordt verspreid, openlijk wordt tentoongesteld, of in bezit gehouden wordt;

c. Jeugdigen worden aangemoedigd of verleid om deel te nemen aan seksueel gedrag en gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.

Het samenvatten van de ratio van artikel 240b Sr draagt bij aan het beoordelen van strafbare kinderporno, dat niettemin in sommige gevallen als moeilijk moet worden aangemerkt. Een complicerende factor is daarbij de leeftijd van het reële of virtuele slachtoffer. De ouderdom van de afbeelding doet voor de leeftijdsbepaling niet ter zake. De Aanwijzing stelt dat aan de hand van de afbeelding een schatting moet worden gemaakt van de leeftijd. Deze leeftijd hoeft niet bewezen te worden. De werkelijke leeftijd van de afgebeelde persoon, indien bekend, is wel een omstandigheid waarmee bij de beoordeling van de zaak rekening moet worden gehouden. Gezien de strekking van artikel 240b Sr gaat het hier tevens om personen die ouder zijn dan achttien jaar maar die zich ten behoeve van de afbeelding voordoen als een kind jonger dan achttien jaar.[48] Naarmate de leeftijd van de betrokken personen op de kinderpornografische afbeelding dichter bij de grens van achttien jaren ligt, is met minder zekerheid vast te stellen of het produceren of verspreiden van die afbeelding als strafbaar moet worden aangemerkt.

[45] Laatstelijk gewijzigd 30 juli 2007, Stcrt. 2007, 162.
[46] HR 10 juni 2003, NJ 2003, 609.
[47] HR 4 december 1990, NJ 1991, 312.
[48] In deze zin HR 7 december 2004, NJ 2006, 62, JOL 2004, 690; LJN AQ8936.

3.4. Bescherming van de persoonlijke levenssfeer

Artikel 8 EVRM bepaalt dat een ieder recht heeft op 'respect of his private and family life, his home and correspondence'. Het tweede lid van het artikel laat een inbreuk op dat recht door of namens de overheid alleen toe vanwege de in het tweede lid genoemde legitieme belangen en indien die inbreuk als noodzakelijk in een democratische samenleving kan worden aangemerkt.

Artikel 8 EVRM heeft in de Nederlandse Grondwet uitwerking gevonden in twee verschillende artikelen. In artikel 13 GW voor zover het gaat over de bescherming van het brief-, telegraaf- en telefoongeheim (figuur 3.6), voor het overige in artikel 10 GW (figuur 3.7). Een inbreuk op de persoonlijke levenssfeer of op de vertrouwelijke communicatie vereist een formeelwettelijke grondslag. Zo is het kennisnemen of vastleggen van internetverkeer door politie en justitie geregeld in het Wetboek van Strafvordering.[49]

Figuur 3.6: Artikel 13 GW

1. Het briefgeheim is onschendbaar, behalve, in de gevallen bij wet bepaald, op last van de rechter; 2. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij wet bepaald, door of met machtiging van hen die daartoe bij wet zijn aangewezen.

Figuur 3.7: Artikel 10 GW

1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. 2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstekken van persoonsgegevens. 3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

Grondrechten vinden, voor zover de aard van het grondrecht zich daartoe leent, niet alleen toepassing in de verhouding overheid-burger (verticale verhoudingen) naar ook tussen burgers onderling (horizontale verhoudingen). Dit wordt in het kader van de Telecommunicatiewet uitgedrukt door artikel 18.13. Deze bepaling werd bij amendement voorgesteld bij de behandeling van het wetsvoorstel van de Telecommunicatiewet 1998, na het mislukken van de grondwetswijziging van onder meer artikel 13 GW in verband met onder meer de juridische duiding van e-mail. Het doel van artikel 18.13 Tw is niet alleen om zeker te stellen dat het communicatiegeheim van artikel 13 GW zich uitstrekt tot modernere communicatietechnieken dan de telefoon en de telegraaf maar vooral om aan te geven dat de aanbieder van een openbare elektronische communicatiedienst in beginsel gehouden is tot naleving van de grondwettelijke norm ten opzichte van de gebruikers van zijn dienst. Internet providers zijn aanbieders van openbare elektronische communicatiediensten en vallen derhalve onder de werking van de Telecommunicatiewet.

Artikel 18.13 Tw staat het door een ISP eenzijdig toepassen van filtering of blokkering, waartoe kennis moet worden genomen van de inhoud van het verkeer, in de weg. Het

[49] Zie Titel VIa, Zevende Afdeling.

kennisnemen van de inhoud van het internetverkeer verdraagt zich niet met de eisen gesteld door genoemd wetsartikel. De ISP behoeft voor het toepassen van filtering derhalve de toestemming van zijn abonnees, op dezelfde voet als dat het geval is met het toepassen van virus- en spamfilters. Aangezien naar de aard van het toe te passen middel en de aard van de te blokkeren informatie geen plaats is voor individuele preferenties van de abonnees zijn de Algemene Voorwaarden daarvoor de meest gerede plaats. Het verdient aanbeveling dat de ISP de criteria vermeldt op grond waarvan aan zijn abonnees geen toegang wordt verleend tot bepaalde domeinen of IP-adressen. In het kader van dit onderzoek is niet nagegaan of en hoe filterende ISP's de instemming van hun abonnees verwerven.

3.5 Verantwoordelijkheid van ISP´s voor het toegankelijk maken van kinderporno

Hier staat centraal de vraag naar de verantwoordelijkheid van internetaanbieders. In dit verband is de richtlijn e-commerce[50] van belang. Uit deze richtlijn blijkt dat Internet Service Providers en Hosting Providers aansprakelijkheid riskeren voor eventueel onrechtmatig gedrag van hun klanten. Echter, de richtlijn verplicht de providers niet tot pro-actief toezicht. In Nederland is de richtlijn omgezet in de Aanpassingswet richtlijn inzake elektronische handel.[51] Deze wet is op 30 juni 2004 in werking getreden. Voor de bespreking wordt uitgegaan van de Nederlandse wetstekst.

In het Burgerlijk Wetboek worden enkele gevallen uitgewerkt waarin een ISP niet aansprakelijk kan worden gesteld. Artikel 6:196c regelt onder welke voorwaarden een ISP niet aansprakelijk is in de gevallen dat zijn dienst eruit bestaat om informatie door te geven, informatie tijdelijk op te slaan of informatie voor langere duur op te slaan. Dit artikel is een uitwerking van de artikelen 12-14 van de Richtlijn 2000/31/EG inzake de elektronische handel. In het niet in nationale wetgeving omgezette artikel 15 van deze richtlijn is opgenomen dat aan ISP´s geen algemene plicht kan worden opgelegd om informatie te monitoren. Betoogd kan worden dat het filteren van kinderporno geen algemene verplichting inhoudt maar een specifieke verplichting, n.l. gericht op het tegenhouden van kinderporno. In meer beperkte zin oordeelde de Nederlandse rechter recentelijk over een op een site voor pedofielen verschenen foto van het Koninklijk huis dat deze ISP vanwege de bijzondere dienst die zij verleent (bedienen van pedofielen) voorzichtig moet zijn bij het opslaan van door derden ter beschikking gestelde informatie[52]: 'Om die reden mag van gedaagde anders dan wellicht van eigenaren of beheerders van websites die door hun aard niet op dergelijk misbruik en onbedoeld gebruik bedacht hoeven te zijn, worden verlangd dat zij bij het beheren van die website en van dat forum zodanige voorzieningen treft dat niet dankzij door haar geopende publicatiemogelijkheden personen, die de grenzen aan hun vrijheid van meningsuiting niet kennen, van die website gebruik kunnen maken om publicaties die inbreuken op de rechten van anderen opleveren te verspreiden.' Voor een doorsnee ISP geldt een dergelijke verplichting uiteraard niet.

Nadere beschouwing verdient het bepaalde in artikel 12 derde lid, artikel 13, tweede lid en artikel 14, derde lid van de e-commerce richtlijn, luidende: 'This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement.'

De bedoeling van deze uitzondering is kennelijk – de *recitals* bij de richtlijn vermelden hieromtrent niets - de mogelijkheid open te laten dat rechterlijke of bestuursrechtelijke autoriteiten in specifieke gevallen de ISP kunnen bevelen dat een onrechtmatige gedraging

[50] Richtlijn 20/31 EG van het Europese Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (*pbEG* 2000, L178/1)

[51] Aanpassingswet richtlijn inzake elektronische handel, Stb. 2004, 210.

[52] Vzr. Amsterdam 1 november 2007 (LJN BB6926), zie ook http://jurel.nl/2007/11/01/koninklijke-foto%e2%80%99s-terechte-specific-obligation-to-monitor/

wordt beëindigd dan wel wordt voorkomen, dit uiteraard met behoud van het beginsel dat de ISP niet-aansprakelijk is voor die gedragingen onder de daarvoor gestelde voorwaarden in genoemde artikelen. Om een dergelijke maatregel te kunnen uitvoeren kan het voor de ISP nodig zijn het door hem verzorgde verkeer of opgeslagen informatie juist wel te monitoren zonder dat dit alsnog tot aansprakelijkheid leidt. De genoemde bepaling vormt, zo mag men aannemen, geen grondslag voor vestigen van een dergelijke bevoegdheid voor rechter of bestuursorgaan. De volzin regelt alleen de gevolgen van het uitoefenen van een dergelijke bevoegdheid die onderdeel is van wetgeving op civiel, strafrechtelijk en administratiefrechtelijk gebied. In het Nederlandse recht is alleen rekening gehouden met maatregelen op strafrechtelijk gebied, zie paragraaf 3.7 hierna over de Nederlandse implementatie in artikel 54a Sr.

3.6 Bevoegdheid van de politie op grond van de Politiewet

De politiewet (Polw) beschrijft de taken van de politie. Artikel 2 van de wet formuleert: 'De politie heeft tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven.'

De daadwerkelijke handhaving van de rechtsorde wordt geacht te omvatten de handhaving van de openbare orde onder het gezag van de burgemeester en de strafrechtelijke handhaving onder het gezag van de officier van justitie. Tot de strafrechtelijke handhaving behoort het voorkomen, het opsporen en het beëindigen van strafbare feiten. Daarnaast worden genoemd het vervolgen, het berechten van de daders en de tenuitvoerlegging van de opgelegde straffen (Michiels, 1997). Deze taakomschrijving is wegens bewezen verdiensten gekopieerd uit de Politiewet van 1957. Het voorkomen van strafbare feiten zoals gedefinieerd in artikel 240b Sr en bestaande in het beschikbaar stellen en het verspreiden van kinderpornografisch materiaal aan de ene kant zowel als in het bezitten van dat materiaal aan de andere kant, kan men rangschikken onder de taak van de daadwerkelijke handhaving van de rechtsorde, zoals in artikel 2 Polw opgedragen aan de politieorganisatie. De voor de vervulling van de in artikel 2 Polw geformuleerde taak benodigde specifieke bevoegdheden worden gegeven in de Politiewet zelf[53] of in andere wetten zoals het Wetboek van Strafvordering. In het andere geval dienen zij mogelijk gegrond te worden op artikel 2 Polw zelf, indien dat nodig is voor het naar behoren uitoefenen van de taak. Hierbij zij echter aangetekend dat artikel 2 Polw niet kan worden ingeroepen, wanneer het optreden van de politie inbreuk zou maken op door de grondwet of door verdragen gewaarborgde rechten en vrijheden van de burger.[54] In die gevallen is een specifieke formeelwettelijke grondslag nodig.

Voor het door of namens de politie filteren of blokkeren van internetverkeer tegen de wil, respectievelijk zonder medewerking van de provider of de betrokken abonnees, biedt artikel 2 Polw derhalve onvoldoende basis. Zowel artikel 1 van het Eerste Additionele Protocol bij het EVRM (inbreuk op eigendomsrecht) als artikel 8 EVRM (inbreuk op vertrouwelijke communicatie) vereisen een formeelwettelijke grondslag, waarvoor artikel 2 Polw als te algemeen van aard niet kan dienen.

Wat hierboven is gesteld voor de politie geldt op overeenkomstige wijze voor het KLPD die volgens artikel 38 eerste lid onder a Polw uitvoering geeft aan de landelijke en specialistische uitvoering van de politietaak.

---

[53] In hoofdstuk III van de Politiewet en in de zgn. Ambtsinstructie op artikel 7 en 8 Polw worden de middelen gegeven die ter uit oefening van die bevoegdheden kunnen worden aangewend, zoals het gebruik van geweld, wapens, fouillering etc.

[54] Idem, p. 41. Zie bijvoorbeeld Rechtbank 's Gravenhage, 28 oktober 2003, LJN: AN9476.

3.7 Specifieke Wettelijke Bevoegdheden

De volgende vraag die behandeling verdient, is of het (doen) filteren of blokkeren van internetverkeer kan worden bereikt door het toepassen van strafrechtelijke of strafvorderlijke bevoegdheden. Het gaat hier om specifieke bevoegdheden. Strafbare feiten kunnen immers ook worden beëindigd door het aanhouden van de dader of door de inbeslagneming van de voor het misdrijf gebezigde (hulp)middelen. Die situaties zijn als het gaat over filteren en blokkeren niet aan de orde. De specifieke bevoegdheden tot het (doen) blokkeren van internetverkeer zijn de volgende. Als specifieke computer-gerelateerde bevoegdheid tot het (doen) blokkeren moet in dit verband artikel 125o Sv worden genoemd. Als tweede specifieke bepaling komt artikel 54a Sr in aanmerking.

Artikel 125o Sv

Genoemd artikel is ingevoerd met de wet Computercriminaliteit II[55]en kan toepassing vinden in het kader van een doorzoeking. Indien gedurende een doorzoeking in een daarbij aangetroffen computer, waartoe de zoekbevoegdheid zich uitstrekt, gegevens worden aangetroffen met betrekking waartoe of met behulp waarvan het strafbare feit is gepleegd, kunnen die gegevens ontoegankelijk worden gemaakt, indien dit noodzakelijk is voor de beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. Met 'het strafbare feit' wordt bedoeld een misdrijf in de zin van artikel 67 eerste lid Sv of een ander strafbaar feit dat op heterdaad wordt ontdekt. Zie artikel 125i Sv dat verwijst naar de artikelen. 96b, 96c, 97 en 100 Sv en die alle dezelfde verwijzing in de aanhef hebben. De formulering 'nieuwe strafbare feiten' sluit in dat het zowel om herhaling van het strafbare feit gaat dat aanleiding vormde voor de doorzoeking, als om andere strafbare feiten, al zullen die vanwege de aard van de ontoegankelijk gemaakte gegevens niet snel van een andere aard zijn. Artikel 125o Sv maakt preventief optreden mogelijk. De Memorie van toelichting gaat uitgebreid in op welke gegevens onder de werking van artikel 125o Sv kunnen worden gebracht, met name in geval van zgn. bijvangst.[56] Aangezien kinderpornografie de kern van het strafbare feit uitmaakt, behoeft in dit kader geen behandeling of aangetroffen kinderporno doel van de doorzoeking was of als bijvangst wordt aangetroffen: in beide gevallen kan artikel 125o Sv worden toegepast. De bevoegdheid komt toe aan de rechter-commissaris in het kader van een gerechtelijk vooronderzoek in andere gevallen aan de Officier van Justitie. Artikel 240b Sr kent een maximumstrafmaat van 6 jaren en valt derhalve in de categorie misdrijven genoemd onder artikel 67, eerste lid Sv.

In een computersysteem aangetroffen kinderpornografische afbeeldingen kunnen voor het onderzoek worden gekopieerd en van de computer verwijderd, maar mogen niet definitief worden vernietigd. Wel kunnen zij ontoegankelijk worden gemaakt, waaronder te verstaan het nemen van zodanige maatregelen dat de oorspronkelijke situatie kan worden hersteld, maar zonder dat gebruikers van het computer systeem nog toegang tot de betreffende gegevens hebben (zie tweede lid). Artikel 125j tweede lid Sv staat onder de daarin geformuleerde voorwaarden toe de doorzoeking uit te strekken tot aangesloten computersystemen. Artikel 125o Sv richt zich op in een computersysteem aangetroffen gegevens. Het wetsartikel specificeert niet of het hier opgeslagen gegevens betreft of het transport van gegevens. De plaats van het artikel en de samenhang met de overige artikelen van de zevende afdeling wijzen echter op het eerste.

De rechter-commissaris dan wel de officier van justitie kunnen volgens het tweede lid van artikel 125o Sv opheffing van de maatregel gelasten zodra het belang van de strafvordering zich daartegen niet (meer) verzet. Deze laatste formulering brengt enige onduidelijkheid

[55] Wet van 1 juni 2006, Stb. 2006, 300, i.w.tr. 1 september 2006.
[56] TK 1998-1999, 26 671, nr. 3, p. 20-21. Zie ook TK 2000-2001, nr. 6, p. 7-10; TK 2004-2005, nr. 10, p. 11-16. 26671, nr

mee, omdat het belang van de strafvordering niet altijd parallel hoeft te lopen aan het belang van het beëindigen of voorkomen van strafbare feiten.

De rechter dient zich krachtens artikel 354 Sv uit te spreken over de vernietiging van de gegevens, resp. de opheffing van de maatregel van artikel 125o Sv. Op grond van artikel 552a, eerste lid Sv kan door iedere belanghebbende worden geklaagd bij het gerecht binnen welk arrondissement de ontoegankelijkmaking heeft plaatsgevonden.

In geval van doorgifte van kinderporno door een ISP ligt toepassing van deze bevoegdheid door de rechter-commissaris of door de Officier van Justitie niet in de rede, of de ISP zou zelf verdachte van het strafbare feit moeten zijn. Voor het (doen) blokkeren van gegevensstromen is deze bevoegdheid niet gegeven.

Figuur 3.8: Artikel 125o Sv, i.w.tr. 1 september 2006

1. Indien bij een doorzoeking in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten. 2. Onder ontoegankelijkmaking van gegevens wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van het in het eerste lid bedoelde geautomatiseerde werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. Onder ontoegankelijkmaking wordt mede verstaan het verwijderen van de gegevens uit het geautomatiseerde werk, met behoud van de gegevens ten behoeve van de strafvordering. 3. Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen, bedoeld in het tweede lid, bepaalt de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris dat de gegevens weer ter beschikking van de beheerder van het geautomatiseerde werk worden gesteld.

Artikel 54a Sr

Artikel 54a Sr is ingevoerd bij de omzetting van de zgn. e-commerce richtlijn in 2004 (zie hierboven onder 3.5).

Figuur 3.9: Artikel 54aSr, i.w.tr. 30 juni 2004

Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

De wetstekst mag worden gekwalificeerd als niet bijzonder helder. Volgens de Memorie van toelichting en andere Kamerstukken lijkt de bedoeling van de bepaling inderdaad te zijn het in het leven roepen van een bevelsbevoegdheid. De wetstekst, in het bijzonder het tweede deel van de volzin ‘voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging

… te verlenen door de rechter-commissaris…' wekt de suggestie dat artikel 54 Sr alleen bedoeld is de aansprakelijkheid van de tussenpersoon weg te nemen, in geval van uitvoering van een dergelijk bevel. Met een tussenpersoon wordt in dit verband gedoeld op de internetprovider die voor derden gegevens beheert en ter beschikking stelt. De bepaling geeft niet aan op grond waarvan en in welke omstandigheden deze tussenpersoon een verplichting kan worden opgelegd tot het nemen van alle maatregelen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken. De wetstekst spreekt van 'ontoegankelijk maken van de gegevens' zonder nadere specificatie of aanduiding. Het staat de Officier van Justitie kennelijk al dan niet met machtiging van de rechter-commissaris vrij te bepalen welke gegevens ontoegankelijk gemaakt dienen te worden en wat de relatie van deze gegevens is met het strafbare feit.

Anders dan men in het vigerende systeem van het strafrecht zou mogen verwachten, verwijst artikel 54a Sr niet naar een in het WvSv gedefinieerde bevoegdheid. Aldaar vinden we alleen artikel 125o Sv aan waarvan de toepassing beperkt is tot de situatie van een doorzoeking. Artikel 125o Sv verschaft de Officier van Justitie een zelfstandige bevoegdheid waarvoor geen machtiging van de rechter-commissaris nodig is. De rechter-commissaris is daarentegen bevoegd binnen het gerechtelijk vooronderzoek maar niet daarbuiten. Anders dan artikel 125o Sv dat verwijst naar een begaan of te begaan strafbaar feit, geeft artikel 54a Sr geen aanduiding van het object van de blokkerende maatregelen. Artikel 125o Sv steunt op artikel 125i Sv (de doorzoeking ter vergaring van gegevens voor de strafvordering), een grond voor toepassing blijkt niet uit de omschrijving of de plaats in het wetboek van artikel 54a Sr.

Een ander belangrijk verschil tussen artikel 54a Sr en artikel 125o Sv is dat alleen het laatste artikel ervan uitgaat dat de rechter het laatste woord heeft over het definitieve karakter van de maatregel. Artikel 54a Sr gaat niet uit van tijdelijkheid of van beperkte duur van de maatregel, noch wordt een rechterlijk oordeel over de gebodenheid en de omvang van de maatregel gevraagd.

Bij toepassing van artikel 125o Sv geeft artikel 552a Sv een belanghebbende het recht van beklag. Tegen de toepassing van het bevel van artikel 54a Sr staat geen strafrechtelijk rechtsmiddel open.

In het kader van deze studie is de vraag relevant waartoe de bevoegdheid van artikel 54a Sr – indien de wetgever inderdaad de bedoeling had een dergelijke bevelsbevoegdheid in het leven te roepen – in concreto strekt. De Memorie van toelichting verwijst bij de uitleg van het begrip ontoegankelijk maken naar de betekenis die daaraan in het kader van art. 125o Sv wordt gegeven. Ontoegankelijk maken betekent ook met behoud van een kopie ten behoeve van de strafvordering (zie wetstekst in figuur 3.8). Deze uitleg geeft aan dat de bepaling – evenals artikel 125o Sv – gericht is op door de ISP al dan niet ten behoeve van derden opgeslagen gegevens en niet op het tegenhouden van gegevensstromen, niet in de laatste plaats omdat van de ISP in redelijkheid niet kan worden gevorderd dat hij gegevens ontoegankelijk maakt die *de jure* en *de facto* niet onder zijn controle zijn.

Artikel 54a Sr is niet alleen ongelukkig geformuleerd maar vooral onvolledig. Als men er een bevelsbevoegdheid in wil lezen – quod non – lijkt toepassing in strijd met de beginselen van een behoorlijke procesorde vanwege de onbepaaldheid van de bepaling en het ontbreken van voldoende rechtswaarborgen. De behoefte om de aansprakelijkheid van internet providers uit te sluiten bij de uitvoering van een bevel à la artikel 54a Sr, was kennelijk aanleiding voor de keuze van de plaats van de bepaling. Als aansprakelijkheidsuitsluiting volgt artikel 54a Sr min of meer de e-commercerichtlijn (zie paragraaf 3.5). Maar indien een bevoegdheid als die van artikel 54a Sr zou zijn opgenomen in het wetboek van strafvordering, behoeft niet ook nog eens te worden voorzien in uitsluiting van de aansprakelijkheid, aangezien de betrokkene die gevolg geeft aan een rechtmatig en bevoegd gegeven bevel van de opsporingsautoriteiten, voor de gevolgen daarvan niet aansprakelijk kan worden gehouden. De e-

commercerichtlijn dwingt ook niet tot de expliciete implementatie van een dergelijke bepaling, maar refereert slechts aan (bestaande) bevoegdheden in andere wetten.

Er lijkt niettemin op andere gronden voldoende aanleiding te bestaan om te voorzien in een bevoegdheid die strekt tot het ontoegankelijk maken van gegevens en tot het blokkeren van bepaalde informatiestromen. Een dergelijke bevoegdheid zou naar zijn aard onderdeel van het Wetboek van Strafvordering dienen te zijn en dan vervolgens aangevuld met toepassingsvoorwaarden en waarborgen zoals hierboven reeds aangeduid. Artikel 54a Sr stelt in huidige redactie geen verdenkingseis of bijzondere verdenkingseis. Een vraag is of een maatregel tot blokkeren van strafbaar materiaal, waarbij het niet de bedoeling is tot (verdere) opsporing over te gaan, past in het bestaande strafvorderlijke stelsel. De strakke grenzen van de strafvordering zijn overigens onder invloed van de terrorismedreiging die in onze landen wordt gevoeld aan verschuiving onderhevig. Naast de invoering van nieuwe strafverzwarende maatregelen en nieuwe bevoegdheden kan men dat aflezen aan de wijziging van artikel 132a Sv.[57] Het artikel definieert wat onder opsporingsonderzoek moet worden verstaan. De grens daarvan wordt ten opzichte van de vorige situatie verruimd, in die zin dat voorbij gegaan wordt aan de verdenkingseis – zowel in de klassieke betekenis als in de gevallen van Titel V eerste boek Sv. Artikel 132a Sv, zoals thans geformuleerd, biedt derhalve ruimte om in het Wetboek van Strafvordering bevoegdheden te introduceren die buiten verdenking kunnen worden toegepast. Borgers (2007) spreekt hier overigens van de periferie van het strafrecht en wijst op het gevaar dat eventuele maatregelen (en sancties) zich kunnen onttrekken aan de *cheques and balances* van het strafrechtelijke systeem. De vraag is of kinderpornografie als een zodanige ernstige inbreuk op de rechtsorde moet worden gezien dat met een (nieuw) artikel 54a Sr aangesloten dient te worden bij bevoegdheden van Titel V. Artikel 240b Sr is weliswaar een ernstig delict, maar naar de mening van de auteurs van een andere orde dan voorzien in de bevoegdheden van Titel V. Een bevoegdheid tot het (doen) blokkeren van kinderporno dient daarom uit te gaan van een verdenking dan wel van een bijzondere verdenking.

3.8 Overwegingen over Rechtsmacht

Wanneer de strafbare gedragingen zich binnen het bereik van de Nederlandse rechtsmacht voordoen of geïnitieerd zijn vanaf een locatie waarvoor rechtshulp of andere internationale bijstand kan worden verkregen, kan een einde worden gemaakt aan de strafbare feiten met het primaire doel de verantwoordelijke daders te vervolgen of doen te vervolgen. Opsporing zal in die gevallen prioriteit hebben en dient ook prioriteit te hebben. Strafrechtelijk optreden kan meebrengen dat nieuwe strafbare feiten feitelijk worden verhinderd. In de gevallen waarin niet direct of indirect kan worden opgespoord, verdient de beëindiging van de criminele gedraging de voorkeur. In een aantal gevallen kan dat worden bereikt via een verzoek om internationale rechtshulp.

In situaties waarin kinderporno wordt aangeboden vanuit landen waar kinderporno niet strafbaar is, of vanuit landen waarmee internationale samenwerking niet op adequate wijze kan worden gerealiseerd, hetzij wegens ontbreken van toepasselijke instrumenten of vanwege andere redenen, blijft als reële mogelijkheid over dat het aanbod van kinderpornografisch materiaal wordt verhinderd.

Politie en justitie zijn bevoegd strafrechtelijk onderzoek te doen naar het aanbieden via internet van kinderporno in de zin van artikel 240b Sr indien het feit zich voordoet op plaats waarover rechtsmacht bestaat. De Nederlandse strafwet sluit in artikel 4 Sr rechtsmacht uit over het aanbod van kinderporno via internet indien de dader zich op het grondgebied van een andere staat bevindt. Artikel 5, eerste lid onder 4 Sr bepaalt wel dat de Nederlander die zich op het grondgebied van een andere staat o.m. aan overtreding van artikel 240b Sr schuldig

[57] Ingevoerd met de Wet van 20 november 2006, Stb 2006, 580.

maakt onder de Nederlandse rechtsmacht valt. Dit laatste artikel eist niet dat de betreffende gedraging ook door de wetgeving ter plaatse strafbaar is gesteld.

Op grond van de leer van de *locus delicti* mag worden aangenomen dat niet alleen de plaats waar de dader handelt, maar ook de plaats waar de gevolgen van dat handelen zich openbaren of de plaats waar het instrument ter uitvoering van het strafbare feit zijn werking heeft, kunnen gelden als plaats van het strafbare feit. De Nederlandse jurisprudentie geeft in 1915 met het Azewijnse Paard[58] een eerste toepassing van de zgn. leer van het consecutieve gevolg. Latere jurisprudentie toont toepassing van wat men de gematigde ubiquiteitsleer zou kunnen noemen. De beslissing in het Singapore-arrest laat zien dat tegelijkertijd meerdere locus delicti mogelijk zijn.[59] Volgens latere rechtspraak op artikel 2 Sr kunnen, wanneer het feit zowel in Nederland als in het buitenland is gepleegd, strafbare handelingen die in het buitenland plaats vinden, niettemin in Nederland worden vervolgd.[60] Artikelen 2-8 Sr – daarbij in aanmerking genomen de onderliggende jurisprudentie en de begrenzingen van het internationaal publiekrecht, verschaffen de Staat der Nederlanden derhalve rechtsmacht over het aanbieden of ter beschikking stellen van kinderporno via aan Nederlandse ISP's aan Nederlandse ingezetenen. Binnen het eigen territorium is de Staat der Nederlanden bevoegd tot nemen van de vereiste strafvorderlijke maatregelen tot opsporing (en beëindiging) van de strafbare gedragingen.

3.9 Vrijheid van meningsuiting

Het (doen) aanbrengen van filtering en blokkering kan een inbreuk op het recht van vrijheid van meningsuiting en vrijheid van informatiegaring van de burger opleveren.

Artikel 10 EVRM

Figuur 3.10: Artikel 10 EVRM

1. Everyone has the right of freedom of expression. This right shall include freedom to hold opinions and to receive and to impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcast, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are described by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation of others, for the preventing the disclosure of information received in confidence, or for the maintaining the authority and impartiability of the judiciary.

[58] HR 6 april 1915, NJ 1915, 427. De verdachte leidde, staande aan gene zijde van de landsgrens met Duitsland, zijn paard Duitsland binnen. De Hoge Raad kwalificeerde deze handeling als een destijds door de strafwet verboden uitvoer van een paard. De betreffende handeling vond weliswaar plaats in Duitsland, maar de handeling had het gevolg dat in Nederland een paard werd uitgevoerd.

[59] HR 6 april 1954, NJ 1954, 368. In geval van oplichting werden de oplichtingsmiddelen te Singapore aangewend tegen een in Nederland verblijvend slachtoffer. In het arrest erkent de Hoge Raad dat er tegelijkertijd meerdere plaatsen van het delict kunnen zijn. In casu geldt Nederland als plaats van het delict ongeacht of ook andere plaatsen als zodanig kunnen gelden.

[60] HR 30 september 1997, NJ 1998, 117; HR 13 april 1999, NJ 1999, 538.

Het Europese Hof voor de Rechten van de Mens heeft reeds in zijn uitspraak van 1976 (Handysde vs UK) bepaald dat artikel 10 EVRM uitdrukkelijk niet alleen van toepassing is op '"information" or "ideas" that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population'.[61]

Als gevolg van het tweede lid van artikel 10 EVRM zijn overheidsorganen bevoegd inbreuk te maken op het recht van de vrijheid van meningsuiting van de burger 'for the prevention of (…) crime' hetgeen zowel repressieve al preventieve actie lijkt in te sluiten, mits voorzien bij wet en mits in overeenstemming met de overige criteria van het tweede lid. Een dergelijk ingrijpen dient noodzakelijk te zijn in een democratische samenleving. De eis van noodzakelijkheid sluit de voorwaarde van proportionaliteit van het betreffende overheidshandelen in. De omvang en het effect van het overheidsingrijpen dienen in balans te zijn met het legitieme doel dat met de ingreep wordt nagestreefd.

Het blokkeren van de toegang tot kinderporno voorkomt dat binnen de Nederlandse rechtsorde het strafbare feit van het verspreiden, dan wel het openlijk tentoonstellen of het invoeren van kinderporno wordt begaan, zoals strafbaar gesteld in artikel 240b Sr. Hiervoor dient een formeel-wettelijke bevoegdheid te bestaan, die in zijn strekking en toepassing aan het noodzakelijkheidscriterium, zoals hierboven omschreven.

Artikel 7 Grondwet

Artikel 7 Grondwet is geredigeerd naar de verschillende media waardoor of waarmee men de vrijheid van meningsuiting kan beoefenen. Hier zijn van belang het eerste lid 1 (vrijheid van drukpers) en het derde lid (andere middelen dan de drukpers en omroep).

Figuur 3.11: Artikel 7, eerste en derde lid GW

1. Niemand heeft voorafgaand verlof nodig om door de drukpers gedachten of gevoelens te openbaren, behoudens ieders verantwoordelijkheid volgens de wet. (…) 3. Voor het openbaren van gedachten of gevoelens door andere dan in de voorgaande leden genoemde middelen heeft niemand voorafgaand verlof nodig wegens de inhoud daarvan, behoudens ieders verantwoordelijkheid volgens de wet. De wet kan het geven van vertoningen toegankelijk voor personen jonger dan zestien jaar regelen ter bescherming van de goede zeden. (…)

De invloed van artikel 10 EVRM en de rechtspraak door het Europese Hof voor de Rechten van de Mens op de rechtsvorming rond de vrijheid van meningsuiting is onmiskenbaar door de directe werking, aan die bepaling door dezelfde grondwetgever toegekend. Vanwege zijn directe werking krachtens artt. 93 en 94 GW lijkt artikel 10 EVRM met de onderliggende rechtspraak inmiddels van grotere betekenis voor de Nederlandse rechtsorde dan artikel 7 GW. De overheid is niettemin evenzeer gebonden aan de grondwettelijke norm.

Verschillen artikel 7 GW en artikel 10 EVRM

Tussen artikel 10 EVRM en artikel 7 GW bestaan enkele verschillen die hier geen uitvoerige bespreking behoeven. Zo noemt artikel 10 dat de vrijheid van informatiegaring uitdrukkelijk

[61] Handyside v. U.K., 7 december 1976, sindsdien staande rechtspraak en herhaald in vele arresten, zie bijvoorbeeld Perna v. Italië, 6 mei 2003.

als onderdeel van de vrijheid van meningsuiting, waar artikel 7 GW dat in het midden laat. Verder is artikel 10 EVRM in belangrijke mate techniek-neutraal geformuleerd, waar artikel 7 GW zich richt op onderscheiden media. Een opmerkelijk verschil is verder dat artikel 7 GW in de eerste drie leden overheidscensuur ('voorafgaande toestemming') verbiedt, waar de toelaatbaarheid van overheidscensuur in het kader van artikel 10 EVRM beoordeeld dient te worden op basis van de door het tweede lid genoemde legitieme belangen en aan de hand van de door de rechtspraak ontwikkelde criteria.

De staande jurisprudentie met betrekking tot de vrijheid van drukpers geeft een ruime uitleg van dit laatste begrip. Onder het begrip drukpers kunnen meerdere informatiedragers worden samengenomen en beperkt zich niet tot tekstuele informatie. Gedachten en gevoelens kunnen immers ook tot uitdrukking worden gebracht door middel van afbeeldingen. Het derde lid van artikel 7 GW erkent dat er naast de klassieke gedrukte media ook andere mogelijkheden bestaan om gedachten en gevoelens te uiten en deze te verspreiden. Deze gedachten en gevoelens kunnen ook tot uitdrukking worden gebracht in de vorm van kinderpornografische afbeeldingen. Of deze afbeeldingen nu onder het eerste lid dan wel onder het derde lid van artikel 7 GW behoren te vallen hangt samen met de context en de presentatievorm waarin die afbeeldingen zijn geplaatst, die verschillend kan zijn. Voor onderstaande verhandeling is die vraag academisch. Van belang is hier alleen vast te stellen dat kinderpornografie in beginsel een door artikel 7 GW te beschermen uiting is. Beperkingen op die vrijheid dienen bij formele wet te worden gesteld. Aan dat vereiste is met artikel 240b Sr voldaan.

Beide geciteerde leden van artikel 7 GW hebben gemeen het uitdrukkelijke verbod op (preventieve) censuur. Dit verbod richt zich tot de overheid en kan alleen worden doorbroken in geval van de zogenoemde uitzonderingstoestand (zie artikel 103 tweede lid GW). De gevallen waarin en de gronden waarop de uitzonderingstoestand kan worden uitgeroepen zijn echter zodanig dat het instellen van censuur – op welke wijze dan ook – niet aan de orde is. De producent, verspreider of terbeschikkingsteller van kinderpornografisch materiaal kan zich wat betreft eventuele voorafgaand toezicht door de overheid beroepen op artikel 7 GW, maar kan uiteraard achteraf wel worden vervolgd wegens overtreding van artikel 240b Sr. ('behoudens ieders verantwoordelijkheid volgens de wet').

Artikel 7 GW is zuinig geformuleerd. Anders dan de overeenkomstige bepalingen uit internationale verdragen (artikel 10 EVRM, artikel 19 BUPO) formuleert artikel 7 niet de omvang van het recht op vrijheid van meningsuiting maar begrenst het de inperkingen op die vrijheid van meningsuiting. De grondwetgever van 1983 koos voor deze benadering, omdat het in het andere geval nodig zou zijn om alle toegelaten inperkingen op het recht van vrijheid van meningsuiting uitdrukkelijk in de wet op te nemen. Niet onbegrijpelijk is dan ook dat wijziging van de tekst van het Grondwetsartikel voorwerp van wijzigingsvoorstellen is geweest en nog is (Grondrechten, 2000).[62]

Onder censuur verstaan wij beperkende maatregelen in verband met de inhoud van een uiting of de verspreiding ervan.[63] De meest voor de hand liggende maatregel is het voorafgaand verlenen (dan wel weigeren) van toestemming. In de uitgebreide jurisprudentie op artikel 7 GW zijn verschillende andere beperkende maatregelen die al dan niet indirect een beperking van de vrijheid van meningsuiting op kunnen leveren, in de zgn. verspreidingsjurisprudentie aan de orde geweest. Toepassing van andere wetten en regelgeving kan een beperking van de vrijheid van meningsuiting betekenen. De Hoge Raad acht die inperkingen in het algemeen toelaatbaar, indien nog een vrij gebruik kan worden gemaakt van elk verspre-

[62] De Grondswetswijziging werd door het parlement afgewezen in 2001. Nieuwe voorstellen worden voorberied in internationale afstemming, maar invoeringstraject en – tijdstip zijn onduidelijk (TK 2007/2008, 30 800 VII, p. 16).

[63] In de literatuur vaak als 'preventieve censuur' aangeduid ter onderscheiding van beperkende maatregelen die achteraf worden genomen.

dingsmiddel met een zelfstandige betekenis (Mey, 2000). In diezelfde rechtspraak is tevens aan de orde geweest in hoeverre bijvoorbeeld de rechter bevoegd is preventieve maatregelen te gelasten, bijvoorbeeld als maatregel in geval van een onrechtmatige daad (artikel 6:162 BW). Het toewijzen van een eis dat de gedaagde partij zich in de toekomst onthoudt van dezelfde of soortgelijke onrechtmatige uitingen, komt in de regel niet voor toewijzing in aanmerking omdat een dergelijk verbod te ruim en te vaag is en daardoor in strijd zou komen met de vrijheid van meningsuiting (Mey, 2000). Niet relevant is of er al dan niet redenen zijn om aan te nemen dat de betrokkene in de toekomst dergelijke uitingen zal doen. Indien dat wel geschiedt, kan de zaak opnieuw voor de rechter worden gebracht. Wel vatbaar voor een beperkende maatregel is de herhaling van de uiting of de verspreiding van deze uiting, omdat de onrechtmatigheid van de uiting door dezelfde rechter is vastgesteld. Het dient hierbij voldoende concreet te zijn wat de gedaagde heeft na te laten. Voor het opleggen van dergelijke maatregelen zal alleen aanleiding bestaan in duidelijke maar ook ernstige gevallen (Mey, 2000).

In het kader van het filteren/blokkeren van kinderporno is de vraag relevant in hoeverre dergelijke maatregelen door of vanwege de overheid, waarbij niet alleen de strafbare uiting wordt tegengehouden, maar ook andere informatie, zich verdraagt met artikel 10 EVRM, resp. artikel 7 GW. In dit rapport wordt hiervoor de technische term *overblocking* gebruikt. Afhankelijk van de gebruikte techniek is onvermijdelijk dat een zekere hoeveelheid niet strafbare informatie wordt tegengehouden die geen directe relatie met de strafbare kinderporno heeft (zie ook hoofdstuk 2 en 4). Ook is het mogelijk, omdat de blokkering gericht is op de veronderstelde bron van de kinderporno, dat na verloop van tijd informatie wordt tegengehouden die niet (meer) strafbaar is. Ten einde te voorkomen dat blokkering door of vanwege de overheid in strijd komt met de vereisten van artikel 10 EVRM en artikel 7 GW, in het laatste geval in het bijzonder met het grondwettelijk censuurverbod, dient permanent en frequent te worden nagegaan of de ingezette maatregelen nog aan hun doel beantwoorden.

3.10 Samenvatting

Aanvankelijk richtte de strafbaarstelling van artikel 240b Sr zich alleen tegen misbruik van jeugdigen. Onder invloed van internationale ontwikkelingen is ook in Nederland de opvatting gemeengoed geworden dat de bijkomende ratio minstens zo belangrijk is, namelijk te voorkomen dat kinderen worden aangemoedigd of verleid tot deelname aan seksueel verkeer, en gedrag te voorkomen dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert. De Aanwijzing van de Procureurs-generaal bevat een uitvoerige toelichting op de wetsgeschiedenis, criteria ter beoordeling of afbeeldingen strafbare kinderporno opleveren en procedurevoorschriften voor de vervolging van kinderporno, met name over de omgang met het inbeslaggenomen materiaal.

Internationaal gezien zijn inspanning verricht te komen tot harmonisatie van kinderpornostrafbepalingen. Hoewel niet kan worden gezegd dat die inspanning zonder resultaat zijn gebleven, blijven niet onbelangrijke verschillen tussen landen bestaan. Een belangrijk aspect is de zogenoemde virtuele porno, dat in bijvoorbeeld de V.S. niet strafbaar is. De Nederlandse rechter had zich tot half maart van dit jaar nog niet eerder over de strafbaarheid van virtuele kinderporno uitgesproken. De verwachting is dat meer zaken zullen volgen.

Binnen de Europese Unie zullen de verschillen in strafbaarstelling tussen de lidstaten uiteindelijk beperkt zijn, in andere gremia treden grotere afwijkingen op. De leeftijd van 18 jaar komt weliswaar uit het bekende UN-verdrag, maar wordt niet door alle landen toegepast. Hierdoor kan de situatie ontstaan dat zelfs met landen waarmee een rechtshulpverdrag van kracht is, toch niet tegen alle hier te lande strafbaar gestelde verschijningsvormen van kinderporno kan worden opgetreden. Daarnaast zijn er landen die aanzienlijk verder gaan in de strafbaarstelling dat Nederland, waardoor de situatie ontstaat dat materiaal dat hier rechtmatig

in het (internet-)verkeer kan worden gebracht, door die landen als strafbaar wordt tegengehouden.

Nederland voldoet overigens niet geheel aan de vereisten van artikel 9 van het Cybercrimeverdrag (paragraaf 3.2). Die situatie behoeft aandacht bij de implementatie van het recent ondertekende Verdrag 201 van de Raad van Europa (*On the Protection of Children Against Sexual Exploitation and Sexual Abuse)*, dat de inhoud van artikel 9 CCC met geringe wijziging en aanvulling heeft overgenomen.

Het toepassen van filtering en blokkeren van internetverkeer houdt in dat door middel van software kennis wordt genomen van de inhoud van bepaalde gegevensstromen. De vertrouwelijkheid van dit gegevensverkeer wordt gewaarborgd door artikel 8 EVRM en de corresponderende bepalingen van de Nederlandse Grondwet. Dat houdt in dat filtering/blokkering door of vanwege de overheid alleen plaats kan vinden indien de wet daartoe de bevoegdheid verschaft, of alleen kan geschieden met toestemming van de betrokken personen. Filtering/blokkering door ISP´s behoeft vanwege de horizontale werking van dit grondrecht de toestemming van de betrokken abonnees.

Internet providers zijn op grond van Europese regelgeving niet aansprakelijk voor gegevensverkeer dat zij niet zelf initiëren of inhoudelijk beïnvloeden. Zij behoeven niet na te gaan of zij strafbare of inbreukmakende informatie hosten, maar zij dienen wel in actie te komen indien zij wetenschap hebben van het strafbare of anderszins onrechtmatige karakter van de informatie die zij hosten. Op dit laatste steunt de ontwikkeling van zgn. *notic-and-takedown-systeem*. De huidige wettelijke regelingen rond provider-aansprakelijkheid geven geen basis voor het vestigen van aansprakelijkheid van providers voor het filteren en blokkeren van aanbod van kinderporno die niet door henzelf voor derden wordt gehost.

De bestaande wettelijke opsporingsbevoegdheden verschaffen geen basis voor het (doen) filteren/blokkeren van internetverkeer. De toepassing van artikel 125o Sv beperkt zich tot de situatie van een doorzoeking en is niet gericht op gegevensstromen. Dat geldt ook voor artikel 54a Sr. De toepassing van artikel 54a Sr is bovendien omgeven door onvoldoende rechtswaarborgen. Overwogen zou kunnen worden een zelfstandige bevoegdheid in het leven te roepen tot het (doen) verwijderen van informatie uit systemen van internetproviders door aanvulling en verbetering van artikel 125o Sv en artikel 54a Sr, dit in onderlinge samenhang.

De politie en dus ook het KLPD beschikt niet over een bevoegdheid tot het (doen) filteren en blokkeren van kinderporno. Een dergelijke bevoegdheid kan niet worden ontleend aan artikel 2 Polw. Aangezien de activiteit van filteren en blokkeren een inbreuk inhoudt op het grondrecht van de vertrouwelijke communicatie (artikel 13 GW) dan wel op de bescherming van de persoonlijke levenssfeer (artikel 10 GW), is in het Nederlandse rechtsstelsel een specifieke formeelwettelijke basis vereist, waarvoor artikel 2 Polw niet kan dienen.

Blokkeren van internetverkeer met aanbieders van kinderporno zal in de regel het internetverkeer met het buitenland raken. De Staat der Nederlanden is bevoegd tot het tegenhouden van internetverkeer omdat het onderliggende strafbare feit van het aanbieden van kinderporno op het Nederlands grondgebied wordt gepleegd, dan wel dat de gevolgen van het strafbare feit zich binnen de Nederlandse rechtsorde manifesteren.

Het vervaardigen en distribueren van kinderporno moet worden beschouwd als het doen van een uiting en het verspreiden van die uiting, in beginsel beschermd door het grondrecht van de vrijheid van meningsuiting. Beperkingen van dit grondrecht dienen bij formele wet te worden gesteld. Gezien de ernst van genoemde gedragingen zal het individuele recht van de vrijheid van meningsuiting en informatiegaring moeten wijken voor het maatschappelijke belang tot bescherming van jeugdigen. In hoofdstuk 2 is besproken welke technische middelen tegen de verspreiding van kinderporno kunnen worden ingezet. In alle gevallen zal sprake zijn van een bepaalde mate van overblocking: er wordt onvermijdelijk naast de strafbare informatie ook niet-strafbare informatie tegengehouden. Bij uitvoering van blokkerings-

maatregelen door of namens de overheid, zo de wet daartoe een bevoegdheid zou geven, roept dat de verplichting in het leven tot doen van een zorgvuldige keuze van het aan te wenden instrument en een permanente verificatie of de maatregel aan zijn doel beantwoordt, teneinde te voorkomen dat toepassing van de maatregel in strijd komt met artikel 10 EVRM dan wel met het censuurverbod van artikel 7 GW.

HOOFDSTUK 4

Buitenlandse ontwikkelingen

4.1 Inleiding

Het blokkeren van informatie op internet gebeurt in minstens veertig landen verspreid over Azië, het Midden-Oosten, Afrika, Canada, de Verenigde Staten en Europa (Deibert e.a., 2008). In Europa namen Engeland en Noorwegen de eerste initiatieven tot het blokkeren van websites met kinderpornografische inhoud. In juni 2004 lanceerde British Telecom (BT) het project CleanFeed. In oktober/november 2004 startten in Noorwegen de internetprovider Telenor en recherche-eenheid Kripos met een kinderpornofilter. Op dit moment blokkeren in Europa in elk geval Engeland, Noorwegen, Zweden, Denemarken, Finland, Italië en sinds kort ook Nederland websites met kinderporno (IT- og Telestyrelsen, 2006).[64]

In Europa zijn momenteel twee filtersystemen: het Noorse/Scandinavische en het Engelse. We richten ons in dit hoofdstuk daarom vooral op Noorwegen, Zweden en Engeland. Het Noorse initiatief en dientengevolge ook de Noorse context bespreken we het uitgebreidst, want dit is het initiatief dat via UPC naar Nederland is gebracht. Vervolgens gaan we in op de stand van zaken in Zweden (dat als eerste de Noorse filtersystematiek overnam) en Engeland (dat een andere filtersystematiek hanteert). Dan bespreken we op hoofdlijnen de situatie in de Verenigde Staten, met name vanwege de daar heersende *First Amendment*-doctrine. Tot slot besteden we, meer ter illustratie, enige aandacht aan enkele niet-Europese landen.

Technische details blijven in dit hoofdstuk achterwege; deze staan beschreven in hoofdstuk 2.[65]

4.2 Noorwegen

Korte chronologie

Voor het overzicht geven we eerst een korte chronologie van de belangrijkste gebeurtenissen in de ontwikkeling van en rondom het Noorse filter:

okt./nov. 2004[66]	Internetprovider Telenor en recherche-eenheid Kripos starten in Noorwegen met het kinderpornofilter. De basis is zelfregulering, tegen de achtergrond van mogelijke wetgeving.
april 2005	De eerste andere Noorse ISP's nemen het filter in gebruik (genoemd worden Freewave, NextGenTel, Tele2 en UPC).
17 mei 2005	Zweden neemt als eerste andere land het Noorse kinderpornofilter in gebruik; het betreft een samenwerking tussen het Zweedse Telenor AB en de Zweedse Nationale Recherche.
20 mei 2005	Kinderpornografie wordt in Noorwegen in een afzonderlijk wetsartikel strafbaar gesteld (was daarvoor onderdeel van een breder pornografieverbod).
juni 2005	Telenor neemt in Noorwegen het filter ook in gebruik voor internet via de mobiele telefoon, naar eigen zeggen als eerste in de wereld.
februari 2006	Europese landen met een filter zijn nu: Engeland, Noorwegen, Zweden, Denemarken (IT- og Telestyrelsen, 2006:5).
mei 2006	De Noorse minister van Economische Zaken, Odd Eriksen, dringt er bij Telenor op aan dat het bedrijf een techniek ontwikkelt om MMS-

[64] http://www.edri.org/edrigram/number5.1/italy_blocking. Laatst bezocht op 13 februari 2008 om 11.30 uur.

[65] De lijst met geraadpleegde overige bronnen bevat een overzicht van nieuwsberichten waarop dit hoofdstuk mede is gebaseerd.

[66] De bronnen die we raadpleegden spreken elkaar tegen over de maand van ingebruikname.

	berichten te controleren op kinderpornografische inhoud.
30 juni 2006	Noorwegen ratificeert het cybercrimeverdrag van de Raad van Europa.
1 oktober 2006	Het cybercrimeverdrag wordt in Noorwegen van kracht.
december 2006	Kripos gaat het Europese CIRCAMP leiden (Cospol Internet Related Child Abusive Material Project) om ander landen te helpen met het stoppen van de verspreiding van kinderpornografisch materiaal via internet. Deelnemers aan het project zijn op dat moment Denemarken, België, Ierland, Italië, Malta, Polen, Zweden en Nederland.
februari 2007	De Noorse Datacriminaliteitscommissie geeft het ministerie van Justitie en Politie een verdeeld advies inzake wetgeving voor het filteren van internetverkeer (Datakrimutvalget, 2007).
november 2007	Aan CIRCAMP doen inmiddels 20 Europese landen mee.

Noorse kinderpornowetgeving

Op 20 mei 2005, een half jaar na de invoering van het kinderpornofilter, werd in Noorwegen kinderpornografie in een afzonderlijk wetsartikel opgenomen. Eerder was het verbod op kinderpornografie geregeld binnen het algemene verbod op pornografie in artikel 204 van de Noorse strafwet. Kinderpornografie is uit dat artikel gehaald en ondergebracht in het nieuwe artikel 204a. De wetswijziging betrof, aldus de toelichting bij het wetsvoorstel, meer een herstructurering van teksten dan een fundamenteel inhoudelijke wijziging van strafbare gedragingen (Innst. O. nr. 66, 2004-2005). Wel zijn met deze herstructurering van de wetstekst twee nieuwe gedragingen strafbaar gesteld: het 'aanschaffen' en het zich 'planmatig op de hoogte stellen van' kinderpornografie. De teksten van artikelen 204 en 204a van de Noorse strafwet staan in figuur 4.1 en 4.2.[67]

De wetswijziging heeft tevens een symbolische functie. Een belangrijk aspect van de wetswijziging is namelijk de nadruk die wordt gelegd op het achterliggende kindermisbruik. Zo wordt in artikel 204 wel gesproken over 'pornografie', maar in artikel 204a wordt niet gesproken over 'kinderpornografie'. De reden daarvoor is dat de wetgever, aldus de toelichting op de wettekst, in navolging van Kripos wil beklemtonen dat kinderpornografie niet zoiets is als alle andere pornografie maar dan met kinderen. De essentie van kinderpornografie is volgens de Noorse wetgever dat het misbruik van kinderen impliceert. Het is geen bijzondere vorm van pornografie, het is een bijzondere vorm van kindermisbruik. Vandaar dat kinderpornografie in de nieuwe wettekst staat omschreven als: 'representaties van seksueel misbruik van een kind'. In de oude redactie, toen kinderporno nog viel onder artikel 204, luidde de omschrijving: 'seksuele uitbeeldingen waarbij gebruik wordt gemaakt van kinderen'. In de toelichting op haar voorstel tot wetswijziging schrijft de Justitiecommissie die het wetsvoorstel voorbereidde: 'De commissie wil benadrukken dat elke afbeelding met kinderpornografisch karakter kindermisbruik inhoudt.' (Innst. O. nr. 66, 2004-2005:2). De Nederlandse wetgever heeft voor het omschrijven van kinderpornografie gekozen voor het gevoelsmatig wat neutralere 'seksuele gedraging met iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt'.

[67] De vertalingen zijn van een van ons (Stol) op basis van het wetsvoorstel met toelichting van de Noorse Justitiecommissie (Innst. O. nr. 66, 2004-2005).

Figuur 4.1: artikel 204 van de Noorse strafwet[68]

Hij die:
a. pornografie uitgeeft, verkoopt of op andere wijze tracht pornografie te verspreiden;
b. pornografie invoert met het oogmerk om het te verspreiden;
c. pornografie ter beschikking stelt aan personen onder de 18 jaar, of
d. een openbare voordracht houdt of een openbare voorstelling of tentoonstelling verzorgt met pornografische inhoud,

wordt gestraft met een boete of met een gevangenisstraf van ten hoogste drie jaar.

Onder pornografie wordt in dit artikel verstaan seksuele uitbeeldingen die aanstootgevend zijn of die op een andere wijze de menselijke waardigheid aantasten, waaronder seksuele uitbeeldingen waarbij gebruik gemaakt wordt van lijken, dieren, geweld of dwang. Tot pornografie wordt niet gerekend seksuele uitbeeldingen met een kunstzinnig, wetenschappelijk, informatief of soortgelijk doel.

Hij die uit onachtzaamheid handelingen verricht zoals bedoeld in het eerste lid, wordt gestraft met een boete of met gevangenisstraf van ten hoogste 6 maanden. Op dezelfde wijze wordt gestraft de eigenaar of leidinggevende die nalaat om te verhinderen dat tijdens het werk handelingen worden verricht zoals genoemd in het eerste lid.

Dit artikel geldt niet voor film, video of vertaling die door Mediatoezicht is toegelaten voor commercieel vertoon.

Figuur 4.2: artikel 204a van de Noorse strafwet

Hij die:
a. een representatie van seksueel misbruik van een kind of een representatie die kinderen seksualiseert produceert, aanschaft, invoert, bezit, ter beschikking stelt aan anderen of zich tegen vergoeding of planmatig op de hoogte stelt van dergelijke representaties,
b. zich bezig houdt met representaties van seksueel misbruik van kinderen of representaties die kinderen seksualiseren, op een andere wijze dan genoemd in artikel 204 eerste lid, of iemand onder de 18 jaar ertoe aanzet zich te laten afbeelden als onderdeel van een commerciële representatie van 'vlottende of vastgelegde'[69] beelden met seksuele inhoud, of dergelijke representaties produceert waarop iemand onder de 18 jaar is afgebeeld, wordt gestraft met een boete of gevangenisstraf van ten hoogste drie jaar.

Onder kind wordt in dit artikel verstaan een persoon die jonger dan 18 jaar is of schijnt.

Hij die uit onachtzaamheid handelingen verricht zoals genoemd in het eerste lid, wordt gestraft met een boete of met gevangenisstraf van ten hoogste 6 maanden. Op dezelfde wijze wordt gestraft de eigenaar of leidinggevende die nalaat om te verhinderen dat tijdens het werk handelingen worden verricht zoals genoemd in het eerste lid.

De straf kan vervallen voor degene die een beeld neemt en bezit van een persoon tussen de 16 en 18 jaar, indien die persoon zijn toestemming heeft gegeven en de twee personen van ongeveer dezelfde leeftijd en ontwikkeling zijn.

Artikel 204 tweede lid, tweede punt en vierde lid zijn van overeenkomstige toepassing.

[68] De Noorse wetsartikelen zijn anders dan de Nederlandse niet onderverdeeld in *genummerde* leden. Elke alinea geldt als een lid.

[69] Deze uitdrukking is toegevoegd na een uitspraak van een Noorse rechter waarin werd bepaald dat kinderpornografie welke zich bevond in de map 'tijdelijke internetbestanden' moet worden gezien als 'vlottende informatie' en niet als 'in bezit' van de gebruiker.

In zowel Noorwegen als Nederland is het kinderpornoverbod ingebed in een bredere zedelijkheidswetgeving. De artikelen aangaande kinderpornografie zijn op hoofdlijnen vergelijkbaar, maar verschillen zijn er ook. We noemden reeds de relatief sterke nadruk die in Noorwegen ligt op het aspect van misbruik. De meest in het oog lopende overige verschillen tussen het Noorse artikel 204a en het Nederlandse artikel 240b zijn:

- in Noorwegen zijn alle uitingen van kinderpornografie strafbaar, de Nederlandse wet spreekt alleen over beeldmateriaal;
- in Noorwegen is ook het (bewust) kijken naar kinderporno strafbaar, in Nederland niet;
- in Noorwegen zijn ook uitingen strafbaar die kinderen 'seksualiseren' – dus los van de vraag of de afbeelding een seksuele handeling bevat, de Nederlandse wet is gericht op afbeeldingen van seksuele *gedragingen*;
- in Noorwegen geldt ook de aanwezigheid van kinderporno in de map 'tijdelijke internetbestanden' ('in cache') als 'in bezit hebben', in Nederland niet (de rechter veroordeelt daarvoor niet);
- in Noorwegen zijn werkgevers en leidinggevenden strafbaar als zij niet verhinderen dat hun medewerkers tijdens het werk het kinderpornoverbod overtreden, in Nederland niet;
- in Noorwegen is de maximum gevangenisstraf 3 jaar, in Nederland 4;
- in Noorwegen is een strafverlichtende omstandigheid als iemand het kinderpornoverbod uit onachtzaamheid overtreedt (maximum straf gaat dan van 3 jaar naar 6 maanden), in Nederland is een strafverzwarende omstandigheid als iemand van overtreding zijn beroep of gewoonte maakt (maximum straf gaat dan van 4 naar 6 jaar).

In deze beknopte vergelijking zien we dat Noorwegen een ruimere strafbaarstelling kent dan Nederland. In Nederland gelden daarentegen hogere maximumstraffen.

Implementatie en verspreiding van het kinderpornofilter

In 2003 riep de Noorse minister van Justitie, Odd Einar Dørum, de politie, het bedrijfsleven en andere partijen op tot een gezamenlijke inzet tegen kinderpornografie. In reactie daarop werd het Noorse internetfilter ontwikkeld door Telenor in samenwerking met Kripos (de Noorse Nationale Recherche) en Redd Barna (de Noorse afdeling van Save the Children) (Innst. O. nr. 66, 2004-2005). Welke rol Redd Barna heeft gespeeld bij de totstandkoming van het filter wordt niet duidelijk uit de door ons geraadpleegde bronnen. Ook het archief met nieuwsberichten van Redd Barna (www.reddbarna.no) geeft hierover geen informatie. Het filter wordt steevast gepresenteerd als het resultaat van samenwerking tussen Telenor en Kripos, waarbij Telenor de technische realisatie van het blokkeren voor haar rekening neemt en Kripos zorgt voor de lijst met te blokkeren websites. Aan het ontstaan van het filter lag weliswaar een oproep vanuit de regering ten grondslag, maar geen wetgeving. Er zijn dan ook geen speciaal voor het filter wettelijke vastgelegde bezwaar- of beroepsprocedures. Op de stoppagina die een internetter te zien krijgt als hij probeert een geblokkeerde pagina te bezoeken, staat dat wie bezwaar heeft tegen de blokkering, de bezwaren bij Kripos kenbaar kan maken per telefoon (nummer 23 20 80 00) of per e-mail (feilfilter@kripos.no).

In september 2004 publiceerden de Noorse media de eerste nieuwsberichten over het filter. Op internetfora werd meteen discussie over deze nieuwe ontwikkeling gevoerd (bv. www.diskusjon.no). In de loop van oktober/november 2004 werd het filter in gebruik genomen.[70] Het filter geldt zowel voor inbelverbinding als breedband. De DNS-server van de provider geeft aan de computer van de klant niet het gevraagde IP-adres maar het door Kripos

[70] Nieuwsberichten uit 2004 spreken over oktober als maand van ingebruikname, in latere berichten staat meestal november.

daarvoor in de plaats gestelde adres met een zogenoemde stoppagina. Het filter blokkeert enkel websites, dus bijvoorbeeld geen e-mailverkeer, berichten in nieuwsgroepen, filesharing of P2P-berichten.[71] Het filter geldt voor alle Telenor-klanten; het is echter vrijwillig op basis van het *opt-out* principe: voor klanten die aangeven het filter niet te willen zal Telenor het uitschakelen (een mogelijkheid waarvan voor zover ons bekend geen gebruik wordt gemaakt). Telenor nodigt van meet af aan andere internetproviders uit om zich aan te sluiten bij de samenwerking en ook het filter te gaan gebruiken.

Kort na de introductie van het filter stelt de Noorse Justitiecommissie zich, in de toelichting op haar voorstel tot wijziging van de pornografiewetgeving, op het standpunt dat alle Noorse internetproviders een dergelijk filter zouden moeten hebben. De commissie roept de regering op om de ontwikkelingen nauwgezet te volgen. Als eind 2006 niet alle internetaanbieders in Noorwegen zo'n filter hebben, dient de regering met voorstellen te komen om dat op te leggen, aldus de commissie. Zij merkt verder op dat voor kinderpornografie vaak moet worden betaald met een creditcard en vraagt de regering derhalve om na te gaan welke mogelijkheden er zijn om het gebruik van creditcards op websites met kinderpornografisch materiaal tegen te gaan en daarover te rapporteren aan het parlement.

In maart 2005, zo'n vier maanden na de ingebruikname van het filter, sluiten ook de Noorse internetaanbieders Freewave, NextGenTel, Tele2 en UPC een overeenkomst met Kripos over het in gebruik nemen van het filter. 'Als Freewave, NextGenTel, Tele2 en UPC hetzelfde doen als Telenor, valt 75 tot 80 procent van de Noorse internetters onder het filter.' (www.digi.no).

Op dinsdag 17 mei 2005 nemen de Zweedse Nationale Recherche (Rikskriminalpolisen) en Telenor AB (de Zweedse tak van Telenor) het Noorse kinderpornofilter in gebruik. Zweden is het eerste land dat het filter van Noorwegen overneemt en in Zweden is Telenor AB de eerste internetprovider met een dergelijk filter. Net als in Noorwegen is Telenor AB verantwoordelijk voor de technische realisatie, terwijl de politie zorgt voor het actueel houden van de lijst met te blokkeren websites.

Eind december 2004, dus kort na de implementatie van het filter, nam Telenor 3G[72] in gebruik als nieuwe transmissiestandaard voor haar mobiele telefonie. Daarmee is het mogelijk te internetten via een GSM-toestel en kan men dus ook via een mobieltje websites met kinderporno bezoeken. Begin juni 2005 plaatst Telenor het kinderpornofilter op haar GSM-netwerk en is daarmee naar eigen zeggen het eerste telecombedrijf ter wereld met gefilterde mobiele telecommunicatie.

In 2005 neemt de Deense telecomprovider TDC het Noorse filter in gebruik, waarna andere Deense providers volgen.

Begin 2006 publiceert het IT- og Telestyrelsen van het Deense Ministerie van Wetenschap, Technologie en Ontwikkeling de resultaten van een onderzoek naar maatregelen tegen kinderporno op internet (IT- og Telestyrelsen, 2006), een onderzoek in het kader van het EU-programma 'Safer Internet Plus'. Volgens het onderzoek is begin 2006 een kinderpornofilter in gebruik in Engeland, Noorwegen, Zweden en Denemarken. Plannen voor een dergelijk filter zijn er dan in Finland, Ierland, IJsland, Italië, Litouwen, Malta, Zwitserland, Spanje en Turkije. Geen plannen voor een kinderpornofilter op internet zijn er in België, Cyprus, Frankrijk, Nederland, Polen, Portugal, Slowakije, Duitsland, Hongarije en Oostenrijk.

In mei 2006 meldt mediabedrijf VG dat de Noorse minister van Economische Zaken, Odd Eriksen, zijn ongerustheid heeft geuit over mediaberichten omtrent het verzenden van kinderpornografisch materiaal per MMS-bericht (www.vg.no, 19 mei 2006). Met MMS, de multimediale opvolger van SMS, kunnen personen behalve tekst ook beelden en film via hun

[71] Hoofdstuk 2 bevat een nadere technische uitleg omtrent de werking van het filter.

[72] 3G staat voor 'Third Generation' – een in 2001 in Japan ontwikkelde transmissietechniek waarmee beelden kunnen worden ontvangen met mobiele telefoons, hetgeen 'mobiel internet' mogelijk maakt.

mobiele telefoon uitwisselen, en dus ook kinderpornografische afbeeldingen. De minister, namens de staat met 54 procent aandelen de grootse eigenaar van Telenor, vroeg Telenor per brief 'een manier te vinden om multimediale berichten met een kinderpornografische inhoud te stoppen'. Telecombedrijven hebben, aldus VG, (nog) geen technische mogelijkheden om MMS-berichten die pornografische beelden van kinderen bevatten te herkennen en te onderscheppen. Zijn die oplossingen er wel, dan overweegt de overheid om strafrechtelijk te reageren op bedrijven die nog steeds dergelijke berichten doorlaten. Telenor kan voorlopig niet tegemoetkomen aan Eriksens verzoek. 'We kunnen niet zien wat de mensen schrijven en wat voor soort beelden ze verzenden. Dat zou zoiets zijn als het openen van brieven van mensen, zegt Atle Lessum van Telenor.' (www.vg.no).

In december 2006 berichten de media dat Kripos is aangewezen om het Europees project CIRCAMP te leiden (Cospol Internet Related Child Abusive Material Project).[73] Noorwegen zal langs die weg andere landen helpen met het stoppen van de verspreiding van kinderpornografisch materiaal via internet. Deelnemers aan het project zijn op dat moment Denemarken, België, Ierland, Italië, Malta, Polen, Zweden en Nederland. Volgens hetzelfde bericht zijn ook Interpol en Europol bij het project betrokken.[74] In december 2006 is het Noorse model ook gepresenteerd aan de Amerikaanse overheid; Nieuw Zeeland en Australië hebben interesse getoond. In november 2007 meldt de Noorse politie op haar website dat aan CIRCAMP 20 Europese landen meedoen (www.politi.no).

Over hoe ver het Noorse filter exact is verspreid per januari 2008 ontbreken ons gegevens. Globaal gesproken is bekend dat in Noorwegen alle grote internetproviders het filter gebruiken, maar we weten dat er ook Noorse providers zijn die dat niet doen (Datakrimutvalget, 2007). Ook is bekend dat het filter buiten Noorwegen, Zweden en Denemarken in nog weer andere Europese landen is geïmplementeerd, zoals Finland en Nederland. Niettemin komt de Noorse Commissie Datacriminaliteit, ingesteld bij Koninklijk Besluit van 11 februari 2002, begin 2007 met een sterk verdeeld advies over hoe het verder moet met het filter. Met name de vraag of het filter wettelijk moet worden geregeld, splijt de commissie.

Advies van de Commissie Datacriminaliteit

Over filtermethoden stelt de voltallige commissie allereerst vast dat men kan kiezen voor filteren op nationaal niveau (met China als voorbeeld) of op ISP-niveau. Noorwegen heeft niet de infrastructuur voor filtering op landelijk niveau en het is volgens de voltallige commissie ook niet aan de orde om een dergelijke filtering mogelijk te maken.

Het kinderpornofilter is een publiek-private samenwerking (PPS) tussen Noorse overheidsinstellingen en internetaanbieders en betreft filtering op ISP-niveau. De regeling is vrijwillig. 'Het filter heeft tekortkomingen in die zin dat het noch volledig effectief noch trefzeker is. De filtermethode kan worden omzeild en er zijn ook dienstverleners te vinden die het filter niet gebruiken. Dat is zowel het geval wanneer de regeling is gebaseerd op afspraken als wanneer zij via wetgeving is opgelegd. Verder kan het een probleem zijn dat filteren ook materiaal blokkeert waarvan het niet de bedoelding is om het te blokkeren ('valse positieven'). Dat probleem is moeilijk te voorkomen, omdat de filtering is gericht tegen de computer die het materiaal verzendt en niet direct tegen het onwettige materiaal. Indien de computer ook legaal materiaal bevat, wordt ook dat geblokkeerd. Ondanks deze zwakke punten kan worden

[73] CIRCAMP is een COSPOL-project (Comprehensive Operational Strategic Planning for the Police). COSPOL is een strategische politiesamenwerking om de slagkracht van het Europese Police Chiefs Task Force (PCTF) te vergroten.

[74] In het *CEPOL Work Programme 2008*, zoals aanvaard door het CEPOL bestuur op 27 September 2007 (www.cepol.europa.eu), staat alleen de betrokkenheid van Interpol vermeld. CEPOL is het European Police College.

gesteld dat filtering een geschikt middel is, omdat het ondanks alles een bepaald deel van het onwettige verkeer kan stoppen. Hoe groot het aandeel is dat wordt gestopt is echter moeilijk met zekerheid te bepalen, in elk geval niet zonder grote inspanningen om het internetgebruik van internetters in kaart te brengen.' (Datakrimutvalget, 2007:121). Tot zover de opvatting van de voltallige commissie.

De meerderheid van de commissie (4 van de 7 leden) neemt vervolgens het standpunt in dat er geen grond is om het filteren wettelijk te regelen. Deze meerderheid vindt de vrijheid van meningsuiting pleiten tegen het censureren (sic) van buitenlandse websites voor Noorse gebruikers. 'Artikel 10 van het EVRM beschermt in beginsel alle uitingsvormen, ongeacht vorm en inhoud. Het feit dat de huidige filtermethoden, inhoudscontrole via zoektermen en blokkeren van bepaalde *hosts*, tegelijk een grote kans inhouden op zogenoemde "valse positieven", hetgeen inhoudt dat ook legitiem verkeer wordt gestopt door het filter, betekent dat de overweging met betrekking tot de vrijheid van meningsuiting hier zwaar moet wegen. Het risico van valse positieven is vooral een probleem bij het blokkeren van bepaalde *hosts* omdat het gebruikelijk is dat materiaal van verschillende personen is samengevoegd op dezelfde server van een dienstverlener. De meerderheid tilt er zwaar aan dat niet te voorzien is in welke mate filtering ingrijpt op de vrijheid van meningsuiting.

Verder zou een wettelijke eis tot filteren zich richten op een tussenpersoon, de aanbieder van de internetverbinding, en niet op de degene die achter de ongewenste inhoud zit. 'Volgens de opvatting van de meerderheid moet strafvervolging zich als regel richten op degene die iets strafbaars doet en niet op de aanbieder van diensten die slechts de communicatie verzorgt. (…) De meerderheid meent dat het effect van zo'n regeling beperkt is, in zo'n mate dat dit tegen een dergelijke regeling pleit. Er zullen zoveel mogelijkheden zijn om het filter te ontwijken dat het nuttig effect beperkt zal zijn. De meerderheid meent verder dat het filteren in de praktijk zo weinig precies is, dat dit ook pleit tegen zo'n regeling.' (…) (ibidem:121).

Kinderpornografie is volgens de meerderheid een uitzonderlijke vorm van illegaal materiaal. Dat wordt nu op basis van een vrijwillige regeling gefilterd. 'De regeling houdt in dat de ISP een filter implementeert dat de toegang bemoeilijkt tot webpagina's die volgens Kripos kinderporno bevatten. Het doel is om op die manier te voorkomen dat Noorse burgers toevallig op zo'n pagina belanden en het hen moeilijker te maken om dergelijke pagina's te vinden.

Wil de regeling kunnen functioneren, dan is voorwaarde dat er weinig tijd verstrijkt tussen het ontdekken van het materiaal en het blokkeren ervan. De meerderheid meent dat ISP's een rechterlijk oordeel wensen over het filteren indien een en ander wettelijk wordt geregeld. Aldus denkt de meerderheid dat het wettelijk regelen van het filteren de reeds bestaande werkwijze zal verzwakken.' (ibidem:121-2).

Verder voert de meerderheid nog aan dat een wettelijke regeling de kosten van het filteren zal doen toenemen. Alle ISP's moeten dan immers administratieve en technische systemen invoeren om aan de wettelijke eisen tegemoet te komen, waarbij het niet logisch is om aan de ISP's te vragen deze kosten te dragen. Zij zijn immers tussenpersoon en niet de eigenlijke overtreder.

Het commissielid Willassen is ook tegen een wettelijke regeling, maar vindt de opvatting van de minderheid dermate vergaand dat hij daarbij nog apart enkele kanttekeningen wil plaatsen. Het voorstel van de minderheid komt volgens hem neer op internetcensuur onder overheidsregie. Het lid Willassen begrijpt de wens om strafbaar materiaal van het net te weren, maar is van mening dat zo'n filtering nauwelijks een wezenlijk verschil zal maken voor de meeste soorten strafbare inhoud.

Zo is bekend dat kinderpornografisch materiaal op grote schaal via internet wordt uitgewisseld. Dat is strafbaar in de meeste landen en dus gebeurt dat in het verborgene. 'De uitdaging is daarom primair om uit te vinden wie het materiaal verspreidt, niet om te verhinderen dat de informatie Noorse burgers bereikt. Lukt het om te ontdekken vanwaar dergelijk materi-

aal wordt verspreid, dan zal het in de meeste gevallen geen probleem geven om de overheid van het betreffende land te laten ingrijpen.' (ibidem: 122).

Filteren is, aldus dit commissielid, niet effectief omdat zo'n filter gemakkelijk te omzeilen is, bijvoorbeeld door gebruik van buitenlandse proxy-servers, en de aanbieders sneller van IP-adres kunnen wisselen dan het censuurorgaan kan reageren, temeer daar voor een blokkade, aldus nog steeds het commissielid, steeds een rechterlijke uitspraak is vereist. Het omzeilen van een filter lijkt misschien iets wat de meerderheid van de internetters niet kunnen, maar gevorderde internetters uit Noorwegen of buitenland zullen faciliteiten voor het ontwijken van filters als (commerciële) dienst gaan aanbieden.

In essentie is volgens het lid Willassen de vraag wat we willen met internet. Het is een wereldwijd systeem voor het bevorderen van contacten en uitwisseling tussen landen. Het invoeren van overheidscensuur op wat burgers in een bepaald land kunnen doen met internet, past niet in zo'n model.

De minderheid van de commissie meent dat in het strafrecht een artikel moet worden opgenomen om het filteren van een wettelijke basis te voorzien. Om te beginnen wijst de minderheid er op dat niet alle ISP's meedoen met de vrijwillige filterregeling tegen kinderpornografie. De justitiecommissie had in 2005 bij het wetsvoorstel aangegeven dat volgens haar een verplichting zou moeten worden opgenomen als eind 2006 niet alle ISP's zouden meedoen (Innst. O. nr. 66, 2004-2005), dus moet dat nu gebeuren.

Behalve kinderporno kan, aldus de minderheid, ook het filteren van sites met ander voor Noren onwettig materiaal aan de orde zijn, zoals sites met kansspelen. Daarom moet het nieuwe wetsartikel algemeen worden geformuleerd. Er kan ook reden zijn om Noren te beschermen tegen frauduleuze sites of sites waar schadelijke software wordt verspreid. Filtering kan ook een middel zijn tegen sites waar eigendoms- of auteursrechten worden geschonden.

De minderheid is het eens met de meerderheid dat een filter niet honderd procent effectief is. Maar dat geldt voor elke aanpak op het vlak van datacriminaliteit. Ook al is het effect niet volledig, het kan toch beduidend zijn. 'Als men het grootse deel van het onwettige verkeer kan stoppen, is al veel bereikt.' (ibidem:123).

'De minderheid is het niet met de meerderheid eens dat de vrijheid van meningsuiting het filteren van sites met voor Noorse burgers strafbare inhoud in de weg staat. De minderheid meent ook dat een filter geen nieuwe beperkingen oplegt aan de vrijheid van meningsuiting boven de grenzen die deze vrijheid al kent.' (ibidem:123) Volgens de minderheid moeten op het net dezelfde regels gelden als in de echte wereld. Dus moeten strafbare uitingen ook op internet kunnen worden aangepakt.

De minderheid ziet het filteren als een verlengde op de Noorse regels voor het afsluiten van binnenlandse sites. 'Filters kunnen worden gebruikt om hetzelfde effect te bereiken bij buitenlandse sites. De minderheid denkt dat een regeling voor filtering niet op grote schaal zal worden gebruikt. Naar mening van de minderheid zal het wetsartikel alleen worden gebruikt na een zorgvuldige afweging tussen wat met het filteren kan worden bereikt en de nadelen (economische en andere kosten) van het invoeren van een bepaalde filtering. Dat geldt niet in de laatste plaats omdat het risico is dat de filteraanpak meer treft dan de bedoeling is (zogenoemde valse positieven, zie de opmerkingen van de meerderheid).' (ibidem:123).

De nieuwe wet moet, aldus de minderheid, zoveel mogelijk aansluiten bij de reeds gehanteerde *notice and take down* (NTD-) procedure voor binnenlandse websites. Om de filterprocedure zo snel mogelijk te laten verlopen, moet het mogelijk zijn om vooruitlopend op de rechterlijke uitspraak dwangmaatregelen te nemen, zoals ook bij de Noorse NTD-procedure het geval is.

Tot zover onze weergave van het advies van de Commissie Datacriminaliteit ten aanzien van het wettelijk regelen van internetfilters. De discussie gaat niet alleen over kinderpornofilters maar meer in het algemeen over het filteren van (buitenlandse) sites met een voor de

Noorse wet strafbare inhoud. In figuur 4.3 staan de door de commissie genoemde voors en tegens samengevat. Hier ontbreekt het elders door ons wel waargenomen argument dat kinderporno dermate verwerpelijk is dat men geen maatregel daartegen achterwege kan laten en dus wel tot filteren moet overgaan; vermoedelijk omdat de Noorse discussie over wel of geen wettelijke grondslag niet uitsluitend gaat over kinderporno maar over alle in Noorwegen strafbare inhoud.

Figuur 4.3: argumenten van de Noorse Commissie Datacriminaliteit tegen en voor wettelijk regelen van internetfilters (Datakrimutvalget, 2007:120-4)

Tegen	*Voor*
Vrijheid van meningsuiting. Filteren is censureren en derhalve in strijd met de vrijheid van meningsuiting (art. 10 EVRM).	Vrijheid van meningsuiting. Het tegengaan van strafbare uitingen is geen schending van de vrijheid van meningsuiting.
Precisie. Filteren treft ook altijd informatie waarvoor het niet is bedoeld (vals-positieven). In welke mate is onbekend. Het probleem met de vals-positieven maken het eerste bezwaar ernstig.	Proportionaliteit. Filter-regelingen zullen alleen na zorgvuldige afweging worden ingezet.
Effectiviteit. Filters kunnen eenvoudig worden omzeild.	Effectiviteit. Het effect is niet volledig maar kan wel beduidend zijn.
Snelheid. Wettelijke procedures verlagen de snelheid van werken.	Snelheid. Vooruitlopend op een gerechtelijke uitspraak kunnen dwangmaatregelen worden opgelegd.
Doelwit. Filteren richt zich op de ISP's, niet op de eigenlijke daders.	Toepassingsgebied. Een filterregeling kan behalve tegen kinderporno ook worden ingezet tegen sites met ander onwettige activiteiten (bv. kansspelen, fraude, internetpiraterij, malware).
Kosten. Wettelijke procedures doen de kosten toenemen. Die kunnen niet op de ISP worden afgewenteld.	Consequentheid. Strafbaarstelling was aangekondigd bij het wetsvoorstel voor het geval niet alles ISP's het kinderpornofilter zouden gaan gebruiken.
Alternatieven. In veel gevallen zal de overheid van het land waar de strafbare informatie vandaan komt willen ingrijpen.	
Aard van internet. Filteren is in strijd met de open aard van het internet.	

Zelfregulering

Het kinderpornofilter in Noorwegen is een vorm van zelfregulering middels publiek-private samenwerking (PPS). De landelijke overheid speelt daarbij een uitgesproken rol. Aanleiding tot het filter was een oproep van de Noorse minister van Justitie aan politie en bedrijfsleven om maatregelen te nemen tegen kinderporno op internet. De justitiecommissie heeft bij het wijzigen van de zedelijkheidswetgeving de regering aangeraden het filter verplicht te stellen als niet alle providers voor het einde van 2006 zouden meedoen. Vooralsnog is wetgeving achterwege gebleven. De realisatie van het filter is nog steeds een zaak van de Noorse Nationale Recherche in samenwerking met ISP's.

De landelijke overheid blijft oproepen tot zelfregulering. In mei 2006 dringt de Noorse minister van Economische Zaken, Odd Eriksen, er bij Telenor op aan dat het bedrijf een techniek ontwikkelt om MMS-berichten te controleren op kinderpornografische inhoud. De minister zegt te overwegen om zodra het technisch mogelijk is MMS-berichten te scannen op kinderporno, dat verplicht te stellen. Telenor wijst erop dat dit zoiets is als alle post van mensen open maken en dat dit dus lastig ligt, maar stelt zich met zoveel woorden open voor discussie

over het onderwerp. Deze discussie zou dan overigens vooral moeten worden gevoerd met de minister van Justitie, aldus Telenor.

In haar onderzoek naar maatregelen tegen kinderporno op internet kijkt het Deense IT- og Telestyrelsen ook naar zelfregulering (IT- og Telestyrelsen, 2006). Begin 2006 hebben in 14 Europese landen de ISP's een gedragscode opgesteld omtrent hoe zij omgaan met kinderporno op het internet: Engeland, Italië, Denemarken, Noorwegen, Zweden, Finland, Ierland, Duitsland, België, Nederland, Frankrijk, Spanje, Oostenrijk en Hongarije. De gedragscodes gaan niet allemaal even ver. In Engeland bevat de code bijvoorbeeld sanctiemogelijkheden tegen ISP's die de code niet naleven, in Denemarken niet. De landen die werken met een filter (Engeland, Noorwegen, Denemarken en Zweden) doen dat op basis van zelfregulering, steeds in de vorm van een PPS tussen in elk geval politie en ISP's, met soms ook nadrukkelijke betrokkenheid van een ideële organisatie op het vlak van jeugd en (internet)veiligheid.

Doelen van het filter

Bij het kinderpornofilter worden in Noorwegen verschillende doelen genoemd.[75] Het einddoel is het verminderen van kindermisbruik. Daaraan gaan verschillende andere doelen vooraf:

- preventie: drempel opwerpen tegen nieuwsgierigen (aanwas van nieuwe kinderpornogebruikers beperken), hen afschrikken door op de strafbaarheid te wijzen; beperken van de vraag naar kinderporno;
- tegenhouden: aanbieders hinderen om met hun klanten in contact te komen en andersom, en daarmee het bedrijf minder rendabel te maken; criminaliteit voorkomen; productie van kinderporno verminderen;
- bescherming: kindermisbruik verminderen.

Tevens wordt als preventiedoel genoemd het beschermen van argeloze internetters. Het filter moet tegengaan dat die per ongeluk met kinderporno worden geconfronteerd.

Aantal keer dat het filter in actie komt

Door Kripos, Telenor en andere betrokkenen wordt het succes van het filter, en de ernst van het kinderpornoprobleem, vaak uitgedrukt in het aantal keren dat de stoppagina door een computer is opgeroepen, ofwel het aantal hits. We geven nu eerst zonder al te veel aanvullend commentaar een overzicht van mediaberichten waarin aantallen worden genoemd; daarna gaan we in de subparagraaf 'betekenis van de cijfers' dieper in op de interpretatie van de in de media genoemde aantallen.

Op 'een willekeurige dag in oktober 2004', enkele dagen voordat het filter door Telenor in gebruik wordt genomen, hebben Telenor en Kripos bijgehouden 'hoe vaak naar kinderporno wordt gezocht'. Dat was 7.000 keer. In de media staat hierover een bericht onder de kop 'Velen zoeken kinderporno'. Een nuancering is er ook: 'Het is niet duidelijk hoeveel Noren er achter deze 7.000 zoekpogingen zitten. Elke persoon kan vele zoekopdrachten hebben gegeven.' Het aantal beangstigt de kinderombudsman Reidar Hjermann en Redd Barna (het Noorse Save the Children). 'Het is erg lastig om deze getallen te accepteren. Het gaat om onze buren, collega's en vrienden die zich interesseren voor misbruik van kinderen,' zegt Elizabeth Skogrand van Redd Barna tegen de krant. (www.dagbladet.no).

Op 14 april 2005 meldt de pers dat 'elke dag 5.000 internetbezoeken aan kinderpornosites worden gestopt door het filter van Telenor en Kripos'. Het filter heeft sinds de start dagelijks 4.000 keer het opvragen van een site met kinderporno gestopt. In april registreerde het filter liefst 5.000 treffers per dag. Er wordt niet bijgehouden wie heeft geprobeerd een site te

[75] We baseren ons hier op uitspraken van Telenor- en Kripos-woordvoerders in de media, op de Noorse Justitiecommissie (Innst.O.nr.66, 2004-2005) en de Noorse Commissie Datacriminaliteit (Datakrimutvalget, 2007).

bezoeken. Daarom is niet bekend hoeveel kinderpornosurfers er zitten achter die 5.000 dagelijkse treffers.

Op 7 augustus 2005 verschijnt een bericht met de kop 'Kinderpornofilter stopt dagelijks 6.700 maal' met daaronder de subkop 'De hang van Noren om in te loggen op sites met kinderpornografie is shockerend groot'. Het bericht presenteert nieuwe cijfers van Telenor: in de periode van 9 november 2004 tot 4 augustus 2005 heeft het filter 1,1 miljoen keer een klant verhinderd om een webpagina te bezoeken met kinderpornografisch materiaal (zo'n 4.000 maal per dag – WS). De auteur extrapoleert het getal naar heel Noorwegen en concludeert dan dat internetklanten in Noorwegen in die periode 1,7 miljoen keer probeerden een site met kinderporno te bezoeken, ofwel 6.700 maal per dag. 'Dat is een verschrikkelijk hoog aantal en dat zegt ons hoe groot het probleem is,' zegt Telenors informatiechef Atle Lessum. Verder meldt het bericht: 'Bovendien heeft Telenors kinderpornofilter 4,36 miljoen andere pogingen van zijn klanten gestopt om onwettige kinderpornobeelden of films te downloaden. Telenorklanten proberen dagelijks 16.207 maal onwettig kinderpornografisch materiaal te downloaden.'[76] (…) 'Elizabeth Skogrand leidt het Redd Barna project 'Misbruik van kinderen op internet'. Volgens haar zijn de cijfers om mistroostig van te worden. De resultaten tonen hoe weinig we nog hebben bereikt om dit probleem te bestrijden. Tegelijk vertellen de cijfers ons hoe belangrijk het filter is in de strijd tegen het misbruik, zegt Skogrand. Het beangstigt haar hoeveel mensen op internet naar kinderporno zoeken.' (www.vg.no).

Op 1 november 2005 meldt een andere journalist van digi.no in een bericht: 'Het kinderpornofilter is tot dusverre een groot succes. Maar liefst 1,7 miljoen keer heeft het filter Noren gestopt op jacht naar kinderporno.'

Op 12 december 2005 komt digi.no op het onderwerp terug: in november schreef digi.no dat het filter 1,7 miljoen keer een Noor had gestopt op jacht naar kinderporno, alleen al met Telenors filter. Nog geen maand later is het aantal volgens Aftenposten opgelopen tot 2,3 miljoen treffers. Deze meting betreft het verkeer via Telenor en samenwerkende providers. 'Dat het het filter lukt om tot maar liefst 2,3 miljoen keer mensen te stoppen zich te verlustigen aan kindermisbruik, is voor ons een groot succes,' zegt informatiechef Atle Lessum van Telenor tegen digi.no. Verder meldt het bericht dat Kripos nu tussen 12.000 en 15.000 treffers per dag stopt. Ter vergelijk: dat was vorig jaar tussen de 6.000 en 7.000 treffers per dag. Via mobieltjes zijn er nu bijna 5.000 treffers geregistreerd.

Het rekenwerk en de berichtgeving zijn nogal slordig. Volgens het laatste bericht zouden er in nog geen maand 0,6 miljoen hits zijn, dus ruim 20.000 per dag. De 1,7 miljoen is echter niet, zoals digi.no in dit bericht beweert, het aantal keren dat het filter in actie kwam, maar een getal dat door extrapolatie is verkregen en dat betrekking zou hebben op alle internetklanten in Noorwegen. Het filter zou 1,1 miljoen keer in actie zijn gekomen in de periode van 9 november 2004 tot 4 augustus 2005 (zo'n 4.000 maal per dag). Digi.no schrijft dat volgens het dagblad Aftenposten het aantal keer dat het filter in actie kwam, op 1 december 2005 is opgelopen tot 2,3 miljoen. Dan zou het filter in de periode van 9 november 2004 tot ongeveer 1 december 2005 2,3 miljoen keer in actie zijn gekomen, ofwel ongeveer 5.900 maal per dag. In de periode van 4 augustus 2005 tot ongeveer 1 december 2005 zou het dan gaan om 1,2 miljoen hits (2,3-1,1), ofwel ongeveer 10.000 per dag. In grote trekken komen deze cijfers (van 4.000 per dag naar 10.000 per dag) wel overeen met wat aan het eind van het laatste mediabericht staat: een stijging van 6.000 à 7.000 hits per dag naar 12.000 à 15.000 per dag.

De aantallen, zo bericht digi.no op 13 december 2005, maken veel reacties los onder lezers van digi.no. Velen hebben er moeite mee te geloven dat zoveel Noren zoeken naar kinderporno. Digi.no besteedt nu, na een jaar na ingebruikname van het filter, aandacht aan de betekenis van de cijfers (zie volgende paragraaf) en kopt: 'De cijfers van Telenor overdrijven

[76] Telenor had destijds zo'n 750.000 internetklanten (www.digi.no; bericht van 1-11-2005).

surfen naar kinderporno.' Vanaf dat moment publiceert digi.no geen berichten meer over aantallen hits, maar schrijft juist meer over de verschillende manieren waarop kinderpornografie wordt bestreden, ook in het buitenland. We vinden in dat verband berichten over hoe creditcardnummers door de politie in Engeland en Duitsland worden gebruikt om kinderpornokopers te achterhalen en over de 'goede resultaten' die de Internet Watch Foundation in Engeland behaalt met een NTD-procedure.

Op 24 oktober 2007 schrijft ABC-nyheter (ABC-nieuws) nog dat het Noorse filter 7 miljoen pogingen tot het zoeken van kinderporno heeft gestopt. Voor de lezer die het narekent is dat een opmerkelijk bericht. Het aantal hits per dag daalt kennelijk weer. Immers, in de periode van 9 november 2004 tot 1 december 2005 waren er 2,3 miljoen hits, dus in de periode van 1 december 2005 tot (ongeveer) 20 oktober 2007 waren er (7 min 2,3) 4,7 miljoen hits. Op basis van de mediaberichten ontstaat dan de reeks:

- van 09-11-2004 tot 04-08-2005 in totaal 1,1 miljoen hits ofwel 4.000 per dag;
- van 04-08-2005 tot 01-12-2005 in totaal 1,2 miljoen hits ofwel 10.000 per dag;
- van 01-12-2005 tot 20-10-2007 in totaal 4,7 miljoen hits ofwel 6.800 per dag.

Dat het aantal hits per dag volgens de in de media bekendgemaakte berichten daalt, wordt door ABC-nyheter niet opgemerkt. Ook elders kwamen we een dergelijke constatering niet tegen. Het filter heeft, aldus informatiechef Atle Lessum van Telenor in het laatstgenoemde persbericht, bij mobiel internetverkeer 30.000 tot 35.000 keer een bezoek aan site met kinderporno verhinderd. Dat komt overeen met ongeveer 40 hits per dag.[77] Volgens de in het bericht aangehaalde Internet Watch Foundation worden, ondanks de toegenomen waakzaamheid, de beelden van misbruik van kinderen steeds grover. Een onderbouwing bij die stelling wordt echter niet geleverd.

Betekenis van de cijfers

In de berichtgeving over de cijfers wordt bij herhaling de suggestie gewekt dat er een verband bestaat tussen het aantal hits en hoe intensief er door Noren naar kinderporno wordt gezocht. Zegslieden van politie, providers en kinderbeschermingsorganisaties laten zich in de media ook in die zin uit. De media en zegspersonen geven geen kritische beschouwingen over de betekenis van de cijfers. Totdat vanuit het lezerspubliek kritische kanttekeningen worden gemaakt bij het hiervoor genoemde aantal van 2,3 miljoen hits. Op 13 december 2005 wijdt digi.no een artikel aan de kritiek.

Digi.no schrijft dat veel lezers er grote moeite mee hebben om te geloven dat zoveel mensen naar kinderporno zoeken. Veel lezers melden dat zij zelf ook op het filter zijn gestuit zonder dat zij op zoek waren naar kinderporno. 'Ik heb ook het idee dat de cijfers krachtig worden opgeblazen door mensen die naar "legale" porno zoeken', schrijft 'Pol Pot' in digi.no's discussieforum. In het artikel bevestigt perswoordvoerder Atle Lessum van Telenor die indruk en hij zegt dat Kripos daar ook oog voor heeft. 'Veel van de treffers zijn puur toevalligheid, en het filter zorgt er dan voor dat mensen gevrijwaard blijven van beelden die ze liever ook niet willen zien.', zegt Lessum. Hij deelt de opvatting dat niet iedereen die op het filter stuit ook geïnteresseerd is in kinderporno en hij vindt het goed dat digi.no de kwestie van het interpreteren van de cijfers oppakt, zodat we niet gaan denken dat op elke straathoek een pedofiel woont. 'Maar we moeten het probleem ook weer niet bagatelliseren,' aldus Lessum.

Het is dus, zo vervolgt digi.no, op basis van de filtergegevens niet mogelijk om een cijfer te noemen voor het aantal mensen dat actief kinderporno zoekt. Veel lezers van digi.no

[77] Het gaat om de periode van 01-06-2005 (implementatie van het filter op het mobiele netwerk) tot ongeveer 20-10-2007. Dat is ongeveer 870 dagen; 35.000 hits gedeeld door 870 dagen is zo'n 40 hits per dag.

melden dat ze op het filter stuiten op sites met gewone porno. Ook wordt gemeld dat mensen op het filter stuiten op Warez-sites (sites met illegale kopieën en hackersmateriaal). Wellicht heeft dat te maken met het feit dat het filter zich uitbreidt, van 300-400 sites in het begin tot 1.600 nu. Kripos stelt de lijst samen. Kripos krijgt van Telenor, aldus Lessum, overzichten van welke geblokkeerde sites werden benaderd en vanaf welke sites deze werden benaderd. Dan kunnen die sites ook worden onderzocht en toegevoegd, zegt hij. Als Warez-sites links hebben naar sites met kinderporno, kunnen die sites ook in het filter terecht komen. Lesum bevestigt dat domeinen in het filter worden opgenomen, zoals xxx.com, en niet alleen de delen van een domein die kinderporno bevatten. Dat kan verklaren dat mensen het filter te zien krijgen ook al waren ze helemaal niet op zoek naar iets wat met kinderen te maken heeft.

Lessum vervolgt over het effect van het filter: 'Er komt minder geld in omloop en daarom zijn er minder kinderen die lijden. Er is reden om dat aan te nemen.' Maar hij geeft niet aan welke reden dat is. Over het filter zegt Lessum verder: 'Telenor was de eerste in de wereld met deze oplossing, samen met British Telecom. Nu kan deze oplossing breder worden toegepast.' Tot zover de weergave van het kritische artikel van digi.no.

De cruciale kanttekening die bij de cijfers wordt gemaakt, is dat het aantal hits voor een deel een gevolg is van *overblocking*. Met het filter worden domeinen geblokkeerd en iedereen die op weg is naar legale inhoud binnen dat domein, veroorzaakt een hit. Het is onbekend welk aandeel van de hits door dergelijke *overblocking* wordt veroorzaakt. Aangezien, aldus Lessum van Telenor, een site reeds in aanmerking komt om te worden geblokkeerd als die site een link bevat naar een site met kinderporno, lijkt de *overblocking* in elk geval niet verwaarloosbaar. Een internetter die op zoek is naar een softwareprogramma en die ergens een link naar een warez-site aanklikt, krijgt de Kripos-stoppagina te zien wanneer die warez-site is geblokkeerd vanwege het feit dat op een van de pagina's binnen die site een link is opgenomen naar een site met kinderporno.

Dat het aantal hits door de tijd heen toeneemt, lijkt logischerwijs het gevolg van het langer worden van de lijst met te filteren sites. We vonden de volgende berichten over de omvang van de lijst, mediaberichten gebaseerd op informatie van Telenor of Kripos:

28-10-2004:	300	-	400
14-04-2005:	500	-	1.000
07-08-2005:			1.000
12-12-2005:			1.600

Waarom het aantal hits na 1 december 2005 weer afneemt (van gemiddeld 10.000 naar 6.800 per dag – zie hiervoor), weten we niet. Het komt niet doordat vanaf dat moment de blokkeerlijst weer krimpt: toen het KLPD in 2007 de lijst van de Noren kreeg, bevatte hij zo'n 2.500 sites, aldus respondenten van het KLPD.

Effectiviteit

Effectiviteit vatten we op als de mate waarin (vooraf gestelde) doelen worden bereikt. Over wat er met het filter moet worden bereikt zijn uitspraken gedaan (zie 'doelen van het filter' hiervoor). De mate waarin het filter succesvol is, wordt door de betrokkenen (Kripos, Telenor, Redd Barna) echter veelal afgemeten aan het aantal keren dat het filter is getoond. Figuur 4.4 bevat daarvan een voorbeeld. Er is ons echter geen onderzoek bekend geworden naar de mate waarin met het filter de beoogde doelen worden bereikt.

Figuur 4.4: deel uit persbericht, over het effect van het Noorse kinderpornofilter

> Sinds december 2004 is het voor Telenor-klanten mogelijk om via de mobiele telefoon internetpagina's te raadplegen en foto's uit te wisselen. Daarom heeft Telenor nu ook op haar mobiele netwerk het kinderpornofilter geplaatst. 'Onze statistieken laten absoluut zien dat zo'n filter effect heeft. Sinds we het filter op internet hebben geplaatst, oktober vorig jaar, heeft het filter elke dag 5000 treffers gehad. Dat laat zien dat het zinvol is,' zegt Berit Kjøll van Telenor.
>
> www.pressemeldinger.no, 7 juni 2005 (geraadpleegd op 20-12-2007)

4.3 Zweden

Inleiding
In mei 2005 nam Zweden het Noorse kinderpornofilter in gebruik. Het betreft in eerste aanleg een samenwerking tussen de Zweedse tak van Telenor (Telenor AB) en de Zweedse Nationale Recherche, specifiek de Groep tegen Seksueel Misbruik van Kinderen en Kinderpornografie. In deze paragraaf beschrijven we de situatie in Zweden, met speciaal aandacht voor de aspecten die in Zweden anders zijn dan in Noorwegen.

Zweedse kinderpornowetgeving
Sinds 1999 is in Zweden alle bezit van kinderpornografie strafbaar, daaronder begrepen het verspreiden en verhandelen ervan. Artikel 10a van paragraaf 16 van de Zweedse strafwet regelt de strafbaarstelling (figuur 4.5).

Figuur 4.5: artikel 10a van paragraaf 16 van de Zweedse strafwet.

> Hij die
> 1. kinderen afbeeldt in een pornografisch beeld;
> 2. een dergelijk beeld van een kind verspreidt, verzendt, toegankelijk maakt, toont, of op andere wijze beschikbaar maakt voor een ander;
> 3. een dergelijk beeld aanschaft of te koop aanbiedt;
> 4. bemiddelt bij het contact tussen koper en verkoper van een dergelijk beeld van een kind of andere activiteiten verricht met als doel om de handel in dergelijke beelden te bevorderen, of
> 5. een dergelijk beeld van een kind in bezit heeft,
>
> wordt veroordeeld voor kinderpornografie gevangenisstraf van ten hoogste twee jaar of, indien het een geringe overtreding betreft, met een boete of een gevangenisstraf van ten hoogste zes maanden.
> Onder een kind wordt verstaan een persoon wiens puberteitsontwikkeling nog niet is voltooid of, voor zover dat volgt uit het beeld of de context daarvan, de leeftijd van 18 jaar nog niet heeft bereikt. (…)
> Is het misdrijf aan te merken als ernstig, dan zal worden veroordeeld voor ernstige kinderpornografie tot een gevangenisstraf van ten minste zes maanden en ten hoogste zes jaar. (…)

Een punt van kritiek op de wetstekst is dat als de puberteitsontwikkeling van een kind is voltooid en uit de foto of de context daarvan niet volgt dat het gaat om een persoon onder de 18 jaar, er niet gesproken wordt van kinderporno. Niet iedere pornografische afbeelding van een

kind onder de 18 jaar is dus strafbaar volgens de Zweedse wet (Barnpornografiutredning, 2007). Als bij een kind van 17 de puberteitsontwikkeling is voltooid en uit de afbeelding of de context daarvan volgt niet dat het kind jonger is dan 18 jaar, is volgens de huidige tekst geen sprake van een strafbaar feit (in Nederland bijvoorbeeld wel). Aan de andere kant vallen kinderen die ouder zijn dan 18 jaar, maar wiens puberteitsontwikkeling nog niet is voltooid, wel onder de Zweedse kinderpornowetgeving.

Begin 2005 maakt minister van Justitie Thomas Bodström bekend dat hij de kinderpornowetgeving wil aanscherpen. Het kijken naar kinderporno zou strafbaar gesteld moeten worden en te overwegen is of kinderen die voorkomen in pornografische afbeeldingen recht zouden moeten hebben op een schadevergoeding. Degenen die kinderpornografisch materiaal downloaden zouden aan zo'n vergoeding moeten bijdragen. De minister kondigt een onderzoek aan naar het functioneren van de kinderpornografiewetgeving (www.dn.se, 27 januari 2005).

Op 3 juni 2005 vraagt Tweede Kamerlid Viviann Gerdin, nadat ze de ernst van het kinderpornoprobleem op internet heeft benadrukt en heeft verwezen naar de filterinitiatieven in Engeland, Noorwegen en Zweden, schriftelijk aan de minister van Justitie welke wettelijke maatregelen hij denkt te nemen in de strijd tegen kinderporno op internet. Op 15 juni geeft de minister antwoord. Het bezit van kinderporno is strafbaar en verder hebben degene die zogenoemde elektronische bulletin boards aanbieden een strafrechtelijke plicht om daar de verspreiding van kinderpornografie tegen te gaan. De regering heeft een evaluatie van de kinderpornowetgeving gepland. Een belangrijke vraag in dat verband is of, gezien de technische ontwikkelingen, de strafbaarstelling aanpassing behoeft. De opdracht tot een dergelijk onderzoek moet deze zomer (2005) gereed zijn. Hoewel, aldus de minister, overheidswetgeving een belangrijk instrument is, heeft de hele samenleving een verantwoordelijkheid in de strijd tegen kinderporno op internet. Hij verwijst in dat verband naar de samenwerking tussen onder meer politie, Ecpat[78] en internetproviders, en de ingebruikname van het kinderpornofilter.[79] Hij sluit af met de conclusie dat er dus al verschillende maatregelen in gang zijn gezet (evaluatie van de wetgeving en implementatie van het filter) voor een effectievere strijd tegen kinderporno op internet (www.riksdagen.se).

Op 25 augustus 2005 stelt de regering de commissie in die de kinderpornowetgeving zal evalueren; de commissie rapporteert op 29 augustus 2007 (Barnpornografiutredning, 2007). De commissie adviseert de minister om de wet op twee punten aan te scherpen. Ten eerste dient, aldus de commissie, het zich tegen betaling, volgens een vooropgezet plan, bij herhaling toegang verschaffen tot kinderpornografische afbeeldingen, strafbaar te worden gesteld, met ingang van 1 januari 2009. Ten tweede dient de leeftijd van 18 jaar een harde grens te worden. De definitie van kind wordt volgens het voorstel per 1 januari 2011: 'een persoon wiens puberteitsontwikkeling nog niet is voltooid of die jonger is dan 18 jaar.' Daarmee valt dus ieder kind jonger dan 18 jaar onder de wet, los van de vraag of de puberteitsontwikkeling is voltooid. Bovendien vallen dan onder de wet kinderen van 18 jaar en ouder wiens puberteitsontwikkeling nog niet is voltooid.

Implementatie en verspreiding

Anders dan in Noorwegen zien we in Zweden bij internetproviders van meet af aan discussie over de wenselijkheid van een filter tegen kinderporno. Toen de Zweedse pers in 2004 berichtte over het toen recentelijk in Engeland ingevoerde filtersysteem Clean Feed, wezen grote Zweedse internetproviders direct op het probleem van internetcensuur. UPC Sverige vindt harde maatregelen tegen kinderporno een goede zaak, maar wie echt kinderporno wil hebben

[78] ECPAT: End Child Prostitution, Child Pornography and Trafficking in Children for Sexual Purposes (www.ecpat.nl)

[79] Hij verwijst naar de bijeenkomst op 27 april 2005, zie subparagraaf *Implementatie en verspreiding*.

vindt het toch wel; Telia Sonera vindt filteren allereerst een politiek vraagstuk en vraagt zich af wat na kinderporno de volgende stap zal zijn, het is volgens Telia Sonera beter het probleem bij de bron aan te pakken; Bredbandsbolaget wil als internetleverancier niet als filter gaan fungeren, bovendien is voor haar de vraag waar de grens van de censuur ligt; Tele2 heeft nog geen standpunt in dit censuurvraagstuk (www.aftonbladet.se, 20 juli 2004).

Op 10 maart 2005 laat de grootste Zweedse telecomprovider, Telia Sonera, optekenen dat zij anders dan providers in Engeland en Noorwegen geen filter zal gaan gebruiken. De chef van de internetdivisie, Ingrid Bardh, voert aan dat filters niet echt deugdelijk zijn, dat ze eenvoudig zijn te passeren en dat het kijken naar kinderpornografie in Zweden niet strafbaar is. De verspreiding van kinderporno moet worden tegengegaan door de bron te bestrijden, aldus Bardh (www.aftonbladet.se, 10 maart 2005). De dag daarop koppen Dagens Nyheter en Aftonbladet 'Telia overstag'. Na forse kritiek op de passieve houding van Telia, onder meer vanuit Ecpat, meldt Bardh dat Telia het filter in gebruik zal nemen als de techniek functioneert en de politie het startsein geeft. Een telefonische rondgang leert dat Spray, Glocalnet en UPC/Chello ook het Britse filter willen gaan gebruiken, dat Comhem voorzichtig positief is en dat Tele2 twijfelt omdat de bestaande werkwijze (na een melding verwijderen van kinderpornografisch materiaal) voldoet. Bredbandsbolaget vindt dat voorafgaand aan het filteren daarvoor eerst een wettelijke basis moet worden gelegd. De minister van Justitie Thomas Bodström laat weten dat als de branche het niet zelf regelt, hij niet zal aarzelen met wetgeving te komen. Nog weer drie dagen later laat Bredbandsbolaget weten met filteren te beginnen zodra de technische problemen zijn opgelost en de politie een opgave doet van de filteren sites (www.aftonbladet.se, 11 maart 2005; www.dn.se, 11 maart 2005; www.dn.se, 14 maart 2005).

In de discussie mengt zich ook de politiek. Op 14 maart 2005 stelt Tweede Kamerlid Conny Fogelström een schriftelijke vraag aan de minister van Infrastructuur Ulrica Messing. Fogelström verwijst naar het filteren in Engeland en Noorwegen en schrijft dat het volgens experts gaandeweg mogelijk zal zijn om kinderporno zo effectief te filteren dat het niet meer loont om het te produceren. Dan merkt ze op dat Telia, de grootste Zweedse provider, heeft meegedeeld om niet te gaan filteren omdat filters niet precies zijn en gemakkelijk te omzeilen, en vraagt aan de minister welke stappen zij beoogt te ondernemen. Op 23 maart beantwoordt de minister de vraag. Ze meldt dat, op initiatief van Ecpat, het Post- en Telebestuur samen met de Nationale Recherche in april 2005 de grootste Zweedse internetproviders zullen uitnodigen voor een discussiebijeenkomst over het filteren van kinderporno. Tijdens die bijeenkomst zullen vertegenwoordigers van de Noorse politie en van Noorse internetproviders hun ervaringen presenteren (www.riksdagen.se).

Dagens Nyheter en *NyTeknik* berichten over die bijeenkomst, die werd gehouden op 27 april 2005. Aanwezig waren onder meer de internetproviders Telia Sonerea, Tele2, Bredbandsbolaget, UPC, Post- en Telebestuur, Mediaraad en Ecpat. Telia benadrukt dat het ondanks het filteren wel zaak blijft om kinderpornosites te sluiten. De filterlijst veroudert snel, want de sites wisselen steeds van adres. Bovendien zijn er altijd mensen die het filter weten te omzeilen. Ook Bredbandsbolaget heeft haar bezwaren nu laten varen en dringt niet langer aan op een wettelijke basis. Annethe Ahlenius van de groep tegen kindermisbruik van de Nationale Recherche, wijst nog op een recent ontwikkeld ander filter, dat kan worden aangeschaft door bedrijven en andere organisaties. Dat werkt op basis van een politielijst met 300.000 kinderpornografische afbeeldingen waarvan de 'vingerafdruk' is bepaald (zgn. hashcode, zie hoofdstuk 2). Het programma slaat alarm als een gebruiker (werknemer) een van die afbeeldingen op het internet bekijkt of downloadt (www.dn.se, 29 april 2005; www.nyteknik.se, 17 mei 2005).

Op dinsdag 17 mei 2005 nemen Telenor en Telia in Zweden het Noorse filter in gebruik. Het filter omvat op dat moment 1.000 sites. Moniqa Löfstedt van Telenor nodigt andere internetaanbieders uit tot samenwerking. Op 19 mei 2005 neemt ook Bredbandsbolaget het

filter in gebruik. Eind 2005 bestaat de samenwerking uit politie, Ecpat en 12 internetproviders (www.dn.se, 25 november 2005). Later wordt ook het aantal van 10 en 11 genoemd (resp. IT- og Telestyrelsen, 2006; www.flashback.se, 24 juli 2007).

Ruim een maand na de invoering van het filter tegen kinderporno lanceert minister van Justitie Thomas Bodström het idee om het filter ook te gaan gebruiken tegen sites die in verband staan met georganiseerde vrouwenhandel. Internetproviders reageren verdeeld. Bredbandsbolaget, eerst zo kritisch tegenover het filter, steunt het idee ronduit. Bahnhof Internet en ComHem, een van Zwedens grootste internetproviders, vragen zich af wat de volgende stap zal zijn, en zijn derhalve terughoudend.

Net als de Noorse politie spant ook de Zweedse politie zich in om het filter verder te verspreiden. De politie pleit voor een aanpak op EU-schaal (www.dn.se, 17 juli 2005, 25 november 2005).

Organisatiefilters

Tijdens de discussiebijeenkomst van 27 april 2005, was er aandacht voor een filter dat is ontwikkeld door het (commerciële) bedrijf NetClean Technologies – een filter op basis van hashcodes, afgeleid van het kinderpornografische afbeeldingenbestand van de Zweedse Nationale Recherche, dat ongeveer 300.000 afbeeldingen omvat. Kort na de ingebruikname van het kinderpornofilter meldt *NyTeknik* dat een gemeentelijke zorginstelling in Zuid-Zweden dit filter als eerste in gebruik heeft genomen. Het wordt omschreven als een soort antivirusprogramma tegen kinderporno. Het programma wordt geïnstalleerd op een computer, waarna het alle stations alsook het dataverkeer controleert op kinderpornografische afbeeldingen. Wie een kinderpornografisch beeld bekijkt of downloadt, wordt meteen betrapt aldus *Nyteknik*t; het systeem zendt een melding naar bijvoorbeeld de afdeling informatiebeveiliging of een leidinggevende. Volgens ondernemer Christian Sjöberg van NetClean is er veel belangstelling binnen gemeenten voor het systeem, vooral bij bibliotheken en scholen.

Het bedrijf heeft twee gratis producten dat het met de inkomsten van dit NetClean Image Filter wil financieren: Netclean Analyse en Keep My Net Clean. Met het laatste programma kan de gebruiker een verdacht plaatje aanklikken, waarna er automatisch een melding gaat naar het Zweedse Ecpat. Sinds de introductie van Keep My Net Clean in maart is het aantal melding bij Ecpat verdubbeld, meldt Sjöberg in *NyTeknik* (www.nyteknik.se, 27 mei 2005, 21 september 2005).

Begin 2007 meldt *Göteborgs-Posten* dat het kinderpornofilter van NetClean Technologies bij rond de honderd particuliere en overheidsorganisaties is geïnstalleerd, waaronder Telia Sonera, de eerste grote klant van het bedrijfje, en de provincie Västra Götaland (www.gp.se, 8 februari 2007, 14 maart 2007).

Op 3 augustus 2007 vraagt kamerlid Fredrik Lundh schriftelijk aan minister-president Fredrik Reinfeldt of hij ervoor wil zorgen dat computers in de departementen worden voorzien van een kinderpornofilter. Op 17 augustus antwoordt minister van Sociale Zaken Görann Hägglund dat inmiddels verschillende technische mogelijkheden voor filteren zijn getest, de juridische kwesties zijn bekeken, en dat nog dit jaar een filter zal worden ingevoerd tegen sites met bijvoorbeeld kinderpornografie, racistische uitingen of geweld (www.riksdagen.se). In september bericht *Dagens Nyheter* dat voor de computers van de departementen een URL-filter is geplaatst (www.dn.se, 2 september 2007, http://sydsvenskan.se, 5 september 2007). Dit is dus niet het NetClean filter, want het betreft een URL-filter en dit blokkeert ook andere dan kinderpornosites.

Op 21 november 2007 besluit het parlementsbestuur dat ook de computers van het parlement worden gefilterd. Het gaat om een kinderpornofilter dat blijkens de beschrijving precies functioneert als het NetClean filter, maar de naam NetClean wordt niet genoemd (www.riksdagen.se).

Zelfregulering

Het Telenor-kinderpornofilter vindt ook in Zweden zijn weg op basis van een publiek-private samenwerking (PPS) tussen politie en internetproviders. Een duidelijke rol in de discussie speelt ook de kinderbelangenorganisatie Ecpat. De Zweedse politiek intervenieert ook op verschillende momenten. De in vergelijking tot Noorwegen wat nadrukkelijker rol van Ecpat en de politiek, is vooral te begrijpen tegen de achtergrond van de wat kritischer opstelling van de Zweedse internetproviders.

Een ander element dat in Zweden voor ons zichtbaar werd, is zelfregulering vanuit de commerciële markt. NetClean heeft een filter ontwikkeld en op de markt gebracht in samenwerking met de politie, die daarvoor een lijst met hashcodes van de bij haar bekende kinderpornoafbeeldingen beschikbaar stelt. Een ander, niet met name genoemd bedrijf heeft een URL-filter tegen sites met kinderpornografie, racistische uitingen en geweld op de markt gebracht.

Effectiviteit

In Zweden gelden dezelfde doelen voor het filteren als in Noorwegen (zie paragraaf 4.2). Ook nu geldt het aantal hits als indicatie van effectiviteit van het filter. Op 17 juli 2005, twee maanden na de ingebruikname van het filter, schrijft *Dagens Nyheter* dat het Zweedse filter 6.000 maal per dag een poging voorkomt om op een site met kinderporno te komen. 'Wat men in gedachte moet houden,' aldus Lars Billström van Telia Soneras, 'is dat dit niet inhoudt dat er 6.000 maal actief geprobeerd wordt om op dergelijke pagina's te komen. Het kan ook betekenen dat men pop-ups aanklikt of onduidelijke links waarvan men niet weet waarheen die leiden.' Het filter omvat nu zo'n 1.000 sites en dat aantal stijgt (www.dn.se, 17 juli 2005).

Op 25 november 2005 stopt het filter tussen de 20.000 en 30.000 pogingen om op een website met kinderporno te komen. *Dagens Nyheter* vraagt Annethe Ahlenius van de Nationale Recherche wat dat aantal zegt over het aantal pedofielen in Zweden. 'Dat kan men zo niet zeggen,' zegt zij, 'want er zijn verschillende categorieën mensen die dit soort pagina's bezoeken. Je kunt niet zeggen dat het allemaal pedofielen zijn, maar ongeacht iemands interesse is het triest dat mensen dergelijke pagina's bezoeken.' (www.dn.se, 25 november 2005). Volgens Helena Karlén van Ecpat wordt het probleem met kinderpornografie groter en groter. Teken daarvan is volgens haar dat het filter elke dag tegen de 30-duizend pogingen registreert om op een pagina met kinderporno te komen. 'Tienduizenden personen die elke dag proberen om bij materiaal te komen dat grof kindermisbruik toont, is op zichzelf een catastrofe.' Het filter bevat nu zo'n 1.100 sites en elke week krijgt Ecpat honderden meldingen over sites met kinderporno (www.sr.se, 25 november 2005).

In de berichten over de aantallen hits en de betekenis daarvan is geen aandacht voor het fenomeen *overblocking*.

In de zomer van 2007 ontstaat commotie omtrent het voornemen van de politie om de populaire site Pirate Bay, een platform voor het uitwisselen van bestanden, op de filterlijst te plaatsen, omdat er volgens de politie na melding kinderpornografisch materiaal op de site is aangetroffen. Uiteindelijk gaat de geplande blokkering niet door. Ook wordt gemeld dat de site van 'The Korean Bonsai Association' (http://koreabonsai.com) met informatie over bonsaibomen om onduidelijke reden is geblokkeerd, hetgeen de vraag oproept hoe deugdelijk de filterlijst precies is (www.piratpartiet.se, 6 juli 2007; http://sakerhet.idg.se, 6 juli 2007; www.flashback.se, 24 juli 2007).

We vonden geen Zweedse studies naar het effect van kinderpornofilters.

4.4 Engeland

Inleiding
De Britse internetprovider British Telecom (BT) nam in juni 2004 het initiatief tot het blokkeren van websites met kinderpornografisch materiaal. Anders dan in Noorwegen en Zweden (en Nederland) houdt in Engeland niet de politie de filterlijst bij. Dat doet de *non-governmental organisation* (NGO) Internet Watch Foundation (IWF). Het commerciële BT verzorgt de technische realisatie van het blokkeren en maakt daarvoor gebruik van het filtersysteem Cleanfeed (www.cleanfeed.co.uk). De Britse regering oordeelde positief over het particuliere initiatief en riep de rest van de branche op hetzelfde te doen. Op dit moment blokkeren alle mobiele telefoonaanbieders die 3G[80] als transmissiestandaard gebruiken en de meeste grote Britse ISP's op vrijwillige basis kinderpornografische websites.[81]

Naast Cleanfeed gebruiken zij andere, soortgelijke, filtersystemen. De brancheorganisatie van ISP's in het Verenigd Koninkrijk, de Internet Services Providers' Association (ISPA UK), wijst er op dat er niet een 'one size fits all' oplossing is om websites te blokkeren (www.theregister.co.uk 07–06–2004). Doordat de ISP's verschillende technische infrastructuren hebben is het niet mogelijk, aldus de ISPA, dat alle ISP's hetzelfde filtersysteem gebruiken.

De ISP's die filteren, bedienen samen negentig procent van de particuliere Britse markt (IWF, 2007). De overheidsbemoeienis met het blokkeren van websites is binnen de *Home Office* belegd bij de *Home Secretary's Taskforce on Child Protection on the Internet*, opgericht in maart 2001 (http://police.homeoffice.gov.uk). De taskforce heeft als doel om het Verenigd Koninkrijk de meest veilige plaats te maken voor kinderen om internet te gebruiken. De taskforce brengt de overheid, de politie, children's agencies en internetgerelateerde bedrijven samen. Het blokkeren van websites met kinderpornografische content is slechts een van de maatregelen waar de taskforce zich mee bezig houdt.

Engelse kinderpornowetgeving
In Engeland en Wales is de belangrijkste wetgeving aangaande kinderpornografisch materiaal de *Protection of Children Act 1978*. Volgens de wet is het verboden om afbeeldingen van kinderen die blijkbaar de leeftijd van 18 jaar nog niet hebben bereikt en die betrokken zijn bij seksuele handelingen of die in seksueel aanstotende houdingen poseren, te maken, in bezit te hebben, te vertonen of te verspreiden. Sectie 1 van deze wet, laatstelijk gewijzigd door de Criminal Justice and Public Order Act 1994, handelt over de verschillende vormen van het maken en verspreiden van strafbare afbeeldingen of pseudo-afbeeldingen van een kind jonger dan 18 jaar (figuur 4.6).

Een belangrijke wijziging van de Protection of Children Act 1978 is doorgevoerd met de Sex Offences Act 2003. De leeftijd van een 'kind' zoals bedoeld in de Protection of Children Act 1978 wordt hierin verhoogd van 16 jaar naar 18 jaar. Daarnaast is er een toevoeging waarin staat dat de verdachte niet schuldig is aan de Protection of Children Act 1978, indien hij kan aantonen dat het maken van de afbeeldingen of pseudo-afbeelding nodig was ter voorkoming, opsporing of vervolging in een opsporingsonderzoek. Onder 'maken' valt bijvoorbeeld ook het downloaden van een kinderpornografische afbeeldingen van internet of het maken van kopieën van een harde schijf.

[80] 3G staat voor 'Third Generation' – een in 2001 in Japan ontwikkelde transmissietechniek waarmee beelden kunnen worden ontvangen met mobiele telefoons, hetgeen 'mobiel internet' mogelijk maakt.
[81] House of Commons Written Answers (2006a) *Column 715W: Child Abuse (Internet)* 15 May 2006.

Figuur 4.6: sectie 1 van de Protection of Children Act 1978

1—(1) (…) it is an offence for a person - (a) To take, or permit to be taken, or to make any indecent photograph or pseudo-photograph of a child; or (b) to distribute or show such indecent photographs or pseudo-photographs; or (c) to have in his possession such indecent photographs or pseudo-photographs, with a view to their being distributed or shown by himself or others; or (d) to publish or cause to be published any advertisement likely to be understood as conveying that the advertiser distributes or shows such indecent photographs or pseudo-photographs, or intends to do so.

De Sex Offences Act 2003 wordt vergezeld door een 'Memorandum of Understanding'. Het doel daarvan is om de positie van personen die zich professioneel bezig houden met de bestrijding van kinderpornografie, tegen vervolging te beschermen (figuur 4.7).

Figuur 4.7: tekstdeel uit Memorandum of Understanding bij de Sex Offences Act 2003

The Crown Prosecution Service and the Association of Chief Police Officers have developed this Memorandum of Understanding. Both signatory organisations recognise the need for investigating and prosecuting authorities to work together and to share information and best practice. We acknowledge that those professionally involved in the management, operation or use of electronic communications networks and services need to be re-assured of protection where they are acting to combat the creation and distribution of images of child abuse. (…) We believe that this Memorandum will encourage better understanding, closer working relationships and greater consistency between those involved in the investigation and prosecution of child abuse cases. We also believe that its introduction will help ensure the signatory organisations work in partnership for the benefit and protection of children to improve public confidence in the criminal justice system.

De wetgeving van Engeland en Wales biedt op deze wijze bescherming aan personen in organisaties die zich bezighouden met de bestrijding van het maken en verspreiden van kinderpornografisch materiaal. Een van die organisaties is de Internet Watch Foundation (IWF).

Implementatie en verspreiding van het kinderpornofilter

Anders dan in Zweden zien we in Engeland bij de ISP's weinig discussies over het invoeren van een filter tegen kinderporno. Op internetfora[82] zien we wel het debat dat we ook zagen in Zweden en Noorwegen. Ook hier vragen tegenstanders zich af wie beslist wat kinderporno is en of sprake is van een glijdende schaal. Sommigen zijn tegen elke vorm van censuur ('Censorship is wrong, period.'). De voorstanders vinden het filter een stap in de goede richting.

Was BT in juni 2004 de eerste met een filter, op dit moment werken de meeste grote ISP's uit Engeland mee aan het op vrijwillige basis blokkeren van kinderpornografische websites. Samen bedienen zij 90 procent van de binnenlandse markt (IWF, 2007). De berichten in de media gaan voornamelijk over de hoeveelheid hits op het filter en bevatten commentaar

[82] Een voorbeeld is: http://www.neowin.net/forum/index.php?showtopic=175168.

van de minister van Binnenlandse Zaken en BT op de doelen van het filter (www.guardian.co.uk 20-07-2004, www.timesonline.co.uk 20-07-2004a, www.timesonline.co.uk 20-07-2004b, http://business.timesonline.co.uk 07-02-2006). Op dat laatste gaan we verderop in. Ook andere organisaties, zoals het National Children's Home (NCH; een liefdadigheidsorganisatie die opkomt voor kinderen) staan achter het initiatief. John Carr (internetveiligheidsadviseur voor de NCH) prijst bijvoorbeeld de deelname van AOL, BT, Yahoo en de mobiele telefoonaanbieders voor hun bijdrage aan het blokkeren van kinderpornografische websites (www.guardian.co.uk 23-11-2005). Carr zegt in hetzelfde artikel dat eenvijfde van de 200 ISP's in het Verenigd Koninkrijk nog geen plannen bekend heeft gemaakt met betrekking tot het blokkeren van kinderpornografische websites.

We hebben niet kunnen achterhalen welke ISP's wel en niet mee doen en wat de eventuele redenen zijn voor het wel of niet deelnemen. De minister geeft op 25 oktober 2006 desgevraagd aan dat de overheid werkt aan het openbaar maken van een lijst met ISP's die kinderpornografie filteren. De meeste ISP's, aldus de minister, zijn overigens nu al bereid om op individuele basis aan te geven of zij al dan niet filteren (figuur 4.8).

Figuur 4.8: House of Commons Written Answers 25 October 2006.[83]

> Helen Goodman: To ask the Secretary of State for the Home Department what steps he has taken to inform the public which internet service providers block access to sites containing child pornography.
> Mr. Coaker: We have not made public which internet service providers (ISPs) block access to sites containing child abuse images. However, transparency and confidence are vital components of effective self-regulation. The majority of ISPs are prepared individually to say whether they are blocking or not. We are working with them to put in place arrangements to publish and maintain the full list of ISPs blocking these websites.

De IWF (www.iwf.co.uk) publiceert de lijst waarop de bedrijven staan die de URL-lijst van de IWF afnemen. Het gaat om ISP's, telefoonaanbieders (welke mobiel internet aanbieden), filterbedrijven en zoekmachines. Er staan op dit moment 60 bedrijven op de lijst. De lijst is echter niet compleet, bedrijven kunnen bijvoorbeeld aangeven dat ze niet op de lijst willen komen. Een opname in de lijst betekent niet dat de bedrijven daadwerkelijk URL's blokkeren. Het gaat om bedrijven die de URL-lijst van de IWF hebben afgenomen. De IWF geeft aan dat enkele van de bedrijven op de lijst al URL's blokkeren.[84]

Zelfregulering

Het blokkeren van websites met kinderpornografie geschiedt op vrijwillige basis, met dien verstande dat de Britse overheid wettelijke maatregelen aankondigt voor het geval de ISP's dit niet regelen (www.aftonbladet.se, 10 en 11 maart 2005). De ISPA UK ondersteunt deze vorm van zelfregulering en werkt nauw samen met de IWF om de ISP's te helpen de toegang tot websites met kinderpornografisch materiaal zo moeilijk mogelijk te maken (IWF, 2007).

De minister van Binnenlandse Zaken zegt op 15 mei 2006 dat uit gesprekken met de ISP's blijkt dat zij willen meewerken aan het blokkeren van websites met kinderpornografie.[85] De grootste ISP's werken al mee, of zijn dat voor het eind van 2006 van plan. Verder zegt de

[83] House of Commons Written Answers (2006b) *Column 2000W: Internet Service Providers* 25 October 2006.
[84] De lijst wordt gepubliceerd op de website van de IWF (www.iwf.co.uk). Op 7 maart 2008 is de lijst voor het laatst bekeken op: http://www.iwf.org.uk/public/page.148.438.htm
[85] House of Commons Written Answers (2006a) *Column 715W: Child Abuse (Internet)* 15 May 2006.

minister dat veel voortgang is geboekt en dat de ISP's zeer betrokken zijn. Negentig procent van de markt vindt de minister echter nog te weinig. Hij zegt dat de ISP's die nog niet filteren, hun klanten binnen negen maanden alsnog een filter dienen aan te bieden. Lukt dat niet, dan worden de mogelijkheden bekeken hoe ervoor gezorgd kan worden dat de inwoners van het Verenigd Koninkrijk geen toegang kunnen krijgen tot de URL's die op de lijst van de IWF staan. In oktober 2006 herhaalt de minister nog eens tijdens een campagne[86] wegens het tienjarige bestaan van de IWF dat alle ISP's moeten meewerken voor het einde van 2007 (IWF, 2007). Het is ons niet bekend of dat is gerealiseerd.

De rol van de IWF

De IWF is opgericht in 1996 en speelt een centrale rol in de zelfregulering op internet. De IWF wordt hierin gesteund door de Britse overheid en politie. De IWF werkt verder samen met internetgerelateerde organisaties zoals ISP's en andere aanbieders van internetdiensten. Het publiek kan bij de IWF meldingen doen betreffende strafbare inhoud op internet, zoals kinderpornografische afbeeldingen.

De IWF houdt de lijst bij met URL's waarop kinderpornografisch materiaal staat (Child Sexual Abuse Images and Content URL Service – CAIC). In 2006 bevatte de lijst 10.656 URL's (IWF, 2007). De lijst wordt twee keer per dag vernieuwd en er komen elke dag ongeveer 50 nieuwe URL's bij. De URL's die op de lijst staan zijn daar opgezet door medewerkers van de IWF (Internet Content Analysts), die de meldingen en klachten over kinderpornografisch materiaal die bij de IWF binnenkomen behandelen.[87] De kans op overblocking is relatief gering, dat wil zeggen geringer dan bij het blokkeren op domeinnaam zoals gebeurt bij het Noorse filter, doordat de IWF-lijst alleen URL's bevat.

De ISPA UK benadrukt dat overblocking zoveel mogelijk dient worden tegengegaan (www.theregister.co.uk 07–06–2004). Het gebruik van URL's (in plaats van domeinnamen) helpt daarbij evenals het regelmatig updaten van de lijst door de IWF. Ook kan tegen opname in de lijst bezwaar worden gemaakt door diegene die verantwoordelijk is voor de hosting van de geblokkeerde URL. Overige klachten van bijvoorbeeld gebruikers moeten gemeld worden bij de ISP's van die gebruikers. Onbekend is hoe vaak er een klacht is ingediend over een URL die geplaatst is op de lijst. Indien de verantwoordelijke voor de hosting van de URL bezwaar maakt bij de IWF, dan wordt door een medewerker van de IWF bekeken of de betreffende pagina voldoet aan de wetgeving (IWF, 2007). Figuur 4.9 bevat de klachtenprocedure van de IWF.

Tenslotte wordt de lijst met URL's namens the Home office geïnspecteerd en geaudit door externe deskundigen.[88] Deze experts beoordelen of de URL's op de lijst inderdaad strafbaar zijn volgens de 'Protection of Children Act 1978'.

Indien iemand bij het IWF kinderporno meldt, bekijkt het IWF of het daadwerkelijk om strafbare inhoud gaat. De specialisten van het meldpunt (zogenaamde Internet Content Analists) hebben allemaal een training gedaan bij de politie over de Britse wetgeving op het gebied van kinderpornografie. Indien de inhoud bij een Engelse provider wordt gehost, dan geeft de IWF een *notice and takedown* bericht naar de betreffende ISP. De ISP wordt geacht het materiaal te verwijderen. De IWF licht ook het politieteam dat zich bezig houd met de bestrijding van kinderpornografie in (the National Crime Squads Paedophile Online Investigation Team). Indien het materiaal niet in Engeland staat gehost, dan geeft de IWF de melding, indien mogelijk, door aan het meldpunt van het land waar het materiaal gehost staat. In ieder

[86] De IWF organiseert, naar aanleiding van hun tienjarige bestaan, in 2006 een aantal conferenties in het Verenigd Koninkrijk die ervoor moeten zorgen dat de strijd tegen online afbeeldingen van kindermisbruik bij het grote publiek bekend wordt (public-facing awareness campaign).

[87] http://www.iwf.org.uk/public/page.148.437.htm 20 februari 2008 om 11.00 uur

[88] http://www.iwf.org.uk/public/page.148.437.htm op 08 februari 2008 om14.50 uur

geval geeft de IWF de melding door aan de politie zodat die de melding aan Interpol kan doorgeven (die vervolgens de politie in het betreffende buitenland kan inlichten).

Figuur 4.9: Klachtenprocedure IWF

If any party responsible for the hosting or content of a URL within the CAIC list complains, appeals or makes representations about the accuracy of the content assessment and inclusion on the list then the following procedure will apply. ALL other enquiries regarding access to online content should be referred to your ISP:

1. The matter will be referred to a relevant member of the senior management team and the Hotline Manager, who is personally responsible for invoking and complying with the reassessment process.
2. The relevant member of the senior management team will record the complaint and delegate the reassessment to the Hotline Manager providing the Hotline Manager wasn't party to the original decision. If that were the case then the relevant member of the senior management team will arrange the reassessment process by the Child Exploitation and Online Protection Team (CEOP) or the Paedophile Unit of the Metropolitan Police.
3. The Hotline Manager will revisit the website and reassess the content at that time and take into account any evidence retained from the original assessment and decision making process against the relevant legislation.
4. IWF will also refer the appeal to the Child Exploitation and Online Protection Team (CEOP) or the Paedophile Unit of the Metropolitan Police, for an independent assessment.
5. If, after due consideration by all involved, the material is still considered to be in breach of the relevant legislation the complainant will be informed accordingly.
6. If the content is no longer considered to breach the relevant legislation the URL will be removed from the Service list and all subscribing organisations will be notified of its withdrawal and the complainant informed of the decision.
7. If the complainant appeals against the reassessment decision the assessment on whether the content is potentially illegal according to the relevant UK legislation made by senior managers in CEOP or the Metropolitan Police will be final.

De IWF heeft officieel de status van autoriteit waar kinderpornografisch materiaal kan worden gemeld en die de verspreiding van dergelijk materiaal tegengaat.[89] Medewerkers van de IWF vallen onder de wetgeving die personen die zich professioneel bezig houden met de bestrijding van kinderpornografisch materiaal, beschermt tegen vervolging (Sex Offences Act 2003).

Doelen van het filter

Volgens de minister van Binnenlandse Zaken, Vernon Coaker, is het blokkeren van websites niet dé oplossing om kindermisbruik tegen te gaan. Deze maatregel kan niet los gezien worden van andere maatregelen om seksueel misbruik te verminderen en het internet veiliger te maken. Het blokkeren van websites is echter wel een stap die nodig is om het internet veiliger te maken en om seksueel misbruik tegen te gaan (IWF, 2007).

[89] http://www.iwf.org.uk/public/page.148.437.htm op 08 februari 2008 om 14.50 uur

Ook BT geeft in de media aan dat het blokkeren van websites geen sluitende oplossing is maar slechts een stap in de goede richting (www.theregister.co.uk 07-07-2004). Het initiatief is slechts een element van een pakket aan maatregelen. Het blokkeren van websites is bedoeld om onschuldige mensen te beschermen, niet om criminelen tegen te gaan die uit zijn op kinderpornografisch materiaal.[90]

Volgens de IWF zijn de doelen van de URL-lijst en het blokkeren van URL's wat uitgebreider, maar nog steeds ligt de nadruk op de bescherming van onschuldige gebruikers (IWF, 2007):

- het beschermen van onschuldige internetgebruikers tegen het ongewenst in aanraking komen met kinderporno;
- het verkleinen van de mogelijkheid dat kinderen hun eigen misbruik tegenkomen op internet;
- het verstoren van het vinden en verspreiden van kinderpornografisch materiaal.

Aantal keer dat het filter in actie komt

Op 21 juli 2004, vlak na de invoering van het filter, lezen we in onder andere de Times Online dat BT in de vorige drie weken 230.000 pogingen heeft geregistreerd om websites te bezoeken die op de zwarte lijst staan (www.timesonline.co.uk 20-07-2004a). Deze aankondiging deed veel stof opwaaien, het zou betekenen dat duizenden klanten van BT kinderpornografische websites bezoeken. De ISPA zegt in een reactie dat zij blij is met de nieuwe ontwikkelingen om kindermisbruik tegen te gaan, maar dat er wel voorzichtig moet worden omgesprongen met de statistieken (www.theregister.co.uk 21-07-2004).

We vonden verschillende berichten over de aantallen keren dat het BT-filter in actie komt. De 230.000 hits tussen 21 juni en 13 juli, komen overeen met zo'n 10.000 hits per dag. Volgens het hiervoor aangehaalde artikel uit de Times Online zei Pierre Danon van BT op 20 juli 2004 dat er 20.000 URL-aanvragen per dag worden geblokkeerd (www.timesonline.co.uk 20-07-2004a). De Zweedse pers meldt op 11 maart 2005, overigens zonder nadere bronvermelding, dat het BT-filter dagelijks 60.000 pogingen stopt om kinderporno te downloaden (www.aftonbladet.se).

Onbekend is wat de cijfers precies inhouden, of het bijvoorbeeld gaat om bezoekersaantallen of aantallen keren dat specifieke bestanden van een webpagina gedownload worden. Het is ook niet bekend of de URL's van specifieke afbeeldingen in de lijst staan, of alleen de URL's van pagina's waarop de afbeeldingen staan; er kunnen meerdere afbeeldingen op één URL staan. Het aantal keren dat het filter in actie komt, en dus de statistiek, is afhankelijk van hoe specifiek er wordt geblokkeerd.

De gebruiker krijgt een zogenaamde 'not found' pagina. Deze pagina wordt getoond indien een opgevraagde website niet bestaat of doordat de verbinding tijdelijk verbroken is. De klant denkt wellicht dat er een storing is en probeert het later nogmaals, waardoor het aantal aanvragen stijgt. De ISPA UK geeft in het artikel aan dat ze graag de statistieken wil evalueren. Het is ons niet bekend of dit reeds is gedaan.

Effectiviteit

Richard Clayton deed in 2005 onderzoek naar de werking van het Cleanfeed filter (Clayton, 2005). Het probleem is volgens hem dat de overheid ervan overtuigd lijkt dat er mensen zijn die per ongeluk kinderporno tegenkomen. De sites waarop kinderpornografisch materiaal staat hebben echter geen alledaagse namen want deze sites willen immers niet gevonden worden door bijvoorbeeld de politie, aldus Clayton (www.guardian.co.uk 29-06-2006). Ook zegt hij

[90] http://www.iwf.org.uk/public/page.148.437.htm op 08 februari 2008 om 14.50 uur;
http://www.iwf.org.uk/media/news.archive-2004.39.htm Op 08 februari 2008 om 1445 uur

dat de URL's die op de lijst van de IWF staan, al geweerd zijn uit de zoekresultaten bij zoekmachines. Het is dus voor de onschuldige gebruiker volgens Clayton niet reëel om 'zomaar' kinderporno tegen te komen. Het lijkt er op dat de overheid het probleem overdrijft en zichzelf positioneert als een harde bestrijder van kinderpornografie. Een risico is bovendien dat pedofielen de lijst in handen krijgen en zo een lijst hebben met URL's waarop kinderporno staat. Verder concludeert Clayton in zijn onderzoek naar Cleanfeed dat een handige internetter kan achterhalen welke websites geblokkeerd worden. In reactie op de bevindingen van Clayton zegt Mike Galvin van BT dat het Clayton echter niet gelukt is om het filter te omzeilen.

Clayton zet, met andere woorden, vraagtekens bij de mate waarin het middel (het filter) geschikt is voor het doel (argeloze internetters beschermen tegen ongewilde confrontatie met kinderporno). Een effectevaluatie biedt hij niet. Ook voor het overige vonden we geen studies over de effectiviteit van het filteren in Engeland.

4.5 Verenigde Staten van Amerika

Inleiding

Ten aanzien van de VS beperken we ons tot enkele hoofdzaken. Het belangrijkste verschil met Europa is waarschijnlijk wel de grote waarde die in de VS wordt gehecht aan het *First Amendment*, dat onder meer de 'freedom of speech' en de 'freedom of the press' garandeert. De Amerikaanse overheid is daarom, althans in Europese ogen, zeer terughoudend met initiatieven in de richting van het filteren van internet. Op dit gebied valt dan ook meer te leren van landen in Europa. Niet toevallig kijkt de *Australian Communications and Media Authority* in haar recente studie naar technieken voor filteren op internet dan ook naar de ontwikkelingen in de EU, en negeert de VS (ACMA, 2008). 'The EU was selected for this survey because it was an early mover in the area of mitigating online risk, and member countries have adopted an array of measures to promote online safety. In addition, the region possesses a culture, legal system and historical approach to control of content that are not significantly different to those in Australia.'(ibidem:5).

Wetgeving

Elke activiteit die in de VS wordt ondernomen aangaande het filteren van informatie moeten we plaatsen tegen de achtergrond van het *First Amendment* van de *Bill of Rights* (figuur 4.10). Dat artikel verbiedt de Amerikaanse overheid om regels te stellen die de vrije meningsuiting of de vrijheid van drukpers beperken. De vrijheid van meningsuiting zoals wij die kennen en zoals vastgelegd in artikel 7 GW en artikel 10 EVRM is geformuleerd als een recht van burgers om zich vrijelijk te uiten. Maar dat is geen absoluut recht: zowel artikel 7 GW als artikel 10 EVRM bevat een clausule die stelt dat dat grondrecht kan zijn of kan worden beperkt volgens de wet. De Nederlandse overheid kan het grondrecht dus begrenzen via (formele) wetgeving. Het *First Amendment* heeft een ander karakter. Dat richt zich niet tot de burger maar tot de overheid en verbiedt haar om de 'freedom of speech' te beperken via wetgeving.[91]

Figuur 4.10: First Amendment (Bill of Rights, United States of America)

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

[91] Een ander verschil tussen het *First Amendment* en het EVRM is dat het *First Amendment* niet een recht op vrije informatie*vergaring* bevat zoals 10 EVRM.

Hoewel het *First Amendment* de Amerikaanse burgers stevig beschermt tegen overheidsingrijpen, impliceert dit grondrecht niet dat *alles* mag, ook niet op internet. Ook in de VS is het aanbieden en verspreiden van kinderpornografie strafbaar.[92] Onder kinderpornografie wordt in de Amerikaanse federale wet verstaan elke visuele voorstelling van een expliciet seksuele gedraging waarbij een kind onder de 18 jaar is betrokken (figuur 4.11).[93] Kinderpornografie is 'a category of material outside the protection of the First Amendment', aldus het Amerikaanse Hooggerechtshof.[94] Het hof laat in dat oordeel het welzijn van kinderen zwaar wegen: 'When a definable class of material, such as that covered by 263.15[95], bears so heavily and pervasively on the welfare of children engaged in its production, we think the balance of competing interests is clearly struck and that it is permissible to consider these materials as without the protection of the First Amendment.'

Figuur 4.11: United States Code, title 18, part 1, chapter 110, section 2256, sub 1 and 8

(1) "minor" means any person under the age of eighteen years;
…
(8) "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:
(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
(B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Filteren

Filteren van internetverkeer staat op gespannen voet met het *First Amendment*, niet in de laatste plaats omdat filteren welhaast per definitie gepaard gaat met een bepaalde mate van overblocking. Dan wordt ander verkeer dan kinderpornografie tegengehouden, terwijl de Amerikaanse overheid volgens het *First Amendment* nu juist geen regels mag stellen die het vrije woord beperken.[96] Dat neemt niet weg dat er wel van overheidswege initiatieven zijn ondernomen om kinderpornografie via filtering te blokkeren.

De staat Pennsylvania voerde in februari 2002 de Internet Child Pornography Act in. Deze wet verplichtte ISP's om kinderpornografie die via hun service toegankelijk was te ver-

[92] United States Code, title 18, part 1, chapter 110, section 2251; section 2252. Vindplaatsen bijvoorbeeld: www.law.cornell.edu/uscode/ of www.access.gpo.gov/uscode/.
[93] Een omschrijving van 'sexually explicit conduct' staat in U.S.C., title 18, chapter 110, section 2256, sub 2.
[94] New York vs. Ferber, 458 U.S. 747 (1982)
[95] New York State Penal Law, article 263, section 263.15 luidt: 'A person is guilty of promoting a sexual performance by a child when, knowing the character and content thereof, he produces, directs or promotes any performance which includes sexual conduct by a child less than seventeen years of age.' (www.public.leginfo.state.ny.us).
[96] Volwassenen-pornografie valt wel onder de bescherming van het *First Amendment*, dus een site site blokkeren die naast kinderpornografie ook volwassenenpornografie bevat, levert onmiddelijk een conflict op met het *First Amendment*.

wijderen of ontoegankelijk te maken indien het OM de ISP daartoe aanmaande. Providers reageerden op dergelijke aanmaningen met het blokkeren van een IP-adres of het instellen van een DNS-filter (filtertechnieken die bijna onvermijdelijk overblocking met zich meebrengen – zie ook hoofdstuk 2). In september 2003 startte het Center for Democracy and Technology samen met het American Civil Liberties Union en Plantagenet Inc (een ISP) een proces tegen de staat Pennsylvania. In september 2004 stelde de federale rechtbank in Pennsylvania[97] vast dat de wet ongrondwettig was, onder meer vanwege onverenigbaarheid met het *First Amendment*. Een expliciet element in het betoog van de rechtbank is dat met de gebruikte filtertechnieken meer wordt geblokkeerd dan alleen kinderpornografie. 'Although URL filtering results in the least amount of overblocking, no ISPs are currently capable of implementing this method. Both DNS filtering and IP filtering result in overblocking.'[98]

Een ander initiatief van de Amerikaanse overheid is de Children's Internet Protection Act (CIPA) van 21 december 2000. Deze wet verplicht scholen en bibliotheken die geldelijke steun van de federale overheid ontvangen alle bij hen in gebruik zijnde computers te voorzien van een filter dat moet voorkomen dat kinderen onder de 17 jaar in aanraking komen met onder andere pornografie. De wet bepaalt overigens ook dat de instelling het filter moet uitschakelen indien een volwassene die een computer wil gebruiken daarom vraagt. Op 23 juni 2003 sprak het hooggerechtshof zich over de grondwettelijkheid van deze wet uit. Het hof oordeelde dat de wet niet in strijd is met het *First Amendment* omdat de overheid de plicht heeft kinderen te beschermen tegen zaken zoals pornografie. Dat filteren leidt tot overblocking is in dat geval geen probleem omdat het filter voor volwassenen desgewenst wordt uitgeschakeld, aldus het hof.[99]

Er zijn 21 staten met een eigen wetgeving aangaande het filteren van internet door openbare scholen en/of bibliotheken. Bovendien heeft Texas een wet die voorschrijft dat een ISP op zijn homepage een link moet plaatsen naar vrij verkrijgbare filtersoftware. De staat Utah heeft bij wet bepaald dat een ISP op verzoek van een klant voor die klant filtersoftware moet inschakelen.[100] In verschillende staten worden processen gevoerd over de rechtmatigheid van het al dan niet filteren van internetverkeer door met name openbare bibliotheken.[101] Het voert te ver om de rechtszaken op deze plaats uitgebreid te bespreken. De hoofdlijn in de Amerikaanse ontwikkeling is de zo-even aangehaalde uitspraak van het hooggerechtshof van 23 juni 2003.

Filters en filtertests

Het (juridische) debat in de Verenigde Staten spitst zich toe op de vraag of filteren door de overheid wel of niet in strijd is met het *First Amendment*. Maar bij filteren door particulieren, is die vraag niet aan de orde. Ook in de Verenigde Staten kunnen huishoudens, werkgevers, particuliere onderwijsinstellingen en ISP's filters instellen of aanbieden aan hun gebruikers. Er zijn dan ook diverse bedrijven die filters maken en aanbieden.

Twee marktleiders in filtersoftware zijn Secure Computing en Websense.[102] Daarnaast zijn er volgens een overzicht van het particuliere initiatief Filtering Facts nog enkele tientallen andere filterproducten op de markt.[103] We hebben niet uitgezocht in hoeverre 'kinderpornografie' in die systemen steeds een aparte categorie is. In ieder geval is dat niet altijd het geval:

---

[97] U.S. District Court, Eastern District of Pennsylvania - *Philadelphia, PA*

[98] Center for Democracy and Technology, American Civil Liberties Union, & Plantagenet Inc, vs. Pappert, 03-5051 (2004). Als het voortschrijden van de techniek tot preciezere filters leidt, is het dus denkbaar dat de rechter tot een ander oordeel komt over filteren.

[99] United States et.al. vs. American Library Association Inc et.al., 02–361 (2003).

[100] www.ncsl.org/programs/lis/cip/filterlaws.htm

[101] http://filteringfacts.org/category/legal/

[102] www.securecomputing.com en www.websense.com

[103] http://filteringfacts.org/filtering/filtering-companies/

in SmartFilter van marktleider Secure Computing valt kinderpornografie onder de meer algemene filtercategorie 'pornografie'.

Naar de kwaliteit van internetfilters wordt geregeld onderzoek gedaan (zie ook paragraaf 2.2). Dan wordt getest of ze ook inderdaad tegenhouden wat ze zeggen tegen te houden en in welke mate er sprake is van overblocking. Diverse sites, zoals die van Filtering Facts en Peacefire, geven een overzicht van dergelijke onderzoeken.[104] 'Most filtering studies attempt to measure effectiveness by replicating user behavior, such as searching for websites that a filter should block, then measuring the degree of "under blocking." Some filtering studies also measure "overblocking" by searching for content that should not be blocked by the filter.'[105]

Twee relatief recente testen genoemd op de site van Filtering Facts zijn die van Haselton (2007) en Stark (2006). De eerste concludeert over het FortiGuard filter, in gebruik bij bibliotheken, dat ruim 15 procent van de in de categorie 'pornografie' geblokkeerde .com- en .org-domeinen ten onrechte in de lijst is opgenomen (*overblocking*). 'Thus, assuming every non-pornographic site blocked in a public library would have a bona fide claim that their First Amendment rights were being violated, the number of .com and .org sites alone with such a claim could be estimated at about 76,800.' (Haselton, 2007:8). Het onderzoek van statisticus Stark heeft niet een bepaald filter als uitgangspunt maar een steekproef van websites. Hij test welke van deze sites worden geblokkeerd door een selectie van 12 verschillende filters tegen websites met pornografische inhoud. Het percentage *overblocking* (valse positieven) varieert van 0,4 tot 23,6 procent; het percentage *underblocking* (valse negatieven) van 8,8 tot 58,4 procent. Hoe minder *overblocking* een filter laat zien, hoe meer *underblocking*. Met andere woorden: een filter dat weinig 'schone websites' ten onrechte tegenhoudt, laat veel websites met pornografische inhoud ten onrechte door. Bijvoorbeeld het filter van de 0,4 procent *overblocking*, is ook het filter van de 58,4 procent *underblocking*. Kortom, de prestaties van filters zijn niet indrukwekkend; als de Amerikaanse overheid met dergelijke filters werkt, is dat al snel in strijd met het *First Amendment*.

4.6 Enkele niet-westerse landen

Inleiding

Een organisatie die onderzoek doet naar filteren op het internet is OpenNet Initiative (ONI). 'Our aim is to investigate, expose and analyze Internet filtering and surveillance practices in a credible and non-partisan fashion. We intend to uncover the potential pitfalls and unintended consequences of these practices, and thus help to inform better public policy and advocacy work in this area,' aldus de ONI-website (http://opennet.net/). ONI deed onderzoek naar filteren van internet in tien niet-westerse landen: Saudi Arabië, Iran, Bahrain, UAE, China, Singapore, Burma, Tunesië, Jemen en Vietnam. We bespreken kort de ONI-rapporten omtrent China, Iran en Saudi Arabië. We kozen die drie uit de reeks omdat die in ons land bekend staan om hun strenge overheidstoezicht op informatiestromen. Volgens Deibert e.a. (2008) filteren deze drie landen in verhouding veel verschillende soorten informatie (breedte) en dat ook nog eens intensief. Op twee andere dimensies verschillen de landen wel onderling. In Saudi Arabië ligt de nadruk op het filteren van materiaal dat ingaat tegen sociale normen (zoals geweld, pornografie) en niet zozeer op het filteren van politieke sites. Iran filtert nadrukkelijk beide categorieën en in China ligt juist weer de nadruk op het filteren van politiek materiaal (Deibert e.a. 2008).

Het bespreken van alle ONI-rapporten gaat de opzet van deze studie te buiten. In Deibert e.a. treft men van veertig verschillende landen een korte weergave van de filterpraktijken, van Afghanistan tot Zimbabwe. In de beschrijvingen van Saudi Arabië (ONI, 2004), Iran

[104] http://filteringfacts.org; http://peacefire.org;
[105] http://filteringfacts.org/research/filter-tests/, zoals op 11 april 2008.

(ONI, 2005a) en China (ONI, 2005b) volgen we niet de korte weergaven in Deibert e.a. maar de uitgebreidere ONI-rapporten, zonder die overigens van commentaar te voorzien of daar ter controle andere bronnen naast te leggen. We sluiten deze paragraaf af met een korte reflectie.

Saudi Arabië

Het koninkrijk Saudi Arabië maakt net als Iran gebruik van SmartFilter. Dat is ontwikkeld door het Amerikaanse bedrijf Secure Computing. De *blocklist* is niet openbaar, zoals gebruikelijk in landen die filteren, maar over de procedures is de overheid op hoofdlijnen helder. Namens de staat voert de nationale Internet Services Unit (ISU) de filtering uit. De ISU geeft expliciet aan dat zij beperkt toegang tot internet verstrekt en noemt ook de categorieën die zij blokkeert: pornografie, drugs, bommen, alcohol, gokken, anti-overheid, en anti-Islamitisch materiaal. Wie een geblokkeerde site opvraagt, krijgt een stopsite met de mededeling dat de gezochte site is geblokkeerd en waarom. De stoppagina geeft de internetter de optie om te vragen dat een site wordt vrijgegeven en de optie om voorstellen in te dienen voor verder nog te blokkeren sites.

Om te kunnen filteren op nationaal niveau plaatst Saudi Arabië proxies tussen de nationale internet *backbone*, die eigendom is van de staat, en de servers in de rest van de wereld. Vragen van Saudische internetgebruikers moeten dan dus altijd via zo'n proxy. Alle informatievragen van Saudische internetters worden vergeleken met de blocklist. De filtering vindt plaats tot op URL-niveau; de *blocklist* bevat domeinen, directories binnen een domein (subdomeinen) en specifieke URL's. Wie vraagt om een adres dat op die lijst staat, krijgt de stoppagina. Als een gebruiker vraagt om een URL die zelf niet op de lijst staat maar welke zich bevindt binnen een (sub)domein dat wel op de lijst staat, wordt de aangevraagde URL ook geblokkeerd.

SmartFilter bevat verschillende categorieën sites die met deze software standaard kunnen worden geblokkeerd. De Saudi Arabische overheid maakt gebruik van de categorieën: gokken, naakt, extreem gewelddadig of angstaanjagend, seks, pornografie, drugs, obsceniteiten, extreem smakeloos, geweld. Daarnaast voegt de ISU aan het systeem een eigen lijst met te filteren sites toe. De ISU is vooral zeer actief in het blokkeren van pornosites; vaak is de ISU sneller met het blokkeren van zo'n site dan de commerciële aanbieder Secure Computing.

Uit haar empirische onderzoek naar welke sites zijn geblokkeerd, concludeert ONI dat Saudi Arabië in de praktijk vooral de volgende categorieën sites ontoegankelijk maakt: pornografie, drugsgebruik, gokken, sites die Moslims trachten te bekeren tot een ander geloof, en sites die internetters in staat stellen om anoniem te surfen en/of filters te omzeilen.

Het gebruik van SmartFilter brengt *overblocking* met zich mee, hetgeen in feite onvermijdelijk is bij het filteren van internet. Daarbij kan van gebruikers in Saudi Arabië niet echt worden verwacht dat ze de overheid attent maken op sites die naar hun mening ten onrechte zijn geblokkeerd, omdat dit de aandacht zou vestigen op hun eigen opvattingen en internetgebruik.

Iran

Ook Iran gebruikt SmartFilter als filtersoftware, maar is minder open over de gebruikte methoden dan Saudi Arabië. Het internetgebruik in Iran neemt snel toe, van ongeveer 1 miljoen gebruikers in 2001 naar 5 miljoen in 2005 en een te verwachten 9 miljoen in 2009. Iran heeft ongeveer 650 ISP's, waaronder twaalf grote.

Iran kent een strenge overheidscontrole op de media. Sinds april 2000 zijn er bijvoorbeeld 110 dagbladen en tijdschriften van de markt gehaald. Journalisten worden ondervraagd door de geheime dienst. 'Irans media rules are highly restrictive, frequently arbitrary, and open to manipulation for political purposes' (ONI, 2005a:7). Voor ISP's is filteren verplicht,

zowel van websites als van e-mail. Sinds 2001 zijn er meer dan 10 ISP's opgeheven, omdat ze overheidsfilters niet hadden geïnstalleerd.

De overheid tracht te reguleren welke sites voor gebruikers beschikbaar zijn, speciaal niet-Islamitische sites gelden als ongewenst. De overheid monitort niet het surfgedrag van gebruikers. De meeste aandacht gaat uit naar het beperken van toegang tot buitenlandse sites en het reguleren van binnenlandse sites.

Sites die beledigend zijn voor de Islam of die schadelijke ideeën inhouden, die het atheïsme of schadelijke boeken promoten, worden gefilterd. In januari 2003 stelde de overheid een commissie in die de *blocklist* samenstelt. Deze lijst omvat zo'n 15.000 sites die de ISP's moeten blokkeren. Over hoe dat verder precies werkt, verschaft de Iraanse overheid geen duidelijkheid. Iran filtert vooral pornografische sites en sites met instrumenten die gebruikers helpen om ongewenste sites te bezoeken, zoals *anonymizers*. Ook worden sites geblokkeerd met een in ogen van de overheid provocatieve inhoud, homo- en lesbo-sites, sites over biseksualiteit, seksuele voorlichting, nieuwssites in Farsi, en sites van politieke oppositiepartijen. Verder worden steeds vaker webblogs geblokkeerd.

Uit haar empirische onderzoek naar welke soorten sites wel en niet worden geblokkeerd en in welke mate, concludeert ONI dat de Iraanse overheid primair inzet op het blokkeren van drie soorten sites:

1. Pornografische sites. Dat daarnaast frequent homo- en lesbo-sites worden geblokkeerd alsook sites over seksuele voorlichting en biseksualiteit, is eerder het gevolg van *overblocking* dan van een gerichte actie tegen dergelijke sites, want die worden namelijk niet *systematisch* geblokkeerd.
2. Sites met de overheid onwelgevallige politieke inhoud (waaronder nieuwssites en blogs).
3. Sites die gebruikers helpen bij het vinden van strategieën tegen het filteren.

Daarnaast worden enkele specifieke sites geblokkeerd zoals *Voice of America* en sommige domeinen met blogs, zoals www.moveabletype.org.

China

China heeft 94 miljoen internetgebruikers, 130 miljoen als we de gebruikers van internetcafé's meerekenen. Het land kent zo'n 60 miljoen unieke IP-adressen; in 2001 waren er al 620 ISP's geregistreerd. Binnen afzienbare termijn zal China meer internetgebruikers hebben dan de Verenigde Staten en daarmee het grootste internetland zijn.

De Chinese overheid voert intensieve controle uit over internet en hanteert daarvoor een complex stelsel van wettelijke en technische maatregelen die op verschillende plaatsen of niveaus ingrijpen op internetgebruik. Daarbij zijn verschillende overheidsdiensten betrokken en duizenden ambtenaren.

De overheid verschaft geen duidelijkheid over het filterbeleid. Gebruikers krijgen ook geen stoppagina maar een algemene foutmelding. Van de landen die ONI heeft onderzocht, heeft China de omvangrijkste, meest geavanceerde, dynamische en effectieve filtersystematiek – effectief in de zin van het onbereikbaar maken van informatie. Dat gaat gepaard met aanzienlijke *overblocking*. Desondanks is de systematiek geenszins sluitend.

De Chinese media staan onder zware overheidscontrole. Informatie die de overheid onwelgevallig is, zoals over Falung Gong, Taiwan, Tibet en de protesten op het Tiananmenplein, wordt zoveel mogelijk uit de publiciteit geweerd. Voor het filteren van internet maakt China onder meer gebruik van producten van Amerikaanse bedrijven, zoals Cisco Systems, Nortel Networks, Sun Microsystems en 3COM. Westerse filtertechnieken om de verspreiding van *worms* tegen te gaan, kunnen bijvoorbeeld worden gebruikt voor het blokkeren van politiek ongewenste informatie. Met name Cisco Systems is nauw betrokken bij de ontwikkeling van het Chinese internet.

China voert om te beginnen controle uit over wie toegang krijgt tot internet en richt zich daarbij zowel op ISP's, ICP's (Internet Content Providers), internetabonnees en internet-café's. Voor elke groep is specifieke wetgeving met specifieke eisen omtrent onder meer het verstrekken van persoonsgegevens, verkeersgegevens en het invoeren van filters. ISP's zijn bijvoorbeeld wettelijk verantwoordelijk voor de inhoud van de sites die zij hosten, hetgeen een zekere mate van zelfcensuur oproept.

Verder voert China controle uit over de inhoud van de op internet beschikbare informatie. Het is internetgebruikers bijvoorbeeld niet toegestaan om informatie te maken of te verspreiden die ingaat tegen wettelijke regels of die de belangen van de staat schaadt. Ook ICP's zijn verplicht om hun systemen inhoudelijk te controleren en het internetgedrag van hun klanten te loggen. Ook voor cybercafé's gelden regels met betrekking tot de inhoud die zij hun klanten aanbieden. De controle richt zich niet alleen op websites maar ook op e-mail en bulletin board systems.

Zoekmachines maken eveneens onderdeel uit van de Chinese filtersystematiek. Zo is Google's cache functie in China niet beschikbaar (want via die route zouden geblokkeerde sites alsnog kunnen worden geraadpleegd) en worden zoekopdrachten geblokkeerd wanneer een internetter niet-toegestane trefwoorden gebruikt. Ook Chinese zoekmachines Baidu en Yisou zijn onderdeel van de filterpolitiek.

Het empirische onderzoek van ONI laat zien dat de Chinese overheid informatie over ongewenste onderwerpen grondig weet te blokkeren. *Overblocking* maakt onderdeel uit van de systematiek. Geblokkeerd worden vooral sites over politiek gevoelige onderwerpen, zoals de eerder genoemde Falung Gong, Taiwan, et cetera. Webblogs zijn ook onderwerp van blokkering. Pornografie, in Iran en Saudi Arabië speerpunt in het filterbeleid, is in China in het Engels slecht, maar in het Chinees juist opvallend goed bereikbaar. Ook sites met informatie over het omzeilen van filters zijn veelal toegankelijk.

Uit het onderzoek volgt verder dat China niet alleen domeinnamen blokkeert, maar ook de betreffende IP-adressen. (Anders dan bij het Noorse filter is het invoeren van een IP-adres dus niet een manier om het Chinese filter te omzeilen.) De Chinese filtersystematiek omvat zowel het blokkeren op domeinnaam als op URL. Het filteren van e-mail gebeurt niet op *backbone* niveau, maar wordt uitgevoerd door de afzonderlijke providers, die dat op verschillende wijzen doen.

Slotsom niet-westerse landen

De ontwikkelingen in Saudi Arabië, Iran en China laten zien dat het mogelijk is om een filtersysteem te ontwikkelen op nationaal niveau. De ONI-onderzoeken tonen ook dat het niet eenvoudig is om bepaalde groepen sites effectief en duurzaam onbereikbaar te maken. China komt daarin het verst, en heeft dan ook een zeer uitgebreide filtersystematiek. Wat betreft de techniek daarin, leunen de niet-Westerse landen op Westerse producten. Verder bestaat de filtersystematiek uit wetgeving en controle op de naleving daarvan. Er zijn wellicht enkele lessen te trekken uit de ontwikkelingen in Saudi Arabië, Iran en China. Ten eerste is het mogelijk om te filteren op nationaal niveau.[106] Ten tweede gaat filteren en blokkeren steevast gepaard met *overblocking*. Vooralsnog lijkt het er op dat hoe grondiger er wordt geblokkeerd, hoe groter dat fenomeen. Ten derde is geen enkel filtersysteem waterdicht, zelfs niet het effectiefste filtersysteem dat internet nu kent, dat van China. In hun wereldwijde overzicht van filterpraktijken komen Deibert e.a. (2008) tot de conclusie dat filtersystemen überhaupt niet waterdicht te krijgen zijn. Filterende overheden lijken de strategieën die gebruikers ontwikkelen mede op basis van nieuwe technologieën, niet bij te kunnen houden.

[106] We gaan even voorbij aan het kostenaspect, aan de ethische kant en aan eventuele vertraging die het verkeer ondervindt.

4.7 Samenvatting

De filteractiviteiten in de besproken niet-westerse landen leren ons voor de Nederlandse situatie dat het werkelijk effectief blokkeren van websites met een bepaalde inhoud geen sinecure is. De niet-westerse landen gebruiken westerse technologie; ze beschikken dus niet over een technologisch geheim. China lijkt het meest effectief bepaalde soorten sites te filteren. Dit land bereikt dat niet zozeer door het toepassen van vernuftige en precieze technische oplossingen, als wel door het toepassen van een rigoureus controlestelsel en het daarbij accepteren van een aanzienlijke mate van *overblocking*. Op technologisch vlak laten de niet-westerse landen zien dat het mogelijk is te filteren op nationaal niveau, als men althans een daarbij behorende nationale filterstructuur in het leven roept, omvattende technologie, wetgeving en controleorganisaties. Maar zelfs het Chinese systeem is duidelijk niet waterdicht.

Wat de ontwikkelingen in Noorwegen, Zweden en Engeland betreft, is een belangrijke bevinding dat er geen serieus onderzoek bestaat naar de effectiviteit van het filteren en/of de mate van *overblocking* van de in gebruik genomen kinderpornofilters. Het is dan ook niet mogelijk om degelijk onderbouwde uitspraken te doen over de mate waarin met het filteren de beoogde doelen worden bereikt en waarin ongewenste neveneffecten optreden. Met name in de Verenigde Staten zijn wel tests gedaan naar de mate waarin bepaalde filters filteren wat ze beogen te filteren, maar dergelijke tests zeggen niets over de accuratesse van bijvoorbeeld het Noorse of Nederlandse kinderpornofilter en ze zeggen eveneens niets over de mate waarin de met het filteren beoogde doelen worden bereikt.

Het uiteindelijke doel van het filteren is in Noorwegen en Zweden ambitieus geformuleerd als het verminderen van het aantal misbruikte kinderen. Het is niet eenvoudig in te zien hoe een verband tussen het gebruik van filters en het aantal misbruikte kinderen in een effectevaluatie zou kunnen worden aangetoond. In Engeland is het hoofddoel realistischer geformuleerd als het voorkomen dat onschuldige internetters ongewild in aanraking komen met kinderporno. Of er überhaupt internetters zijn die, terwijl zij op het world wide web bijvoorbeeld informatie zoeken over nekkramp, snoeien van fruitbomen, het IJslandse paard of de wijkagent, zomaar met kinderporno worden geconfronteerd, is een goed bewaard geheim.[107] Wij troffen niemand die van iets dergelijks een concreet voorbeeld kon geven. Dan is ook niet goed te bepalen waarop of op wie een effectstudie zich zou moeten richten. De eerste vraag die zou moeten worden beantwoord, luidt wie er eigenlijk stuiten op het filter, in welke omstandigheden en wat het stuiten op het filter tot gevolg heeft. Dit is tot op heden onbekend.

Statistieken over aantallen keren dat het filter in actie komt ('hits') worden door voorstanders van filteren al snel geïnterpreteerd als bewijs van de omvang van het probleem. Wie zich in de cijfers verdiept, moet echter al snel concluderen dat onzeker is wat de cijfers precies betekenen. Het is onduidelijk hoe de aantallen hits precies tot stand komen. Bovendien, als de cijfers al iets zeggen over de omvang van het probleem, dan is nog de vraag wat zij zeggen over de effectiviteit van het filteren. Wellicht omzeilen de surfers het filter vervolgens massaal. We weten het niet. Totdat in een nader onderzoek precies is uitgezocht hoe de aantallen hits tot stand komen, is het voor zowel voor- als tegenstanders onverstandig om deze aantallen te gebruiken als argument in de discussie over kinderpornofilters.

Er zijn in Europa twee filtermodellen. Het Scandinavische model is organisatorisch gezien gebaseerd op een in eerste aanleg[108] vrijwillige publiek-private samenwerking tussen met name politie en ISP's (met op de achtergrond een dreiging met wetgeving) en technisch gezien op het blokkeren van domeinen. De rolverdeling tussen ISP's en politie is als volgt: de politie beoordeelt sites en stelt de filterlijst samen; de ISP's verzorgen de technische realisatie van het filteren. Het Engelse model is organisatorisch gezien gebaseerd op zelfregulering door

[107] We hebben het hier over zoeken op internetpagina's en niet over gebruik van bijvoorbeeld P2P-systemen of chat – maar daarop hebben de filters waarover het hier gaat ook geen betrekking.

[108] Komt de samenwerking eenmaal tot stand, dan worden wel dwingende afspaken gemaakt (zie ook hfst 6).

commerciële ISP's ondersteund door de ngo IWF (met wederom op de achtergrond een dreiging met wetgeving) en technisch gezien op het blokkeren van URL's – hetgeen ingewikkelder en duurder is dan het filteren op domeinnamen, maar wel een preciezere blokkering toelaat. In Engeland vervult de IWF de rol die in het Scandinavische model de politie vervult. De medewerkers van de IWF zijn wettelijk beschermd, in die zin dat ze niet strafbaar zijn voor het in bezit hebben van kinderpornografische afbeeldingen.

Wat wetgeving betreft lijkt de tendens te zijn dat de strafbepalingen van de Europese landen steeds meer op elkaar gaan lijken (bijvoorbeeld het strafbaar stellen van het doelgericht bekijken van kinderporno). Toch zijn er nog steeds opmerkelijke onderlinge verschillen. De Noorse wet is bijvoorbeeld op diverse punten strenger dan de Nederlandse. Strikt genomen kunnen de Noren dus sites in hun filter opnemen die in Nederland legaal worden gehost.

Naast de filtersystemen die door de overheid worden gestimuleerd via zelfregulering of een publiek-private samenwerking (PPS), brengen commerciële bedrijven in bijvoorbeeld de VS en Zweden weer andere filters op de markt. Kennelijk is er sprake van een commercieel interessante markt.

Filteren gaat steeds gepaard met discussie over overheidscensuur. De mate waarin die discussie wordt gevoerd, verschilt per land. Er is geen verschil van mening over de vraag of kinderporno mag worden tegengehouden. Het probleem is dat elk filtersysteem leidt tot *overblocking*: een overheid die filtert moet willen incalculeren dat zij ook legale informatie blokkeert. De vraag in Europa is dan hoe dat zich verhoudt tot artikel 10 van het EVRM, waarin de vrijheid van meningsuiting en het recht op vrije informatievergaring zijn vastgelegd (figuur 3.6). Ondanks deze discussie vindt filteren van kinderpornografie in Europa steeds meer ingang. In de Verenigde Staten ligt dat anders omdat de overheid daar rekening heeft te houden met het *First Amendment*, dat de overheid verbiedt om regels te stellen die de vrijheid van meningsuiting en de vrijheid van drukpers beperken.

Het belangrijkste argument voor filteren, althans het argument dat in discussies het langste stand houdt, is dat daarmee – afgezien van opsporingsinspanningen – in elk geval *iets* wordt gedaan tegen kinderpornografie op internet. Het delict geldt in de samenleving als dermate ongewenst dat elke maatregel die mogelijk is, moet worden genomen, kennelijk los van de vraag of enig effect kan worden aangetoond. Zo lijkt het althans. In werkelijkheid zagen we in verband met filteren niet vaak discussie over welke àndere maatregelen (buiten opsporing om) wellicht ook nog genomen zouden kunnen worden tegen de verspreiding van kinderporno op internet. Dat is opvallend omdat immers ook op andere manieren *iets* kan worden gedaan om de verspreiding van kinderporno tegen te gaan – zeker als niet de vraag is hoe effectief de maatregelen zijn. Wellicht speelt bij filteren een rol dat het een technische maatregel is. Voor velen kleeft aan technische maatregelen 'de magie van de machine' (Frissen, 1989) en niet zelden gaat dat gepaard met een 'naïef optimisme' aangaande de effectiviteit van technische maatregelen. 'Naïef optimisme ontstaat door een gebrek aan kennis over technologische principes en systemen bij bestuurders en handhavers, waardoor zij zich te gemakkelijk laten meeslepen in het enthousiasme van verkopers en technici.' – zo staat te lezen in een uitgave van het Expertisecentrum Rechtshandhaving van het Nederlandse ministerie van Justitie (Stol, 2004:23).

Tegenstanders van filteren wijzen vooral op het gemak waarmee filters kunnen worden omzeild. Ook wijzen ze er op dat dit weinig of geen technisch vernuft vraagt: hoe een filter te omzeilen kan men eenvoudig achterhalen op internet. Ook waarschuwen ze voor 'de glijdende schaal'. Nu kinderpornosites filteren, straks goksites, haatsites, warez-sites, et cetera. Politici geven de tegenstanders wel enige aanleiding voor die redenering. Twee leden van Noorse Commissie datacriminaliteit willen een wet die de mogelijkheid biedt om alle mogelijk strafbare inhoud te blokkeren, de Noorse minister van Justitie wil naast websites ook tele-

foonverkeer gaan filteren op kinderporno, de Zweedse minister van Justitie wil dat het filter ook wordt gebruikt tegen websites die verband houden met vrouwenhandel.

We zagen dat er bij het samenstellen van de filterlijst door de politie soms fouten worden gemaakt, waardoor sites onbedoeld worden geblokkeerd. Voor zover we hebben kunnen nagaan zijn eenmaal aangekaarte fouten steeds snel gecorrigeerd en zijn er in Europa geen procedures gevoerd voor schadevergoeding wegens onrechtmatige overheidsdaad. De kinderpornofilters zijn echter niet getest op accuratesse (mate van *over-* en *underblocking*). Uit tests van commerciële filtersoftware, met name in de Verenigde Staten, blijkt dat filters nooit honderd procent doen wat ze beogen te doen; bij een filter van enige omvang is sprake van structurele *overblocking*. Het percentage vals-positieven (ten onrechte geblokt) loopt in de verschillende onderzoeken uiteen van een half tot vijftig procent (paragraaf 2.2 en 4.5), waarbij zij opgemerkt dat filters met weinig vals-positieven (geringe *overblocking*) relatief veel sites doorlaten die eigenlijk geblokkeerd zouden moeten worden (hoge *underblocking*).[109] Een overheid die serieus aan de slag gaat met filteren en een filter ontwikkelt met een laag percentage vals-negatieven (lage *underblocking*), moet dus bereid zijn om structureel en redelijk substantieel informatie ten onrechte te blokkeren. Omdat dergelijke accuratesse-tests voor de kinderpornofilters die hier besproken zijn, niet zijn uitgevoerd, is onbekend hoe goed die filters doen wat ze beogen te doen (de mate van *underblocking* en van *overblocking*).

Ondanks alle onduidelijkheden, leert de oriëntatie in het buitenland ons dat het mogelijk is om ongewenste sites met een filtersysteem voor internetters moeilijker bereikbaar te maken, als men maar bereid is om de daarmee verbonden *overblocking* te accepteren. Verder leert een wereldwijd overzicht van internetfiltering (Deibert e.a. 2008) dat filtersystemen niet waterdicht te krijgen zijn omdat filterende overheden geen gelijke tred kunnen houden met de strategieën die gebruikers mede door nieuwe technologieën ontwikkelen.

[109] Het filter met 0,4% *overblocking* had meer dan 50% *underblocking*. Met andere woorden: dat filter hield minder dan de helft van de te blokkeren sites ook werkelijk tegen.

HOOFDSTUK 5

Nederlandse situatie

Dit hoofdstuk beschrijft hoe op dit moment in Nederland de verspreiding van kinderporno op internet wordt tegengegaan. Daarnaast beschrijven we de effecten van de op dit moment gehanteerde methoden en geven we een impressie van de maatschappelijke en politieke discussie die hieromtrent wordt gevoerd.

5.1 Inleiding

De levendige discussie en soms ook commotie die in Nederland is ontstaan over de manier waarop kinderporno op internet kan worden aangepakt, is wellicht typerend voor dit land. In deze inleiding geven we een beeld van deze politiek-maatschappelijke discussie.

De afgelopen jaren is het onderwerp kinderpornografie op internet – in al zijn verschijningsvormen - verscheidene keren in het nieuws geweest. Ook in de Tweede Kamer was er veel aandacht voor het onderwerp. Hier volgen slechts een paar voorbeelden. Zo publiceerde de Nieuwe Revu in 2004 twee artikelen.[110] In deze artikelen wordt beweerd dat de doorgewinterde liefhebbers van kinderpornografisch materiaal allerlei methoden en technieken gebruiken om bij hun zoektocht naar nieuw materiaal buiten het bereik van justitie te blijven en dat zij daar ook succesvol in zijn. Deze artikelen hebben geleid tot Kamervragen.[111] Naar aanleiding hiervan verrichtte het Nederlands Forensisch Instituut in opdracht van de minister van Justitie een onderzoek.[112]

In 2006 nam de Tweede Kamer een motie[113] aan om de verdere uitbouw en toepassing van de technische mogelijkheden tot het blokkeren, filteren of afsluiten van kinderpornografisch materiaal op internet en andere media te bevorderen en de Kamer daarover nader te berichten. Deze motie is het startpunt geweest voor dit onderzoek.

Het programma Netwerk kwam in februari 2007 met een reportage over Second Life, een online game. Hieruit kwam naar voren dat deelnemers aan deze game hun alter ego's - in de vorm van met de computer ontworpen menselijke figuurtjes op het beeldscherm, zogenoemde avatars - seksuele handelingen laten verrichten met virtuele kinderen. In dezelfde maand nog stellen kamerleden hierover vragen.[114] Er wordt onder meer een verbod bepleit.

Parool-columniste Karin Spaink publiceerde op 19 februari 2008 een artikel over een door haar onderzochte lijst met websites die kinderpornografisch materiaal bevatten. De lijst die door Spaink nader is onderzocht, is aanvankelijk opgesteld door de Fin Matti Nikki. Hij verrichte een eigenstandig onderzoek naar door de Finse politie geblokkeerde websites met kinderporno. Spaink ontdekt dat 138 van de 1000 sites die staan vermeld op de lijst van Nikki in Nederland worden gehost. Ook meldt Spaink dat enkele sites die in Finland worden geblokkeerd, niet staan vermeld op de blacklist van het KLPD. Op internetfora wijten diverse personen dit aan geruzie tussen internationale politiediensten over wat wel of geen kinderporno is.[115] We beschikken niet over een volledig overzicht van de resultaten van de door Spaink uitgevoerde scan. Of er sprake is van ruzie kunnen we niet beoordelen. Het is in elk geval aannemelijk dat de wet- en regelgeving tussen Nederland en Finland verschilt en dat de auto-

---

[110] J. van Kleef, 'Kinderporno kinderspel', *Nieuwe Revu* 15 december 2004. H. Lensink, 'Ziek & Slim', *Nieuwe Revu* 15 december 2004.

[111] *Kamervragen met antwoord*, 2003-2004, nr. 1102.

[112] M. Oosterink, E.J. van Eijk, *Opsporing kinderpornografie op internet. Een statusoverzicht*. Nederlands Forensisch Instituut, 2006.

[113] *Kamerstukken II* 2005/06, 30 300VI nr. 160.

[114] Kamervragen met antwoord, 2006-2007, nr. 2060708170 en nr. 1031.

[115] Op diverse internetfora worden de bevindingen van Spaink bediscussieerd, zie bijvoorbeeld www.webwereld.nl/articles/kinderporno en www.blogger.xs4all/kspaink/archive/2008/02.

riteiten in beide landen (mede daardoor) andere opvattingen huldigen over wat precies onder kinderporno moet worden verstaan. Zoals we in hoofdstuk 4 opmerkten, is de wetgeving op het gebied van kinderpornografie in Scandinavische landen op verschillende punten strenger dan de Nederlandse wetgeving. De blacklist uit Noorwegen is bij implementatie in Nederland met 90 procent gereduceerd (van 2500 sites naar 250 sites). Dat heeft niet alleen met verschil in wetgeving te maken, maar ook met de criteria die de politie hanteert bij het samenstellen van de lijst. De Noorse politie laat bijvoorbeeld sites die niet meer bestaan, bewust in de blacklist staan. Volgens het KLPD horen dergelijke adressen op de lijst niet thuis. Ook neemt de Noorse politie sites in de lijst op waarop met een link naar kinderporno wordt verwezen die op een andere plaats beschikbaar is. Het KLPD neemt alleen sites op die zelf kinderpornografisch materiaal tonen.

Genoemde verschillen in wet- en regelgeving nuanceren de resultaten van de door Spaink uitgevoerde internetscan. Toch is er volgens Spaink wel degelijk sprake van overblocking. Zij is van mening dat een aantal sites ten onrechte op de (door Nikki samengestelde) Finse blokkeerlijst staat. 'Sommige sites bevatten helemaal geen kinderporno,' aldus Spaink, 'en sommige sites zijn "op het randje".'

De bevindingen van Spaink leiden op 20 februari 2008 tot kamervragen van zowel Gerkens van de SP als Azough van Groen Links. Men wil onder andere van de minister weten waarom het KLPD de sites die in Nederland zijn gehost ongemoeid heeft gelaten en of er inderdaad sites op de lijst staan die daar helemaal niet thuishoren. Op dezelfde dag dat in Nederland kamervragen worden gesteld over overblocking (het ten onrechte blokkeren van websites), stemt het Europees Parlement in (571 voor en 38 tegen) met het voorstel van Jules Maaten (VVD) om internetcensuur als handelsbarrière te beschouwen. [116] Wanneer dit voorstel door de Raad wordt overgenomen, kunnen aan landen die internetcensuur toepassen sancties worden opgelegd. Ook al richt dit voorstel zich vooral op landen als China, Cuba en Tunesië, ook in Europa vindt internetcensuur soms plaats. Zo is de persoonlijke website van Matti Nikki vrijwel direct na openbaarmaking van de door hem gereconstrueerde blokkeerlijst door de Finse politie geblokkeerd en is een onderzoek naar zijn activiteiten gestart.[117]

Het particuliere Meldpunt Kinderporno op Internet publiceert in haar jaarverslag van 2007 dat het aantal meldingen van websites met kinderporno die in Nederland zijn gehost, is verzevenvoudigd (van 100 sites in 2006 naar 700 sites in 2007). Volgens het Meldpunt is deze grote stijging vooral te wijten aan de populariteit van Nederlandse hostingbedrijven. De makers van het strafbare materiaal komen vaak uit het buitenland, maar kiezen Nederland als verspreidingspunt vanwege de goede infrastructuur en hostingfaciliteiten. Het jaarverslag van het particuliere Meldpunt Kinderporno op Internet is als vertrekpunt genomen in een documentaire van het actualiteitenprogramma NOVA dat op 11 april 2008 op de Nederlandse televisie is uitgezonden. De documentaire laat zien bij welke provider de meeste kinderpornosites zijn gehost. De directeur van het betreffende bedrijf geeft in de documentaire aan dat hij de inhoud van het internetverkeer dat zijn bedrijf faciliteert niet kent (en gezien de omvang van dit verkeer ook niet kan kennen). Minister Hirsch Ballin van Justitie komt ook in NOVA aan het woord. Hij zegt: 'de verspreiding via Nederland heeft een specifieke verklaring, maar er is geen sprake dat wij daarin berusten.' Ook refereert hij aan onderhavig onderzoek naar het filteren van kinderporno en vermeldt hij dat inmiddels 40.000 internetgebruikers op het filter – zoals thans in Nederland door UPC, Scarlet en Kliksafe wordt gebruikt – zijn gestuit. Echter, zoals in hoofdstuk 4 reeds was te lezen, is het aantal hits noch een betrouwbare indicator voor de mate waarin door internetters naar kinderporno wordt gezocht, noch een betrouwbare indicator voor de effectiviteit van het filter.

[116] Internetcensuur in Europa, NRC Handelsblad, 22-02-2008.
[117] 'Finnish police censors a critic on censorship', www.effi.org , 12-2-2008.

5.2 Tegengaan van de verspreiding van kinderporno op internet

Inleiding
Uit de interviews komt naar voren dat in Nederland via drie methodes de verspreiding van kinderporno op internet wordt tegengegaan:

1. Kennisopbouw
   - Het opbouwen van kennis en expertise over de verspreiding van kinderporno op internet. In dit kader kan worden gedacht aan (internationale) kennisuitwisseling en samenwerking en het verrichten van onderzoek (o.a. case studies).
2. Preventie
   - *Identificatie van risicogroepen*
     Hierbij kan worden gedacht aan het opstellen van een profiel van verspreiders en verzamelaars die beginnen met het ontplooien van hun activiteiten op internet en zij die reeds gebruik maken van geavanceerde technische middelen om (anoniem) kinderporno te verzamelen en te verspreiden. Dit om de grens te bepalen tussen beide groepen, opdat preventieve maatregelen kunnen worden ingezet waarmee zogenoemde 'first offenders' niet terecht komen in het circuit van de 'advanced offenders'.
   - *Technische beveiliging*
     Het opwerpen van een drempel voor gebruikers en/of downloaders om toegang te verkrijgen tot kinderpornografisch materiaal. In het verlengde hiervan wordt het tevens voor aanbieders moeilijker om hun klanten te bereiken (technische beveiliging);
   - *Voorlichting*
     Het geven van voorlichting over de 'donkere' kanten van internet en het aanreiken van beschermende maatregelen (o.a. virus- en spamfilters) voor gebruikers;
3. Opsporing
   - Het opsporen van (commerciële) aanbieders van kinderporno en de personen die daadwerkelijk seksueel misbruik maken van kinderen; (internationale) harmonisatie van wet- en regelgeving.

Waar het gaat om kennisopbouw zijn meerdere actoren te onderscheiden. Te denken valt aan speciale teams binnen het KLPD, zoals het team High-Tech Crime en het team Bestrijding Kinderpornografie, het NICC, het meldpunt tegen kinderporno, onderzoeksinstituten als bijvoorbeeld het WODC en het NFI en universitaire faculteiten op het gebied van ICT en Recht.

We hebben niet onderzocht en dus ook geen zicht op de mate waarin risicogroepen thans kunnen worden geïdentificeerd. Wel geven respondenten aan dat zij waar mogelijk trachten te achterhalen of mensen die kinderpornografisch materiaal verzamelen, mogelijk zelf ook misbruikers of aanbieders zijn. In het verlengde hiervan wijzen we op het onderscheid tussen oud (periode 1970-1980), recent (periode 1980 tot wetswijziging in 1996) en nieuw materiaal (vanaf 1996 tot heden), dat gehanteerd wordt in de aanwijzing kinderpornografie van het college van procureurs-generaal. (stcrt, 2007, 162). Het college meldt in deze aanwijzing dat ongeveer 60 tot 70 procent van de bekende afbeeldingen in de categorie *oud* valt. Voorkomen dient te worden dat 'first offenders' zich ook gaan toeleggen op het maken en verspreiden van *nieuwe* afbeeldingen. Aangezien het onmogelijk is om eenmaal op het internet verspreid kinderpornografisch materiaal definitief te verwijderen – dit impliceert namelijk dat slachtoffers blijvend worden geëxposeerd - is het des te urgenter om te voorkomen dat *nieuw* materiaal wordt geproduceerd en verspreid.

Op het gebied van technische beveiliging is onderscheid te maken tussen beveiliging aan de kant van de aanbieder en beveiliging aan de kant van de gebruiker. Op dit moment trekken het KLPD en enkele ISP's gezamenlijk op om de toegang tot kinderporno op internet

te bemoeilijken (door het blokkeren van websites). Met alle ISP's zijn samenwerkingsroutines aangaande het fysiek verwijderen van websites (NTD). Daarnaast is het voor gebruikers mogelijk om zich te beschermen tegen strafbare, illegale of ongewenste content op internet door gebruik te maken van een van de vele commerciële aanbieders van filters of andere beschermende software.

Meerdere actoren geven op dit moment voorlichting over manieren aan de hand waarvan internetters zich kunnen beschermen tegen strafbare, illegale of ongewenste content. Dit gebeurt onder andere aan de hand van door de overheid geïnitieerde voorlichtingscampagnes, op scholen, door ISP's en door commerciële aanbieders van beschermende software. Tijdens ons onderzoek hebben we overigens geen specifieke voorlichting over bescherming tegen kinderporno op internet aangetroffen. Voorlichting heeft doorgaans een breder karakter en is gericht op protectie tegen onder andere spam en virussen. Ook wordt recent een mede door de overheid gesubsidieerde voorlichtingscampagne uitgevoerd over veilig internetbankieren.

De als laatste genoemde maatregel is opsporing. Dit is expliciet een taak van de politie. De door ons geïnterviewde zedenrechercheurs geven aan dat zij de opsporingstaak ook veruit het belangrijkst vinden bij het tegengaan van de verspreiding van kinderporno op internet: 'het is effectiever om de bron te zoeken en weg te nemen, dan om je te richten op de eventuele downloaders van kinderpornografisch materiaal.'

Hierna gaan we nader in op één aspect van de tweede methode: preventie door middel van technische beveiliging. De overige methoden vallen immers buiten het bestek van dit onderzoek.

Technische beveiliging door de gebruiker

Het treffen van maatregelen door internetgebruikers om zich te beschermen tegen kinderporno op internet (en eventueel andere ongewenste content) zonder dat de overheid daar enige invloed op uitoefent, is te beschouwen als spontane zelfregulering. Gebruikers kunnen door commerciële bedrijven ontwikkelde beschermende softwarepakketten op hun personal computer installeren. Diverse van dergelijke pakketten zijn reeds voorhanden. Ook is het mogelijk voor gebruikers om op hun pc een antivirusprogramma te koppelen aan een blacklist. Bij sommige computers is dit zelfs al standaard ingebouwd.

Als voorbeeld van spontane zelfregulering bespreken we de werkwijze van Internetwegwijzer OpenDNS. OpenDNS biedt thans circa dertig verschillende filtercategorieën aan, die gebruikers zèlf kunnen activeren om het bezoek aan bepaalde websites tegen te gaan. Opvallend is dat dit bedrijf eigen klanten inzet om deze filters samen te stellen en te verbeteren. Gebruikers kunnen een website bijvoorbeeld nomineren als kinderpornografisch, racistisch of haatzaaiend. Andere gebruikers kunnen deze kwalificaties of 'tags' bevestigen of juist tegenspreken. Pas als voldoende gebruikers de kwalificatie van een site hebben bevestigd, wordt die door OpenDNS ook opgenomen in het desbetreffende filter. Uiteraard zitten ook de nodige haken en ogen aan dit systeem. Zo is een exacte afbakening van het begrip 'voldoende' bevestiging of ontkenning volstrekt onduidelijk. Ook is onduidelijk op welke wijze 'voldoende bevestiging' wordt verkregen. Zo kan iemand die sterk overtuigd is van het kinderpornografische karakter van een site allerlei manieren bedenken om dit aan OpenDNS meermaals te bevestigen. In deze systematiek bepaalt dus de macht van de meerderheid (of de macht van de slimme internetter) wat al dan niet gefilterd dient te worden. Een oordeel van een rechterlijke of andere onafhankelijke instantie met voldoende kennis om tot een weloverwogen oordeel te komen is hierbij volstrekt niet aan de orde. Dit kan vertroebeling in de hand werken. Dit bleek al toen recent de homepage van Hillary Clinton op de (ter verificatie aan gebruikers aangeboden) lijst te boek stond als 'racistisch en haatzaaiend'. Ondanks genoemde onvolkomenheden van deze systematiek, kunnen gebruikers echter wel zelf bepalen wat gefilterd wordt en maken zij ook zelf de keuze om al dan niet gebruik te maken van een filter.

Technische beveiliging door de ISP's, in samenwerking met de politie
Technische beveiliging door ISP's vindt in Nederland op twee manieren plaats. Op de eerste plaats kunnen websites, nieuwsgroepen en chatboxen door ISP's fysiek van het internet worden verwijderd. De tweede methode van aanpak betreft het blokkeren van open websites waardoor ze niet meer toegankelijk zijn (tenzij men de blokkade weet te omzeilen). We geven eerst een illustratie van de werkwijze op basis waarvan wordt besloten tot het fysiek verwijderen of tot het blokkeren van websites (zie ook figuur 5.1). Deze werkwijze is toegelicht door het hoofd van het team Bestrijding Kinderpornografie van het KLPD.

Het team Bestrijding Kinderpornografie van het KLPD ontvangt regelmatig meldingen over websites waarop kinderporno zou staan. Deze meldingen komen van het particuliere Meldpunt Kinderporno op Internet, het Meldpunt Cybercrime van de politie, het Meldpunt M (Meld Misdaad Anoniem), individuele internetgebruikers, bedrijven, de Nederlandse politieorganisatie of buitenlandse politiediensten. Ook meldingen van het particuliere Meldpunt Kinderporno op Internet kunnen van oorsprong uit het buitenland komen. Het meldpunt is aangesloten bij de internationale organisatie INHOPE (International Association of Internet Hotlines). INHOPE is in 1999 opgericht door de 'European Commission's Safer Internet Action Plan'. Het is een koepelorgaan van meldpunten uit 27 landen en stelt zich als doel 'to work towards a safe environment for Internet users which will protect our children and respect the privacy and dignity of our citizens' (www.inhope.org). Een bij INHOPE aangesloten meldpunt geeft een melding die betrekking heeft op een ander land, door aan het INHOPE-meldpunt in dat land.

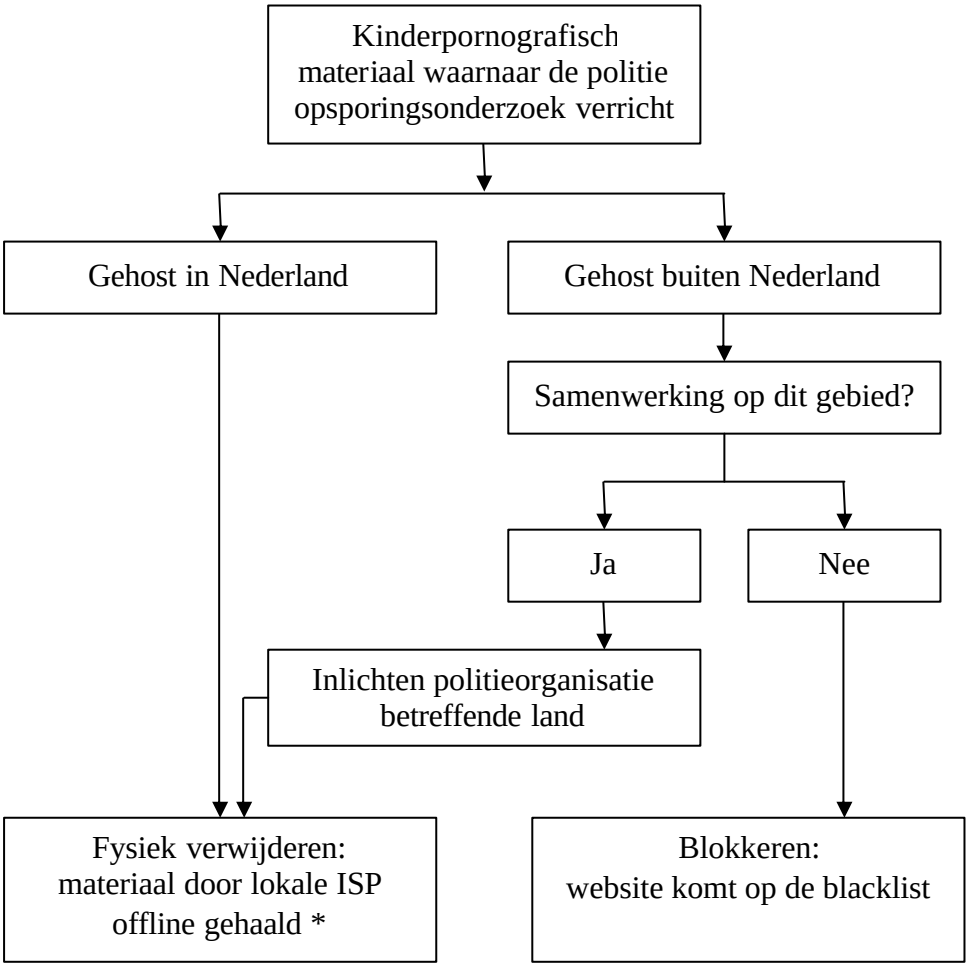
Het KLPD-team Bestrijding Kinderpornografie liet ons weten dat zij de nationale en internationale meldingen over kinderpornografisch materiaal op internet in onderzoek neemt, voor zover althans de beschikbare personele capaciteit dat toestaat. Zedenrechercheurs onderzoeken eerst of de gemelde sites daadwerkelijk kinderporno bevatten. Na de vaststelling of er sprake is van kinderporno, onderzoeken internetrechercheurs wie de eigenaar is van de site en in welk land de site is gehost. Zo mogelijk worden zaken vervolgens door het team zelf in onderzoek genomen, dan wel overgedragen aan een politieregio of een buitenlandse politiedienst. Het starten van een onderzoek heeft altijd de hoogste prioriteit, aldus nog steeds het KLPD-team Bestrijding Kinderpornografie. Als direct politieoptreden lastig is of lang gaat duren, dan komen de sites op de blokkeerlijst, als het althans gaat om buitenlandse sites.

Het KLPD-team Bestrijding Kinderpornografie houdt naar het zegt in jaarverslagen onder meer bij hoeveel meldingen zij krijgt, alsook het aantal processen-verbaal dat zij voor verder onderzoek overdraagt aan politieregio's of buitenlandse politiediensten. Het KLPD-team gaf ons, ondanks ons verzoek tot inzage in die stukken, geen inzage in jaarverslagen of andere cijfermatige overzichten aangaande de door het team ontvangen meldingen en behandelde zaken.

Hosting in Nederland
Websites, chatrooms en nieuwsgroepen met kinderpornografische content die in Nederland zijn gehost, kunnen na melding door het KLPD direct worden verwijderd door de betreffende ISP. Onder de Europese e-commerce richtlijn (2000/31/EG) zijn internetproviders namelijk aansprakelijk voor eventueel onrechtmatig materiaal van hun klanten, als zij van het bestaan daarvan op de hoogte zijn gekomen. Deze aansprakelijk is uitsluitend reactief: de e-commerce richtlijn vrijwaart ISP's van de plicht tot pro-actief toezicht (zie ook paragraaf 3.5). Het risico van aansprakelijkheid bestaat verder uitsluitend in het geval van hosting: ISP's bieden dan ruimte aan voor websites of homepages. Bij het maken van een tijdelijke kopie om technische doorgifte mogelijk te maken ('caching') en bij 'mere conduit', het bieden van bijvoorbeeld bandbreedte, geldt deze aansprakelijkheid niet.

ISP's moeten na een klacht zelf beoordelen of de publicaties van hun klanten eventueel onrechtmatig of illegaal zijn, en als dat het geval is, onmiddellijk de toegang tot de informatie blokkeren. In Nederland is de richtlijn omgezet in de Aanpassingswet richtlijn inzake elektronische handel, die op 30 juni 2004 in werking is getreden.[118] De manier waarop providers omgaan met inhoudelijke klachten over websites die zij hosten heet 'Notice and Take-down' (NTD).

Figuur 5.1 Schematische weergave van de keuze tussen fysiek verwijderen of blokkeren, in gevallen waarin de politie opsporingsonderzoek verricht



* Of dit bij sites die worden gehost in het buitenland ook altijd daadwerkelijk gebeurt, is nog maar de vraag. We hebben, zoals gezegd, geen cijfers gekregen over het aantal zaken en de wijze waarop ze zijn afgehandeld.

NTD vindt momenteel plaats indien er een wettelijke basis is: de content is onmiskenbaar onrechtmatig. De meeste internetproviders hebben bovendien zelf algemene voorwaarden opgesteld die NTD mogelijk maken. Deze voorwaarden gaan overigens soms veel verder dan wat puur wettelijk moet. Een opvallend voorbeeld in dezen is het NTD-beleid van de ISP Kliksafe: zij filteren voor hun gebruikers een veelheid aan sites die zij ongewenst of schadelijk ach-

[118] Aanpassingswet richtlijn inzake elektronische handel, Stb. 2004, 210.

ten – zoals onder andere sites met porno, goksites of sites die kunnen oproepen tot haat – maar die juridisch gezien lang niet altijd strafbaar zijn.

Alle ISP's hebben zelf procedures over hoe om te gaan met meldingen. Deze procedures verschillen per provider. Beperkingen in het huidige systeem zitten vooral in de omgang met meldingen die niet onmiskenbaar onrechtmatig zijn. Hierbij gaat het om meldingen waarbij de wettelijke kaders ontbreken of die niet eenduidig zijn. De Nationale Infrastructuur ter bestrijding van Cybercrime (NICC) organiseert op dit moment expertmeetings en overige activiteiten ter verkenning van de mogelijkheden om tot een landelijke uniformering van het NTD-beleid te komen.

Wanneer er sprake is van kinderpornografisch materiaal op internet dat in Nederland is gehost, is het dus mogelijk dat de hosting provider de betreffende content na een melding fysiek verwijdert. Het KLPD kan dan een recherchetactisch onderzoek starten om de slachtoffers te traceren en de daders op te sporen.

Politiedatabank met kinderpornografische afbeeldingen

Een aanzienlijk deel van de op het internet ter beschikking gestelde kinderpornografische afbeeldingen zijn bij het KLPD of bij Interpol bekend. Van deze afbeeldingen beheert het KLPD op nationaal niveau en Interpol op internationaal niveau een databank. In deze databank staan de hashcodes van kinderpornografische afbeeldingen uit eerdere rechercheonderzoeken.

De afbeeldingen die in de databank van het KLPD zijn opgenomen, zijn ondergebracht in drie categorieën: 1) 'oud', vervaardigd in de periode 1970-1980; 2) 'recent', vervaardigd in de periode 1980-1996; 3) 'nieuw', vervaardigd in de periode van 1996-heden. Deze rubricering is conform de Aanwijzing van Procureurs-generaal[119]. Aanleiding tot deze Aanwijzing was ondermeer de constatering dat veel van het op internet aangeboden kinderpornografische materiaal niet actueel of nieuw vervaardigd is.

De afbeeldingen in de politiedatabank zijn voor het overgrote deel vergaard in het kader van strafrechtelijk onderzoek. Dat betekent echter niet dat deze afbeeldingen alle aan een rechterlijke toets zijn onderworpen. De Aanwijzing schrijft voor dat, ten einde te voorkomen dat dergelijke afbeeldingen onbedoeld worden verspreid, dat deze afbeeldingen niet aan het strafdossier worden toegevoegd. Om dezelfde reden mogen ze niet in de tenlastelegging worden opgenomen. Volstaan wordt met een beschrijving van maximaal 25 afbeeldingen, waarbij de selectie in ieder geval plaatjes uit de zogenoemde prioriteitenlijst dient te bevatten én een algemeen beeld van de collectie dient te geven. De rechter steunt voor zijn oordeel op deze door de zedenexperts van de politie opgestelde beschrijving. Behoudens in geval van betwisting van door de verdachte van het strafbare karakter van de afbeelding(en), vormt de rechter zich geen oordeel op basis van de betrokken afbeeldingen zelf. Dat geldt *a fortiori* voor de onder verdachte in beslaggenomen afbeeldingen, waarvan in de tenlastelegging geen beschrijving is opgenomen, maar die wellicht eveneens in bovengenoemde databanken worden opgenomen.

Hosting in het buitenland

Websites met kinderporno die in het buitenland zijn gehost, vallen juridisch gezien buiten het bereik van de Nederlandse politie en justitie. Er is echter wel een aantal landen waar Nederland een algemeen rechtshulpverdrag heeft afgesloten. Ook heeft Nederland samen met vele andere landen het Cybercrimeverdrag ondertekend (zie ook paragraaf 3.2). Tot slot is Nederland vertegenwoordigd in het internationale project CIRCAMP (Cospol Internet Related Child Abusive Project). Naast Nederland nemen ook andere West-Europese landen deel aan

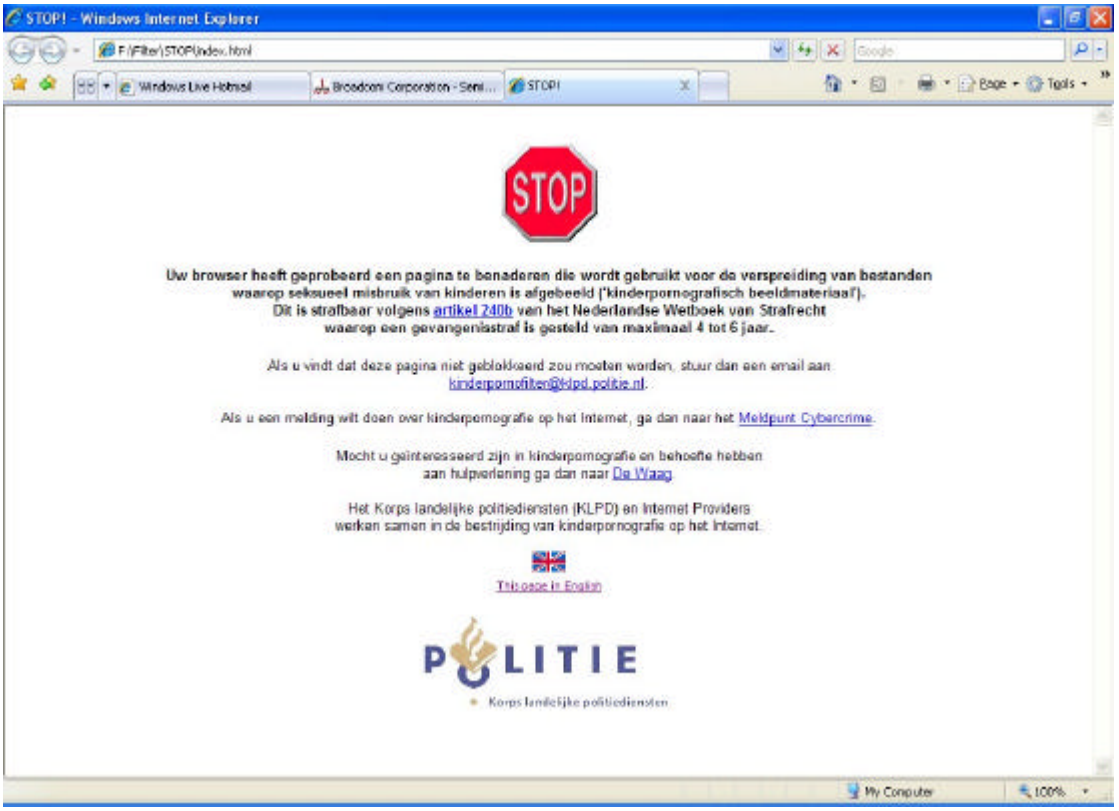
[119] Aanwijzing Kinderpronografie (art. 240b Sr), Strcrt 2007, 162.

dit project (zie paragraaf 4.2). Indien het kinderpornografische materiaal op een server staat die in een van deze landen wordt gehost, dan halen deze landen op verzoek van het KLPD de betreffende content van het internet. Er zijn geen cijfers bekend over het aantal internationale meldingen en de wijze waarop hieraan een gevolg wordt gegeven.

Er zijn echter ook meldingen van kinderporno die in landen zijn gehost waarmee geen rechtshulpverdrag of andersoortig verdrag is afgesloten. Er is dan geen mogelijkheid om de content fysiek van het internet te verwijderen. Indien het gaat om een website, dan kan de betreffende site wel worden geblokkeerd door ISP's in Nederland. Het KLPD heeft hiertoe in navolging van en analoog aan de wijze van blokkeren in Noorwegen een eerste stap gezet. Websites met kinderporno die in landen zijn gehost waarmee geen samenwerkingsverband bestaat, worden op een zogenaamde blacklist geplaatst. Internetproviders kunnen op vrijwillige basis websites met kinderporno blokkeren. Hiervoor kan een convenant worden afgesloten met het KLPD (zie hoofdstuk 6 en bijlage IV). In het convenant is vastgelegd dat de ISP voor haar abonnees de toegang tot websites blokkeert die door het KLPD zijn geïdentificeerd als websites met content die binnen de reikwijdte valt van het verbod van artikel 240b van het Wetboek van Strafrecht. Het zedenteam van het KLPD neemt dus de facto het besluit of de content wel of niet kinderpornografisch is. Het KLPD vermeldt in een interview dat zij hierbij gebruik kunnen maken van de Landelijke Database Kinderpornografie van het KLPD (zie vorige subparagraaf over de politiedatabank).

De ISP's waarmee een convenant is gesloten, blokkeren op domeinnaam (zie hst 2). De DNS-server levert niet het IP-adres van de op de blacklist vermelde website, maar leidt de gebruiker naar het IP-adres met de 'stoppagina' van het KLPD (zie figuur 5.2). Op deze pagina staat uitleg over de blokkade. Ook vermeldt de pagina een e-mailadres waar de bezoeker zich kan melden als hij meent dat de blokkade onterecht is. Het KLPD levert elke twee maanden een geactualiseerde versie van de blacklist aan. De ISP brengt hier geen wijzigingen in aan.

Figuur 5.2 De 'stop-pagina' van het KLPD



Drie ISP's hebben op dit moment een convenant met het KLPD afgesloten over het blokkeren van websites met kinderporno. Dit zijn UPC, Kliksafe en Scarlet. Het KLPD is nog in onderhandeling met andere ISP's.

Van 31 augustus 2007 tot 13 september 2007 zijn er 39.000 hits geweest op websites die op de blacklist staan. Net zoals in Scandinavië (zie hoofdstuk 4) wordt dit substantiële aantal hits door enkele respondenten in Nederland als een indicatie beschouwd van het 'grote aantal personen met belangstelling voor kinderporno.' Het is echter niet bekend hoeveel unieke ip-adressen (unieke gebruikers) hebben geprobeerd om de geblokkeerde websites te bezoeken. Ook is niet bekend hoe vaak unieke ip-adressen hebben geprobeerd om in te loggen. Bovendien blijkt uit interviews met technische experts dat het aantal geregistreerde hits ook voor een deel kan worden veroorzaakt door zoekmachines (zoals Google) die met geautomatiseerde programma's (zogenoemde 'crawlers') het internet afstruinen op zoek naar nieuwe informatie. Uit de cijfers kan daarom niets geconcludeerd worden over de omvang van het probleem of effectiviteit van het filter.

5.3 Effectiviteit van verwijderen en filteren

Het fysiek verwijderen van kinderpornografisch materiaal op internet is zonder meer effectief: de content wordt niet geblokkeerd, maar volledig uit de lucht genomen. Bij de duurzaamheid van deze maatregel kunnen echter vraagtekens worden geplaatst. De door ons geïnterviewde zedenrechercheurs geven aan dat de inhoud van verwijderde sites toch weer snel opduikt op allerlei andere sites. Internet is wereldwijd en kinderpornografisch materiaal kan op vele manieren worden aangeboden, gedownload en weer zichtbaar worden gemaakt.

Het blokkeren van websites aan de hand van een blacklist, werpt voor gebruikers een extra drempel op om toegang te verkrijgen tot kinderporno op internet. Ook kan worden gesteld dat (commerciële) aanbieders hun producten minder gemakkelijk aan hun doelgroep kunnen aanbieden. Op internetfora wordt het initiatief van het KLPD door veel mensen toegejuicht. De morele verontwaardiging ten aanzien van kinderporno is groot en elke daad om misbruik en exploitatie van kinderen tegen te gaan, lijkt daarmee gerechtvaardigd. Maar niet alle geluiden zijn positief. De blacklist staat eveneens ter discussie. Sceptici betwijfelen de accuraatheid van de lijst. Zo noemt Frank Kuitenbrouwer, medewerker van NRC Handelsblad, het blokkeren van websites 'een technische storing waar door zowel aanbieders als gebruikers simpelweg omheen kan worden gerouteerd.' De structuur van internet biedt ook vele mogelijkheden voor alternatieve routes. Het is mogelijk – en volgens technische experts vaak ook de praktijk – dat de inhoud van een verboden website vrijwel direct wereldwijd op allerlei andere websites verschijnt. Een ander kritiekpunt betreft *overblocking*. De inhoud van websites kan veranderen: door te blokkeren wordt niet alleen de toegang ontzegd tot de huidige content, maar ook tot de (legale) content die in de toekomst op de website kan komen te staan. De advocaat Remy Chavannes spreekt in het laatste geval over preventieve censuur. Het voorkómen van onrechtmatig blokkeren vraagt om het voortdurend up-to-date houden van de blacklist. Een laatste kritiekpunt heeft betrekking op het ontbreken van transparantie in de samenstelling van de lijst. Critici vinden dat het bepalen van hetgeen internetgebruikers wel of niet mogen zien geen taak is van de politie. Uitsluitend een rechter zou kunnen bepalen of een website strafbare of onrechtmatige content bevat. Het feit dat het KLPD de afweging maakt om een website wel of niet te blokkeren, impliceert volgens de critici een vertroebeling van verantwoordelijkheden. Bovendien kan een resultante van genoemd gebrek aan transparantie zijn dat het recht op vrije informatievergaring van burgers ten onrechte wordt beperkt.

De ISP's waarmee een convenant is gesloten, blokkeren op domeinnaam. Zoals we in hoofdstuk twee reeds hebben beschreven, is dit niet de meest fijnmazige methode. De kans op *overblocking* is vrij groot. Verder komt in de interviews met technische experts steeds naar

voren dat het blokkeren op domeinnaam relatief gemakkelijk is te omzeilen. Op de eerste plaats kan de blokkade door de gebruiker worden omzeild door rechtstreeks het numerieke ip-adres in te typen. Als de gebruiker het ip-nummer niet kent en toch toegang wil hebben tot de geblokkeerde sites, kan hij abonnee worden van een andere provider (in of buiten Nederland) waarmee geen convenant is afgesloten. Zo zijn er in Nederland op dit moment circa 300 ISP's die het internetverkeer faciliteren en heeft het KLPD met slechts drie ISP's een convenant afgesloten. Ten slotte is het voor een gebruiker ook mogelijk om zelf een DNS-server op zijn computer aan te sluiten waardoor hij – zonder tussenkomst van de provider – toegang blijft behouden tot alle sites. In het verlengde hiervan attenderen de technische experts ons op een arsenaal aan websites waar commerciële aanbieders DNS-servers te koop aanbieden voor thuisgebruik en op (non-profit) websites waar tot in detail wordt uitgelegd hoe gebruikers zelf een DNS -server kunnen maken of op andere wijze internetfilters kunnen omzeilen (bv. www.peacefire.org).

Ter relativering van het bovenstaande moet opgemerkt worden dat toch wel enige kennis is vereist om een DNS-blokkade te kunnen omzeilen. Het is zeer plausibel dat de gemiddelde internetgebruiker niet de technische know-how voorhanden heeft om een alternatieve route te bedenken waarmee de door de DNS-server opgeworpen blokkade kan worden ontweken. Tegelijk moet het voor mogelijk worden gehouden dat tegenstanders van filtering anti-filtersoftware op het internet plaatsen die ook voor leken eenvoudig op de computer is te installeren. Een voorbeeld hiervan is te vinden op www.zensur.freerk.com, waar internetters tot in detail uitleg krijgen aangaande 'how to bypass internet censorship.'

5.4 Resultaten schouw blacklist KLPD

Om inzicht te krijgen in de criteria waarmee het KLPD de blacklist samenstelt en de wijze waarop het KLPD de blacklist actualiseert, hebben de onderzoekers twee keer een bezoek gebracht aan het KLPD te Zoetermeer.

Direct voorafgaand aan de eerste schouw is gevraagd aan het hoofd van het team Bestrijding Kinderporno van het KLPD welke criteria worden gehanteerd om te kunnen vaststellen of de content strafbaar in de zin van artikel 240b WvSr. Het KLPD hanteert de volgende criteria:

- Een rechercheur bepaalt of er sprake is van een afbeelding van een seksuele handeling waarbij een minderjarige ('iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt) is betrokken;
- Indien er geen sprake is van een expliciete seksuele handeling – de jeugdige is alleen afgebeeld - wordt gekeken naar zowel het karakter van de afbeelding als de context van de afbeelding (o.a. onnatuurlijke pose, aanwezigheid voorwerpen met een seksueel karakter). Deze uitbreiding op het eerder genoemde begrip 'seksuele handeling' is op aanwijzing van het College van Procureurs-generaal. Als zowel het karakter als de context van de afbeelding sterk seksueel getint zijn, wordt de afbeelding alsnog als kinderpornografisch bestempeld. In geval van twijfel wordt incidenteel een tweede rechercheur geraadpleegd.

Bij de beoordeling wordt niet gewerkt aan de hand van de criterialijst voor kinderpornoonderzoeken die is opgesteld door het College van Procureurs-generaal en in werking is getreden op 1 september 2007[120]. Het KLPD heeft omtrent het beheer van de blokkeerlijst geen procedures vastgelegd en heeft geen protocollen met criteria op basis waarvan een specifieke site wordt beoordeeld om al dan niet aan de blacklist te worden toegevoegd.

[120] In genoemde criterialijst worden de afbeeldingen getypeerd als 1) (pre)puberaal (<14 jaar) of postpuberaal (14-18 jaar); 2) onbekend of bekend materiaal; 3) oud, recent of nieuw materiaal; 4) aanwezigheid rechercheerbare elementen op de afbeelding; 5) bekendheid met dader en/of slachtoffer; 6) check door digitale expert; 7) beschrijving van materiaal: handelingen-geweld-poseren-karakter-context-leeftijd.

Tijdens beide schouws is onderzocht wat precies de aard en de herkomst is van de informatie die op dit moment wordt geblokkeerd. Tevens is beoordeeld of er sprake is van overblocking. Om te kunnen verifiëren of het op een website getoonde beeldmateriaal strafbaar is volgens art. 240b Sr, hebben naast de onderzoekers ook enkele deskundigen meegekeken. Naast de onderzoekers waren tijdens de eerste schouw rechercheurs van het KLPD en medewerkers van het particuliere Meldpunt Kinderporno op Internet aanwezig. De tweede schouw werd uitgevoerd door een van de onderzoekers en een rechercheur van het KLPD.

We selecteerden de eerste keer uit de lijst van 110 sites steekproefsgewijs een serie van 36 en de tweede keer uit de lijst van 103 een serie van 34 sites. We selecteerden beide keren elke derde site op de lijst. Een medewerker van het KLPD toonde ons de betreffende sites, die we vervolgens beoordeelden aan de hand van een protocol (bijlage III).

Resultaten eerste schouw

De blacklist van het KLPD bevat tijdens de eerste schouw in totaal 110 domeinnamen. Dit betekent dat de omvang van de aanvankelijke lijst sinds de introductie ervan in september 2007 met bijna 60 procent is gereduceerd (van 250 sites naar 110 sites). Het KLPD heeft de blacklist zes weken voorafgaand aan de schouw voor het laatst geactualiseerd.

Tabel 5.1 Resultaten eerste schouw blacklist

Aantal sites	Toegankelijkheid site	Land van herkomst host	Kinderporno
4	Site bestaat niet meer	1 USA 2 Nederland 1 host onbekend	n.v.t.
1	Site heeft geen content	1 USA	n.v.t.
2	Site is vrij toegankelijk	2 USA	Geen kinderporno
29	Site is vrij toegankelijk	1 Engeland 4 Nederland 24 USA	Sites bevatten kinderporno

Van de 36 onderzochte domeinen die thans worden geblokkeerd, zijn 4 sites inmiddels opgeheven. Eén site heeft geen inhoud: de bezoeker ziet slechts een lege pagina. Van de 31 sites die wel bestaan, bevatten er twee, ook naar het oordeel van de politie, geen kinderporno. Op de sites worden wel kinderen afgebeeld, maar de afbeeldingen zijn niet pornografisch. Omgerekend naar percentage blijkt dat 20 procent van de websites uit de steekproef ten onrechte in de blacklist staat vermeld.[121]

De overige 80 procent van de sites bevat allemaal evidente kinderporno. De betreffende websites zijn vrijwel allemaal volgens eenzelfde stramien opgebouwd: elke site bestaat uit circa 15 à 25 symmetrisch geordende fotografische afbeeldingen van minderjarigen. Op de meeste foto's staat een minderjarige alleen afgebeeld, soms helemaal gekleed, soms deels gekleed en soms naakt. De jeugdigen zijn vrijwel steeds in een onnatuurlijke pose afgebeeld of in een seksueel getinte houding, waarbij een nadruk op de geslachtsdelen wordt gelegd. Op enkele foto's is duidelijk sprake van een seksuele gedraging, waarbij meestal een andere minderjarige is betrokken en incidenteel slechts een meerderjarige. Geen van de onderzochte sites bevat bewegende beelden. Ook bevat geen van de onderzochte websites virtuele kinderporno.

[121] Waarbij moet worden benadrukt dat in vijf van die gevallen de site niet meer bestond of geen inhoud bevatte. Dergelijke sites horen volgens het KLPD niet op de lijst thuis. In die gevallen wordt echter geen content ten onrechte geblokkeerd. Dat is alleen het geval in de twee gevallen waarin wel content maar geen kinderporno werd aangetroffen.

Dat wil zeggen dat geen van de afbeeldingen met behulp van (digitale) manipulatie zijn vervaardigd. Tot slot hebben geen van de aangetroffen handelingen een expliciet gewelddadig karakter, wel is er – vooral wanneer er sprake is van een seksuele handeling met een meerderjarige – sprake van machtsmisbruik.

Alle onderzochte websites zijn vrij toegankelijk: de gebruiker heeft geen autorisatie nodig om de inhoud van de website te kunnen bekijken. Het kinderpornografische materiaal is direct op domeinniveau aanwezig; het is dus niet zo dat de gebruiker eerst naar een onderliggend niveau moet doorklikken om zich toegang te kunnen verschaffen tot de strafbare content. Overigens bieden alle 29 geblokkeerde websites wel de mogelijkheid om door te klikken naar andere afbeeldingen of films. Rechercheurs van het KLPD geven aan dat de meeste geblokkeerde websites als centrale portal fungeren, bedoeld om de interesse van gebruikers op te wekken. Wanneer de gebruiker via de aangeboden links op de website probeert om toegang te krijgen tot meer pornografisch materiaal zal hij in de meeste gevallen eerst moeten betalen. Door te blokkeren op domeinniveau krijgt de gebruiker dus ook geen toegang meer tot de onderliggende (veelal) commerciële sites en wordt de makers een mogelijke inkomstenbron ontnomen.

Vier van de websites met een strafbare content zijn in Nederland gehost. Deze sites zijn door het KLPD niet aan de betreffende hosts gemeld en daarom zijn deze sites ook nog niet verwijderd. Door politie en justitie is eveneens nog niet ingegrepen: er is nog geen zaak gestart om de eigenaars van de site op te sporen en te vervolgen. Eén site die we bezochten is gehost in Engeland, alle overige in de Verenigde Staten. Zoals eerder vermeld zijn de Verenigde Staten en Engeland vertegenwoordigd in het CIRCAMP project. Het is dus mogelijk om melding te doen aan de politionele zusterorganisaties in deze landen, waarna de sites zouden moeten worden verwijderd en in de betreffende landen een rechercheonderzoek kan worden gestart. Ook dit is blijkbaar niet gebeurd.

Resultaten tweede schouw

De lijst van het KLPD is mede op basis van onze eerste schouw, teruggebracht naar 103 websites. Ook nu treffen we enige 'vervuiling' aan. Twee van de 34 aselect onderzochte domeinen bestaan niet meer en één site blijkt (inmiddels) ten onrechte te worden geblokkeerd. De overige 31 sites bevatten wel kinderpornografisch materiaal. Op twee sites treffen we ditmaal ook virtuele kinderporno aan (een enkel plaatje tussen een mix van gewone porno en kinderporno). De 31 websites met kinderporno zijn allen vrij toegankelijk. Net zoals bij de eerste schouw fungeren de meeste sites als een soort portal en bevatten een mix van gewone porno en kinderporno. De kinderporno valt doorgaans in de categorie van 12-plussers. [122] Er zijn slechts drie websites waar expliciet kinderporno met zeer jonge kinderen op voorkomt. Twee van deze sites zijn gehost in de VS en één in Engeland). Ook richt een aantal sites zich op incest, waarbij kinderen misbruikt worden.

Daarnaast vinden we drie sites die in een vrij grijs gebied liggen. Ook de internetrechercheur van het KLPD heeft twijfels of de afbeeldingen wel als kinderpornografisch zijn te bestempelen. Hij vermoedt dat de betreffende sites toch op de lijst staan, omdat de getoonde afbeeldingen overeenkomen met afbeeldingen uit de politiedatabank. Aangezien er bij de tweede schouw geen zedenrechercheurs aanwezig waren, kon hierover geen uitsluitsel worden gegeven.

[122] Een schatting van de onderzoeker, geen vaststaand feit.

Tabel 5.2: Resultaten tweede schouw blacklist

Aantal sites	Toegankelijkheid site	Land van herkomst host	Kinderporno
2	Site bestaat niet meer	1 Nederland 1 host onbekend	n.v.t.
1	Site is vrij toegankelijk	1 USA	Geen kinderporno
31	Site is vrij toegankelijk	1 Belize 1 Frankrijk 1 Oekraïne 1 Rusland 2 Korea 3 Engeland 22 USA	Sites bevatten kinderporno

Slotbeschouwing

Uit beide schouws komt op de eerste plaats naar voren dat zeer regelmatige (wellicht dagelijkse) controle is vereist om de blacklist up-to-date te houden. De sites op de blacklist die thans in Nederland zijn gehost, hadden bij tijdige controle immers direct uit de lucht kunnen worden gehaald en justitieel kunnen worden aangepakt. De internetrechercheur van het KLPD geeft aan dat de makers/eigenaars van websites met kinderporno hun sites zeer frequent op een andere plaats hosten om zodoende verwijdering van de site en vervolging te voorkomen. Op het moment van plaatsing op de lijst zouden de betreffende sites nog in het buitenland zijn gehost en daarmee buiten het bereik vallen van het KLPD. Het blijft echter merkwaardig dat de eigenaren van de sites ervoor hebben gekozen om hun website in een later stadium in Nederland te hosten waar zowel verwijdering als vervolging reële mogelijkheden zijn. Hetzelfde geldt overigens voor de Verenigde Staten en Engeland. Vooraf hadden we de verwachting – mede op basis van interviews met diverse zedenrechercheurs - dat de meeste sites in landen als Wit-Rusland of de Oekraïne zouden zijn gehost. Deze schouw heeft echter uitgewezen dat hiervan geen sprake is.

Volgens het KLPD vraagt het opstellen en actualiseren van de blacklist veel tijd. Een rechercheur spreekt zelfs over een onevenredig grote aanslag op de beschikbare capaciteit binnen het korps. 'Dit experiment is, mede gezien de commotie eromheen, enigszins uit de hand gelopen. We zijn een weg ingeslagen die onomkeerbaar lijkt en waarvan de resultaten vooralsnog onduidelijk zijn.' Het team Bestrijding Kinderporno ziet zeker belang bij het opwerpen van een drempel om gebruikers de toegang tot kinderporno op internet te ontzeggen, maar ziet dit zeker niet als een hoofdtaak: 'Onze eerste prioriteit is het achterhalen van de slachtoffers en het vervolgen van de daders.' Overigens zijn de rechercheurs van het KLPD wel van mening dat zij gezien hun expertise en ervaring de aangewezen partij zijn om te bepalen of content al dan niet strafbaar is. In dit kader geven ze ook aan dat bij een rechterlijke toets de rechter in kwestie zijn uitspraak vrijwel altijd baseert op het oordeel van het team Bestrijding Kinderporno van het KLPD. 'De meeste rechters hebben geen behoefte om zelf kennis te nemen van het als kinderpornografisch bestempelde materiaal en baseren zich bij hun oordeel uitsluitend op onze beschrijving van het materiaal om de strafbaarheid ervan te kunnen bepalen'.

Kerntakendebat

Politiemensen bij het KLPD ervaren de tijdsinvestering die het (goed) bijhouden van de blacklist vergt, als een onevenredig grote aanslag op hun beschikbare tijd. Dat roept de vraag op hoe het bijhouden van een blacklist zich verhoudt tot het zogenoemde kerntakendebat (Van der Vijver e.a. 2001, Van der Vijver 2004). De kern van dat debat is de vraag welke werk-

zaamheden de politie gezien haar wettelijke taakstelling zeker moet doen (kerntaken) en welke werkzaamheden zij beter kan beëindigen en aan anderen overlaten – zodat meer tijd vrijkomt voor de specifieke kerntaken.

Volgens de eerste twee kabinetten Balkenende voerde de politie haar wettelijke plicht tot hulpverlening te ruim uit en moest de politie zich meer concentreren op haar eigenlijke kerntaken: toezicht, handhaving, noodhulp en vooral opsporing (Nota 2002, 2003). Daarbij komt, aldus de veiligheidsnota uit 2003, dat resultaten van politiewerk in meetbare termen moeten kunnen worden gevat. In managementcontracten dienen kwantificeerbare doelstellingen te worden opgenomen waarop politiechefs worden afgerekend.

In de zogenoemde kerntakenbrief van 15 juli 2004[123] trachten de politieministers de taken van de politie in te kaderen. De primaire politietaak is criminaliteitsbestrijding en daartoe verricht de politie opsporingsactiviteiten.[124] Over het door de politie geïntroduceerde 'tegenhouden' (populair gezegd: het dwarsbomen van criminelen zodat zij hun misdadige plannen niet ten uitvoer kunnen brengen), schrijven de politieministers: 'Deze werkwijze gaat niet ten koste van het opsporen van criminelen, maar is aanvullend aan de opsporingstaak: de politie beziet in het onderzoek tevens hoe criminele processen verlopen en op welke wijze en door welke instantie drempels opgeworpen kunnen worden om de criminele activiteiten onmogelijk te maken.' Dat betekent niet dat de politie zich moet storten op allerlei preventieve werkzaamheden; zij dient juist een wat andere rol te kiezen, aldus de ministers: 'minder uitvoerend, meer signalerend en adviserend daar waar anderen verantwoordelijk zijn.'[125]

Het vierde kabinet Balkenende noemt in haar coalitieakkoord veiligheid een kerntaak van de overheid. Ze vertaalt dat direct naar criminaliteitsbestrijding, waarvan het voorkomen van crimineel gedrag deel uitmaakt. Het coalitieakkoord rept herhaaldelijk van criminaliteitspreventie als onderdeel van veiligheidsbeleid. Maar dat moet echter niet leiden tot nieuwe ballast: 'Het functioneren van politie en OM wordt versterkt; er wordt optimaal gebruik gemaakt van nieuwe technologie om het ophelderingspercentage te verbeteren. Knelpunten worden weggenomen en er komen geen nieuwe belemmeringen, procedures of beperkingen.' (Nota 2007:33).

Past het bijhouden van een blacklist in dit beleid? Om te beginnen is er nu in vergelijking met enkele jaren terug in het denken over politiekerntaken weer meer ruimte voor criminaliteitspreventie, speciaal in de vorm van 'tegenhouden' (dwarsbomen van criminelen). Filteren van internet kan men daaronder scharen voor zover dat is gericht op het verstoren van criminele activiteiten (de aanbieders). Het beschermen van burgers tegen ongewilde confrontatie met kinderpornografie is geen 'tegenhouden' maar is gericht op het voorkomen van slachtofferschap. Deze klassieke preventievorm (een soort helpen aanbrengen van hang- en sluitwerk, maar dan in de virtuele wereld) is niet echt goed af te leiden uit de actuele beleidsuitgangspunten. Dan rest nog de vraag of de politie zelf de blokkerlijst moet bijhouden of dat liever dient over te laten aan een andere partij. Op grond van de kerntakenbrief ('minder uitvoerend, meer signalerend en adviserend') en het coalitievoornemen om geen nieuwe belemmeringen, procedures en beperkingen bij de politie te introduceren, ligt het voor de hand dat de politie niet zelf een blacklist gaat onderhouden (met alle juridische complicaties van dien, zie hoofdstuk 3 en 6) maar dat overlaat aan andere partijen, zoals particuliere informatiebeveiligingsbedrijven of een non-profitorganisatie zoals het particuliere Meldpunt Kinderporno op Internet.

[123] TK 2003-2004, 29628, nr. 4

[124] Andere kerntaken die de ministers noemen zijn: handhaving van de openbare orde, het verlenen van noodhulp, signaleren en adviseren.

[125] TK 2003-2004, 29628, nr.4, blz. 6-7.

5.5 Samenvatting

In Nederland wordt een levendige politiek-maatschappelijke discussie gevoerd over de wijze waarop de verspreiding van kinderporno op internet kan worden tegengegaan. De discussie beweegt zich tussen twee polariteiten, waarbij enerzijds de gevaren van internetcensuur worden benadrukt en anderzijds de noodzaak van een daadkrachtig optreden waarin elke maatregel lijkt te zijn gerechtvaardigd. Ook de huidige regering wil een daad stellen in de bestrijding van kinderporno en daarmee gehoor geven aan de morele verontwaardiging in de samenleving.

Op dit moment kunnen websites met kinderpornografisch materiaal die in Nederland zijn gehost door de hosting provider fysiek worden verwijderd. Is het materiaal gehost in een land waarmee Nederland een rechtshulpverdrag heeft gesloten, dan zal het materiaal na een daartoe strekkend verzoek vanuit Nederland door het desbetreffende land verwijderd (dienen te) worden. Voor websites die in landen zijn gehost waarmee Nederland geen rechtshulpverdrag heeft, zal dit niet altijd mogelijk blijken. Een optie die dan overblijft is het blokkeren van sites. Het KLPD heeft hiertoe in navolging van en analoog aan de wijze van blokkeren in Noorwegen een eerste stap gezet.

Uit dit onderzoek blijkt dat de blacklist van het KLPD op basis waarvan ISP's kinderpornosites kunnen blokkeren, slechts een topje van de ijsberg representeert. De lijst heeft namelijk betrekking op circa 100 websites, terwijl we menen vrij veilig te mogen aannemen dat het totale aantal kinderpornosites op internet – die vallen binnen de reikwijdte van art. 240b Sr – hiervan een veelvoud is. Verder blijkt uit de door ons uitgevoerde schouws dat de blacklist ook sites bevat die (inmiddels) niet meer bestaan of die (inmiddels) geen kinderporno meer bevatten. Tenslotte bevat de lijst ook diverse sites die worden gehost in Nederland en bestaat de lijst voor het overige overwegend uit sites die worden gehost in landen waarmee Nederland rechtshulpverdragen heeft (vooral de VS) – terwijl we op grond van interviews vooraf in de overtuiging verkeerden dat de lijst juist zou zijn gericht op sites in landen waarmee Nederland geen rechtshulpverdrag heeft en waarbij dus verwijderen en opsporen niet tot de opties behoort. Wellicht vinden we een deel van de verklaring hiervoor in de uitspraak van het team Bestrijding Kinderporno dat het starten van een onderzoek weliswaar hoogste prioriteit heeft maar dat buitenlandse sites op de blokkeerlijst komen als direct politieoptreden lastig is of lang gaat duren (paragraaf 5.2).

Het KLPD heeft aangaande het beheer van de lijst geen procedures vastgelegd en zij heeft geen protocollen met criteria op basis waarvan sites worden beoordeeld. De vereiste tijdsinvestering voor het actualiseren van de blacklist vormt, gezien de opsporingstaak van het KLPD, een onevenredig grote aanslag op de beschikbare tijd van de rechercheurs. Mede in het licht van het kerntakendebat is het dan ook de vraag of deze taak niet aan andere partijen zou moeten worden overgelaten.

HOOFDSTUK 6

Juridische analyse filterpraktijk in Nederland

6.1 Inleiding

Het KLPD werkt samen met drie ISP's, op basis van een convenant waarvan de tekst is opgenomen in bijlage IV. Deze tekst is in belangrijke mate ontleend aan het in Noorwegen gebruikte convenant (zie hoofdstuk 4). Inmiddels lopen nog onderhandelingen met andere internet-providers.[126] Dit heeft geleid – en zal nog leiden – tot aanpassing en aanvulling van de tekst van het convenant. Voor een uitvoerige bespreking van de teksten van nog te sluiten convenanten is in deze studie geen plaats. Dat is ook niet nodig want in essentie komt de strekking van de nog te onderhandelen convenanten op hetzelfde neer, zij het omgeven door mogelijk verschillende randvoorwaarden. Onderstaande tekst beperkt zich tot het convenant zoals weergegeven in bijlage IV.

In het onderstaande wordt geanalyseerd wat het convenant inhoudt, in hoeverre het KLPD bevoegd is tot het sluiten van een dergelijk convenant en welke juridische knelpunten zich in verband met het sluiten en de uitvoering van het convenant voordoen.

6.2 De strekking van het convenant

Een convenant wordt veelal gesloten tussen overheidsonderdelen onderling of tussen overheidsonderdelen en een of meer private partijen. Het onderwerp is onder meer het uitruilen van prestaties ter bereiking van bepaalde overheidsdoelen. Een convenant is geen overeenkomst in de zin van het Burgerlijk Wetboek, maar brengt wel gebondenheid met zich mee. Partijen zijn vrij om te bepalen op welke wijze zij de gevolgen van opzegging, niet-nakoming en andere zaken regelen. Anders dan bij een civielrechtelijke overeenkomst kan worden betwijfeld of nakoming van een convenant afdwingbaar is.[127] Het rechtskarakter van een convenant is daarom moeilijk te bepalen en hangt sterk samen met doel en inhoud van het convenant. Van de zijde van de overheid of van het overheidsorgaan gaat het in de meeste gevallen om de regeling van publiekrechtelijke bevoegdheden. Bevat een convenant privaatrechtelijke aangelegenheden dan treedt het overheidsorgaan op als privaatrechtelijk rechtspersoon.[128] Een convenant staat in geen geval gelijk aan een besluit in de zin van de Algemene wet bestuursrecht (Awb).

Het Convenant tussen het KLPD en een internet-provider bepaalt dat het KLPD aan de ISP-wederpartij een lijst aanlevert met (buitenlandse) domeinnamen die naar het oordeel van het KLPD kinderporno aanbieden of ter beschikking stellen. Het Convenant stelt geen voorwaarden aan de samenstelling van de lijst, welke criteria daarbij worden gehanteerd en op welke wijze in het onderhoud van de lijst is voorzien. Het KLPD verplicht zich algemeen gesteld tot het actueel houden van deze lijst. Het convenant laat de samenstelling van de lijst geheel aan de competentie van het KLPD. Deze lijst wordt, ten einde te voorkomen dat derden daarvan misbruik maken, versleuteld ter beschikking gesteld. Een gemuteerde lijst wordt periodiek – het convenant spreekt zich niet uit over de duur van deze periode – ter beschikking gesteld van de aangesloten providers. Zowel KLPD als providers verplichten zich tot geheimhouding van de inhoud van de lijst.

De overwegingen in de individuele bepalingen laten samengenomen geen andere conclusie toe dan dat de ISP zich *verplicht* om aanvragen van domeinnamen die zich op de door het KLPD geleverde zwarte lijst bevinden, te blokkeren en in plaats daarvan door te geleiden naar een website waarop de zogenoemde stoppagina staat (zie figuur 5.2). Artikel 3 eerste lid

[126] http://www.nu.nl/news/1527649/52/Grote_providers_weren_kinderporno.html geraadpleegd 21 april 2008.
[127] Convenanten: Naar goed gebruik, Bans-Werkgroep Convenanten, BZK 2001, p. 13, zie actuele verwijzing naar de notitie maart 2008 http://www.minbzk.nl/actueel/publicaties?ActItmIdt=7272
[128] Idem, p. 42.

van het Convenant luidt: 'De ISP verplicht zich de lijst onverwijld in gebruik te nemen.' De ISP is vrij om de techniek van de toe te passen (filter-)systemen te kiezen, maar heeft niet de vrijheid het gebruik ervan na te laten dan wel op door hemzelf gekozen momenten toe te passen, noch is het hem toegestaan om de (versleutelde) lijst bijvoorbeeld voor naar eigen keuze te bepalen deel toe te passen.

Het convenant geeft niet aan voor welke situaties toepassing van het convenant is bedoeld, zoals: gericht tegen buiten Nederland gehoste websites die door ontbreken of slecht functioneren van internationale rechtshulpinstrumenten buiten de greep van de Nederlandse justitie blijven.

In artikel 8 van het Convenant is bepaald dat de samenwerking het KLPD geen recht aanspraak geeft op 'informatie over de abonnees van de ISP'. Dit staat uiteraard buiten de wettelijke bevoegdheden tot het opvragen van persoonsgegevens, zoals geregeld in artikel 126na e.v. Sv, hoewel deze bepalingen alleen toepassing vinden in geval van verdenking van een (concreet en specifiek) strafbaar feit.

Hoewel niet met zoveel woorden gezegd, is de strekking (en de uitwerking) van het convenant dat de experts van het KLPD, die immers de zwarte lijst samenstellen, bepalen welke sites en welke informatie door deelnemende ISP's niet aan de daartoe toegang zoekende internetgebruiker wordt doorgegeven. Het convenant spreekt zich niet uit over de specifieke taak van het KLPD in verband met de bestrijding van kinderporno. Duidelijk is dat aansluiting gezocht moet worden bij de taken van politie en justitie ter bestrijding van kindermisbruik in het algemeen en van kinderporno in het bijzonder, zoals uitgevoerd door het team Bestrijding Kinderporno van het KLPD. Ter uitvoering van of ter assistentie bij de uitvoering van deze publiekrechtelijke taak sluit het KLPD een convenant met een of meer internetproviders.

Artikel 7 Convenant verplicht het KLPD tot vrijwaring van de provider voor civielrechtelijke aansprakelijkheid in verband met de uitvoering van het convenant. Aansprakelijkheid kan ontstaan bij fouten in de blacklist of bij toepassing van de blacklist bij gewijzigde doch niet opgemerkte omstandigheden. Het Convenant geeft geen regeling voor een klachtenprocedure. Bij het ontvangen van een klacht zal worden nagegaan of de blokkering dient te worden voortgezet dan wel dient te worden beëindigd.

Uit het bovenstaande volgt dat een ISP zich tegenover het KLPD verplicht tot het op diens instructie uitvoeren van filtering/blokkering van bepaalde internetverkeersstromen, zonder eigen toets of beslissing over uitvoeringsmodaliteiten. Het KLPD levert de lijst, de ISP blokkeert en leidt naar de stoppagina. Dat een ISP het convenant vrijwillig is aangegaan, ontneemt daaraan niet het verplichtende karakter. Evenmin is voor dit verplichtende karakter relevant dat een eventuele beëindiging van het convenant door een van de partijen niet aan termijnen of voorwaarden is gebonden en geen juridische sancties afroept.

Indien men het Convenant als een samenwerkingsovereenkomst zou willen zien, dient de ISP de mogelijkheid te hebben voor een eigen afweging ten aanzien van de werking en de inrichting van het filterinstrument. De ISP heeft dan de keuze om die afweging toe te passen of achterwege te laten. Dat zou betekenen dat de ISP kennis zou moeten nemen van de blacklist ten einde de werking daarvan te kunnen bepalen. Vanuit KLPD-gezichtspunt houdt het niet versleuteld vertrekken van de blacklist risico's in voor de onbedoelde verspreiding van kinderporno.

Is het KLPD bevoegd tot het sluiten van een convenant?

Anders dan aan de reguliere politieregio's is aan het KLPD door de wet geen rechtspersoonlijkheid verleend, maar heeft het de status van een agentschap. Dat betekent dat in beginsel de Minister van BZK bevoegd is, behoudens mandatering aan de korpschef KLPD. Op dat gebied bestond een regeling van 2001 en een van 2003, zeer recent vervangen door de regeling

van 2008.[129] In deze regelingen wordt het beheer in de zin van het derde lid van artikel 38 Polw, gemandateerd aan de korpschef KLPD. Het is niet onredelijk te veronderstellen dat het aangaan van convenanten ter uitvoering van de politietaak als beheer kan worden gezien. De korpschef KLPD is dus bevoegd tot het aangaan van overeenkomsten, convenanten daaronder begrepen. In algemene zin verzet de mandateringsregeling zich niet tegen het aangaan van convenanten met ISP's.

Is het KLPD inhoudelijk bevoegd tot het sluiten van dit convenant?
In het bovenstaande wordt vooronderstelt dat het KLPD ter uitoefening van zijn veronderstelde publiekrechtelijke taak tot het terugdringen van seksueel misbruik van kinderen door de bestrijding van de productie, de verspreiding en het bezit van kinderpornografie, over wettelijke bevoegdheden beschikt om internetverkeer in verband met kinderporno te (doen) filteren en blokkeren. In hoofdstuk 3 is al vastgesteld dat, zo de wet in een dergelijke bevoegdheid zou voorzien en deze bevoegdheid op de in het convenant bedoelde wijze toepassing zou kunnen vinden, deze niet aan het KLPD of aan de Minister van BZK toekomt. Nog daargelaten of de relevante bepalingen van het Wetboek van Strafrecht (artikel 54a) en het Wetboek van Strafvordering (artikel 125o) op filteren/blokkeren kunnen worden toegepast, richten deze bepalingen zich tot de Officier van Justitie (met machtiging van de rechter-commissaris), respectievelijk tot de Officier van Justitie (zonder zo'n machtiging). Gezien de aard van de maatregel tot filteren/blokkeren kan artikel 2 Polwet geen basis bieden voor een dergelijke bevoegdheid.

Kortom, het KLPD voorziet zich van een convenant met een privaatrechtelijke partij ter uitoefening van bepaalde activiteiten waartoe het zelf geen bevoegdheid heeft. Hierdoor wordt gehandeld in strijd met de voorwaarde dat een convenant tussen overheidsorgaan en privaatrechtelijke partijen publiekrechtelijke waarborgen en bevoegdheden niet op een onaanvaardbare wijze mag doorkruisen, zoals geformuleerd onder de zogenoemde Twee-wegenleer, zoals deze in de Nederlands rechtsorde toepassing vindt.[130] Op grond van die leer ontbeert het convenant rechtsgeldigheid.[131]

Ook al zou dit voor de uitvoering van blokkeringpraktijk geen consequenties hebben – ISP's zouden uitvoering aan het convenant kunnen geven vanuit hun gevoel van maatschappelijke verantwoordelijkheid – en al lijkt het risico klein dat andere belanghebbenden, zoals buitenlandse partijen, zich tegen die praktijk in rechte zullen verzetten, dan nog is het vanuit rechtstatelijk oogpunt ongewenst dat de overheid ter bereiking van een overigens legitiem doel gebruik maakt van dit juridisch ondeugdelijk middel.

Een tweede punt, waarvan het belang na voorgaande conclusie sterk wordt gerelativeerd, maar dat in andere omstandigheden zijn actualiteit kan behouden, betreft de vrijwaring. Op grond van de meest recente mandatering is de korpschef gemandateerd tot het aangaan van civielrechtelijke verplichtingen tot een bedrag van € 450.000,- (excl. Btw). Aangezien het convenant met meerdere ISP's is en wordt afgesloten kan dit bedrag te beperkt zijn. In dat geval treedt beter de korpsbeheerder (de Minister van Binnenlandse Zaken) op als wederpartij voor de vrijwaringsverplichting. Over de omvang en effectiviteit van een vrijwaringsbeding in een relatie tussen een overheidsorgaan en private partijen bestaan geen wettelijke regels. Als inspiratiebron dient hier rechtspraak met betrekking tot door de overheid verleende zogenoemde vrijwarende vergunningen. Uit deze rechtspraak valt af te leiden dat de omvang van de vrijwaring aan beperkingen onderhevig kan zijn. Al zal het vrijwaringsbeding voor de meeste situaties aan de verwachtingen voldoen, ISP's houden een zekere eigen verantwoorde-

[129] Stcrt 2001, 249, p.7; Stcrt 2003, 161, p. 6; Stcrt 2008, 54, p. 10.
[130] HR 26 januari 1990, NJ 1991, 393, AB 1990, 408. Zie voor bevoegdhedenovereenkomsten HR 3 APRIL 1998, NJ 1998, 588, AB 1998, 241.
[131] Bans-Werkgroep, *a.w.*, p. 44.

lijkheid, die niet in alle gevallen op de Staat der Nederlanden kan worden afgewenteld[132], zeker indien zijzelf fouten zouden maken bij het juist, volledig en tijdig implementeren van de lijst.

6.3 De blacklist van het KLPD

Inleiding
Alle in de blacklist opgenomen sites bevatten een of meerdere afbeeldingen uit onderstaande categorieën (gemengd karakter):
- Afbeeldingen welke zonder meer vallen onder de in de Aanwijzing genoemde criteria.
- Afbeeldingen van naakte minderjarigen die niet aan deze criteria voldoen. Dit is niet altijd eenvoudig vast te stellen.
- Pornografie waarbij geen kennelijk minderjarigen zijn betrokken.
- Overige tekst en beeldinformatie betreffende de inrichting en de gebruiksaanwijzing van de site en de wijze waarop eventueel beeldmateriaal kan worden verkregen.

De inrichting van de sites is niet statisch, maar onderhevig aan veranderingen, waarbij nieuw of ander materiaal wordt geplaatst en/of wijziging wordt gebracht in de verhouding tussen de hierboven genoemde categorieën gegevens. In sommige gevallen wordt dit mogelijk opzettelijk gedaan om opsporingsautoriteiten te misleiden of om filtercriteria te omzeilen.

In de literatuur en in het debat over filtering wordt wel de eis gesteld dat sites met kinderpornografisch materiaal pas geblokkeerd mogen worden indien door de rechter is vastgesteld dat die sites dergelijk strafbaar materiaal bevatten of beschikbaar stellen.[133] Deze eis is weliswaar begrijpelijk, maar in de praktijk niet uitvoerbaar. Voorafgaand aan het blokkeren van bepaalde afbeeldingen of bepaalde sites met afbeeldingen, zou dan namelijk voor iedere nog niet eerder door een rechter beoordeelde afbeelding of iedere nog niet eerder door een rechter beoordeelde site steeds een rechterlijk oordeel moeten worden gevraagd. Het is daarom niet onredelijk om bij het bepalen of sprake is van strafbare kinderporno op het oordeel van de zedenexperts te vertrouwen. Dat oordeel moet dan wel toetsbaar zijn, in het bijzonder met betrekking tot:
a. Welke criteria liggen aan de beslissing om een site in de lijst op te nemen ten grondslag?
b. Wanneer en met welke regelmaat is geconstateerd dat de site (nog) aan die criteria voldoet?
c. Is strafrechtelijk optreden tegen de betreffende aanbieder van kinderporno niet alsnog mogelijk of wordt dit niet alsnog ondernomen?
d. Kan tegen opname in de lijst in rechte worden opgekomen?

We gaan op deze vier punten achtereenvolgens kort in.

Criteria voor opname?
Dat houdt niet alleen een oordeel in over de strafbare afbeelding(en) die wordt of worden aangeboden, maar – in geval men blokkeert op domeinniveau, zoals nu de praktijk is – ook een oordeel over de verhouding met de overige informatie op het betreffende domein die wanneer men het domein blokkeert in de vorm van *overblocking* wordt tegengehouden. Met artikel 10 EVRM voor ogen dient te worden nagegaan hoe het tegenhouden van die informatie zich verhoudt met de proportionaliteitseis van het tweede lid. Duidelijk is dat informatie op een site die zelf niet strafbaar is maar die ten dienste staat van het aanbod van de strafbare

[132] HR, 10 maart 1972, AB 1972, 193 (Vermeulen / Lekkerkerker), HR 17 januari 1997, AB 1997, 265 (Franse Kalimijnen), HR 21 oktober 2005, NJ 2006, 418 (Ludlage / Paradijs).
[133] Zie o.a Karin Spaink, Het Parool, 19 februari 2008, p. 13.

kinderporno, rechtmatig kan worden geblokkeerd. In andere gevallen, wanneer er geen duidelijk verband is tussen de kinderporno en de overige informatie of wanneer de (hoeveelheid) kinderporno van volstrekt ondergeschikte betekenis is aan de overige informatie, kan die afweging anders uitvallen. Het verdient aanbeveling hiervoor criteria te ontwikkelen en deze in de zogenoemde Aanwijzing op te nemen.

Controle op actualiteit?
Het CEOP (UK) – zie de beschrijving in paragraaf 4.4 – geeft aan dat zij vanwege het dynamische karakter van internet vrijwel elke dag nagaat of een gefilterde site nog in de lucht is en of deze nog kinderporno bevat. Genoemde periodiciteit steekt schril af tegen de door het KLPD (vanwege een tekort aan menskracht) gehanteerde periode voor controle van de actualiteit van de blacklist (zie paragraaf 5.4). Zoals in paragraaf 3.9 betoogd, is een adequate en frequente controle vereist ten einde te voorkomen dat het KLPD als onderdeel van de overheid een ontoelaatbare inbreuk maakt op de vrijheid van meningsuiting, zoals verwoord in artikel 10 EVRM en artikel 7 GW. Uiteraard dient administratie te worden gehouden van de periodieke controles.

Mogelijkheid tot strafrechtelijk optreden
In de steekproef zijn enkele gevallen aangetroffen die in het kader van een opsporingsonderzoek of NTD-procedure tot verwijdering van het strafbare materiaal hadden kunnen leiden. Enkele sites bleken namelijk in Nederland te zijn gehost. Strafrechtelijk optreden door het KLPD zou in die gevallen tot een effectief resultaat hebben moeten leiden. Verreweg de meeste sites van de lijst bleken te zijn gehost in landen waarmee Nederland een juridisch samenwerkingsverdrag in werking heeft en samenwerkt in het CIRCAMP-project ter bestrijding van kindermisbruik. Ook in die gevallen ligt (het initiëren van) strafrechtelijk optreden binnen de mogelijkheden. We hebben niet onderzocht of tegen de sites in de blokkeerlijst die zijn gehost in landen waarmee Nederland een justitieel samenwerkingsverdrag heeft, al dan niet een onderzoek is gestart. Het team Bestrijding Kinderporno verklaart dat het starten van een onderzoek weliswaar hoogste prioriteit heeft maar dat buitenlandse sites op de blokkeerlijst komen als direct politieoptreden lastig is of lang gaat duren (paragraaf 5.2). In dergelijke gevallen fungeert de lijst dus als (tijdelijk) alternatief voor strafrechtelijk optreden.

Bezwaren tegen opname
Het KLPD geeft aan domeinen van de lijst te verwijderen indien over de blokkering terecht wordt geklaagd. Klachten kunnen het KLPD bereiken via de aangesloten ISP's of direct van een domeineigenaar/belanghebbende die een klacht mailt naar het voor dat doel op de stoppagina aangegeven e-mailadres (kinderpornofilter@klpd.politie.nl, zie figuur 5.4). Duidelijkheid over de mogelijkheid van indienen en wijze van behandeling van klachten is wenselijk, niet alleen tegenover ISP's maar ook tegenover het publiek. De lijst dient echter van een zodanige kwaliteit en actualiteit te zijn dat klachten achterwege blijven. De in de vorige alinea's genoemde punten dragen hieraan in belangrijke mate bij. Ons onderzoek strekte zich niet uit tot de wijze waarop precies is voorzien in een onafhankelijke behandeling van eventuele klachten als gevolg van filteren en blokkeren.

6.4. Naar een wettelijke filterplicht?
In het bovenstaande zijn elementen aangedragen, die relevant zijn indien men een wettelijke filter- en blokkeringsplicht voor ISP's overweegt. Gegeven het ontbreken van bevoegdheden op dit gebied voor de politie, respectievelijk het KLPD, ligt het voor de hand om de lijst niet onder verantwoordelijkheid van het KLPD, maar onder verantwoordelijkheid van het Openbaar Ministerie bij te houden. De gesignaleerde problemen bij de samenstelling van de lijst

gelden onverkort in een systeem dat uitgaat van een wettelijke verplichting. Naar derden hoeft niet bekend te worden wat en wie op de lijst voorkomt,[134] wel dienen de *criteria* voor de samenstelling van de lijst transparant en openbaar te zijn. Wanneer een wettelijke blokkeringsplicht zou worden ingesteld, behoeft de aansprakelijkheid van ISP's jegens derden geen nadere regeling. Zoals in de huidige praktijk voorzien, kan de overheid de technische inrichting van de blokkeringssystemen overlaten aan de ISP's en softwareontwikkelaars. Indien op aanwijzing van de overheid wordt geblokkeerd, dient het instrument voldoende precies en actueel te zijn, opdat geen onevenredige mate van overblocking plaats vindt. Het is in die situatie aan te bevelen dat de wetgever voorschriften stelt ten aanzien van de inrichting van de techniek en aangeeft welke selectiecriteria mogen worden toegepast. Het verdient aanbeveling om in geval van wettelijke filterplicht een rechtsmiddel tegen de toepassing van de bevoegdheid open te stellen.

Het instellen van wettelijke filter- en blokkeringsplicht van kinderporno luistert nauw en vraagt van de overheid, respectievelijk van politie en justitie, een nauwkeurige en arbeidsintensieve inzet.

6.5 Samenvatting

Het KLPD sluit convenanten met internetproviders die er toe strekken dat de ISP's internetverkeer naar en van door het KLPD als aanbieders van strafbare kinderporno aangemerkte domeinen blokkeren. De ISP verplicht zich de lijst van het KLPD te gebruiken en tot blokkering over te gaan en leidt de internetgebruiker naar een zogenoemde stoppagina. Het KLPD vrijwaart de ISP voor aanspraken van derden vanwege de op instructie van het KLPD toegepaste blokkering.

Het KLPD is onderdeel van de politieorganisatie, maar bezit anders dan de politieregio's geen rechtspersoonlijkheid. Het KLPD heeft de status van agentschap. Dit betekent dat in beginsel de minister (van BZK) verantwoordelijk is. De korpschef KLPD is gemandateerd tot het verrichten van beheershandelingen. Het aangaan van een convenant ter uitvoering van de veronderstelde publiekrechtelijke taak is als beheer aan te merken. De korpschef is op die grond bevoegd tot het aangaan van dergelijke convenanten. De korpschef is bevoegd tot een bedrag van € 450.000. Gezien het totale bedrag waartoe de aansprakelijkheid in verband met deze convenanten kan strekken, dient niet de korpschef KLPD, maar de Minister van Binnenlandse Zaken zich tot vrijwaring te verbinden. Aangetekend dient te worden dat ISP's ondanks deze vrijwaring niettemin een zekere eigen verantwoordelijkheid houden.

Het KLPD heeft als taak de daadwerkelijke handhaving van de rechtsorde, zoals geformuleerd in artikel 2 Polw. In dit verband kan die taak worden omschreven als de bescherming van jeugdigen en de bestrijding van kinderporno. De convenanten strekken ertoe dat private partijen zich tegenover het KLPD verplichten tot het filteren/blokkeren van bepaald internetverkeer. Een bevoegdheid tot het blokkeren van internetverkeer, zo deze al bestaat, komt niet toe aan het KLPD en evenmin biedt artikel 2 Polw geen grondslag voor een dergelijke bevoegdheid. Genoemde convenanten vormen daardoor een onaanvaardbare doorkruising van publiekrechtelijke bevoegdheden en daarmee van publiekrechtelijke waarborgen. Op grond van de Twee-wegenleer ontberen deze convenanten rechtsgeldigheid.

Indien men de invoering van een wettelijke blokkeringsplicht zou overwegen, zijn de volgende zaken van belang. Onvermijdelijk is bij filteren/blokkeren sprake van een zekere mate van *overblocking* (zie ook hoofdstuk 2 en 4). De wetgever dient voorwaarden te scheppen waardoor het blokkeringsinstrument voldoende precies en zorgvuldig is, zodat het verenigbaar is met de vrijheid van meningsuiting en het verbod van censuur. Dat kan betekenen dat wettelijke voorschriften worden gegeven voor de inrichting en werking van de blokke-

[134] Aangenomen wordt dat de uitzonderingsgrond van art. 10, tweede lid onder c van de WOB met succes kan worden ingeroepen in geval van een WOB-verzoek om verstrekking van de lijst.

ringssoftware en van de KLPD-blacklist, waarvan thans kan worden gesteld dat de selectiecriteria voor de lijst weinig transparant zijn, dat het onderhoud van de lijst weinig frequent is, en dat op de lijst sites voorkomen die binnen het bereik van de opsporing zijn gelegen.

HOOFDSTUK 7

Hoe nu verder?

In dit laatste hoofdstuk presenteren we onze voornaamste conclusies (paragraaf 7.1), beantwoorden we de in het eerste hoofdstuk gestelde vragen (7.2) en schetsen we enkele scenario's aangaande de toekomstige Nederlandse aanpak van kinderporno op internet (7.3). Bij elk scenario gaan we in op de technische methoden, maken we op basis van onze onderzoeksbevindingen een globale inschatting van de effectiviteit van de genoemde maatregelen en beschrijven we de eventuele juridische implicaties. Het hoofdstuk eindigt met een slotoverweging (7.4).

7.1 Conclusies

Discussie over filteren en blokkeren op instigatie van de overheid
In Nederland is zowel in de media als op internetfora de nodige commotie ontstaan over de huidige wijze van blokkeren op aanwijzing van het KLPD. Tegenstanders laten zich in de discussie het meest frequent horen. Het is echter de vraag of de personen die op internetfora met verve hun bezwaren tegen blokkeren ventileren ook representatief zijn voor de algemene publieke opinie. Dit hebben we niet onderzocht.

Tegenstanders, met uitzondering van de heel principiële, hebben in de regel geen bezwaar tegen het blokkeren van kinderpornografie op internet als ook alles wordt gedaan om de daders op te sporen en te vervolgen èn zeker is dat het blokkeren zich tot het strafbare materiaal beperkt. Ze wijzen er op dat filters altijd meer blokkeren dan men beoogt en dat dus altijd ook legaal materiaal wordt geblokkeerd. Als de overheid internet filtert, ontstaat dus een spanningsveld met de in grondrechten van burgers verankerde vrijheid van meningsuiting en de vrijheid van informatievergaring.

De tegenstanders wijzen ook op het gevaar van het hellend vlak: nu gaat het om kinderporno, daarna om het blokkeren van radicaliserende sites, sites met terroristische content, sites die inbreuk maken op het auteursrecht, enzovoort. Het is minimaal lastig om aan te geven wat nu precies het principiële verschil is tussen het blokkeren van sites met kinderporno en het blokkeren van sites die andere strafbare content bevatten. Zonder grond is de veronderstelling dat het filteren zich zal gaan uitbreiden niet; politici geven wel enige aanleiding voor die redenering. Twee leden van de Noorse Commissie datacriminaliteit willen een wet die de mogelijkheid biedt om strafbare inhoud in het algemeen te blokkeren, de Noorse minister van Justitie wil naast websites ook telefoonverkeer gaan filteren op kinderporno, de Zweedse minister van Justitie wil dat het filter ook wordt gebruikt tegen websites die verband houden met vrouwenhandel.

Overheidsregulering zou bovendien in strijd zijn met het open karakter van internet. In dat kader wordt gesproken over overheidscensuur: de overheid – en niet de gebruiker zelf – bepaalt immers welke informatie voor internetgebruikers toegankelijk is. Andere stellingen die regelmatig worden betrokken, hebben te maken met het ontbreken van transparantie in de samenstelling van de blacklist en het ontbreken van een toets door een rechterlijke of andere onafhankelijke partij.[135] Het statische karakter van blokkeren doet bovendien onrecht aan de dynamiek van internet. Niet alleen wordt informatie op websites op het moment van toewijzing aan de blacklist geblokkeerd, maar ook informatie die in de (zeer nabije) toekomst op deze websites kan komen te staan.

[135] Zie in deze zin ook de aangehouden Motie Gerkens van 6 november 2007, TK 2007-08, 31200 VI, nr. 17.

Voorstanders van blokkeren willen dat de overheid zichtbare maatregelen treft om de verspreiding van kinderporno tegen te gaan. Zij pareren het argument dat blokkeren in strijd zou zijn met de vrijheid van meningsuiting, door te stellen dat die vrijheid ophoudt wanneer het om strafbare feiten gaat. Reacties op internetfora en in de media geven in elk geval blijk van een in de samenleving breed gedragen morele verontwaardiging ten aanzien van kinderporno. In het verlengde hiervan is de roep om daadkrachtig op te treden tegen misbruik en exploitatie van kinderen steeds vaker te horen. In interviews beamen representanten van ISP's dat zij deze morele druk terdege voelen en dat zij in toenemende mate op hun verantwoordelijkheid worden gewezen om maatregelen te treffen tegen kinderporno op internet.

Doelstellingen en effectiviteit

Om bovengenoemde discussie over de (on)mogelijkheden van filteren en blokkeren van kinderporno op internet op een zinvolle manier te voeren, is het van wezenlijk belang om eerst te bepalen wàt nu precies met deze activiteit wordt beoogd. Een concrete, laat staan meetbare doelstelling ontbreekt veelal. Wellicht het meest ambitieuze doel dat we in ons onderzoek tegenkwamen, is het tegengaan van seksueel misbruik van kinderen. In ons onderzoek troffen we echter geen enkele evaluatiestudie aan naar de effectiviteit van filteren. Ook de empirische onderzoeken van het OpenNet Initiative (ONI) – die zijn gericht op de accuratese waarmee filters filteren wat ze beogen te filteren – geven geen antwoord op de vraag in welke mate ongewenste informatie op een effectieve en *duurzame* wijze voor internetters onbereikbaar kan worden gemaakt. Evenmin wordt in studies de vraag beantwoord of door het filteren een achterliggend doel is bereikt. Wel kunnen we concluderen dat het mogelijk is gebleken om met filteren de verkrijgbaarheid van bepaalde internetinformatie te bemoeilijken, zij het dat geen enkel filtersysteem waterdicht is. Dat leert ons de situatie in niet-westerse landen. We hebben geen reden om aan te nemen dat minder rigoureuze filtersystemen – die thans in de Scandinavische landen, Engeland en Nederland worden gebruikt – geheel geen effect zouden hebben: ze werpen in elk geval tot op zekere hoogte een drempel op. Het is echter nog maar de vraag of het bemoeilijken van de toegang tot kinderpornografisch materiaal op internet leidt tot een vermindering van seksueel misbruik van kinderen. We hebben in elk geval geen aanwijzingen gevonden dat filtertechnieken tegen kinderpornografie dit effect bewerkstelligen. Op dit gebied is nog geen onderzoek verricht en het is zelfs de vraag is of dit op zinvolle wijze mogelijk is. De afstand tussen filteren en kindermisbruik is daarvoor te groot.

Een andere vaak genoemde doelstelling is het onaantrekkelijk maken van het commercieel aanbieden van kinderporno. De afzetmarkt voor kinderpornografie is ten gevolge van internet groter geworden en liefhebbers zijn bereid geld te betalen voor kinderpornografisch materiaal. Door filter- en blokkeertechnieken – zo luidt de veronderstelling – wordt een extra drempel opgeworpen tegen deze lucratieve handel: aanbieders en afnemers kunnen elkaar immers niet meer zo gemakkelijk bereiken, waardoor de afname en dus de omzet daalt. Aanbieders zoeken dan wellicht een andere bron van inkomsten, waardoor er minder kinderporno wordt gemaakt en dus ook – want dat blijft het einddoel – het misbruik van kinderen vermindert. In dit onderzoek zijn geen feiten gevonden, waarmee bovengenoemde oorzaak-gevolgketen kan worden gestaafd. Ook hebben we geen informatie gevonden op grond waarvan we kunnen zeggen in welke mate het aantal misbruikte kinderen samenhangt met de commerciële markt en in welke mate dat aantal samenhangt met de 'liefhebbers-markt'. Het enige dat met zekerheid gesteld kan worden is dat een filter een activiteit van de afnemer blokkeert en slechts in beperkte mate van de aanbieder.

Onze bevindingen wijzen er op dat filteren niet effectief is tegen 'liefhebbers' die onderling kinderpornografisch materiaal uitwisselen. Zij weten elkaar toch wel te vinden. Het meest reële doel dat men blijkens ons onderzoek kan nastreven met filteren, is dan ook het beschermen van argeloze gebruikers tegen kinderporno op internet. Op basis van vooral slacht-

offeronderzoek en in mindere mate statistieken omtrent meldingen kan worden achterhaald of deze doelstelling wordt behaald. Verder kan het filteren worden gehanteerd als onderdeel van een samenhangend pakket van maatregelen, waarvan met name ook opsporing deel uitmaakt. Tegelijk roepen onze bevindingen de vraag op in hoeverre een willekeurige internetter zomaar ongevraagd met kinderporno zal worden geconfronteerd. Zeker als internetters gebruikmaken van een spamfilter, niet op zoek zijn naar sekssites, niet deelnemen aan seksueel getinte nieuwsgroepen of fora en niet ingaan op schimmige berichten die ondanks voorzorgsmaatregelen toch doorkomen, lijkt de kans om op kinderporno te stuiten vrijwel uitgesloten. Alleen medewerkers van het particuliere Meldpunt Kinderporno op Internet hebben de indruk dat ook 'keurige' internetters wel eens een melding bij hen doen van kinderporno op het internet, hoewel zij ook ervaring zeggen te hebben met minder argeloze melders (personen die zoeken naar porno met jeugdigen, maar bepaald materiaal te ver vinden gaan). Er is echter geen onderzoek naar het surfgedrag van internetters die kinderporno melden. Zo bezien is het dus nog maar de vraag in hoeverre 'het beschermen van argeloze internetters' wel als een reëel doel kan worden aangemerkt. Daar komt bij dat de filters waarover dit onderzoek gaat, gericht zijn op websites. We troffen niemand die ons een voorbeeld kon geven van een 'keurige' internetter die onverwacht kinderporno op een website aantrof.

Met name in de Verenigde Staten zijn filters geregeld aan tests onderworpen om te bepalen hoe accuraat ze zijn: of ze ongewenst materiaal doorlaten (*underblocking*) dan wel materiaal dat niet tegengehouden zou moeten worden toch blokkeren (*overblocking*). In het eerste geval is het filter slechts ten dele effectief, in het tweede geval ontstaat spanning met de vrijheid van meningsuiting (en kans op schadeclaims). Uit dergelijke tests blijkt dat het ideale filter niet bestaat en dat het steeds een kwestie is van zoeken naar een balans tussen *under-* en *overblocking* (bij elk filter is van beide steeds sprake, alleen de verhouding ligt steeds anders: hoe minder *underblocking* hoe meer *overblocking*). Een groot probleem blijkt de snelheid waarmee internet verandert; een filter loopt altijd achter de feiten aan. Dergelijke tests zijn waardevol, maar zeggen nog niet alles over de effectiviteit van het filter. Een filter kan nog zo accuraat zijn, als gebruikers het filter omzeilen, is het nog steeds niet effectief. Als het filter wordt ingezet voor een probleem dat niet bestaat (zoals wellicht: de onschuldige gebruiker die zomaar met kinderporno wordt geconfronteerd) of voor een probleem waarop het filter geen registreerbare invloed heeft (aantal misbruikte kinderen), kan geen effectiviteit worden aangetoond. Voor de filters waarnaar in dit onderzoek de aandacht uitgaat zijn geen accuratessetests uitgevoerd of effectstudies gedaan, noch in het buitenland, noch in Nederland. Dat betekent dat de inzet van filters door of namens de Nederlandse overheid niet is gebaseerd op enige onderbouwde kennis omtrent de effectiviteit van deze maatregel.

Cijfers over het aantal hits zijn wel bekend, maar deze geven geen valide indicatie van de omvang van het kinderpornoprobleem. Daarvoor is te onduidelijk wat deze cijfers precies betekenen. Over de effectiviteit van de filters zeggen de aantallen hits nog minder. Er is geen onderzoek naar wie of wat het filter precies stopt en wat er dus achter de aantallen hits steekt. Het is dan ook zonder meer onverstandig om aantallen hits op te voeren als argument voor of tegen het filteren.

Seksueel misbruik van kinderen is een complex maatschappelijk probleem. Dergelijke problemen laten zich niet met eenvoudige maatregelen oplossen, maar vergen in de regel een combinatie van elkaar versterkende maatregelen. Het filteren van sites met kinderpornografisch materiaal moet dan een element zijn in een integrale aanpak, omvattende een samenstel van elkaar aanvullende maatregelen. Een van die maatregelen is de uitbreiding van het aantal gekwalificeerde rechercheurs dat zich bezighoudt met de opsporing van kinderporno op internet. Daarnaast zijn (internationale) kennisuitwisseling, harmonisatie van wet- en regelgeving en het intensiveren van internationale samenwerking in de bestrijding van kinderporno essentieel om seksueel misbruik van kinderen effectief tegen te gaan.

Filtertechnieken

Er zijn verschillende technische mogelijkheden om internetverkeer te filteren. Niet alle soorten verkeer laten zich even eenvoudig filteren, niet alle technieken zijn even praktisch toepasbaar en niet alle filtertechnieken zijn even precies en/of effectief. Dynamische filtertechnieken, dat wil zeggen op basis van vooraf opgestelde algemene criteria, bijvoorbeeld 'blokkeer alle sites met daarin de tekst "preteensex"', worden voor zover wij weten in Europa niet gebruikt (welke filtertechnieken bijvoorbeeld China gebruikt, is niet precies bekend). Het probleem met dergelijke *dynamic filtering* technieken – we zouden ook kunnen spreken van proactief filteren, omdat de filters ook ingrijpen op sites die niet door personen van de filterende instantie zijn beoordeeld – is dat ze moeilijk precies zijn af te stellen: te algemene criteria leiden tot forse *overblocking*; bij criteria die te toegespitst zijn ligt *underblocking* voor de hand. Een probleem van overblocking is dat het kan gaan om sites die in de verste verte niets met kinderpornografie van doen hebben.

De basis onder in elk geval de Europese filtersystemen is een blokkeerlijst: een lijst met adressen en/of codes die horen bij informatie waarvan door personen van de filterende instantie is vastgesteld dat die moet worden geblokkeerd. Dat heet *blacklist filtering*; we zouden ook van reactief filteren kunnen spreken. De blokkeerlijst van het KLPD wordt samengesteld door KLPD-medewerkers die bepalen of een site wel of niet op de lijst wordt geplaatst (*human review*).

De ontwikkeling die we zagen bij filters van commerciële aanbieders is dat blokkeerlijsten niet enkel worden gevormd doordat medewerkers van de filterbedrijven items toevoegen, maar ook doordat items op de lijst worden toegevoegd door zoekrobots – die op basis van algemene criteria (*dynamic filtering*) het internet afzoeken naar te blokkeren sites. *Human review* maakt dan plaats voor *automated review*. De blokkeerlijst is dan gedeeltelijk of soms wellicht geheel een resultante van *dynamic filtering* – met de bijbehorende extra kans op *overblocking*. Het op basis van *human review* actueel houden van een blokkeerlijst is kennelijk op een gegeven moment, als er veel materiaal te blokkeren is en het aanbod voortdurend van plaats wisselt, niet meer kosten-effectief.

Blokkeren op basis van een blokkeerlijst kan met IP-adressen (dan worden complete machines geblokkeerd), met domeinnamen (blokkeren van websites), URL's (blokkeren van een deel van een website) of hashcodes (blokkeren van een bepaalde afbeelding). Blokkeren op IP-adres komt niet voor. Dat is te weinig precies. Blokkeren op basis van domeinnamen kan relatief eenvoudig, is relatief goedkoop, maar is niet zo precies en relatief eenvoudig te omzeilen. Dit is de Noorse methode die ook in Nederland wordt toegepast. Blokkeren op URL of hashcode is preciezer en minder eenvoudig te omzeilen, maar vergt substantiële technische investeringen, omdat alle internetverkeer inhoudelijk moet worden gecontroleerd.

Een technische oplossing voor dat laatste probleem is een tweetrapsfiltermethode waarbij uit alle verkeer eerst op hoofdlijnen (bijvoorbeeld IP-adres) een verdachte stroom wordt gefilterd, waarna alleen dat verdachte verkeer nader inhoudelijk wordt gecontroleerd op ongewenste content (bijvoorbeeld op basis van URL's of hashcodes). Er is dan bijvoorbeeld een blacklist met IP-adressen voor de eerste, grove filtering en een blacklist met URL's of hashcodes voor de tweede, precieze filtering. Deze tweetrapsmethode is in Engeland in gebruik.

Gezien de problemen die *overblocking* met zich meebrengt, lijkt dynamisch of proactief filteren door de overheid vooralsnog geen reële optie. Blokkeren op domeinnaam (huidige methode in Nederland) is nogal grofmazig en kent daarom ook al gauw problemen met underen overblocking: ofwel men besluit bepaalde kinderporno niet te blokkeren omdat men dan het gehele domein daarmee treft, ofwel men blokkeert wel en accepteert een bepaalde mate van overblocking. Deze methode brengt daarom als vanzelf morele discussies over (over-

heids)censuur met zich mee. Bij de 'Engelse methode' is de kans daarop kleiner want zij is preciezer.

De prijs voor een preciezere filtertechniek is een grotere investering in apparatuur (en de discussie wie dat betaalt). Een ander financieel aspect van filteren is wie de blokkeerlijst samenstelt en wie dat dus betaalt. Wil het KLPD dat goed doen (*human review*) dan moet zij het bijhouden van de lijst niet 'erbij' doen maar daarin duidelijk investeren.

Filteren kan op verschillende plaatsen: op de computer van de internetter, in zoekmachines, op de centrale server van een organisatie, op de server(s) van ISP's, of op landelijk niveau. Dat laatste vergt grote investeringen. Die worden gedaan door diverse niet-westerse landen waar de overheid strikte controle tracht uit te oefenen op het media-aanbod. In Europa ligt die aanpak niet voor de hand. Uitgaande van filters op basis van blokkeerlijsten, komen we uit bij filters op het niveau van gebruiker, organisatie en ISP's.

Er zijn geen technische belemmeringen (en zoals we verderop zullen zien ook geen juridische) om op gebruiker- of organisatieniveau te filteren. Op beide niveaus kan gebruik worden gemaakt van het filteren op basis van URL en/of hashcode. De vertraging die dat in het verkeer oplevert lijkt, gezien de daarmee opgedane ervaringen, geen overwegend bezwaar. De overheid kan met het filteren op organisatieniveau een voorbeeldfunctie vervullen, zoals parlement en regering in Zweden laten zien.

Op ISP-niveau kan men gebruik maken van filteren op domeinnaam en het kwalitatief betere (want preciezere) filteren via twee trappen (de 'Engelse methode'). Het op ISP-niveau filteren van chatkanalen, P2P-netwerken, MMS- en webcamverkeer is technisch aanzienlijk lastiger dan het filteren van websites op het (vaste of mobiele) internet. Dergelijke verbindingen lopen namelijk langs minder gestructureerde wegen. Bovendien kan dan niet altijd op basis van blokkeerlijsten worden gewerkt. Dan komt het aan op inhoudelijke inspectie (DPI) van het verkeer. Nieuwsgroepen worden door verschillende ISP's van oudsher al (reactief) gefilterd, waarbij nieuwsgroepen met een expliciet kinderpornografisch karakter niet aan de gebruikers ter beschikking worden gesteld. De huidige filtermethode in Nederland laat de nieuwsgroepen ongemoeid, terwijl men juist daar informatie aantreft over waar kinderpornografie kan worden gevonden. Overigens kunnen nieuwsgroepen wel aan de hand van een Notice-and-take downprocedure (NTD) door een ISP aan hun klanten worden onthouden.

Juridische aspecten

Het centrale juridische vraagstuk is in welke mate het filteren en blokkeren op gespannen voet staat met het in de Grondwet en het EVRM vastgelegde recht op vrije meningsuiting en vrije informatievergaring. Direct daaraan gekoppeld is de vraag of het blokkeren, zoals thans in Nederland wordt uitgevoerd, een overheidstaak is. Burgers, ISP's en werkgevers hebben ruimere mogelijkheden om informatie te blokkeren (voor achtereenvolgens zichzelf, hun klanten en hun werknemers) dan de overheid heeft om informatie te blokkeren. De garanties in Grondwet en EVRM zijn er immers speciaal om burgers te beschermen tegen overheidscensuur.

Hoe minder precies de technische oplossing, hoe minder secuur het overheidsoptreden kan zijn, dus hoe eerder het in strijd komt met de wettelijke waarborgen.

De Nederlandse politie heeft ten opzichte van de meewerkende ISP's een positie gekozen waarin zij verantwoordelijk is voor wat er wordt geblokkeerd. Daarmee is het blokkeren van bepaald verkeer de facto een overheidsdaad. Het gaat daarbij niet enkel om criminaliteitspreventie (zoals hang- en sluitwerk waarmee nog eens wordt bemoeilijk wat toch al niet mag, namelijk tegen iemands wil diens woning ingaan), maar om het beperken van (grond)wettelijk beschermde mogelijkheden van burgers tot het doen van een uiting of het vergaren van informatie. Dat ingrijpen ontbeert een wettelijke grondslag en is niet met wettelijke waarborgen omkleed. Men doet de (grond)wettelijke waarborgen in elk geval recht wan-

neer blokkeeractiviteiten die beperkingen in de vrijheid van meningsuiting en informatievergaring en van het recht op vertrouwelijke communicatie met zich mee kunnen brengen bij wet worden geregeld, waarvan de rechtmatige toepassing door de rechter kan worden getoetst.

Huidige situatie in Nederland
De aan de filtersystematiek deelnemende ISP's verzorgen de technische realisatie van het filteren. Het KLPD beheert de blokkeerlijst en heeft voor die lijst de inhoudelijke verantwoordelijkheid. De politie heeft omtrent het beheer van de lijst geen procedures vastgelegd, noch houdt zij bij hoe de geblokkeerde sites precies zijn beoordeeld. De lijst van ongeveer 100 websites bestaat geheel of grotendeels uit sites die worden gehost in landen waarmee Nederland een goede justitiële samenwerking heeft; de lijst bevat ook sites die worden gehost in Nederland. Het KLPD heeft eigenlijk niet de capaciteit om het werken met de blokkeerlijst grondig aan te pakken, dat wil zeggen volgens heldere regels en criteria gestructureerd te werken aan het systematisch, frequent en goed gedocumenteerd bijhouden van de blokkeerlijst.

Het capaciteitsvraagstuk brengt ons bij de zogenoemde kerntakendiscussie. Voor zover de blokkeerlijst werkt als instrument voor criminaliteitsbestrijding ('tegenhouden') past het werken ermee in het actuele beleid – mits het middel effectief is en geen onevenredige inspanningen vraagt (hoofdstuk 5). Naar de effectiviteit van kinderpornofilters als instrument voor 'tegenhouden' is geen serieus onderzoek verricht; hoge verwachtingen van die effectiviteit mogen we op voorhand niet hebben (hoofdstuk 2 en 4). Verder vergt het goed bijhouden van een blacklist (*human review*) een grote tijdsinvestering. En dat de politie bepaalt wat zal worden geblokkeerd, levert juridische complicaties op (hoofdstuk 3 en 6). Op grond van het actuele politiebeleid ('minder uitvoerend, meer signalerend en adviserend'; 'geen nieuwe belemmeringen, procedures en beperkingen') ligt het voor de hand dat de politie het bijhouden van een blacklist die dient om kinderporno op internet tegen te gaan, overlaat aan anderen.

Zelfregulering / marktwerking
Uit het buitenland leren we dat het filteren van kinderpornografie door ISP's wordt opgepakt, zij het soms na aanvankelijke weerstand en dreiging met wettelijke maatregelen. De ISP's werken in sommige gevallen nadrukkelijk samen met ideële organisaties (zoals in Engeland de IWF). De ontwikkelingen in het buitenland laten verder zien dat er inmiddels een markt aan het ontstaan is van filtertechnieken tegen kinderpornografie. ISP's die gebruik maken van een politielijst maken daarmee reclame in hun voorlichting aan (toekomstige) klanten. Bedrijven ontwikkelen eigen filters, mede op basis van door de politie aangeleverde blokkeerlijsten, en gaan daarmee de markt op. Commerciële bedrijven vermarkten op die manier het werk dat de politie als het ware voor hen doet.

7.2 Antwoorden op de onderzoeksvragen
De vijf onderzoeksvragen,[136] elk weer onderverdeeld in subvragen, beantwoorden we hier beknopt op basis van onze bevindingen. Aanvullende informatie vindt men in eerste aanleg in paragraaf 7.1 en uiteraard verder in de betreffende voorgaande hoofdstukken.

Vraag 1: Technische mogelijkheden (hoofdstuk 2)
a. Welke technische mogelijkheden zijn er?
b. Welke ervaringen zijn daarmee opgedaan?
c. Zijn de tools effectief, haalbaar en duurzaam?

[136] We herhalen de vragen hier ingekort. Voor de volledige tekst verwijzen we naar paragraaf 1.4.

(a) Filteren kan op basis van een blokkeerlijst (*blacklist filtering*) en op basis van algemene criteria (*dynamic filtering*). Een blokkeerlijst kan worden samengesteld door mensen (*human review*) of door een zoekrobot (*automated review*) of een combinatie van beide. In elk systeem kan in principe worden geblokkeerd op IP-adres, domeinnaam, URL, hashcode of andere unieke kenmerken van een afbeelding. In Engeland kent men een tweetrapsmethode: eerst verdachte domeinen selecteren en dan alleen die domeinen nader inspecteren op URL. Het Noorse systeem, dat ook in Nederland in gebruik is, filtert op domeinnaam. Een filter kan worden ingesteld bij de gebruiker, een LAN, een ISP of aan de landsgrenzen.

(b) In de Verenigde Staten wordt gebruik gemaakt van filters van commerciële bedrijven. Uit tests blijkt dat alle filters een zekere mate van *underblocking* en *overblocking* hebben. Hoe minder *underblocking* (dus hoe meer van het ongewenste materiaal het filter tegenhoudt, dus hoe strenger het filter) hoe meer *overblocking*. Een goed filter vergt veel onderhoud. Commerciële bedrijven gaan daarom over op *blacklists* op basis van *automated review* (in plaats van *human review*). Daardoor neemt de *overblocking* toe. Het Noorse (ook Nederlandse) systeem filtert op domeinnaam. Dat is een relatief grove filtermethode maar wel eenvoudig (en goedkoop) te implementeren. De Engelse tweetrapsmethode is accurater, vergt meer investeringen in apparatuur en is derhalve duurder. Filters die alle internetverkeer controleren zijn op ISP-niveau niet in gebruik, omdat ze het verkeer teveel vertragen dan wel, als men die vertraging wil voorkomen, te veel investeringen vergen. Dergelijke systemen zijn wel bruikbaar op LAN- of gebruiksniveau.

(c) Bij elk filter is sprake van *under*- en *overblocking*. Aan een goed filter zijn hoge onderhoudskosten verbonden, zeker bij *blacklist filtering* op basis van *human review* (zoals in het huidige Nederlandse systeem). Men moet immers alle wijzigingen op internet voortdurend bijhouden. De huidige Europese filters (op basis van domeinnamen en/of URL's) grijpen alleen in op informatie afkomstig van webpagina's en niet op informatie die wordt uitgewisseld via P2P-systemen, chat of nieuwsgroepen; ook kunnen de filters niet uit de voeten met gecomprimeerde of versleutelde informatie (die passeert dus zonder meer). Niet alle ISP's doen mee met de politie om te filteren en verder zijn op internet op verschillende plaatsen handleidingen beschikbaar over hoe filters te omzeilen. Vooral het Noorse (Nederlandse) DNS-filter is eenvoudig te passeren. Er is geen enkel onderzoek beschikbaar naar de mate van effectiviteit van kinderpornofilters. Informatie echt duurzaam blokkeren lijkt technisch en organisatorisch gezien onhaalbaar: de informatie duikt altijd ergens weer op, desnoods versleuteld, terwijl de kosten voor geheel duurzaam blokkeren enorm zijn. Zolang onderzoek niet anders aantoont, lijkt het enige haalbare effect van het filteren van kinderporno in Nederland dat men het de gemiddelde internetter moeilijker maakt om de ongewenste informatie te verkrijgen.

Vraag 2: Juridische context (hoofdstuk 3 en 6)

a. Wat zijn juridische mogelijkheden tot filteren?
b. Wat zijn juridische belemmeringen en kunnen die worden opgelost?

(a) Het is juridisch zonder meer mogelijk dat ISP's, LAN-beheerders of particulieren hun internetverkeer filteren. Problemen ontstaan wanneer het filteren een overheidsdaad is. Nog steeds zijn er dan mogelijkheden, maar die worden wel begrensd door in de Grondwet en het EVRM vastgelegde grondrechten. De overheid kan kinderpornografie blokkeren; het gaat immers om strafbaar materiaal. Echter, het filteren van kinderpornografie die wordt gehost in Nederland of in een land waarmee Nederland op justitieel gebied samenwerkt, zal wel vragen oproepen omtrent welke (juridische) middelen de overheid primair dient in te zetten bij de strijd tegen kinderpornografie.

(b) Juridische grenzen worden met name gesteld aan filteren door de overheid. Die grenzen, vastgelegd in Grondwet en EVRM, kunnen reëel gesproken niet worden weggeno-

men. Wel kan men ervoor kiezen deze grenzen niet op te zoeken door het filteren over te laten aan ISP's, LAN-beheerders en particulieren, eventueel in samenwerking met een non-profitinstelling zoals in Engeland het IWF. De overheid kan regels stellen die dat stimuleren en faciliteren. In Noorwegen zijn werkgevers bijvoorbeeld verplicht tot filteren van kinderporno, in de Verenigde Staten hebben openbare scholen en bibliotheken tot op zekere hoogte een dergelijke verplichting, in Zweden zijn aanbieders van elektronische bulletin boards verplicht om maatregelen te nemen tegen kinderporno, in Engeland heeft het IWF een wettelijk beschermde status waar het gaat om werken met kinderpornografisch materiaal (het IWF verzorgt de *blacklist*).

De politie (dus ook het KLPD) beschikt niet over de bevoegdheid tot het (doen) filteren van internetverkeer en het blokkeren van kinderpornografie. Een dergelijke bevoegdheid kan namelijk niet worden afgeleid uit artikel 2 Politiewet. Zo'n bevoegdheid vereist een formeel-wettelijke basis vanwege de mogelijke inbreuk op grondrechten. Op basis van de huidige regelgeving kan het KLPD dan ook niet per convenant met een ISP overeenkomen dat die ISP verplicht is om internetverkeer te filteren. Verder kent het convenant een clausule waarin het KLPD de ISP's vrijwaart tegen aanspraken van derden (mensen die zich door het filter gedupeerd achten en schadeloos willen worden gesteld). De mandateringsregeling mandateert de korpschef van het KLPD tot het aangaan van civielrechtelijke verplichtingen tot een bedrag van 450.000 euro. Aangezien het convenant met meerdere ISP's wordt afgesloten, lijkt het aangewezen dat het ministerie van BZK als wederpartij optreedt voor het vrijwaringsdeel van het convenant.

De strijd tegen kinderpornografie wordt internationaal gezien gevoerd tegen een achtergrond van verschillen in nationale wetgevingen. Ook tussen landen die op juridisch gebied nauw samenwerken doen die zich voor, zoals we bijvoorbeeld zagen in vergelijkingen tussen Nederland, Noorwegen en Zweden (par. 4.2 en 4.3). Dat doet de samenwerking geen goed. Verdergaande internationale harmonisatie van wetgeving kan helpen om de samenwerking te vereenvoudigen.

Vraag 3: Zelfregulering (hoofdstuk 4)

a. Kan filteren duurzaam via zelfregulering door ISP's?
b. Welke mogelijkheden heeft de overheid voor 'gecontroleerde zelfregulering'?
c. Welke ervaringen zijn met zelfregulering opgedaan?

(a) Filteren kan duurzaam worden geregeld via zelfregulering, zij het dat de opmerkingen over effectiviteit van filteren ook dan van toepassing zijn (zie vraag 1). Bij zelfregulering hoeven we niet alleen te denken aan ISP's. Internetgebruikers, LAN-beheerders en ISP's gebruiken al tal van filters (spam, virus, ouderlijke toezicht). Een kinderpornofilter kan van zo'n pakket deel uitmaken. Ouders, scholen en bibliotheken kunnen op hun verantwoordelijkheid worden aangesproken, zodat ook een vraag ontstaat naar filterproducten. Providers in Noorwegen maken op hun sites reclame met hun kinderpornofilter, een Zweeds bedrijf ontwikkelt een kinderpornofilter op commerciële basis, in Engeland functioneert het kinderpornofilter zonder directe overheidsbemoeienis op basis van samenwerking tussen providers en het IWF. Ook in de Verenigde Staten filtert niet de overheid maar legt de overheid scholen en bibliotheken de plicht op om te filteren en is er een groot aantal bedrijven dat commerciële filters op de markt brengt. Er zijn tal van voorbeelden van zelfregulering en daarvan laat het Engelse voorbeeld het meest direct zien dat duurzame zelfregulering door ISP's mogelijk is.

(b) Bij de meeste vormen van zelfregulering zien we op de achtergrond enige vorm van overheidsbemoeienis. We noemden onder (a) al de wetgeving in de VS. Werkgevers en leidinggevenden in Noorwegen zijn strafbaar als zij niets doen om te voorkomen dat werknemers kinderporno kunnen downloaden. Het Engelse IWF is wettelijk beschermd. Maar voor

zover bekend heeft tot dusverre geen Europese overheid ISP's wettelijk verplicht om internetverkeer te filteren. De Noorse commissie Datacriminaliteit heeft zich gebogen over de vraag of het verstandig zou zijn om dat te doen en kwam in meerderheid tot een negatief advies (paragraaf 4.2). In plaats van het filteren wettelijk te regelen, kiezen Europese overheden voor debat en het overtuigen van hun ISP's – met op de achtergrond wel nadrukkelijk de dreiging van een wettelijke regeling. In Zweden organiseerde de overheid een voorlichtings- dan wel discussiebijeenkomst met ISP's, waarna de eerste Zweedse ISP's het Noorse filter implementeerden. De mogelijkheden die de overheid heeft voor een gecontroleerde zelfregulering zijn dus: overtuiging, voorlichting (bij ISP's maar ook bij ouders, scholen en bibliotheken), en het scheppen van wettelijke randvoorwaarden. Een vrij vergaande vorm van gecontroleerde zelfregulering is het, zoals in Noorwegen, strafbaar stellen van werkgevers en leidinggevenden die geen maatregelen nemen om te voorkomen dat hun werknemers kinderporno downloaden. Zo stelt men niet het filteren verplicht, laat staan een bepaalde manier van filteren, maar voor de werkgever/leidinggevende is de stap naar het installeren van een filter dan wel erg voor de hand liggend geworden.

(c) Zowel in de Verenigde Staten als in Engeland is het niet de overheid die filtert. De situatie in de VS laat zich niet eenvoudig vertalen naar de Nederlandse situatie vanwege het grote gewicht dat het *First Amendment* in de VS heeft. We vonden geen berichten dat het Engelse systeem niet goed zou functioneren vanwege een tekort aan overheidsbemoeienis. De ervaring in Engeland is dus dat zelfregulering een alternatief kan zijn voor actieve overheidsbemoeienis met het feitelijke filteren.

Vraag 4: Buitenland (hoofdstuk 4)

a. Hoe tracht men in het buitenland kinderpornografisch materiaal te blokkeren?
b. Welke technische middelen worden daarvoor gebruikt?
c. Hoe is het filtreren juridisch ingebed?
d. Welke praktijkervaringen deed men op (effectiviteit, haalbaarheid, duurzaamheid)?
e. Zijn de buitenlandse ervaringen te vertalen naar Nederland?

(a) In de Verenigde Staten tracht de overheid pornografisch materiaal, inclusief kinderpornografie, te blokkeren door openbare scholen en bibliotheken te verplichten pornografie te filteren indien minderjarigen hun computers gebruiken. In Saudi Arabië, Iran en China tracht de overheid kinderpornografie (en nog veel meer) te blokkeren door strikte technische en organisatorische overheidscontrole. In Noorwegen, Zweden en Denemarken (en ook in het niet door ons onderzochte Finland en Italië) tracht de overheid kinderporno te blokkeren middels samenwerking tussen politie en ISP's, waarbij de politie de blacklist samenstelt en de ISP's het feitelijke filteren realiseren. In Engeland tracht men kinderporno te blokkeren in een samenwerking tussen ISP's en het IWF.

(b) In de VS worden voor het filteren filtersystemen gebruikt van verschillende commerciële aanbieders (we weten niet in hoeverre 'kinderpornografie' in die systemen steeds een aparte categorie is, in ieder geval niet altijd: bij marktleider Secure Computing valt kinderpornografie onder de filtercategorie 'pornografie'). De niet-westerse landen gebruiken eveneens filtersystemen uit de VS. Verder gebruiken zij een technische infrastructuur die het mogelijk maakt te filteren aan de landsgrenzen (*backbone filtering*). In Engeland gebruikt men een systeem dat een combinatie kent van domeinfiltering en URL-filtering. Die tweetrapsmethode selecteert eerst de 'verdachte' domeinen en leidt die dan om via een proxy voor een nadere inspectie op URL-niveau. Dat voorkomt dat alle verkeer op URL-niveau moet worden gecontroleerd, hetgeen het verkeer teveel zou vertragen, en het maakt het mogelijk om vrij precies te blokkeren, namelijk op URL-niveau. In de landen die het Noorse systeem gebruiken, waaronder Nederland, wordt gefilterd op basis van domeinnamen (DNS-filter).

(c) In de VS is het filteren geregeld in de federale Children's Internet Protection Act (CIPA) van 2000. Die wet verplicht de scholen en bibliotheken die overheidssteun ontvangen om hun computers te filteren wanneer kinderen daarvan gebruik maken. In de niet-westerse landen is het filteren juridisch ingebed in een breder stelsel van overheidscontrole op de media. In Engeland is in het Memorandum of Understanding bij de Sex Offences Act van 2003 vastgelegd dat partijen die professioneel betrokken zijn bij de bestrijding van kinderpornografie, niet zullen worden vervolgd voor het in bezit hebben daarvan. Maar dat is geen speciale juridische maatregel voor het filteren. In Noorwegen, Zweden en Denemarken is eveneens geen speciale wetgeving voor het filteren van internet.

(d) Bij vraag 1, met name onder (c) gingen we in op ervaringen met effectiviteit, haalbaarheid en duurzaamheid. De belangrijkste bevinding in dit verband is dat er voor de Europese filters geen onderzoek beschikbaar is naar de werking en effectiviteit van de filters.

(e) De ervaringen uit de VS laten zich niet eenvoudig vertalen naar de Nederlandse situatie vanwege het zware gewicht dat daar wordt toegekend aan het *First Amendment*. Wat de VS ons wel leert is: dat filters altijd onvolkomen zijn, ook als het producten zijn van grote commerciële bedrijven (*under*- en *overblocking*); dat er een markt is voor commerciële filterproducten; dat openbare instellingen verplicht kunnen worden om internet te filteren zonder dat de overheid zelf een filter hoeft te onderhouden.

De ervaringen in de niet-westerse landen laten zich nog moeilijker vertalen naar de Nederlandse situatie. De belangrijkste les die deze landen ons leren is dat het mogelijk is om bepaalde informatie voor de modale internetter moeilijker bereikbaar te maken, maar dat ook een strikt, in westerse ogen totalitair controlesysteem lang niet waterdicht is.

De ervaringen in Noorwegen en Zweden leren ons dat de overheid ISP's kan overtuigen om deel te nemen aan een filtersysteem, zij het wel na enig dreigen met wetgeving. Het is echter nog maar de vraag of Nederlandse ISP's uiteindelijk even makkelijk meedoen als hun collega's in Scandinavië, zeker nu zoveel vragen zijn gesteld over de inhoud van het KLPD-filter en de door het KLPD gevolgde werkwijzen (hoofdstuk 5 en 6).[137]

De ervaringen in Engeland laten zich mogelijk maar niet zonder meer vertalen naar de Nederlandse situatie. In Engeland vervult de non-profit organisatie IWF een belangrijke rol in de samenwerking aangaande het filteren van kinderpornografie. Het IWF houdt bijvoorbeeld de blacklist bij. De Nederlandse overheid kan een (bestaande of nog op te richten) Nederlandse ideële organisatie eenzelfde rol toekennen als het IWF in Engeland, als het gaat om het filteren van kinderpornografie, waarna de politie niet langer de lijst bijhoudt. Men kan deze rol toedenken aan het particuliere Meldpunt Kinderporno op Internet. Alvorens het MKI deze rol daadwerkelijk toe te delen, is het zaak te bezien of de daarvoor vereiste randvoorwaarden zijn dan wel kunnen worden ingevuld (juridisch, personeelstechnisch, financieel). Relatief los daarvan staat de vraag of de Nederlandse providers willen overschakelen op een accurater filtersysteem, zoals de Engelse tweetrapsmethode. Dat is waarschijnlijk vooral een financieel vraagstuk, maar wellicht toch ook een juridisch vraagstuk omtrent het risico op schadeclaims die kleven aan het filteren op domeinnaam. Tot slot kan Nederland van de VS en Zweden nog leren dat het bijhouden van een filterlijst ook kan worden overgelaten aan marktpartijen.

Vraag 5: Technische doorontwikkeling (hoofdstuk 2, 4 en 5)

a. Is het zinnig om de bestaande technische mogelijkheden uit te bouwen?
b. Welk type applicatie zou dan gebouwd moeten worden?
c. Wie zou dat moeten doen?
d. Heeft de overheid daarin een rol?

[137] Op 15 en 16 april 2008 werd in de media bekend gemaakt dat alle grote Nederlandse internetaanbieders websites met kinderponro gaan blokkeren en dat zij naar verwachting op korte termijn een overeenkomst daarover zullen afsluiten met het KLPD (bv. *de Volkskrant*, 16 april 2008).

(a) Het is zinnig de bestaande technische filtermogelijkheden verder uit te bouwen – en vooral te verbeteren. Er is eenvoudig geen weg terug. Internet zal meer dan in de afgelopen jaren niet alleen een vrijplaats maar ook een terrein van (overheids)controle zijn. In die maatschappelijke trend past de ontwikkeling van controletechnieken.

(b) Als de overheid het filteren van internet ter hand neemt, moeten daaraan hoge eisen worden gesteld in termen van technische accuratesse. De overheid heeft nu eenmaal een bijzondere verantwoordelijkheid op grond van artikel 7 Grondwet en artikel 10 EVRM. Gaat de overheid filteren, dan past daarbij een applicatie gebaseerd op *blacklist filtering* en *human review*. *Dynamic filtering* brengt de overheid structureel in een lastig parket, inclusief het moeten verweren en voeren van juridische processen tegen schadeclaims, omdat die technologie noodzakelijkerwijs *overblocking* impliceert. Om dezelfde reden kan dan niet volstaan worden met filteren op domeinnaam (te grofmazig), maar zal moeten worden uitgekeken naar preciezere methoden zoals filteren op URL en/of unieke kenmerken van afbeeldingen. Het principe van een tweetrapsmethode kan worden doorontwikkeld. In zo'n systeem zou de eerste schifting (verdachte domeinen) overigens wel kunnen worden gedaan op basis van *dynamic filtering*, want die schifting impliceert nog geen blokkade, waarna het verdachte verkeer nader wordt gefilterd op basis van een *human reviewed blacklist* met URL's en bijvoorbeeld hashcodes.

Als de overheid het filteren overlaat aan particuliere partijen, kan eenvoudig gebruik worden gemaakt van filtersystemen die door particuliere bedrijven worden ontwikkeld. Ook daaraan zullen natuurlijk eisen worden gesteld in termen van technische accuratesse, maar de systeemontwikkelaars kunnen zich meer *overblocking* veroorloven, omdat zij niet zoals de overheid gebonden zijn aan artikel 7 Grondwet en artikel 10 EVRM. Het laat zich, gezien de ontwikkelingen in de VS, raden dat de applicaties dan vooral zullen zijn gebaseerd op *dynamic filtering*, aangevuld met een steeds noodzakelijke menselijke check.

(c/d) Het ontwikkelen van systemen is een zaak voor informatiebeveiligingsbedrijven. Als de overheid filtert, hoeft zij niet zelf het filter te maken of te onderhouden, maar dient zij wel eisen te stellen aan het systeem waarmee zij filtert en te weten hoe dat systeem precies werkt (transparantie).[138] Het is in onze westerse samenleving immers niet goed denkbaar dat een overheid het internet filtert en het aan het bedrijfsgeheim van een softwarefabrikant overlaat of en in welke mate zij de grondrechten van burgers schendt. Als het filteren niet een overheidsdaad is, kan de ontwikkeling van nieuwe applicaties aan particuliere bedrijven worden overgelaten.

7.3 Vier scenario's

In onderstaande paragrafen schetsen we vier scenario's. In elk scenario expliciteren we welke actoren een rol spelen en waar verantwoordelijkheden liggen. Ook geven we aan welke technische methoden kunnen worden aangewend en welke juridische implicaties er zijn. Als we spreken over effectiviteit hebben we het oog op de laatstgenoemde, minst ambitieuze doelstelling: het beschermen van internetgebruikers tegen kinderporno.

De scenario's bevinden zich binnen het spectrum van spontane zelfregulering tot aan een door de overheid gecontroleerd internetverkeer. In onze westerse ogen extreme varianten van het laatste scenario zijn reeds te zien in landen als China, Saoedi-Arabië en Iran (zie hoofdstuk 4). Dergelijke varianten zijn in Nederland en overige landen van de Europese Unie niet aan de orde. Wel zijn op Europees niveau sinds 1996 verschillende beleidslijnen uitgezet

[138] Vergelijk de wegens gebrek aan transparantie afgekeurde stemmachines (Rb. Amsterdam, oktober 2007).

waardoor een zelfregulerende benadering geleidelijk is geëvolueerd tot een model dat kenmerken vertoont van co-regulering (Lievens en Dumortier, 2005).[139]

Scenario 1: geen overheidsbemoeienis

Het voor de overheid misschien wel eenvoudigste scenario is om geen actie te ondernemen op het gebied van filteren. Zij richt zich dan op opsporing, harmonisatie van wetgeving en het verbeteren van de internationale samenwerking. Het ontwikkelen, beheren en invoeren van filters tegen kinderpornografisch materiaal laat zij over aan particuliere bedrijven, ideële organisaties en internetgebruikers. Dat is zelfregulering pur sang.

Bij deze strategie kan de overheid haar energie steken in haar kerntaken. Particuliere bedrijven bieden kinderpornofilters in hun pakket aan omdat een groot deel van de samenleving daarom vraagt, vergelijkbaar met de vraag naar antivirus-software en spamfilters. De overheid blijft zo buiten de discussie omtrent overheidscensuur. Uitsluitend private partijen spelen een rol en gebruikers kunnen kiezen op welke wijze, onder welke voorwaarden en bij welke partij zij zich willen beschermen tegen kinderporno (en mogelijk andere strafbare, illegale of ongewenste content) op internet. Een 'bottom-up' benadering, waarbij burgers op een geïndividualiseerde manier kunnen beslissen met welke inhoud zij op internet wensen te worden geconfronteerd (white listing) of met welke juist niet (black listing), doet recht aan de vrijheid van meningsuiting.

Ook voor het overige zijn er geen juridische complicaties. De overheid volgt nauwgezet de ontwikkelingen, want de beslissing om nu niet in te grijpen impliceert niet de beslissing dat de overheid nooit zal ingrijpen.

De politie draagt haar activiteiten op het gebied van filteren over aan een bestaande of nog op te richten ideële organisatie, conform het Engelse model (zie par. 7.2, onder vraag 4). Ze kan de daardoor vrijgekomen tijd steken in bijvoorbeeld opsporingsactiviteiten. Tevens wordt hiermee voorkomen dat producten worden ontwikkeld met overheidsgeld die vervolgens worden vermarkt door commerciële bedrijven. De politie ontwikkelt daarentegen nieuwe opsporingsmethoden, bijvoorbeeld gericht op het traceren van kinderpornogebruikers via digitale financiële sporen. De politie blijft actief in de internationale samenwerking tegen kinderporno. Ze zet ook daar in op het verbeteren van de opsporing en efficiëntere samenwerking. Figuur 7.1 toont de rolverdeling binnen dit scenario.

Figuur 7.1: rolverdeling bij scenario 'geen overheidsbemoeienis'

stakeholders / rollen	politie/justitie	wetgever	private partijen	burgers
samenstellen blacklist			x	
actualiseren blacklist			x	
installeren filter			x	x
bekostigen filter			x	x
besluiten tot filteren			x	x

[139] E. Lievens en J. Dumortier, *Bescherming van minderjarigen online: stand van zaken en blik op de toekomst.* (2005).

Scenario 2: stimuleren van zelfregulering zonder uitvoerende taken voor de overheid
Omdat de ervaringen in het buitenland laten zien dat overheidsbemoeienis, vooral het dreigen met wetgeving, de bereidheid tot filteren onder ISP's vergroot, kiest de overheid nu voor een actieve rol. Uitgangspunt is zelfregulering. De overheid neemt geen uitvoerende taken op zich, maar stimuleert en faciliteert de ontwikkeling van filters. Het feitelijk ontwikkelen, beheren en invoeren van filters tegen kinderpornografisch materiaal laat zij over aan commerciële bedrijven, ideële organisaties en internetgebruikers. De overheid adviseert en stimuleert. Daarnaast richt de overheid zich op opsporing, harmonisatie van wetgeving en het verbeteren van de internationale samenwerking.

Door niet zelf te bepalen wat ISP's al dan niet mogen doorgeven aan hun klanten blijft de overheid buiten de discussie omtrent overheidscensuur. Ook voor het overige zijn er geen juridische complicaties. De overheid volgt nauwgezet de ontwikkelingen in binnen- en buitenland om te zien op welke wijze ze haar stimulerende rol kan invullen.

Net als in het vorige scenario draagt de politie haar uitvoerende activiteiten op het gebied van filteren over aan een bestaande of nog op te richten ideële organisatie en ze richt zich meer op de opsporing en internationale samenwerking.

Het belangrijkste verschil met het eerste scenario is dat dat zich kenmerkt door spontane zelfregulering terwijl dit tweede scenario is te typeren als een meer gecontroleerde zelfregulering. In dit tweede scenario heeft de overheid tot op zekere hoogte de regie in handen en is er op onderdelen sprake van een publiek-private samenwerking (PPS). De overheid probeert – zonder het treffen van wettelijke maatregelen en zonder zelf uitvoerende taken op zich te nemen – invloed uit te oefenen op het doen en laten van de ISP's en andere partijen.

De overheid stimuleert een zo secuur mogelijke manier van filteren en initieert onderzoek naar de werking en effectiviteit van filtersystemen. De huidige wijze van filteren (op domeinnaam) is relatief goedkoop, maar deze methode is noch de meest fijnmazige, noch de meest effectieve. De kans op overblocking is vrij groot en het filter is eenvoudig te omzeilen. Daarom bevordert de overheid de ontwikkeling van betere methoden, ook al hangt daaraan een hoger prijskaartje. In dat verband stimuleert de overheid de totstandkoming van een *Keurmerk Veilig Internetten* voor internetfilters en introduceert dat initiatief op Europees niveau. Onderdeel van het keurmerk is een gestandaardiseerde test om de accuratesse van internetfilters vast te stellen (mate van *under*- en *overblocking*).

Scenario 3: stimuleren van zelfregulering met uitvoerende taken voor de overheid
Het zo-even geschetste scenario kan overgaan in een andere variant van gestimuleerde zelfregulering indien de overheid, met name de politie, uitvoerende taken op zich neemt. Voor opsporingsdoeleinden beheert de politie al een bestand met kinderpornoafbeeldingen. In een publiek-private samenwerking (PPS) stelt de politie die lijst, of een lijst met hashcodes die de afbeeldingen representeren, ter beschikking aan marktpartijen die deze gebruiken bij het ontwikkelen van kinderpornofilters.[140] De keuze omtrent welke afbeeldingen uit die lijst worden gefilterd, laat de politie over aan de marktpartijen. Zo faciliteert de politie het werk van ISP's door een deel van het uitvoerende werk voor haar rekening te nemen terwijl zij niet bepaalt wat er gefilterd zal worden (voor dat laatste is immers een aanvullende wettelijke bevoegdheid vereist, zie hoofdstuk 3 en 6).

In een wat andere variant van dit scenario houdt de politie, zoals nu, een lijst bij van websites waarop naar haar oordeel kinderporno is aangetroffen. Ze stelt deze lijst in een PPS ter beschikking aan marktpartijen, op vergelijkbare wijze als het in de vorige alinea genoemde bestand met kinderpornoafbeeldingen.

[140] Bij deze vorm van PPS moet ermee rekening worden gehouden dat het verspreiden van kinderpornografisch materiaal strafbaar is gesteld. De politie kan dus niet *zonder meer* lijsten met kinderpornografisch materiaal ter beschikking stellen.

Omdat een PPS vereist dat overheid en particuliere organisaties van elkaar weten hoe ze te werk gaan, stelt de politie protocollen op voor het beheren van de bestanden die onder haar verantwoordelijkheid vallen en legt zij zorgvuldig vast hoe kinderpornografisch materiaal is beoordeeld. Het protocol voor de lijst met websites bevat ook regels over de frequentie waarmee wijzigingen worden doorgevoerd en regels omtrent een politie-externe, onafhankelijke controle op de kwaliteit van de lijst (een testmethode voor de mate van *under-* en *over-blocking*). Gezien de snelheid waarmee websites wijzigen, kiest de politie ervoor om de juistheid van de lijst dagelijks te verifiëren.

Figuur 7.2 toont de rolverdeling binnen het scenario met uitvoerende taken.

Figuur 7.2: rolverdeling bij scenario 'gestimuleerde zelfregulering met uitvoerende taken voor de overheid'

stakeholders / rollen	politie/justitie	wetgever	private partijen	burgers
samenstellen blacklist	x			
actualiseren blacklist	x			
installeren filter			x	
bekostigen filter	x		x	x
besluiten tot filteren			x	x

Scenario 4: wettelijk geregeld filter

In het vierde scenario stelt de overheid het invoeren van kinderpornofilters verplicht op basis van formele wetgeving. Zij verplicht ISP's om filters te installeren waarmee websites met kinderporno worden geblokkeerd.

De hierna voorgestelde regeling is niet eenvoudig van aard. Providers zijn op grond van de Europese e-commerce richtlijn en de Richtlijn elektronische communicatie nu eenmaal niet aansprakelijk te houden voor de inhoud van door hen onderhouden internetverkeer. Een verplichting tot filteren en blokkeren kan dan ook alleen binnen het domein van het strafrecht worden gerealiseerd. In het onderzoek is niet meegenomen wat de consequenties zijn van het EU-Verdrag van Lissabon dat per 1 januari 2009 door de lidstaten moet zijn geratificeerd.[141]

In dit scenario dient er een wettelijke bevoegdheid te bestaan op grond waarvan kan worden bevolen dat internetgebruikers geen toegang krijgen tot aanbieders van kinderporno in de zin van artikel 240b Sr. Onderwerp van het bevel zijn in beginsel de ISP's. Aansluitend bij het begrippenapparaat van artikel 1 van de Telecommunicatiewet: aanbieders van een openbare elektronische communicatiedienst waarmee tevens aanbieders van telefonie zijn inbegrepen. De regeling dient providers te verplichten tot het beschikbaar hebben van de benodigde technische voorzieningen.

Indien men de bevoegdheid vorm wil geven langs de lijnen van het onderscheppen van elektronische communicatie, dient in de Telecommunicatiewet in hoofdstuk 13 een verplichting te worden opgenomen dat voornoemde aanbieders verplicht zijn om filterfaciliteiten operationeel te hebben, alsmede een verplichting uitvoering te geven aan een op grond van het Wetboek van Strafvordering hierna te omschrijven gedane vordering.

Een Amvb geeft nadere regeling over de functionaliteit, het gebruik, en verdere procedureregels. Kosten van de ontwikkeling, gebruik en onderhoud van de filterapparatuur komen

[141] Trb. 2008, 11.

geheel of gedeeltelijk voor rekening van de personen en organisaties tot wie het bevel is gericht.

De bevoegdheid kan een plaats krijgen in het eerste boek, Titel IVA, zevende afdeling van Sv, zo nodig met een parallelbepaling in Titel V.[142] Hier wordt aangesloten bij de definities van artikel 126m Sv.

De bevoegdheid wordt uitgeoefend door de officier van justitie dan wel door de rechter commissaris indien een gerechtelijk vooronderzoek aan de orde is. In praktische zin zal het KLPD de maatregel blijven voorbereiden en coördineren.

De bevoegdheid wordt toegepast in geval van het aanbod van kinderporno. Het Wetboek van strafvordering bevat geen bevoegdheden die gericht zijn op een bepaald delict. Directe verbinding met artikel 240b Sr is dan ook niet gewenst. Evenmin is gewenst dat deze bevoegdheid toepassing kan vinden in geval van welk delict dan ook. Afgrenzing kan geschieden door een beperking tot zeer ernstige delicten en tot delicten die men als uitingsdelict kan aanmerken.

De bevoegdheid is niet bedoeld ter vervanging van opsporingsinspanningen, zowel nationaal en internationaal. Nochtans kan het nodig zijn de maatregel toe te passen als een voorlopige maatregel, indien ingrijpen in het kader van opsporing niet mogelijk is of gezien het belang van handhaving van de rechtsorde niet kan worden afgewacht. Figuur 7.3 bevat een richtingbepaling aangaande hoe de bevoegdheid zou kunnen worden verwoord.

Figuur 7.3: richtingbepaling aangaande een tekst voor een filter/blokkeer-bevoegdheid

Art. xxx Sv:

1. In geval van verdenking van strafbaar feit, waarop naar de wettelijke omschrijving een gevangenisstraf van zes jaren of meer is gesteld, kan de officier van justitie, dan wel tijdens het gerechtelijk vooronderzoek de rechter-commissaris, indien voortduren van het strafbare feit een ernstige bedreiging van de rechtsorde vormt, bevelen dat bepaalde niet voor het publiek bestemde communicatie die plaats vindt met gebruikmaking van de diensten van een aanbieder van een communicatiedienst door middel van een technisch hulpmiddel wordt verhinderd.
2. De bevoegdheid van het eerste lid vindt slechts toepassing indien de communicatie deel uitmaakt van het strafbare feit.
3. Het bevel is schriftelijk….en vermeldt….
4. Van de toepassing van de maatregel wordt proces-verbaal opgemaakt. Het proces-verbaal vermeldt de feiten en omstandigheden die aanleiding gaven voor het bevel.
5. Indien uit feiten en omstandigheden blijkt dat aan het bevel van het eerste lid de grondslag is ontvallen, stelt de officier van justitie, dan wel tijdens het gerechtelijk onderzoek de rechter-commissaris, de aanbieders van een communicatiedienst onverwijld schriftelijk op de hoogte.
6. De inrichting en het gebruik van het technisch hulpmiddel worden geregeld bij Amvb.

Niet naleving van het bevel door providers levert een strafbaar feit op (art. 184 Sr). Handhaving van de bepalingen van de Telecommunicatiewet, in dit geval bijvoorbeeld niet-

[142] De zevende afdeling geeft maatregelen die zich richten tot zowel aanbieders van een openbare als niet openbare elektronische communicatiediensten. De Telecommunicatiewet richt zich alleen tot de eerste groep, zodat politie en justitie in het tweede geval eigen technische voorzieningen dienen te treffen ter effectuering van het bevel.

implementatie van de technische voorziening, is opgedragen aan het agentschap Telecommunicatie.

Een variant van het scenario 'wettelijk geregeld filter' is dat de overheid, zoals in sommige andere landen gebeurt, bepaalde personen of organisaties de verplichting oplegt maatregelen te nemen tegen de verspreiding van kinderporno op internet. De overheid regelt dan niet voor zichzelf de bevoegdheid om te filteren maar verplicht bijvoorbeeld werkgevers (Noorwegen) of openbare bibliotheken en scholen (VS) om maatregelen te nemen. Die maatregelen zullen praktisch gesproken al gauw filteren impliceren. De instantie die maatregelen tegen kinderporno neemt, kan zo'n filter betrekken bij een particulier bedrijf.

7.4 Slotoverweging

Welk scenario men ook kiest, met enkele aspecten heeft men steeds op de een of andere wijze te maken:

1. Het is onbekend hoe effectief filteren en blokkeren is tegen (al dan niet commerciële) verspreiding van kinderporno op internet, tegen het op internet ongewenst in aanraking komen met kinderporno of tegen kindermisbruik. Effectiviteitsclaims berusten derhalve op veronderstellingen.
2. Het is technisch onmogelijk een filter te maken dat 100 procent kinderporno tegenhoudt en tegelijk alle legale informatie doorlaat. Daar komt bij dat het informatieaanbod op internet voortdurend verandert. Wat nu terecht wordt gefilterd, kan over enkele momenten ten onrechte zijn. Wie met een filter een serieuze drempel tegen kinderporno wil opwerpen, moet dan ook reëel gesproken[143] een bepaalde mate van structurele *overblocking* accepteren.
3. Filteren van kinderporno door of in opdracht van de overheid betekent een inmenging in het grondrecht van de vrijheid van meningsuiting en informatiegaring (art. 7 Grondwet en art. 10 EVRM). Getoetst aan het laatste artikel is de bestrijding van kinderporno een van de legitieme belangen die een dergelijke inmenging rechtvaardigt, mits sprake is van een formeel-wettelijke grondslag en de inmenging als noodzakelijk in een democratische samenleving kan worden beschouwd (*pressing social need*) en proportioneel is.
4. Als de overheid het filteren zelf ter hand neemt, vergt het forse investeringen (overheidsgeld en -tijd) om een serieuze drempel op te werpen die tegelijkertijd voldoende precies is, om niet in strijd te komen met deze eis van proportionaliteit
5. De (Nederlandse) politie beschikt niet over de bevoegdheid tot het filteren en blokkeren van kinderpornografie op internet. Zo'n bevoegdheid kan niet worden afgeleid uit artikel 2 van de Politiewet (dat is te algemeen).
6. Kinderporno op internet is een grensoverschrijdend probleem. Er zijn ondanks de inspanningen tot harmonisatie nog steeds verschillen in wetgeving tussen landen die nauw samenwerken in de strijd tegen kinderpornografie. Hoe men kinderporno ook aanpakt, gezien het grensoverschrijdende karakter van het probleem verdient verdergaande harmonisatie van wetgeving aandacht.

[143] Theoretisch maar niet reëel is de optie dat men alle items op de blokkeerlijst voortdurend door deskundigen op hun juistheid laat controleren.

Literatuurlijst

Adviescommissie (1980). *Eindrapport van de Adviescommissie Zedelijkheidswetgeving*, 's-Gravenhage: Staatsuitgeverij.

Akdeniz, Y. (1996). Computer Pornography: a Comparative Study of the US and the UK Obscenity Laws and Child Pornography Laws in Relation to the Internet. *International Review of Law Computers & Technology*, 10, 2, pp. 235-261.

Barnpornografiutreding (2005 års barnpornografiutreding) *Barnet i fokus: en skärpt lagstiftning mot barnpornografi.* Stockholm: SOU.

Bijnen, E.J. (1980) Steekproeven. In J.H.G. Segers en J.A.P. Hagenaars (red.) *Sociologische onderzoeksmethoden. Deel II: technieken van causale analyse.* Assen: Van Gorcum, pp. 93-118.

Boerstra, E. (1997) Rechercheren in cyberspace. *Algemeen Politieblad*, 146, 21, 8-9.

Borgers, M.J. (2007) *De vlucht naar voren*, Den Haag: Boom.

Commissie Grondrechten in het digitale tijdperk (2000). *Grondrechten in het digitale tijdperk*, Den Haag: Ministerie van Jusitie.

Clayton, R. (2005) *Failures in a Hybrid Content Blocking System*. Cambridge: Cambridge MIT Institute (CMI).

Datakrimutvalget (2007) *Lovtiltak mot datakriminaliet.* Oslo: Lobo Media AS.

Deibert, R.J., J.G. Palfrey, R. Rohozinski en J. Zittrain (2008) *Access Denied; The Practice and Policy of Global Internet Filtering*. Cambridge, Mass: The Mitt Presss.

Deshmukh, A. en Rajagopalan, B. (2005) Performance analysis of filtering software using Signal Detection Theory. *Decision Support Systems* 2006, 42, 1015 - 1028.

Duncan, M. (1997). Making Inroads Against Crime on the Internet. *RCMP Gazette*, 59, 10, pp. 4-11.

Durkin, K.F. (1997). Misuse of the Internet by Pedophiles: Implications for Law Enforcement and Probation Practice. *Federal Probation: a journal of correctional philosophy and practice*, 61, 3, pp. 14-18.

Eecke, van P. (1997). *Criminaliteit in cyberspace: misdrijven, hun opsporing en vervolging op de informatiesnelweg.* Gent: Mys en Breesch.

Edelman, B. (2003) *Web Sites Sharing IP Addresses: Prevalence and Significance*. Harvard Law School: Berkman Center for Internet and Society.

Engelfriet, A (2007) Richtlijnconform filteren van peer-to-peer verkeer, *IER* 2007, 97.

Elias, N. (1984, oorspr. 1939) *Het civilisatieproces.* Utrecht/Antwerpen: Het Spectrum.

Fleck, M.M., Forsyth, D.A., Bregler, C., 1996. Finding naked people. *4th European Conf. on Computer Vision* 2, 592–602.

Foucault, M. (1975). *Discipline and punish; the birth of the prison.* New York: Vintage Books.

Gerstendörfer, M. (1993) Computerpornographie und virtuelle Gewalt: die digital symbolische Konstruction von Weiblichkeit mit Hilfe der Informationstechnologie. *Beitrage zur feministischen Theorie*, 17, 38, p. 11-22.

Grabowsky NP/ Russell G. Smith /Crime in the digital age, 1998, p.131.

Greenfield, P., R. Rickwood en H. Tran (2001) *Effectiveness of Internet filtering software products*, CSIRO Mathematical and Information Sciences.

Griffith, R.E. (2005) How Criminal Justice Agencies Use The Internet. In A. Pattavina (red.) *Information Technology and the Criminal Justice System.* Thousand Oaks: Sage, pp. 59-77.

Hulst, van der R.C. & Neve, J.M. (2008). *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie.* Den Haag: WODC.

Hunter, P. (2004) BT's Bold pioneering child porn blocks wins plaudits amid Internet censorship concerns. In: *Computer Fraud & Security*, 2004, 9, 4-5

IT- og Telestyrelsen (2006) *Status for europæiske initiativer til bekæmpelse af børneporno på internettet.* København: Ministeriet for Videnskab Teknologi og Utvikling.
IWF (Internet Watch Foundation) (2007) *Annual and Charity report, 2006*. Cambridge: IWF.
Jones, M.J. en J.M. Rehg (1998) *Statistical color models with application to skin detection. Technical Report Series.* Cambridge Research Laboratory.
Kaspersen, H.W.K. (2006) Bestrijding van kinderporno. *Computerrecht*, 314, p.235.
Kaspersen, H.W.K. (2007) Strafbaar bezit van kinderporno. *Computerrecht*, p.56.
Kleef, van J. (2004) Kinderporno kinderspel. *Nieuwe Revu,* nr. 52.
Kranich, N (2004) Why filters won't protect children or adults. *Library Administartion and Management* 18, 1, 14 – 18.
LPDO (Landelijk Project Digitale Opsporing) (2003) *Visie op digitaal opsporen.* Zoetermeer: LPDO.
Lünnemann, K., S. Nieborg, M. Goderie, R. Kool en G. Beijers (2006) *Kinderen beschermd tegen seksueel misbruik. Evaluatie van de partiële wijziging in de zedelijkheidswetgeving.* Den Haag/Utrecht: WODC/.Verwey Jonker Instituut.
Mey, de J.M. (2000) *Uitingsvrijheid,* Amsterdam, p. 97, 98, 128.
Michiels, F.C.M.A., J. Naeyé e.a. (1997). Artikelsgewijs Commentaar Politiewet 1993, Den Haag, p. 38-39.
MKI (Stichting Meldpunt ter Bestrijding van Kinderporno op Internet) (2003) *Jaarverslag 2002* Amsterdam.
MKI (Stichting Meldpunt ter Bestrijding van Kinderporno op Internet) (2004) *Jaarverslag 2003* Amsterdam.
MKI (Stichting Meldpunt ter Bestrijding van Kinderporno op Internet) (2005) *Jaarverslag 2004* Amsterdam.
MKI (Stichting Meldpunt ter Bestrijding van Kinderporno op Internet) (2006) *Jaarverslag 2005* Amsterdam.
MKI (Stichting Meldpunt ter Bestrijding van Kinderporno op Internet) (2007) *Jaarverslag 2006* Amsterdam
Noyon, T.J., Langemeijer, G.E. & J. Remmelink (1982), *Het Wetboek van Strafrecht,* voortgezet door A.J.A van Dorst, J.W. Fokkens, A.J.M. Machielse, Deventer: Kluwer, aant. 1 bij artikel 240b (suppl. 120, 2002).
ONI (OpenNet Initiative) (2004) *Internet Filtering in Saudi Arabia in 2004*.
ONI (OpenNet Initiative) (2005a) *Internet Filtering in Iran in 2004-2005*.
ONI (OpenNet Initiative) (2005b) *Internet Filtering in China in 2004-2005*.
Oppen Gundhus, H. (2006) *For sikkerhets skyld; IKT, yrkeskulturer og kunnskapsarbeid i politiet.* Oslo: Universitetet i Oslo.
Oosterink, M., Eijk E.J. van (2006) *Opsporing Kinderpornografie op internet. Een statusoverzicht.* Den Haag: Ministerie van Justitie.
PO (Projectgroep Opsporing) (2003) *Tegenhouden troef. Een nadere verkenning van Tegenhouden als alternatieve strategie van misdaadbestrijding.* Den Haag: NPI.
PWC (2001) *Kinderpornografie en internet in Nederland: een overzicht van de huidige situatie, knelpunten in de bestrijding, suggesties voor verbeteringen.* Haarlem: PWC.
Resnick, P., Hansen, D. en Richardson, C. (2004) Calculating error rates for filtering software. *Communications of the ACM* 47, 9, 67– 71.
Richardson, C., Resnick, P., Hansen, D. en Derry, A. (2002) Does pornographyblocking software block access to health information on the Internet? *Journal of American Medical Association* 22, 2887– 2894.
Savornin Lohmann, J de (1999) *Evaluatie van wet- en regelgeving inzake kinderpornografie*. Utrecht: Verweij-Jonker Instituut.

Schell, B.H., M.V. Martin, P.C.K. Hung en L. Rueda (2007) Cyber child pornography: A review paper of the social and legal issues and remedies and a proposed technological solution. *Aggression and Violent Behavior* 2007, 12, 45–63.

Shih, J.L., Lee, C.H. en Yang, C.S. (2007) An adult image identification system employing image retrieval technique. *Pattern Recognition Letters* 28, 16, 2367-2374

Stol, W.Ph. (2002) *Kinderporno in cyberspace.* www.wodc.nl.

Stol, W.Ph. (2004) Trends in cybercrime. *Justitiële Verkenningen.* 30, 8, 76-94.

Stol, W.Ph. (2004b) *Handhaven: eerst kiezen dan doen: technische mogelijkheden en beperkingen*. Den Haag: Ministerie van Justitie.

Stol, W. Ph., R.J. van Treeck e.a., (1999) *Criminaliteit in Cyberspace; een praktijkonderzoek naar aard, ernst en aanpak in Nederland*, Den Haag, Elsevier.

Stol, W.Ph., N. Kop en A. Koppenol (2005) *Eén spoor is geen spoor.* Den Haag: Elsevier.

TK (1998) *Nota Wetgeving voor de elektronische snelweg*. Kamerstukken 25 880 nr. 1, Den Haag, Sdu.

Wang, J.Z., J. Li, G. Wiederhold en O. Firschein (1998) System for screening objectionable images. *Computer Communication* 1998, 21, 1355 – 1360.

Wit, L.A.J.M. de (1986) *Verslag van de werkgroep kinderpornografie*. 's-Gravenhage, Ministerie van Justitie.

Yang, J., Z. Fu, T. Tan en W. Hu (2004) A novel approach to detecting adult images. *17th International Conference on Pattern Recognition* 4, 479–482.

Yoo, S.J. (2004) Intelligent multimedia information retrieval for identifying and rating adult images. *KES* 2004, 164–170.

Zeng, Wei, Gao, Wen, Zhang, Tao, Liu en Yang (2004) Image Guarder: An Intelligent Detector for Adult. *Asian Conf. on Computer Vision*, 2004, 198–203.

Zittrain, J en Edelman, B (2002) Documentation of Internet Filtering in Saudi Arabia.Harvard Law School: Berkman Center for Internet and Society.

Overige bronnen

Mediaberichten Noorwegen:

21-09-2004: 'Telenor nøler med barneporno-filter', (www.digi.no)
21-09-2004: 'Filter mot barneporno', (www.teleavisen.no)
23-09-2004: 'Filter mot barneporno på internett' (www.regjeringen.no)
24-01-2005: 'Mange søker etter barneporno', (www.dagbladet.no)
03-03-2005: 'Internettilbydere siler ut barneporno', (www.digi.no)
03-03-2005; 'Blokkering av nettsider gir falsk trygghet', (http://itpro.no)
14-04-2005: 'Flere teleselskaper får barnepornofilter', (www.digi.no)
18-05-2005: 'Telenors barneporno-filter tas i bruk i Sverige', (www.digi.no)
07-06-2005: 'Telenor med filter mot barnepornografi på mobil', (www.pressemeldinger.no)
07-06-2005: 'Plugger igjen smutthull: Telenor med mobilt barneporno-filter', (www.digi.no)
07-06-2005: 'Filter stopper ikke søk etter barneporno', (www.ta.no)
07-08-2005: 'Barnepornofilter stanser 6700 daglig', (www.vg.no)
01-11-2005: 'Filter mot barneporno på mobilen', (www.digi.no)
12-12-2005: 'Ekspansivt marked for barneporno', (www.digi.no)
13-12-2005: 'Tallene fra Telenor: Overdriver surfing etter barneporno', (www.digi.no)
18-01-2006: 'Avslører pengene bak nett-barneporno', (www.digi.no)
14-03-2006: 'Norge langt fremme i kampen mot barneporno', (www.digi.no)
19-05-2006: 'Krever tiltak mot barnepornografi', (www.vg.no)
21-07-2006: 'Engelsk politi får nytt våpen mot barneporno', (www.digi.no)
23-10-2006: 'Godt besøkte sider: stadig flere anmeldelser av barneporno', (www.digi.no)
25-10-2006: 'England avdekker barnepornografi på nett', (www.digi.no)
11-12-2006: 'Norge skal lede kampen mot barneporno', (www.vg.no)
13-12-2006: 'Europa laerer av norsk barneporno-tiltak', (www.digi.no)
10-01-2007: 'Sjekker 22 millioner for barneporno-kjøp', (www.digi.no)
24-10-2007: 'Stoppet 7 millioner barnepornosøk', (www.abcnyheter.no)
05-11-2007: 'Europol avdekker verdensomspennede nettverk av pedofili', (www.politi.no)

Telenor Norge (2004). *Telenor and KRIPOS introduce Internet child pornography filter.* Telenor Press Release, 21 Sep 2004.

Mediaberichten Zweden:

20-07-2004: 'Nytt system stoppar barnporr på internet', (www.aftonbladet.se)
01-10-2004: 'Filter för övervakning', (www.nyteknik.se)
24-01-2005: '7.000 norrmän sökte barnporr på nätet under ett dygn', (www.dn.se)
27-01-2005: 'Bodström vill skärpa lag mot barnpornografi', (www.dn.se)
10-03-2005: 'Telia säger nei till barnporrspärr', (www.aftonbladet.se)
11-03-2005: 'Telia tvärvänder om barnporrfilter', (www.dn.se)
11-03-2005: 'Telia tvärvänder: stoppar barnporr', (www.aftonbladet.se)
14-03-2005: 'Ny sajt för annmälan av parnporr på nätet', (www.dn.se)
29-04-2005: 'Polisen vill blockera barnporr på nätet', (www.dn.se)
16-05-2005: 'Filter införs mot barnpornografi på internet', (www.dn.se)
16-05-2005: 'Teleoperatörer inför barnporrfilter', (http://svt.se)
17-05-2005: 'Telenor AB och Rikskriminalpolisen inför filter mot barnporr på internet', (www.newsdesk.se)
17-05-2005: 'Rikskriminalpolisen inför filter mot barnporr på Internet', (www.webfinanser.se)
17-05-2005: 'Telenor först med filter mot barnporr', (www.nyteknik.se)
27-05-2005: 'Barnporr stoppas med teknikk från virusskydd', (www.nyteknikk.se)

27-06-2005: ‘Trafficking på internet skal stoppas’, (www.sr.se)
28-06-2005: ‘Branschen delad om filter på internet’, (www.sr.se)
17-07-2005: ‘Filter mot barnporrsurfing effectivt’, (www.dn.se)
21-09-2005: ‘Bildfilter stopper förbjuden porr’, (www.nyteknik.se)
25-11-2005: ‘Tiotusentals blockeras från barnporr’, (www.dn.se)
25-11-2005: ‘Filter stopper tusentals pedofiler’, (http://tv4nyheterna.se)
25-11-2005: ‘Växande problem med barnporr i Sverige’, (www.sr.se)
08-02-2007: ‘De bekämpar barnporren på nätet’, (www.gp.se)
14-03-2007: ‘28000 datorer får barnporrfilter’, (www.gp.se)
06-07-2007: ‘Swedish Police Shuts Down Pirate Bay – Again’, (www.piratpartiet.se)
06-07-2007: ‘Rikspolisstyrelsen bekräftar planerad filtering av Pirate Bay’, (http://sakerhet.idg.se)
24-07-2007: ‘Bonsai inte längre klassat som barnporr?’, (www.flashback.se)
02-09-2007: ‘Inget porrsurfande på regeringsdator’, (www.dn.se)
05-09-2007: ‘Politoker i Riksdagen får inte se hemsidor de lagstiftar om’, (http://sydsvenskan.se)
21-11-2007: ‘Riksdagen inför filter mot barnpornografi på internet’, (www.riksdagen.se)
21-11-2007: ‘Barnporrfilter i riksdagen’, (www.svd.se)
21-11-2007: ‘Riksdagen skaffar filter mot barnporr’, (www.dagen.se)
21-11-2007: ‘Barnporrfilter i riksdagen’, (http://hd.se)
21-11-2007: ‘Barnporrfilter i riksdagen’, (http://sydsvenskan.se)

Mediaberichten Engeland
07-06-2004: ‘BT's modest plan to clean up the Net’ (www.theregister.co.uk)
07-07-2004: ‘BT to block child pornography’ (www.theregister.co.uk)
20-07-2004: ‘BT blocks 23,000 child abuse net requests daily’ (www.guardian.co.uk)
20-07-2004: ‘Q&A: Cleanfeed, the anti-child porn software’ (www.timesonline.co.uk)
20-07-2004: ‘250,000 blocks on internet child porn reveal 'shocking' problem’ (www.timesonline.co.uk)
21-07-2004: ‘ISPA seeks analysis of BT's 'Cleanfeed' stats’ (www.theregister.co.uk)
26-10-2005: ‘Bid to block online child porn’ (www.guardian.co.uk)
23-11-2005: ‘Hi-tech fight against internet child abusers’ (www.guardian.co.uk)
07-02-2006: ‘BT concern as child porn traffic spirals’ (http://business.timesonline.co.uk)
29-06-2006: ‘Surfing with a safety net’ (www.guardian.co.uk)

Mediaberichten Nederland
Lensink, H. (2004). Ziek & Slim, *Nieuwe Revue*, 52, p.33-34.
Kleef, J. van (2004). Kinderporno, kinderspel. *Nieuwe Revue*, 52, p.28-32.

20-06-1998: ‘Kinderen voor het grijpen; Justitie laat Internetpedofielen uit onmacht hun gang gaan,’ NRC Handelsblad
23-07-1998: ‘Kinderporno via internet en ondergronds’, NRC Handelsblad
23-01-1999: ‘UNESCO wil internet zuiveren van kinderporno’, NRC Handelsblad
24-01-1999: ‘CDA bepleit internationale wetgeving kinderporno Internet’, ANP
12-01-2000: ‘EO wil provider worden van internet zonder ranzigheid’, de Volkskrant
19-07-2000: ‘Kinderporno via internet neemt toe: Britten willen pedofielen hun creditcard afpakken’, Brabants Dagblad
03-08-2000: ‘Vrije informatie via internet bezorgt regeringen hoofdbrekens’, De Gelderlander
21-02-2001: ‘Filternet EO niet waterdicht’, Dagblad van het Noorden
26-03-2002: ’14 Bibliotheken VS tegen filteren web’, NRC Handelsblad

12-03-2004: ‘EU verhoogt actie tegen websites kinderporno’, ANP
13-03-2004: ‘EU-geld voor veiliger internet’, De Tijd
28-02-2005: ‘Notice en takedown’(www.bof.nl/takedown)
02-06-2005: ‘Kat-en-muisspel met online criminelen’ (www.netkwesties.nl/editie129)
31-01-2006: ‘Kinderporno niet uit te bannen; Advocaat: pak niet de kleine rommelaar, maar de bron’, BN/DeStem
17-03-2006: ‘Morele plicht, Politici eisen hardere aanpak kinderporno via internet’, AD
17-03-2006: ‘Financiële instellingen bestrijden kinderporno’, Reformatorisch dagblad
05-07-2006: ; Filters variëren fors in kostprijs en prestatie’, NRC Handelsblad
21-07-2006: ‘Meldpunt: aantal websites met kinderporno neemt toe’, De Gelderlander
11-09-2006: ‘Duitse politie neemt TOR-servers in beslag’ (www.webwereld.nl/articles/)
29-11-2006: ‘Dweilen met de kraan wijd open’, Provinciale Zeeuwse Courant
12-01-2007: ‘EO wil kinderporno op internet filteren’, NRC Handelsblad
30-01-2007: ‘Internet met filter veiliger?, Niels Huijbregts (www.xs4all.nl/opinie/)
06-02-2007: ‘Over het filteren van kinderporno, Menno Heus (www.xs4all.nl/opinie/)
07-02-2007: ‘UPC blokkeert kinderporno’, De Telegraaf
08-02-2007: ‘Internetprovider gaat websites met kinderporno blokkeren’, De Gelderlander
13-02-2007: ‘Brein blij met klachtenprocedure xs4all en KPN’ (www.tweakers.net)
21-02-2007: ‘Notice & Takedown’, Niels Huijbregts (www.xs4all.nl/opinie/)
23-03-2007: ‘Ook KPN wil kinderporno blokkeren’ NRC Handelsblad
27-03-2007: ‘Onzichtbare kinderporno’, Niels Huijbregts (www.xs4all.nl/opinie/)
29-03-2007: ‘Website in de ban, en dan?: vier redenen waarom kinderpornomaatregel niet werkt’, NRC.NEXT
30-03-2007: ‘Het wegfilteren van uitingsvrijheid’, Remy Chavannes (www.nu.nl)
06-04-2007: ‘Pornofilter onder vuur; kritiek op manier blokkeren kinderpornosites’, NRC.NEXT
02-05-2007: ‘Internetfilters op een hellend vlak’, Frank Kuitenbrouwer, Lex&Libertas, NRC Handelsblad
19-05-2007: ‘Rapport: Censuur op internet in tientallen landen’, Trouw
19-05-2007: ‘Staten trekken hun grenzen ook in cyberspace’, Trouw
11-08-2007: ‘Australië geeft ouders filter voor internet’, de Volkskrant
10-09-2007: ‘Kliksafe met KLPD in zee tegen kinderporno’, Reformatorisch Dagblad
12-09-2007: ‘Meer filtering kinderporno nodig’, Reformatorisch Dagblad
12-09-2007: ‘EU wil zoektermen verbieden’, Niels Huijbregts (www.xs4all.nl/opinie/)
19-09-2007: ‘Prinsjesdag: Cybercrime aanpakken’, Niels Huijbregts (www.xs4all.nl/opinie/)
01-10-2007: ‘Ter Horst steunt blokkadeplannen Frattini (www.xs4all.nl/opinie/)
04-10-2007: ‘Tweede Kamer verliest geduld met providers: Wettelijke plicht kinderporno te weren’, Reformatorisch dagblad
04-10-2007: ‘Kamer: dwing providers kinderporno te weren’, ANP
05-10-2007: ‘Wie echt wil, vindt altijd kinderporno’, DAG
05-10-2007: ‘Rechter moet kinderporno zelf bekijken’, Leeuwarder Courant
05-10-2007: ‘Verplichte blokkade kinderporno’, NRC.NEXT
11-10-2007: ‘Blokkeer kinderporno’, Reformatorisch dagblad
13-10-2007: ‘Kinderporno te bizar om op internet te laten staan’, Brabants Dagblad
13-10-2007: ‘Kinderpornofilter leidt ip-verkeer om’, (www.webwereld.nl/articles/48281)
25-10-2007: ‘Alleen kijken naar kinderporno ook strafbaar’ (www.webwereld.nl/articles/48426)
07-11-2007: ‘KLPD begrijpt klacht providers over ‘morele chantage’ niet’, (www.webwereld.nl/articles/ 48595)
16-11-2007: ‘NFI kan computers met kinderporno vaak niet kraken’

(www.webwereld.nl/articles/48719)
20-11-2007: ‘Porno achter een poort: CDA-Kamerlid wil miljoenen euro’s voor internet-filters’, NRC Handelsblad
15-02-2008: ‘Zoekmachines moeten porno beter afschermen’(www.nu.nl)
19-02-2008: ‘Kinderporno, niet bestrijden maar verstoppen’, het Parool
19-02-2008: ‘Politie laat kinderporno lopen’, het Parool
19-02-2008: ‘GroenLinks: Kinderporno op internet beter aanpakken’, ANP
19-02-2008: ‘Kamervragen over filterfouten bij pedofilter’ (www.webwereld.nl/articles/49951)
20-02-2008: ‘Kinderporno internet beter aanpakken’, De Stentor/Sallands Dagblad
23-02-2008: ‘Een slechte week voor het open internet’, Trouw
15-04-2008: ‘Grote providers weren kinderporno’, Trouw

Technische begrippenlijst

3G	'Third Generation' – een in 2001 in Japan ontwikkelde transmissietechniek waarmee beelden kunnen worden ontvangen met mobiele telefoons, hetgeen 'mobiel internet' mogelijk maakt.
Deep Packet Inspection	Een methode die 'in' de informatie(pakketjes) kijkt die over een netwerk verstuurd worden.
DNS-server:	Een server die de alfanumerieke domeinnaam van een website vertaalt in het numerieke IP-adres.
Domeinnaam:	Een eenvoudig te onthouden alfanumerieke naam die verwijst naar een numeriek IP-adres.
Hash-code:	Een code die op basis van de pixelstructuur van een afbeelding aan die afbeelding gegeven kan worden. Iedere pixel van de afbeelding krijgt een bepaalde waarde toegekend. Hierdoor heeft iedere unieke afbeelding een unieke hashcode.
Hosting:	Het aanbieden van ruimte voor het op een via internet toegankelijke computer opslaan van informatie (bijvoorbeeld in de vorm van een website).
Internet Service Provider (ISP):	Een organisatie of persoon die diensten levert op of via het internet. Bijvoorbeeld de verzorging van de verbinding van een gebruiker met het internet.
Internetter:	Gebruiker van het internet.
IP-adres:	Een unieke code voor een machine die is aangesloten op internet.
Local Area Network (LAN):	Een groep computers die rechtstreeks, of via een gedeeld medium met elkaar verbonden zijn.
Overblocking:	Het tegenhouden van andere content dan men beoogt tegen te houden.
Peer-2-Peer (P2P) systeem	Een computernetwerk dat geen gebruik maakt van servers. De gebruikers van het netwerk zijn direct met elkaar verbonden.
Proxy:	Een machine die staat tussen de computer van de gebruiker en de computer waarmee die gebruiker communiceert.
Underblocking	Het doorlaten van content die men beoogt tegen te houden.
URL (Uniform Resource Locator):	Een specifieke verwijzing naar een bestand of gegeven op een machine. Bijvoorbeeld een webpagina, databasegegeven of e-mail adres.
Webbrowser / browser:	Een computerprogramma waarmee een internetter webpagina's opvraagt. Bijvoorbeeld Windows Internet Explorer, Mozilla Firefox of Safari.
Webserver / Server	Een computerprogramma dat via een netwerk informatieverzoeken ontvangt en vervolgens documenten naar de aanvrager terugstuurt.
Website	Een verzameling van samenhangende webpagina's met één startpagina (homepage). Elke website is op de een of andere manier verbonden aan een unieke domeinnaam.
Webpagina	Een onderdeel van een website.

Afkortingen

3G:	Third Generation
Amvb:	Algemene maatregel van bestuur
Awb:	Algemene wet bestuursrecht
BT:	British Telecom
CCC:	Convention on Cybercrime (Cybercrimeverdrag)
CEOP:	Child Exploitation and Online Protection Team
CEPOL:	European Police College
COSPOL:	Comprehensive Operational Strategic Planning for the Police
CSAADF:	Child Sexual Abuse Anti-Distribution Filter (het 'Noorse'filter)
CIRCAMP:	Cospol Internet Related Child Abusive Material Project
ECPAT:	End Child Prostitution, Child Pornography and Trafficking in Children for Sexual Purposes
EVRM:	Europees Verdrag voor de Rechten van de Mems
GSM:	Global System for Mobile Communication
GW:	Grondwet
ICP :	Internet Content Provider
ICT:	Informatie- en Communicatie Technologie
IP :	Internet Protocol
ISP:	Internet Service Provider
ISPA:	Internet Services Providers' Association
IT:	Informatie Technologie
IWF :	Internet Watch Foundation
KLPD :	Korps Landelijke Politie Diensten
MMS:	Multimedia Messaging Service
NGO:	Non-Governmental Organization
NTD:	Notice and Take Down
P2P:	Peer to peer
PCTF:	Police Chiefs Task Force
PPS:	Publiek-Private Samenwerking
SMS:	Short Message Service
Sr:	Wetboek van strafrecht
Sv:	Wetboek van strafvordering
URL:	Uniform Resource Locator
WOB:	Wet openbaarheid van bestuur

Bijlage I: begeleidingscommissie

de heer prof. mr. R.V. De Mulder MBA EUR – Faculteit der Rechtsgeleerdheid, voorzitter
de heer S. van de Geer Ministerie van Justitie, Dir. Rechtshandhaving & Criminaliteitsbestrijding
de heer drs. M. Kruissink Ministerie van Justitie, WODC
mevrouw mr. M.J.C. Spoormaker Arrondissementsrechtbank Rotterdam
de heer C.S. Groeneveld KLPD / DNRI

Bijlage II: lijst met geïnterviewde personen

Naam	Instelling / bedrijf	Functie
R. van der Aart	UPC. Communications and Public Policy	Public Relations Manager
L. Arzooyan	KLPD. Dienst Nationale Recherche. Unit Operationele Expertise	Internet Rechercheur
Ir. E.J. van Eijk	Ministerie van Justitie. Nederlands Forensisch Instituut.	Wetenschappelijk Onderzoeker Digitale Technologie/OOCI
C.S. Groeneveld	KLPD, Team Bestrijding Kinderporno	Producteigenaar Bestrijding Kinderpornografie
Drs. L. Groeneveld	Meldpunt Kinderporno op Internet	Directeur Meldpunt Kinderporno
Mr. Drs. B. Den Hartigh	Openbaar Ministerie. Landelijk Parket. Nationale Recherche Eenheid Rotterdam	Officier van Justitie High Tech Crime
B. Heinink	Orange	Manager Public Affairs
Drs. J. van Hoorn	Corgwell / KLPD. Dienst Nationale Recherche Informatie	Algemeen projectleider Internetsurveillance
Drs. N. Huijbregts	XS4ALL	Public Affairs/Woordvoering
T. Jekel	Comsenso	Managing Director
E. van Laarhoven	Comsenso	Director Interworking Technology
Mr. R. Kolthek	UPC. Legal and Regulatory Affairs	Senior Legal and Regulatory Counsel
E. Kuijl	KLPD. Dienst Nationale Recherche Informatie	Sr.specialist expertise Team Kinderpornografie en Pedosexuele Misdrijven
S. McIntyre	XS4ALL	Security Officer
B.J. Peters	Kliksafe	Directeur Kliksafe
Ing. P. Peters	SURFcert / Universiteit Twente Dienst Informatietechnologie, Bibliotheek & Educatie (ITBE)	Senior Netwerkbeheerder Universiteit Twente. SURFcert Officer voor SURFcert
Ir. R. Prins	Fox-IT	Managing Director
H. van Rhijn	Kliksafe	Productmanager
Drs. J. Schuurman	SURFcert	Directeur SURFcert
G. Smit	KLPD. Dienst Nationale Recherche. Unit Operationele Expertise	Internetrechercheur
Mr. M. Verhulst	XS4ALL	Public Affairs/Strategie
G. Vleerbos	Politie Twente. Divisie Recherche. Bureau Commerciële Zedenzaken.	Regionaal Coördinator Kinderpornografie
P. de Wolf	Kliksafe	Contentbeheerder
F. Zanderink	Politie Twente. Divisie Recherche. Bureau Commerciële Zedenzaken.	Regionaal Coördinator Kinderpornografie
Mr. M. Zoetekouw	KLPD. Dienst Nationale Recherche. Unit Operationele Expertise	Jurist

Bijlage III: schouwprotocol blacklist KLPD

Procedure vooraf (filteren)	
1. Bekendheid met site	ÿ Op basis digitale recherche door KLPD
	ÿ Melding Meldpunt Kinderporno op Internet
	ÿ Melding Particulier
	ÿ Melding internationale zusterorganisatie
	ÿ Melding overig, namelijk….
2. Toetsing 240 Sr	ÿ Rechterlijke toets KP
	ÿ Toetsing KLPD
3. Criteria toetsing	ÿ Afbeelding komt overeen met afbeelding uit landelijke database KP
	ÿ KP op basis van eigen beoordeling
4. Borging	ÿ Toetsing door 1 persoon
	ÿ Toetsing door 2 personen
	ÿ Toetsing door 3 of meer personen
5. Andere criteria	ÿ Overig, namelijk,……..
6. Datum van toevoegen website aan blacklist	
7. Datum meest recente controle site blacklist	
Schouw blokkeren	
8. Bestaat website nog?	ÿ Ja ÿ nee
9. Is KP op de site aanwezig?	ÿ Ja ÿ nee
10. Niveau KP	ÿ IP adres ÿ Domein ÿ URL: niveau…….
11. Overblocking	ÿ Ja ÿ nee
12. Typering site	ÿ Website bevat overwegend kinderpornografisch materiaal ÿ Website bevat overwegend pornografisch materiaal ÿ Website met incidenteel kinderporno ÿ Website bevat overige strafbare of illegale content, namelijk…..
Aanbieder	
13. Land van herkomst	
14. Commercieel	ÿ Ja ÿ nee
Gebruiker	
15. autorisaties	ÿ vrij toegankelijk ÿ inlogcode ÿ alleen toegang na betaling

Bijlage IV: convenant KLPD

Convenant KLPD en ISP

INVOERING BLOCKER TER BEPERKING VAN DE VERSPREIDING van kinderporno op internet

ondergetekenden:
Het Korps landelijke politiediensten, gevestigd te Hoofdstraat 54, te 3972 LB Driebergen, te dezen rechtsgeldig vertegenwoordigd door (nader te benoemen namens de Korpschef),
hierna te noemen: KLPD;

en (naam van de provider en vertegenwoordiger provider) ,

hierna te noemen: ISP;

Verklaren te zijn overeengekomen als volgt:

1. KLPD en ISP (hierna: Partijen) zijn van mening dat de verspreiding van kinderporno via Internet onwenselijk is en dient te worden tegengegaan, en dat zij door deze samenwerking een bijdrage kunnen leveren aan deze doelstelling in aanvulling op de voortdurende inspanningen van KLPD ter bestrijding van kinderporno.
2. ISP is bereid om een blokkade te introduceren (hierna: de Blocker) die voor haar abonnees de toegang blokkeert tot websites die door KLPD zijn geïdentificeerd als websites met content die binnen de reikwijdte valt van het verbod van artikel 240b van het Wetboek van Strafrecht (dergelijke content wordt hierna aangeduid als: Kinderporno). Onder de websites met Kinderporno vallen ook de websites die deze faciliteren de zogenaamde betaalpagina's (hierna te samen verder te noemen: Websites).
3. KLPD zal hiertoe regelmatig geactualiseerde lijsten aanleveren met Websites (hierna: de Lijsten). Zo nodig zullen Partijen met elkaar nadere afspraken maken over de regelmaat en de wijze van aanlevering van de Lijsten door KLPD aan ISP.
4. ISP zal de Lijsten zonder wijziging opnemen in de Blocker. Hierdoor wordt voor haar abonnees de toegang tot de in de Lijsten opgenomen Websites geblokkeerd. Indien een abonnee het adres van een dergelijke Website opgeeft in de browser, zal ISP ervoor zorgen dat in plaats daarvan de door KLPD aangeleverde "Stop-pagina" wordt doorgegeven. De Stop-pagina zal in elk geval een mededeling bevatten dat abonnees voor vragen of klachten terecht kunnen bij KLPD (met relevante contact-gegevens). De huidige versie van de Stop-pagina is aangehecht als Bijlage. Indien KLPD de Stop-pagina wil wijzigen, zal zij hierover eerst in overleg treden met ISP.
5. Om het risico op verdere verspreiding van Kinderporno tegen te gaan, zullen Partijen de inhoud van de Lijsten uitsluitend gebruiken voorzover nodig om de Blocker te laten functioneren.

6. ISP treedt niet in de beoordeling van de Websites die door KLPD op de Lijsten worden geïdentificeerd als websites met Kinderporno dan wel daaraan faciliterende websites, maar verlaat zich op de expertise van KLPD als landelijke opsporingsautoriteit die belast is met de bestrijding van (onder meer) Kinderporno op Internet.
7. KLPD draagt volledige verantwoordelijkheid voor het opstellen van de Lijsten ten behoeve van de Blocker en vrijwaart ISP voor eventuele schade die voortvloeit uit fouten in de Lijsten. Indien derden zich bij ISP beklagen dat een website ten onrechte door de Blocker geblokkeerd wordt omdat die geen Kinderporno bevat dan wel daaraan faciliterende websites, zal ISP deze partijen doorverwijzen naar KLPD.
8. Deze samenwerking geeft KLPD geen aanspraak op informatie over de abonnees van ISP, zulks onverminderd de bestaande wettelijke bevoegdheden van de opsporingsautoriteiten om gegevens binnen de grenzen van de wet van ISP te vorderen.
9. Partijen zullen deze samenwerking minstens eens per half jaar gezamenlijk evalueren, waarbij ook de effectiviteit van de Blocker kan worden besproken.
10. Elk der Partijen is gerechtigd om de samenwerking op elk gewenst moment te beëindigen. Indien een Partij het voornemen hiertoe heeft, zal hij de andere Partij daarvan zo tijdig mogelijk op de hoogte stellen, zo mogelijk met opgave van redenen.
11. Bij externe communicatie zullen Partijen met elkaar in overleg treden over de inhoud van hun communicatie, voorzover redelijkerwijs mogelijk voorafgaand aan die externe communicatie. Bij beëindiging van deze samenwerking zullen Partijen in elk geval tevoren met elkaar in overleg treden over de externe communicatie.

Aldus overeengekomen en opgemaakt in tweevoud te (plaats en datum)

Korps landelijke politiediensten (naam provider)