

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

© 2008 WODC, ministerie van Justitie, auteursrecht voorbehouden
Behoudens de in of krachtens de Auteurswet van 1912 gestelde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen of enige andere manier, zonder voorafgaande schriftelijke toestemming van de uitgever. Voor zover het maken van reprografische verveelvoudigingen uit deze uitgave is toegestaan op grond van artikel 16h Auteurswet 1912 dient men de daarvoor wettelijk verschuldigde vergoedingen te voldoen aan de Stichting Reprorecht (Postbus 3060, 2130 KB Hoofddorp, www.reprorecht.nl). Voor het overnemen van (een) gedeelte(n) uit deze uitgave in bloemzangen, readers en andere compilatiewerken (art. 16 Auteurswet 1912) kan men zich wenden tot de Stichting PRO (Stichting Publicatie- en Reproductierechten Organisatie, Postbus 3060, 2130 KB Hoofddorp, www.cedar.nl/pro).
No part of this book may be reproduced in any form, by print, photoprint, microfilm or any other means without written permission from the publisher.

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

Inhoudsopgave

Voorwoord.....	i
Samenvatting	ii
Summary.....	viii
1. Inleiding en verantwoording.....	1
1.1 Aanleiding tot dit onderzoek	1
1.2 Onderwerp en doel van onderzoek	1
1.3 Zelfregulering en regie	2
1.4 Onderzoeksvragen.....	2
1.5 Methodische verantwoording	4
2. Filtertechnieken.....	6
2.1 Digitale verspreiding van kinderporno	6
2.2 Technische methoden om te blokkeren.....	10
2.3 Beheersgebieden.....	20
2.4 Samenvatting	22
3. Juridische context	24
3.1. Strafrechtelijke definitie van kinderporno	24
3.2 Internationale harmonisatie van strafwetgeving.....	30
3.3 Kinderporno volgens de Aanwijzing van het College van Procureurs-generaal.....	33
3.4. Bescherming van de persoonlijke levenssfeer.....	34
3.5 Verantwoordelijkheid van ISP's voor het toegankelijk maken van kinderporno	35
3.6 Bevoegdheid van de politie op grond van de Politiewet	36
3.7 Specifieke Wettelijke Bevoegdheden.....	37
3.8 Overwegingen over Rechtsmacht	40
3.9 Vrijheid van meningsuiting	41
3.10 Samenvatting	44
4. Buitenlandse ontwikkelingen	47
4.1 Inleiding.....	47
4.2 Noorwegen.....	47
4.3 Zweden.....	60
4.4 Engeland	65
4.5 Verenigde Staten van Amerika.....	71
4.6 Enkele niet-westerse landen.....	74
4.7 Samenvatting	78
5. Nederlandse situatie	81
5.1 Inleiding.....	81
5.2 Tegengaan van de verspreiding van kinderporno op internet	83
5.3 Effectiviteit van verwijderen en filteren.....	89
5.4 Resultaten schouw blacklist KLPD.....	90
5.5 Samenvatting	95

6. Juridische analyse filterpraktijk in Nederland	96
6.1 Inleiding.....	96
6.2 De strekking van het convenant	96
6.3 De blacklist van het KLPD.....	99
6.4. Naar een wettelijke filterplicht?	100
6.5 Samenvatting	101
7. Hoe nu verder?	103
7.1 Conclusies.....	103
7.2 Antwoorden op de onderzoeksvragen.....	108
7.3 Vier scenario's	113
7.4 Slotoverweging.....	118
Literatuurlijst	119
Overige bronnen.....	122
Technische begrippenlijst.....	126
Afkortingen.....	127
Bijlage I: begeleidingscommissie	128
Bijlage II: lijst met geïnterviewde personen.....	129
Bijlage III: schouwprotocol blacklist KLPD	130
Bijlage IV: convenant KLPD	131

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 geëlitimeerd 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 informatie, 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.

Filbertechnieken

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 gesproken¹ 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 hier toe 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, heeft 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 allerlei 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 deduced 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 spoken² 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 technically 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 behalf 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.