

Filteren van kinderporno op internet

Een verkenning van technieken en reguleringen in binnen- en buitenland

Samenvatting

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 bloemzingen, 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

Samenvatting

2008

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 geëgitimeerd 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.

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 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

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

beantwoordt. 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 overheidsbemoediging 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, 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 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.