Aan het Ministerie van Justitie
T.a.v. Directie Wetgeving

Datum: 29 september 2010-09-29
Onderwerp: Internetconsultatie wetsvoorstel bestrijding computercriminaliteit

Geachte heer, mevrouw,

XS4ALL maakt hierbij graag gebruik van de mogelijkheid om te reageren op de Internetconsultatie over het wetsvoorstel bestrijding computercriminaliteit.

XS4ALL beperkt zich in haar reactie tot de vordering tot het ontoegankelijk maken van gegevens.

De reactie van XS4ALL mag worden gepubliceerd. XS4ALL zal dat zelf ook doen op haar website.

Inleiding

1 De Minister van Justitie (de "Minister") heeft op 28 juli 2010 het concept-wetsvoorstel 'versterking bestrijding computercriminaliteit' (het "wetsvoorstel") en een bijbehorende Memorie van Toelichting (de "Toelichting") ter consultatie gepubliceerd. Het wetsvoorstel bevat een zelfstandige regeling van de bevoegdheid van de officier van justitie om gegevens op het internet ontoegankelijk te (laten) maken, eventueel met oplegging van een dwangsom.

2 XS4ALL is een van de eerste internetaanbieders van Nederland en legt bij haar dienstverlening de nadruk op kwaliteit, veiligheid en vertrouwelijkheid. Op grond van haar technische expertise en maatschappelijke betrokkenheid neemt zij actief deel aan de publieke discussie over technische, juridische en maatschappelijke aspecten van internettechnologie.

3 XS4ALL heeft om technische, juridische en maatschappelijke redenen kritiek op de voorgestane regeling. Het wetsvoorstel creëert een zeer ruime bevoegdheid om aan internetaanbieders en derden te bevelen dat informatie op internet ontoegankelijk wordt gemaakt, zonder voldoende noodzaak en zonder adequate beperkingen en

waarborgen. Het voorstel heeft daarbij onvoldoende oog voor wat wel en niet mogelijk is als het gaat om het blokkeren en verwijderen van informatie en wat de (juridische) gevolgen zijn van toepassing van verschillende technieken. Het voorstel heeft in het geheel geen oog voor de belangen van verzenders en ontvangers van informatie en elementaire grondrechten.

4 In deze zienswijze licht XS4ALL de kritiek die zij heeft op de voorgestelde bevoegdheid toe. Ter nadere onderbouwing van haar standpunten voegt XS4ALL een rapport bij waarin zij haar standpunt met betrekking tot filteren op last van justitie uiteenzet. Daarin komen niet alleen de feitelijke en juridische dimensie van het ontoegankelijk maken van informatie op internet aan de orde, maar wordt ook besproken aan welke randvoorwaarden een wettelijke regeling die filteren mogelijk maakt – zoals de voorgestelde regeling – minstens moet voldoen, waaronder voorafgaande rechterlijke toetsing en beperking tot specifiek omschreven, ernstige strafbare feiten.

De voorgestelde regeling

5 In de kern komt de voorgestelde regeling, vast te leggen in artikel 54a Sr en de artikelen 125p en 125q Sv, neer op het volgende:

- Het voorgestelde artikel 125p Sv geeft iedere officier van justitie de bevoegdheid om van de aanbieder van een communicatiedienst of van iemand die de beschikkingsmacht heeft over een geautomatiseerd werk, te vorderen om onverwijld alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit nodig is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.

- Indien de aanbieder voldoet aan een vordering op grond van artikel 125p Sv, wordt hij als zodanig niet vervolgd bij een strafbaar feit dat door middel van de door hem geleverde dienst wordt begaan.

- Indien de aanbieder niet voldoet aan een vordering, kan hij wel worden vervolgd in verband met het strafbare feit dat door middel van de door hem geleverde dienst wordt begaan. Bovendien kan aan hem op grond van het voorgestelde artikel 125q Sv een dwangsom worden opgelegd.

- De officier van justitie heeft geen machtiging van de rechter-commissaris (R-C) nodig om een vordering op grond van artikel 125p Sv te doen. Wel kan de betrokken informatieaanbieder of degene aan wie de vordering wordt gericht, achteraf een klaagschrift indienen bij de rechtbank (artikel 552a Sv).

- De bevoegdheid is beschikbaar bij het dreigen of voortduren van elk strafbaar feit, ongeacht de ernst daarvan.

Reikwijdte

6 De bedoeling van de voorgestelde Regeling is "de strafrechtelijke mogelijkheden om "strafbare content" effectief en doelmatig van het internet te verwijderen, verder te versterken, vooral in gevallen waarin internetproviders daartoe niet op basis van vrijwilligheid overgaan", aldus de Toelichting.[1] De Toelichting onderkent de bereidwilligheid van internetproviders om mee te werken aan de Gedragscode Notice and Takedown en strafvorderlijke bevelen en onderbouwt niet dat, en waarom, de huidige wetssystematiek onvoldoende zou zijn voor de aanpak van strafbare feiten op of via internet (laat staan dat is gemotiveerd waarom de voorgestelde bevoegdheid daarvoor noodzakelijk is).[2]

7 Daarbij wordt op meerdere plaatsen de indruk gewekt dat de voorgestelde bevoegdheid een beperkte strekking zou hebben. Bij bestudering van de voorgestelde wetsbepalingen blijkt echter dat van enige beperking geen sprake is. Zo suggereren de titel van het Wetsvoorstel ('versterking bestrijding computercriminaliteit'), en passages in de Toelichting dat de nieuwe bevoegdheid alleen kan worden ingezet tegen delicten in de sfeer van computercriminaliteit.

> *De snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit roepen voortdurend de vraag op of de juridische instrumenten nog voldoende zijn toegesneden om computercriminaliteit effectief te bestrijden.*[3]

8 De voorgestelde bevoegdheid is echter niet beperkt tot delicten in de sfeer van computercriminaliteit, maar kan ter voorkoming en beëindiging van ieder strafbaar feit worden ingezet.

9 Op meerdere plaatsen in de Toelichting wordt bovendien gesuggereerd dat de bevoegdheid alleen een *achtervang* is voor weigerachtige *hosting* providers die op basis van de Gedragscode niet bereid zijn strafbare informatie te verwijderen.

> *De bevoegdheid is van belang in die gevallen waarin de aanbieder van een communicatiedienst of degene die de beschikkingsmacht heeft over een geautomatiseerd werk, niet bereid is op basis van de gedragscode "Notice and Take Down" de gege-*

1 Ontwerp Toelichting, p. 1.
2 Over de bereidwilligheid van internetproviders zie: Ontwerp Toelichting, p. 26.
3 Ontwerp Toelichting, p. 2.

vens ontoegankelijk te maken en de vordering nodig is om het strafbare feit te beeindigen of om nieuwe strafbare feiten te voorkomen.[4]

en:

Zoals gezegd is de voorgestelde regeling, evenals de bestaande regeling van artikel 54a Sr, bedoeld voor de gevallen waarin de zelfregulering binnen de bedrijfstak tekort schiet.[5]

10 Uit de voorgestelde wetstekst volgt echter dat de bevoegdheid niet alleen uitgeoefend kan worden tegen hosting providers die een Notice and Takedown-verzoek (een "NTD-verzoek") hebben genegeerd. De bevoegdheid kan in de eerste plaats worden gericht tot aanbieders van communicatiediensten, als omschreven in artikel 126la van het Wetboek van Strafvordering (Sv). Daaronder vallen niet alleen *hosting* providers, maar ook *access* providers, alsmede alle andere aanbieders van andere openbare en besloten communicatiediensten. Daarbij kan het bovendien om zowel opgeslagen als getransporteerde communicatie gaan. De bevoegdheid kan daarnaast worden gericht tegen elke andere persoon "die beschikkingsmacht heeft over een geautomatiseerd werk". Daarover stelt de Toelichting:

Dat is degene die een website op het internet geplaatst heeft en die in staat moet worden geacht de website aan te passen of de inhoud daarvan van het internet te verwijderen.

11 Als hieruit moet worden opgemaakt dat deze zinsnede alleen op een beperkte groep websiteaanbieders ziet, dient dat expliciet te worden vastgelegd, bij voorkeur in de tekst van de wettelijke bepaling zelf. In de huidige formulering kan de bevoegdheid tegen iedereen worden ingezet.

12 Door te stellen dat de nieuwe bevoegdheid is gericht op verankering van de Gedragscode wordt bovendien gesuggereerd dat de voorgestelde bevoegdheid ook het uitgangspunt van die gedragscode deelt, namelijk *verwijdering* van strafbare content door een tussenpersoon van wiens diensten de aanbieder van de strafbare informatie gebruik maakt. Het uitgangspunt van de Gedragscode blijkt expliciet uit de artikelen 2a, 3 en 6b van de Gedragscode. Dat verwijdering dient te geschieden door een tussenpersoon van wiens diensten de informatieaanbieder gebruik maakt blijkt uit de Toelichting op de Gedragscode:

Hierbij dient de melder de juiste tussenpersoon te vinden: de inhoudsaanbieder gebruikt een faciliteit op Internet van de tussenpersoon.[6]

---

4 Ontwerp Toelichting, p. 3.
5 Ontwerp Toelichting, p. 4.

En de toelichting op artikel 6b van de Gedragscode:

Omdat er geen twijfel bestaat over de onrechtmatigheid of strafbaarheid van de betreffende inhoud, dient de tussenpersoon onverwijld maatregelen te nemen die ertoe leiden dat de inhoud off-line gaat. Zo mogelijk neemt de tussenpersoon hierover eerst contact op met de inhoudsaanbieder, bijvoorbeeld als verwacht mag worden dat deze onmiddellijk zal meewerken.

13 Dit uitgangspunt sluit een vordering jegens partijen van wiens diensten een informatieaanbieder *geen* gebruik maakt, zoals *access* providers van potentiële consumenten van strafbare informatie, uit. Het uitgangspunt van het wetsvoorstel is echter veel ruimer: op basis daarvan kunnen niet alleen *hosting* providers, maar (onder andere) ook *access* providers worden aangesproken. Uit de Toelichting blijkt dat de bevoegdheid niet alleen strekt tot het *verwijderen* van strafbare informatie, maar dat het ook gaat om het *filteren* en *blokkeren* van strafbare informatie.[7]

14 Ten slotte is de voorgestelde koppeling tussen de voorgestelde artikelen 54a van het Wetboek van Strafrecht (Sr) en 125p Sv verstrekkender dan, en daarom in strijd met, de Richtlijn Elektronische handel (de "Richtlijn").[8] Artikel 14 van de Richtlijn bepaalt dat hosting providers onder de daar genoemde voorwaarden niet aansprakelijk zijn voor de vervoerde of opgeslagen inhoud. Uit het tweede lid van het artikel blijkt weliswaar dat deze uitsluiting van aansprakelijkheid niet in de weg staat aan een rechterlijk verbod of bevel, maar (a) het voldoen aan zo'n verbod of bevel is geen voorwaarde voor toepassing van de aansprakelijkheidsuitsluiting en mag door lidstaten ook niet als zodanig worden gesteld; en (b) een vordering op grond van het voorgestelde artikel 125p Sv wordt gedaan door de officier van justitie en is dus geen rechterlijk verbod of bevel. De Richtlijn stelt voor *hosting* providers als enige voorwaarde voor aansprakelijkheidsuitsluiting dat zij geen kennis hebben van de onmiskenbaar illegale informatie en ingrijpen zodra zij die kennis wel hebben. Voor *access* providers geldt dat zij nooit aansprakelijk zijn voor vervoerde op opgeslagen inhoud, ook wanneer zij kennis dragen van de illegaliteit van de informatie en niet prompt handelen om gegevens ontoegankelijk te maken. De voorgestelde regeling van artikel 54a Sr en 125p Sv gaat – in strijd met de richtlijn - veel verder.

15 De samenvatting op pagina 13 van de Toelichting van de artikel 12-14 van de Richtlijn is dan ook onjuist, omdat daarin het onderscheid tussen hosting providers en access

---

[6] Toelichting op de Gedragscode Notice and Takedown, p. 2. Zie: http://www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf.

[7] Ontwerp Toelichting, p. 23.

[8] Richtlijn 2000/31/EG van het Europees 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 („richtlijn inzake elektronische handel"), *Pb EG* L 178/1.

providers wordt miskend. Acces providers zijn immers ook niet aansprakelijk wanneer zij níet prompt handelen om gegevens ontoegankelijk te maken. Daarbij is de verwijzing naar de Memorie van Toelichting bij de Aanpassingswet richtlijn elektronische handel (Kamerstukken II 2001/02, 28 197, nr. 3, blz. 25) misleidend, omdat daarin het onderscheid wel correct wordt gemaakt.

16 Bij het voorgaande moet bedacht worden dat het wetsvoorstel voorafgaande rechterlijke controle (de op grond van artikel 54a Sr vereiste machtiging van de R-C) vervangt door de *mogelijkheid* van rechterlijke controle achteraf (door middel van een klaagschrift als omschreven in artikel 552a Sv). Op het moment van een eventuele rechterlijke beoordeling van de vordering, is de vordering al gedaan en de informatie al verwijderd of geblokkeerd. XS4ALL verwacht bovendien dat in praktijk niet vaak tot een dergelijke toetsing zal komen (hetgeen hierna in § 30 nader zal worden toegelicht). Rechterlijke controle *achteraf* heeft daarom geen of nauwelijks begrenzende werking ten aanzien van de hiervoor besproken (te) ruime reikwijdte van de bevoegdheid.

Toepassingssystematiek

17 XS4ALL heeft om praktische en principiële redenen kritiek op de voorgestelde toepassing(systematiek) van de voorgestelde bevoegdheid. Op basis van de voorgestelde systematiek is het voor XS4ALL niet duidelijk hoe zij aan een vordering op grond van artikel 125p Sv zou moeten voldoen. Het baart XS4ALL daarbij zorgen dat een vordering op grond van artikel 125p Sv kan worden versterkt met een dwangsom en de voorafgaande rechterlijke toetsing, waar het huidige artikel 54a Sr in voorziet, vervalt.

Uitvoering

18 Het voorgestelde artikel 125p Sv behelst een verplichting om gegevens 'ontoegankelijk te maken'. Uit de verwijzing in het derde lid van het artikel naar artikel 125o lid 2 Sv volgt dat het gaat om "het treffen van maatregelen om te voorkomen dat [...] derden verder van die gegevens kennisnemen of gebruikmaken [alsmede] het verwijderen van de gegevens uit het geautomatiseerde werk". Uit de Toelichting blijkt dat het dus gaat om (a) het verwijderen en (b) het filteren of blokkeren van informatie op internet.[9]

19 In de discussie over filteren (of in algemene zin het ontoegankelijk maken van informatie op internet) heeft XS4ALL altijd benadrukt dat het noodzakelijk is om onderscheid te maken tussen de verschillende manieren waarop informatie 'ontoegan-

[9] Ontwerp Toelichting, p. 15.

kelijk gemaakt' kan worden. Het is daarbij van belang scherp onderscheid te bewaken tussen verschillende hoedanigheden waarin tussenpersonen acteren, enerzijds die van (1) hosting provider, die informatie van klanten opslaat en beschikbaar stelt, en anderzijds die van access provider, die alleen voor haar klanten verbindingen levert en data transporteert (ook wel: mere conduit). Bij mere conduit moet dan nog onderscheid gemaakt worden tussen (2) de situatie waarin de informatieaanbieder een klant is van XS4ALL, in die zin dat XS4ALL de verbinding levert tussen de server waarop de informatie staat en het internet, en (3) de situatie dat XS4ALL geen relatie heeft met de informatieaanbieder maar alleen een klantrelatie heeft met degene die de – elders op het internet opgeslagen – informatie wil raadplegen.

20 Kort gezegd kan een hosting provider in situatie 1 de informatie verwijderen, kan een access provider in situatie 2 de informatie voor het gehele internet onbereik-baar maken, maar kan een access provider in situatie 3 hoogstens de toegang tot die elders opgeslagen informatie blokkeren oftewel filteren. In alle gevallen wordt de beschikbaarheid van informatie beperkt. Bij verwijdering wordt alle toegang ertoe geblokkeerd, maar wanneer een access provider informatie blokkeert of filtert heeft dat alleen gevolgen voor de eigen klanten van die provider. Verwijderen, onbereikbaar maken en filteren leiden tot heel andere gevolgen wat betreft (1) omzeilingsmogelijkheden (underblocking), (2) bijvangst (overblocking) en (3) kosten.

21 Voor een nadere toelichting op het voorgaande, zie de paragraaf "De feitelijke dimensie van filteren" van het bijgevoegde standpunt van XS4ALL inzake filteren.

22 Dit onderscheid wordt in het Wetsvoorstel en de Toelichting ten onrechte niet gemaakt of onderkend. Als gevolg daarvan is het voor XS4ALL niet duidelijk hoe zij aan een vordering op grond van artikel 125p Sv zou moeten voldoen. Daarmee blijft ook onduidelijk om welke aanpassingen in haar bedrijfsvoering de voorgestelde regeling vraagt en welke kosten daarmee voor XS4ALL gemoeid zijn. Door het ontbreken van een onderscheid tussen verschillende manieren waarop informatie ontoegankelijk kan worden gemaakt, brengt het wetsvoorstel bovendien geen rangorde aan tussen verschillende maatregelen die daaronder kunnen vallen.

23 In de discussie over filteren heeft XS4ALL altijd benadrukt dat waar bepaalde, door justitie als strafbaar beschouwde informatie wordt gehost bij een in Nederland gevestigde hosting provider, filteren niet aan de orde kan zijn. In dat geval kan justitie immers altijd de betreffende hosting provider (of de informatieaanbieder) rechtstreeks aanspreken: het is uiteraard disproportioneel om alle access providers van Nederland een website of IP-adres te laten blokkeren, terwijl justitie beschikt over middelen om de strafbare content van het internet te doen verwijderen. Datzelfde heeft de minister van Justitie zelf geschreven aan de Tweede Kamer in zijn brief van 26 juni 2009:

Ik wil hier stellen dat het niet de bedoeling is om het middel van filteren en blokkeren in te zetten voor sites met kinderporno (of ander strafbaar content) die in Nederland worden gehost. Daar zal na signalering tegen worden opgetreden: door middel van NTD en strafrechtelijk onderzoek.[10]

Dwangsom

24 XS4ALL heeft met zorg kennis genomen van het voorgestelde artikel 125q Sv, op basis waarvan de Officier van Justitie (OvJ) een dwangsom kan opleggen aan degene tot wie een bevel tot ontoegankelijkmaking wordt gericht.

25 De toepassing van dwangmiddelen op internetproviders is nu nog, tot op zekere hoogte, een dialoog tussen behoeftestellers en internetproviders, waarin providers behoeftestellers vaak (moeten) wijzen op gebreken in hun vorderingen. De mogelijkheid voor de OvJ om een dwangsom op te leggen zal in praktijk betekenen dat vrijwel alle aanbieders, wanneer gerede twijfel bestaat over de rechtmatigheid van een vordering, hun verzet snel zullen staken. Het gevolg daarvan is dat de bestaande uitwisseling van kennis en ervaring verloren gaat. Dat is zorgelijk, omdat met een vordering tot ontoegankelijkmaking inbreuk wordt gemaakt op elementaire grondrechten en de praktijk leert dat behoeftestellers weinig vertrouwd zijn met de digitale omgeving waarop hun vorderingen betrekking hebben en fouten in deze vorderingen veel voorkomen.

Zie voor de relevante grondrechtelijke en verdragsrechtelijke argumenten de paragraaf “De juridische dimensie van filteren” van het bijgevoegde standpunt van XS4ALL inzake filteren.

26 XS4ALL vindt de onderbouwing van de noodzaak voor een dwangsombevoegdheid daarbij niet overtuigend. De Toelichting onderkent de medewerking van internetproviders aan de Gedragscode en de bereidwilligheid van internetproviders om mee te werken aan strafvorderlijke bevelen. Het geval waarin niet wordt voldaan aan een vordering tot ontoegankelijkmaking is dus in de eerste plaats nogal hypothetisch.[11] Volgens de Toelichting zou in dat geval een dwangsom doelmatiger zijn dan vervolging op grond van artikel 184 Sr, gelet op de tijd die pleegt te verstrijken met strafvervolging en het relatief lage geldboetemaximum van artikel 184 Sr . Daarbij wijst de Toelichting op het WODC-rapport “De WED op de helling”, waarin volgens de Toelichting geconstateerd wordt dat het sanctiepakket van de Wet op de Economische Delicten (WED) herijking behoeft. De Toelichting gaat echter voorbij aan het juridisch terrein dat centraal staat in het rapport: het ‘bijzondere’ economische strafrecht. Boven-

10 *Kamerstukken II* 2008–2009, 28 684, nr. 232, pp. 5-6.
11 Ontwerp Toelichting, p. 26.

dien kan uit de inhoud van dat rapport geen argument worden ontleend om in deze situatie dwangsommen aan providers op te leggen.

27 Ten slotte is het in de ogen van XS4ALL onwenselijk dat de voorgestelde dwangsombevoegheid op geen enkele manier beperkt is. De gevallen waarin een OvJ tot het opleggen van een dwangsom kan overgaan, de hoogte van een eventuele dwangsom en de termijn waarbinnen aan een vordering moet worden voldaan op straffe van de dwangsom, zijn op geen enkele manier geclausuleerd. Daarbij moet bedacht worden dat een internetprovider geen realistische mogelijkheid heeft om zich tegen een opgelegde dwangsom te verzetten vóórdat deze verbeurd wordt. Tegen het opleggen van de dwangsom staat immers geen bezwaar en beroep open op grond van de Algemene wet bestuursrecht. Beklag op de voet van artikel 552a Sv heeft geen schorsende werking en de procedure zal veelal niet snel genoeg zijn om het verbeuren van een dwangsom te voorkomen. Daarmee rest slechts de mogelijkheid om een opgelegde dwangsom aan te vechten in een civiele kort gedingprocedure, welke procedure tijdrovend en kostbaar is.

Bevoegde autoriteit

28 Volgens de Toelichting is ervoor gekozen de bevoegdheid tot het doen van een vordering op grond van artikel 125p Sv neer te leggen bij de OvJ *"gelet op de aard van de vordering en de rol van de officier van justitie bij de beoordeling van strafbare feiten"*.[12] De toelichting waarom de bevoegdheid niet aan opsporingsambtenaren toekomt is zeer overtuigend:[13]

> *Aangezien bij het ontoegankelijk maken van gegevens op het internet terughoudendheid moet worden betracht teneinde onrechtmatige inperkingen van de vrijheid van meningsuiting en de het vrije verkeer van gegevens te voorkomen, is niet wenselijk dat deze bevoegdheid ook aan opsporingsambtenaren wordt toebedeeld.*

29 De daaropvolgende toelichting waarom de bevoegdheid niet bij de rechter wordt gelegd is dat des te minder. Daartoe overweegt de Toelichting in de eerste plaats dat het een maatregel van tijdelijke aard betreft. Dat tijdelijk karakter blijkt echter niet uit de voorgestelde wetsbepalingen. Nergens blijkt dat een vordering slechts van beperkte duur zal zijn en dus vervalt, tenzij deze tijdig wordt verlengd.

30 In de tweede plaats wijst de Toelichting op de mogelijkheid dat over de vordering beklag kan worden gedaan op de voet van artikel 552a Sv. Daarover merkt XS4ALL het volgende op. Een vordering op grond van artikel 125p Sv vormt een ernstige en rechtstreekse beperking van de uitings- en ontvangsvrijheid. Daarmee wordt immers in-

---

12 Ontwerp Toelichting, p. 22.

13 Id.

formatie van overheidswege uit de openbaarheid verwijderd. Op een dergelijke inperking van elementaire grondrechten behoort een onafhankelijke rechter te beslissen.

31 Daarbij komt dat de mogelijkheid van rechterlijke toetsing achteraf niet gelijkwaardig is aan voorafgaande rechterlijke controle. Rechterlijke toetsing achteraf vindt namelijk alleen plaats als een belanghebbende bereid is daar tijd en geld aan te besteden. Een buitenlandse informatieaanbieder zal dat zelden doen. Het algemene publiek van potentiële informatieontvangers wordt evenzeer geraakt door een vordering op grond van artikel 125p Sv, maar zal vermoedelijk geen beklag kunnen doen op grond van artikel 552a Sv.[14] Daarmee rest feitelijk alleen beklag door tussenpersonen tot wie een vordering op grond van artikel 125p Sv gericht wordt. Zij zullen doorgaans echter onvoldoende direct, commercieel belang hebben bij deze rechtsgang. Controle op de toepassing van overheidscensuur zal dus in praktijk afhankelijk zijn van de bereidheid van internetproviders om zich in voorkomend geval 'principieel' op te stellen, in plaats van – zoals het naar het oordeel van XS4ALL zou moeten – in alle gevallen voorwerp te zijn van voorafgaande rechterlijke toetsing.

32 Ten slotte stelt de Toelichting dat het civiele recht al bijzondere procedures kent om onrechtmatige activiteiten snel te kunnen beëindigen. De verwijzing in de Toelichting naar artikel 1019 e.v. van het Wetboek van Burgerlijke Rechtsvordering (Rv) is in dat verband instructief, omdat die regeling zich juist kenmerkt door het feit dat een voorafgaande rechterlijke machtiging is vereist voor het treffen van de bedoelde snelle maatregelen.[15] Ook de procedures op grond van de artikelen 26d van de Auteurswet en 15e van de Wet op de Naburige rechten kenmerken zich door voorafgaande rechterlijke toetsing. Als rechtvaardiging voor het *weglaten* van een rechterlijke toetsing vooraf, zijn deze verwijzingen dus niet afdoende. Dat "dit wetsvoorstel [...] daarbij aan[sluit] door de bestaande strafrechtelijke bevoegdheid van de officier van justitie om te bevelen gegevens ontoegankelijk te maken, te versterken" – zoals de Toelichting stelt – kan geen onderbouwing zijn voor het feit dat het voorliggende wetsvoorstel niet de rechter, maar de OvJ laat beslissen over ontoegankelijkmaking.

Waarborgen

33 De voorgestelde Regeling introduceert een zeer ruime bevoegdheid om content op internet ontoegankelijk te maken, hetzij door informatie te verwijderen, hetzij door

---

14 In die zin de toelichting op Artikel II, onderwerp F van de Ontwerp Toelichting (p. 31).

15 Onjuist is de stelling op p. 22 en 23 van de Toelichting "Teneinde de snelheid van deze procedure te waarborgen, zijn deze zaken geconcentreerd bij de Rechtbank Den Haag." Elke rechter die in de bodemzaak bevoegd is, is bevoegd voorlopige maatregelen te bevelen op grond van artikel 1019 e.v. Rv. Dat voor zaken over octrooien en gemeenschapsmerken alleen de Rechtbank Den Haag is, heeft niets met artikel 1019 e.v. Rv of met snelheid te maken maar met de keuze van de wetgever om vanuit het oogpunt van specialisering alle zaken over gemeenschapsmerken en octrooien te concentreren in Den Haag.

informatie af te sluiten of te filteren. Deze maatregel raakt aan belangrijke grondrechten van zowel informatieaanbieders als –ontvangers, in het bijzonder rechten op vrijheid van meningsuiting, privacy, communicatiegeheim, een eerlijk proces en internettoegang. Daarnaast raakt de voorgestelde verplichting aan de rechten en belangen van internetaanbieders, zoals deze zijn verankerd in de Europese Machtigingsrichtlijn en Richtlijn Elektronische handel.

34 Deze inbreuk is in elk geval niet toelaatbaar als niet wordt voldaan aan minimumrandvoorwaarden, die worden gevormd door de verplichtingen op grond van het EVRM, de Grondwet en het EU-recht. De vereiste waarborgen komen deels vanuit het Europese internemarktrecht (Machtigingsrichtlijn en E-Commerce richtlijn) en strekken tot bescherming van de belangen van tussenpersonen zoals XS4ALL. Gezamenlijk bieden deze waarborgen een stringente begrenzing van de toepassingsmogelijkheden voor een bevel op grond van artikel 125p Sv: in welke gevallen, aan wie, door wie, hoe en met welke rechtsbescherming. De noodzakelijkheid van deze waarborgen vindt zijn grondslag in voornoemde juridische normen: het gaat dus niet om waarborgen die XS4ALL wenselijk vindt, maar om waarborgen waartoe Nederland verdragsrechtelijk verplicht is als zij een bevoegdheid die filteren mogelijk maakt in het leven wil roepen.

35 In haar standpunt inzake filteren heeft XS4ALL – onder protest – de minimumrandvoorwaarden geschetst voor een bevoegdheid die filteren mogelijk maakt.[16] De voorgestelde regeling voldoet niet aan deze minimumrandvoorwaarden. XS4ALL zal haar analyse daarvoor hier niet herhalen, maar schetst hieronder de belangrijkste punten waarop de bevoegdheid verder begrensd zou moeten worden:

- De groep adressanten tot wie een bevel op grond van artikel 125p Sv gericht kan worden moet beperkt worden. Onderscheid moet gemaakt worden tot een bevel jegens een informatieaanbieder, jegens een hosting provider en jegens een access provider. Daarbij moet onderscheid gemaakt worden naar locatie waar het als strafbaar aangemerkte materiaal wordt gehost. Als dat in Nederland is, moet justitie eerst de Nederlandse hosting provider aanspreken tot verwijdering van de informatie. Als strafbare informatie wordt gehost in een land dat is aangesloten bij het Cybercrimeverdrag moet gebruik worden gemaakt van de rechtshulpbepalingen uit dat verdrag. Een filterbevel dient een ultimum remdium te zijn, welke alleen kan worden gericht tot Nederlandse access providers met betrekking tot informatie die gehost wordt in landen waarmee Nederland geen rechtshulpverdrag heeft.

- De uitoefening van de voorgestelde bevoegdheid van artikel 125p Sv dient beperkt te zijn tot zeer ernstige delicten. Daarbij kan aangesloten worden bij de

[16] Zie de paragraaf “Minimumrandvoorwaarden voor filteren” van het bijgevoegde standpunt van XS4ALL inzake filteren.

toepassingsvoorwaarden voor bevoegd aftappen op grond van artikel 126m Sv: inzet van de bevoegdheid op grond van artikel 125p Sv is uitsluitend mogelijk voor het beëindigen of voorkomen van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert. Een bevel gericht tot een access provider om informatie te filteren kan alleen worden gedaan teneinde een in Nederland kennelijk strafbaar uitingsdelict te beëindigen of voorkomen.

- Omdat een bevel op grond van artikel 125p Sv een ernstige inbreuk maakt op grondrechten en de bedrijfsvoering van internetproviders vergaand belast, dient voor de inzet van de bevoegdheid een zwaar regime te gelden dat voorziet in een rechterlijke toets, in de vorm van goedkeuring van de R-C;

- De aansprakelijkheidsregeling neergelegd in artikel 54a Sr dient in overeenstemming gebracht te worden met de Richtlijn, met eerbiediging van de daarin opgenomen beoordelingsruimte van hosting providers;

- Een effectieve beroepsprocedure, een regeling voor herziening, periodiek en op aanvraag, en het verlenen van een vrijwaring door de Staat (Zie de paragraaf "Minimumrandvoorwaarden voor filteren" van het bijgevoegde standpunt van XS4ALL inzake filteren.)

Conclusie

36 Naar de mening van XS4ALL onderbouwt de Toelichting op het concept-wetsvoorstel niet waarom het nodig is de voorgestelde bevoegdheid in te voeren, laat staan op deze manier. Het van overheidswege verwijderen van informatie van internet is een ingreep waarmee in een democratische samenleving uiterste terughoudendheid betracht moet worden, zowel naar vorm als naar inhoud. Dat betekent onder meer dat de ingreep uitsluitend mogelijk is in beperkte, specifieke en zeer ernstige gevallen en alleen op last van een onafhankelijke rechter, waarbij dient te worden voorzien in een effectief beroepsrecht voor getroffen burgers.

37 De voorgestelde regeling is onnodig en disproportioneel en voldoet ruimschoots niet aan verdragsrechtelijke bepalingen en EU-richtlijnen waaraan Nederland is gebonden op het gebied van uitingsvrijheid, ontvangstvrijheid, privacy, elektronische handel en telecommunicatie. Zij introduceert een vrijwel ongeclausuleerde bevoegdheid voor de officier van justitie om een onduidelijk afgebakende groep burgers bij vermeende overtreding van elk strafbaar feit te dwingen tot niet gespecificeerde feitelijke handelingen, op straffe van dwangsommen en aansprakelijkheid voor de inhoud van niet aanstonds verwijderde informatie.

38 XS4ALL roept de minister op af te zien van de voorgenomen regeling, of deze in elk geval grondig aan te passen langs de lijnen zoals in het voorgaande besproken.

XS4ALL is graag bereid deze reactie nader toe te lichten.

Met vriendelijke groet,

Margreth Verhulst
XS4ALL / Public & Regulatory Affairs
xsmar@xs4all.net

Bijlage: Standpunt XS4ALL over filteren op last van Justitie

Standpunt XS4ALL over filteren op last van Justitie

12 Maart 2010

De feitelijke dimensie van filteren

Inleiding

1 De maatschappelijke en wetenschappelijke discussie over filtering van internetverkeer is al enige tijd gaande.[1] Uit alle rapporten blijkt dat het van groot belang is te beginnen met een goed begrip van wat filteren is, wat het kan en niet kan en wat de gevolgen zijn van toepassing van filtering op internet.

Verwijderen, afsluiten en blokkeren

2 Het is van belang het onderscheid te bewaken tussen verschillende hoedanigheden waarin tussenpersonen acteren, enerzijds die van (1) *hosting provider* die informatie van klanten opslaat en beschikbaar stelt en anderzijds die van *access provider* die alleen voor haar klanten verbindingen levert en data transporteert (ook wel: *mere conduit)*. Bij *mere conduit* moet dan nog onderscheid gemaakt worden tussen (2) de situatie waarin de informatieaanbieder een klant is van XS4ALL, in die zin dat XS4ALL de verbinding levert tussen de server waarop de informatie staat en het internet, en (3) de situatie dat XS4ALL geen relatie heeft met de informatieaanbieder maar alleen een klantrelatief heeft met degene die de – elders op het internet opgeslagen – informatie wil raadplegen.[2]

3 Deze drie hoedanigheden worden in het hiernavolgende nader toelicht. Vooraf zij benadrukt dat waar bepaalde, door justitie als strafbaar beschouwde informatie wordt gehost bij een in Nederland gevestigde hosting provider, filteren niet aan de orde is. In zo'n geval zal justitie altijd die partij (of de informatieaanbieder) rechtstreeks kunnen aanspreken: het is uiteraard disproportioneel om alle access providers van Nederland een website of IP-adres te laten blokkeren, terwijl justitie beschikt over middelen om de strafbare content van het internet te doen verwijderen.

4 Bij hosting van informatie wordt vaak gedacht aan websites. In het vervolg van dit stuk wordt ook primair gesproken over het filteren van de inhoud van websites. Bedacht moet echter worden dat het (al dan niet illegale) informatieaanbod op internet bestaat

---

1 Zie de studie van het Open Society Institute: H. Dries-Ziekenheiner e.a., *Internet blokcing: balancing cybercime responses in democratic societies*, oktober 2009; .J. Dommering, 'Filteren is gewoon censuur, en daarmee basta', in: *Tijdschrift voor Internetrecht* 2008, [1], nr 5, p. 124-125; R. Deibert e.a., *Access Denied,* Cambridge, Massachusetts: MIT (2008); W.Ph. Stol c.s., "*Filteren van kinderporno op internet, een verkenning van technieken en reguleringen in binnen- en buitenland*", Den Haag 2008; M.H.M. Schellekens, B.J. Koops en W.G. Teepe, "Wat niet weg is, is gezien: een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime", Tilburg, november 2007.

2 Sommige bedrijven nemen de hier bedoelde diensten van XS4ALL af en leveren ze vervolgens weer door aan eigen klanten. De vraag rijst dan wie de feitelijke mogelijkheid en de juridische verplichting zou hebben om te filteren. Als men meer 'upstream' kijkt, is ook denkbaar dat hoger gelegen providers een rol spelen bij filteren. De rol van beheerders van internetverkeersknooppunten zoals AMS-IX is in de discussie tot op heden onderbelicht gebleven.

uit veel meer dan alleen dat. Providers geven oneindig veel *soorten* data door – plaatjes, video's, geluidsbestanden, tekstbestanden, etc. – en samenstellingen en verzamelingen daarvan. Dat informatieaanbod wordt opgeslagen en beschikbaar gesteld via allerlei verschillende standaarden en protocollen – naast webpagina's zijn er bijvoorbeeld FTP-servers, peer-to-peer netwerken, chatservers, anonieme proxy-netwerken, etc. Per geval verschilt wat de provider te weten kan komen, wat hij kan doen om toegang te voorkomen en hoe bewerkelijk, effectief en overigens schadelijk dat is. In het debat over filteren dienen deze verschillen en complexiteiten steeds onderkend te worden, om te voorkomen dat in algemene bewoordingen wordt gesproken over dingen die feitelijk niet kunnen of niet bestaan.

1: De informatie staat op een server van XS4ALL (hosting)

5 XS4ALL biedt als *hosting provider* aan particulieren of bedrijven ruimte op haar servers aan voor het opslaan van informatie, afbeeldingen, of andere inhoud die toegankelijk is via een website of via een andere dienst, applicatie of protocol. Deze diensten worden aangeduid als *hosting*-diensten.

6 XS4ALL *host* zowel statische als dynamisch gegenereerde websites. Bij statische websites is de inhoud van de website niet afhankelijk van door de bezoeker van de pagina ingevoerde parameters, zoals zoekwoorden. De website correspondeert met één of meer bestanden en geeft bij een bezoek aan de webpagina altijd hetzelfde weer. De inhoud van een dynamische website wordt bepaald aan de hand van bijvoorbeeld zoekvragen of instellingen van de gebruiker en wordt dus per geval – uniek – samengesteld.

7 Zowel bij statische als bij dynamisch gegenereerde websites zullen verschillende onderdelen van de website vaak op verschillende plaatsen staan. Een deel kan staan op de server van de ISP, maar de website kan ook 'achter de schermen' informatie ophalen bij servers elders, bijvoorbeeld bij de website-aanbieder (een computer, laptop of zelfs smartphone; thuis, op kantoor of in een serverpark) of elders in binnen- of buitenland. De pagina die de bezoeker op zijn scherm krijgt, bestaat dus feitelijk uit informatie die al dan niet dynamisch wordt samengesteld uit verschillende bronnen, die staan op verschillende servers van verschillende eigenaars op verschillende locaties. Die informatie kan deels bestaan uit afzonderlijk toegankelijke bestanden, maar kan ook opgevraagd worden uit databases die niet zelfstandig benaderbaar zijn.[3]

8 Het is voor XS4ALL of derden vaak niet eenvoudig vast te stellen welke inhoudselementen van een zichtbare webpagina uit welke bron en van welke server afkomstig zijn. Soms is dat af te leiden uit de broncode van een webpagina, maar vaak is dat uiterst lastig of zelfs onmogelijk. Een klant kan die informatie bewust verbergen, of om rede-

[3] Schellekens c.s., a.w., p. 11

nen van technische efficiëntie opslaan in een gecomprimeerde vorm die computers wel – maar mensenogen niet – gemakkelijk kunnen ontwaren ("packing").

9 Deze complexiteit brengt aanzienlijke beperkingen met zich mee als het gaat om wat XS4ALL kan doen. Zij kan een statische webpagina die is gehost op haar servers verwijderen. De onrechtmatige informatie wordt in dit geval bij de bron verwijderd van het internet (zij het dat de informatieaanbieder vrijwel altijd zelf nog zal beschikken over een lokale kopie en de website dus met geringe moeite elders weer online zal kunnen zetten).[4] Zij kan niet informatie die op servers elders staat verwijderen. Zij kan doorgaans evenmin de inhoud van een database bewerken om illegale informatie te verwijderen, althans niet zonder aanzienlijke kosten en risico op beschadiging van overige – niet-illegale – informatie.

10 Denkbaar is ook dat klanten hun website niet plaatsen op servers van XS4ALL, maar op eigen of van XS4ALL gehuurde servers die fysiek geplaatst worden in datacenters van XS4ALL ("dedicated server"of "co-location"). XS4ALL heeft geen rechtstreekse toegang tot (de inhoud van) dergelijke servers.

2. De informatie wordt aangeboden vanaf een server van een klant van XS4ALL en XS4ALL levert de verbinding tussen de server en het internet (mere conduit)

11 Klanten van XS4ALL die het beheer van hun website of andere informatiedienst in eigen hand willen houden, richten zelf een server in, die via XS4ALL met het internet is verbonden. De dienstverlening van XS4ALL wordt in dit geval aangeduid als *mere conduit.* Als XS4ALL een website op een server van één van haar klanten ontoegankelijk wil maken, dan kan dat alleen door de verbinding tussen de server en het internet af te sluiten. Dit resulteert niet in verwijdering van het onrechtmatig materiaal: dat staat op de eigen server van de klant en daartoe heeft XS4ALL geen toegang.

12 Het afsluiten van een verbinding is een zware maatregel met vergaande consequenties voor een klant: diens gehele server en de informatie die daarop staat is niet langer toegankelijk. Alle ingaande en uitgaande communicatie wordt geblokkeerd: hij kan zelf het internet niet op, kan niet e-mailen, etc. XS4ALL zou ook de verbinding slechts gedeeltelijk kunnen afsluiten, dus bijvoorbeeld voor een bepaalde poort of IP-adres. Ook in dat geval wordt niet alleen de illegaal bevonden informatie getroffen, maar alle informatie die via die poort of dat IP-adres wordt verzonden of ontvangen.

13 De klant kan de blokkade eenvoudigweg omzeilen door bij een andere internet provider een verbinding van zijn server met het internet te realiseren.

---

[4] Een nuancerende opmerking is echter op zijn plaats: in praktijk zullen er veelal *mirrors* van de website toegankelijk blijven op het internet.

3. De informatie staat op een server van een derde partij en van XS4ALL wordt verlangd dat zij verhindert dat haar klanten de informatie kunnen raadplegen

14 In dit scenario is XS4ALL niet in staat om het onrechtmatige materiaal te verwijderen. XS4ALL is ook niet de partij die de verbinding tussen de server en het internet levert en kan die verbinding dus ook niet afsluiten. XS4ALL kan in dit geval slechts trachten de toegankelijkheid van het materiaal voor haar eigen klanten te beïnvloeden door het materiaal te blokkeren met gebruik van filters. Door middel van filters wordt getracht om internetverbindingen die het onrechtmatige materiaal transporteren af te sluiten. XS4ALL zal hierna ingaan op de technische aspecten van verschillende methoden (en niveaus) van filteren.

Filtertechnieken

15 Er zijn in theorie verschillende technieken voor een ISP om netwerkconnecties die onwenselijk materiaal transporteren te blokkeren. De belangrijkste zijn IP-blokkering, DNS-filtering en *deep packet inspection (DPI).* De vraag hoe ingrijpend en effectief het blokkeren is hangt af van de hoeveelheid bijvangst (onschuldig materiaal dat onterecht geblokkeerd wordt), de vraag of de wijze van blokkeren gemakkelijk te omzeilen is en de kosten die met het blokkeren gemoeid zijn.

IP Blokkering

16 De meest grofmazige manier van filteren is het blokkeren van een IP-adres.[5] Alle verkeer naar dat IP-adres wordt dan tegengehouden. Om op basis van IP-adres te kunnen laten blokkeren moet een *blacklist* worden opgesteld: een lijst met IP-adressen die niet bezocht mogen worden. XS4ALL zou haar netwerkapparatuur vervolgens zo kunnen instellen, dat alle verkeer van en/of naar deze IP-adressen wordt geblokkeerd.

17 Er bestaat echter geen rechtstreekse, exclusieve relatie tussen bepaalde informatie en een IP-adres. Achter een IP-adres gaan doorgaans meerdere, soms (tien)duizenden websites en andere informatiediensten, aangeboden door evenveel aanbieders die niets met elkaar te maken hebben. Als een IP-adres geblokkeerd wordt, wordt alle aanbod van al die aanbieders onbereikbaar. Bij een IP-filter wordt dus met een kanon op een mug geschoten. Gevolg is dat schade wordt berokkend aan legitieme activiteiten van zowel de aanbieder van de illegale informatie, als aan andere informatieaanbieders wiens aanbod via hetzelfde IP-adres wordt aangeboden.

18 Met zogenoemde Layer 4 filtering is het mogelijk bepaalde verkeersstromen (poorten) te blokkeren en andere niet. In theorie kan zo bijvoorbeeld mail- en chatverkeer worden doorgelaten maar webverkeer niet. Daarmee kan de actieradius van een filterbevel

[5] Een IP-adres is een unieke code voor computers en andere apparatuur aangesloten op internet. Ook een server waarop een website gehost wordt heeft een IP-adres.

enigszins worden beperkt. Het is echter niet mogelijk slechts een deel van de communicatie met bepaalde poort te blokkeren: als de website van één gebruiker van een bepaald IP-adres wordt geblokkeerd, geldt dat ook voor alle andere websites. Bovendien kunnen informatieaanbieders gebruik maken van non-standaard poortnummers. Hoewel websites *meestal* worden aangeboden via poort 80, is dat niet technisch noodzakelijk of verplicht. Een website kan dus ook via elke andere poort worden aangeboden en via poort 80 kan ook elke andere dienst aangeboden worden. Anders gezegd: het blokkeren van poort 80 blokkeert niet per definitie alle webverkeer maar blokkeert wel *alle* verkeer via poort 80.

19 Gevolg van het voorgaande is dat IP-filtering geen effectieve blokkade opwerpt tegen het illegale aanbod, maar providers wel blootstelt aan enorme en onvoorzienbare schadeclaims van aanbieders van volkomen legale informatie. Die aanbieders kunnen zijn gevestigd in verschillende landen en de rechtsrelatie tussen die aanbieders en XS4ALL zal beheerst worden door verschillende straf-, bestuurs- en civielrechtelijke stelsels. Zelfs met een 'vrijwaring' door Justitie is de provider niet beschermd tegen procesrechtelijke (dwang)maatregelen die verschillende nationale rechtsstelsels mogelijk kennen, daargelaten dat Justitie niet snel een vrijwaring zal willen afgeven voor geheel onkenbare en onbeheersbare schaderisico's.

DNS Blokkering

20 Een andere manier van filteren is het blokkeren van bepaalde domeinnamen (DNS-blokkering). DNS-blokkering komt in wezen neer op een omleiding van het internetverkeer (*DNS-redirect*). Als een gebruiker een URL intikt met een domeinnaam die op de zwarte lijst staat (bijvoorbeeld http://www.foutesite.com/), krijgt zijn computer van de DNS server niet het juiste IP-adres voor die website, maar ofwel een foutmelding ofwel een ander IP-adres (waarop bijvoorbeeld een waarschuwing of uitleg staat.[6] Dit is de techniek die in Noorwegen wordt toegepast.

21 Als XS4ALL DNS-blokkering toepast werpt ze voor haar klanten een drempel op een bepaald domein te bereiken. Een DNS-blokkade treft niet alle websites op een bepaald IP-adres, maar wel alle pagina's van de website onder een bepaalde domeinnaam (als bijvoorbeeld www.site.com geblokkeerd wordt, raakt dat niet alleen de illegale pagina www.site.com/foutepagina maar ook www.site.com/onschuldigepagina. Het is dus in elk geval niet geschikt om individuele pagina's op grote websites te blokkeren (zoals een profielpagina op een sociale-netwerksite als Hyves)

22 DNS-blokkering belemmert één manier om het te vinden maar maakt informatie niet ontoegankelijk. De ongewenste informatie blijft gewoon beschikbaar en eenvoudig bereikbaar: als een gebruiker de URL intoetst met het IP-adres in plaats van de domeinnaam (dus http:// 77.245.92.64), krijgt hij de website gewoon te zien.

---

6 Zie ook Stol e.a., a.w., p. 13 e.v.

23 Bovendien kan een gebruiker relatief makkelijk zijn internetverkeer via een andere DNS-server laten verlopen, in plaats van die van zijn eigen ISP, en op die manier het filter omzeilen. Dat gebeurt niet per se bewust of met het doel om een filterverplichting te omzeilen. Sommige gebruikers gebruiken andere DNS-servers omdat die sneller werken. Sommige bedrijfsnetwerken maken gebruik van eigen DNS-servers, of van netwerkrouters die DNS proxydiensten aanbieden en die gebruiken met autoritatieve DNS-servers hoger in het netwerk.

24 De enige manier om dit onmogelijk te maken, is om alle verkeer verplicht via een door de ISP beheerde *proxy* te laten verlopen. Voor kleine ISP's is dat wellicht doenlijk, maar voor een ISP van de omvang van XS4ALL is dat technisch onwenselijk en bovendien onbetaalbaar: er is simpelweg te veel verkeer om het allemaal via één proxy server te laten verlopen. Zo'n werkwijze zou bovendien een punt in het netwerk creëren waar alle internetverkeer langskomt, een *single point of failure* dat de dienstverlening kwetsbaar maakt voor storingen en aanvallen. Daarnaast worden op deze manier allerlei legitieme functionaliteiten kapot gemaakt, zoals de hiervoor genoemde eigen (bedrijfs) DNS-servers.

25 Zelfs bij verplicht gebruik van een webproxy is een DNS-blokkade nog eenvoudig te omzeilen: het IP-adres van een bepaalde webhost kan via allerlei publieke bronnen op internet worden opgezocht, waarna de gebruiker alsnog dat IP-adres in zijn browser kan opvragen.

26 Tot slot wijst XS4ALL erop dat deze filtertechniek toepassing onmogelijk maakt van een veelbelovende nieuwe standaard om het DNS-systeem beter bestand te maken tegen cyberaanvallen: DNS-SEC.[7]

URL Blokkering

27 Een iets fijnmazigere manier om webverkeer te filteren is het blokkeren van bepaalde URL's (dus alleen www.site.com/foutepagina.html, maar niet www.site.com/anderepagina). Op die manier kan ook een specifiek bestand op een website worden geblokkeerd, zoals een enkele afbeelding. Ook voor het blokkeren op URL is het gebruik van een *proxy* vereist, waardoor alle verkeer naar de webserver wordt geleid. Aan deze *proxy* wordt een lijst met URL's gekopppeld die niet mogen worden doorgelaten.[8]

28 Technisch gezien is URL-blokkering een enigszins precieze, maar extreem dure oplossing. Wederom moet alle webverkeer door een verplichte *proxy*. In het geval van XS4ALL is dat op dit moment 20 gigabit aan data oftewel 3 miljoen pakketten aan webverkeer *per seconde*, een hoeveelheid die met de transitie naar glasvezelnetwerken exponentieel zal groeien. Vervolgens moet het adres van iedere opgevraagde pagina

7 http://www.dnssec.net/.
8 Stol e.a., a.w., p. 15.

(en van alle inhoudselementen daarin, dat zijn voor een gemiddelde HTML-pagina tientallen bestanden) worden vergeleken met de zwarte lijst van URL's. Filteren op URL niveau leidt daarmee tot een aanzienlijke vertraging van het internetverkeer. Filteren op URL niveau heeft bovendien een grote privacyimplicatie, omdat er een punt in het netwerk van een ISP ontstaat waar de inhoud van het dataverkeer technisch eenvoudig in te zien is.[9]

29 URL blokkering werkt alleen met onbeveiligde websites (adressen die beginnen met http://), niet met beveiligde websites (https://). Het werkt ook niet bij informatie die via andere standaarden of protocollen wordt verspreid, zoals FTP-servers, peer-to-peer-netwerken, instant-messaging applicaties of Usenet-nieuwsgroepen. Het is dus heel eenvoudig informatie aan te bieden op een manier die niet door URL blokkering kan worden geraakt. Zelfs voor onbeveiligd webverkeer is URL blokkering te omzeilen op dezelfde manieren als DNS-blokkering, onder meer door het instellen van een eigen webproxy of proxy-netwerk.

30 Een variant op URL-blokkering is wanneer het internetverkeer eerst door een IP-filter geleid wordt en vervolgens de IP adressen die als verdacht worden aangemerkt door een URL-filter worden geleid.[10] Op deze manier wordt het reguliere afhandelen van internetverkeer nog gecompliceerder, trager, duurder en foutgevoeliger gemaakt. De verdere gevolgen en schaalbaarheid zijn niet in te schatten: netwerkapparatuur is gemaakt om internetverkeer snel en efficiënt af te handelen, en dus niet om elk afzonderlijk verzoek te moeten controleren aan de hand van een zwarte lijst.

Deep Packet Inspection

31 Internetcommunicatie is pakketgeschakeld. Dat betekent dat de communicatie niet 'als één geheel' naar zijn bestemming wordt vervoerd, maar wordt opgedeeld in pakketjes, die via verschillende routes getransporteerd worden en bij aankomst weer samengevoegd worden tot één geheel. Een afzonderlijk 'pakketje' is maximaal 1,5 kb (in zeldzame gevallen 4 kb) groot: één muziekbestand bestaat dus uit honderden of duizenden pakketten.

32 *Deep Packet Inspection* in zijn meest basale vorm is soft- en hardware die als het ware de inhoud van afzonderlijke pakketjes bekijkt en die inhoud vergelijkt met een *blacklis*t (met niet toegestane informatie) of met een *whitelist* (toegestane informatie). Via sommige DPI-technieken kan de inhoud kan ook – tegen nog hogere kosten – worden gewist, aangepast, vertraagd etc. DPI gaat dus inherent gepaard met kennisname van de inhoud en met verwerking van verkeers- en persoonsgegevens. Er vindt inspectie plaats op een zeer laag niveau in het netwerk. Al het verkeer moet langs een specifiek

9 Schellekens c.s., a.w., p. 12.

10 Een voorbeeld van een dergelijk filter is het Cleanfeed filter dat door *British Telecom* in Engeland gebruikt wordt, zie Stol e.a., a.w., p. 16.

controlepunt worden gerouteerd. Het implementeren van DPI creëert een *single point of failure* in het netwerk en vereist dat XS4ALL haar netwerk op een manier inricht die indruist tegen basale beginselen van veiligheid, betrouwbaarheid en efficiëntie.

33 Gezien de verkeersvolumes en de snelheid van het internetverkeer is DPI (nog) niet mogelijk, althans zou DPI gepaard gaan met grote vertraging van het internetverkeer en zou een investering vergen van miljoenen euro's.[11] De apparatuur die XS4ALL met die investering zou verkrijgen, heeft geen verder bedrijfsnut voor XS4ALL. Het is ook onduidelijk hoe XS4ALL deze kosten zou kunnen doorberekenen aan klanten: die betalen XS4ALL immers om netwerkverkeer efficiënt en betrouwbaar te vervoeren, niet om het te vertragen en verhaspelen.

34 Daarbij moet bedacht worden dat DPI relatief eenvoudig te omzeilen is door gebruik van proxy's of encryptie. DPI laat encryptie (SSL) namelijk met rust, omdat anders beveiligde verbindingen (bijvoorbeeld tussen bedrijfslocaties of met internetbankieren websites) worden verstoord.

Nadelen: omzeiling, bijvangst en kosten

In het voorgaande zijn de beperkingen en nadelen van de verschillende verplichte filtertechnieken al kort aangeduid. Filteren is onvoldoende effectief in dat het eenvoudig te omzeilen is en tegelijkertijd te effectief in dat het ook veel niet-ongewenste informatie blokkeert.

Omzeilingsmogelijkheden (underblocking)

35 Voor alle hiervoor beschreven filtervarianten, geldt dat deze gemakkelijk zijn te omzeilen.

– IP-blokkering is door internetgebruikers eenvoudig te omzeilen door gebruik te maken van *proxies* of *tunnels*, die het internetverkeer op zodanige wijze routeren dat het filter bij de ISP omzeild wordt. Het eindpunt van de tunnel kan evengoed in een ander land zijn. De informatieaanbieder wiens informatieaanbod wordt bestreden met een IP-filter kan het filter eenvoudig omzeilen door het IP-adres van zijn server te veranderen, door meerdere IP-adressen te gebruiken of door gebruik te maken van andere technieken om snel van IP-adres te veranderen.[12]

---

[11] Om een indicatie te geven: de prijs van de desbetreffende apparatuur is ongeveer USD 840.000 voor 20 gigabit per seconde aan verkeer. Daarbij zou XS4ALL enkele 10 gigabit netwerkkaarten moeten aanschaffen voor nog eens tenminste USD 100.000. Het systeem zou bovendien redundant moeten worden uitgevoerd, wat de kosten verdubbelt. Aangezien XS4ALL apparatuur heeft staan op verschillende locaties, zouden deze kosten per locatie moeten worden genomen.

[12] Grote, internationaal opererende webdiensten zoals Akamai gebruiken verschillende IP-adressen in verschillende landen. Cybercriminelen maken bijvoorbeeld gebruik

– DNS-blokkering en URL-blokkering zijn door internetgebruikers eenvoudig te omzeilen door in hun *browser* niet de domeinnaam (www.foutesite.com) in te voeren maar het achterliggende IP-adres (194.109.6.92). Ook is het vrij eenvoudig om een webproxy te gebruiken, een eigen DNS-server te onderhouden of gebruik te maken van de DNS-server van een andere provider (en op die manier de herroutering van het filter te omzeilen).

– DPI is te omzeilen door gebruik te maken van geëncrypteerde verbindingen of een VPN (virtual private network) verbinding. Bovendien is het ten aanzien van afbeeldingen relatief eenvoudig te omzeilen door de *hash code* van een afbeelding, filmpje of muziekbestand aan te passen. Er hoeft maar één pixel of frame te veranderen om niet door het filter geblokkeerd te worden.

Bijvangst (overblocking)

36 Bij iedere wijze van filteren is sprake van bijvangst. Bijvangst is al het rechtmatig materiaal dat ten onrechte wordt verwijderd, afgesloten of geblokkeerd.

37 In geval XS4ALL in haar hoedanigheid van hosting provider wordt aangesproken om onrechtmatige informatie te verwijderen, kan in geval sprake is van een bijzonder eenvoudige website de bijvangst nul zijn indien elke pagina en elk bestand illegaal is. Vaak zal een website met illegale content echter ook in meer of mindere mate content bevatten die niet illegaal is. Bij wijze van voorbeeld: een website waarop wordt aangezet tot rassenhaat of terrorisme zal vaak ook persoonlijke, politieke opvattingen bevatten of andere informatie die valt onder de vrijheid van meningsuiting; een website met (links naar) illegale film- of muziekbestanden kan ook recensies of discussiefora bevatten, of (links naar) materiaal dat legaal op internet wordt aangeboden. Het feit dat op dezelfde site ook illegale informatie staat, doet niet af aan de rechtmatigheid van de overige informatie, die dus niet door ISP's of overheden geblokkeerd mag worden.

38 Bij meer ingewikkelde websites, zeker wanneer die gebruikmaken van databases, zal de bijvangst al snel een heel domein zijn. In geval sprake is van *mere conduit* en XS4ALL de server van een van haar klanten afsluit van het internet, is de hoeveelheid bijvangst het hele informatieaanbod van de klant – en mogelijk ook van andere klanten en klanten van klanten.

---

van DNS Fast Fluxing (http://en.wikipedia.org/wiki/Fast_flux), waarmee gebruik wordt gemaakt van geïnfecteerde pc's van gewone internetgebruikers om het IP-adres van een foute website constant te wijzigen.

39 Bij IP-blokkering is de hoeveelheid bijvangst het grootst. Immers, achter een enkel IP-adres kunnen duizenden websites zitten. Ook bij DNS-blokkering is de hoeveelheid bijvangst groot. Er verdwijnt immers in ieder geval een heel domein en niet het specifieke strafbaar of onrechtmatig onderdeel van een domein. Zelfs bij meest fijnmazige manier van filtering, op URL-niveau, zal nog sprake zijn van bijvangst, omdat een hele webpagina gefilterd wordt en niet specifieke informatie.

40 Bij het voorgaande is nog van belang dat informatie op internet niet statisch is, maar aan voortdurende verandering onderhevig is: een pagina, website of IP-adres kan worden veranderd, waardoor illegale informatie wordt verwijderd (en filteren dus hoegenaamd onterecht zou zijn) of juist toegevoegd.

Kosten

41 Afhankelijk van de vraag of XS4ALL informatie verwijdert, afsluit of filtert moet XS4ALL kosten maken om aan een bevel tot ontoegankelijkmaking te kunnen voldoen. Het betreft zowel investerings- en instandhoudingskosten die zijn gemoeid met aanpassing van haar technische infrastructuur om überhaupt uitvoering te kunnen geven aan een bevel als administratieve kosten die zijn verbonden aan het behandelen van individuele bevelen.

42 De exacte implementatiekosten van filteren zijn niet begroot en zouden pas begroot kunnen worden als de exacte technische en functionele eisen bekend zijn. Hierboven is onderbouwd dat implementatie van DPI miljoenen euro's zal kosten, schadelijke effecten op de kwaliteit van de dienstverlening niet meegerekend.

43 De kosten voor een vrijwillig URL filter zouden aanzienlijk lager zijn, omdat het alleen zou worden gebruikt door klanten die daarvoor kiezen en daarmee niet zou nopen tot fundamentele ingrepen in de netwerkarchitectuur.

Tussenconclusie

44 XS4ALL kan betrekkelijk eenvoudig materiaal verwijderen of ontoegankelijk maken dat is gehost op haar servers. Verwijdering van een website heeft het nadeel van bijvangst: ook de niet-illegale delen van een website worden verwijderd. Een bevel tot het afsluiten van de internetverbinding van de server van een klant is ook technisch eenvoudig, maar heeft een nog veel serieuzer bijvangstprobleem: alle communicatie wordt afgesloten.

45 Filteren is voor XS4ALL in theorie op IP- of DNS-niveau technisch uitvoerbaar, maar heeft verstrekkende gevolgen in termen van netwerkontwerp, dienstfunctionaliteiten en kosten. De maatregelen die XS4ALL zou moeten treffen om blokkades op DNS-niveau en URL-niveau mogelijk te maken, zouden haar netwerk veel kwetsbaarder ma-

ken. Filteren op URL-niveau of door middel van DPI zou leiden tot een onaanvaardbare vertraging van haar netwerk en is om die reden praktisch niet uitvoerbaar. DPI-techniek staat sowieso nog in de kinderschoenen; het vergt meer verwerkingscapaciteit en -snelheid dan de huidige netwerkapparatuur aankan. In alle gevallen geldt dat de beschikbare techniek niet voldoende is getest en dus onvoorziene technische of commerciële implicaties zal hebben.

46 Wel is reeds duidelijk dat alle beschreven technieken eenvoudig zijn te omzeilen, zonder dat de gebruiker daarvoor noemenswaardige kosten hoeft te maken en zonder dat hij daarvoor meer dan eenvoudige kennis van netwerktechnieken nodig heeft.

De juridische dimensie van filteren

Rechtsmacht

47 Bij filtering van internetverkeer gaat het steeds om blokkeren van *strafbaar* materiaal: de overheid heeft uiteraard geen taak bij het blokkeren van legaal materiaal. In de hiernavolgende paragrafen zal blijken dat, zelfs waar het Europees Verdrag voor de Rechten van de Mens (hierna: "EVRM") of EU-recht de mogelijkheid van beperking van de besproken (grond)rechten open laten, zij daaraan strikte voorwaarden stellen. In elk geval is vereist dat de beperking proportioneel is en noodzakelijk ter waarborging van een of meer essentiële belangen.

48 In het geval van filteren zal als essentieel belang vooral het belang van het bestrijden of voorkomen van strafbare feiten worden aangevoerd. Daarom dient vooraf bezien te worden onder welke omstandigheden het Nederlandse strafrecht überhaupt van toepassing is: waar dat niet het geval is, zal Nederland filteren ook niet kunnen rechtvaardigen met een beroep op de noodzaak voor het voorkomen of opsporen van strafbare feiten. Bovendien dient per strafbaar feit in het vizier gehouden te worden welke handelingen de Nederlandse strafwet verbiedt: soms is het vervaardigen, verspreiden of ter verspreiding in voorraad hebben van materiaal strafbaar, maar het enkel raadplegen ervan niet. Als Nederland in zo'n situatie alleen rechtsmacht heeft ten aanzien van de raadplegingshandeling, is geen sprake van schending van de Nederlandse strafwet en is voor het uitvaardigen van een filterbevel geen plaats.

49 De Nederlandse strafwet is in het algemeen slechts van toepassing op strafbare feiten die in Nederland worden gepleegd (het territorialiteitsbeginsel, artikel 2 Sr) en Nederlandse opsporingsdiensten hebben (enkele uitzonderingen daargelaten) alleen de bevoegdheid om in Nederland opsporingshandelingen te verrichten. Slechts ten aanzien van een beperkt aantal misdrijven komt Nederland op grond van internationale verdragen rechtsmacht toe, ook indien zij in het buitenland zijn begaan (het universali-

teitsbeginsel, zie onder andere artikel 4 Sr en de Wet internationale misdrijven). Auteursrechtinbreuk valt daar niet onder.

50 Internet heeft per definitie een grensoverschrijdend karakter. Bij in het buitenland gehoste websites is bepaald niet vanzelfsprekend dat het Nederlandse strafrecht van toepassing is. De aanbiedingshandeling wordt dan buiten het Nederlandse territoir verricht. Over situaties waarin strafbare inhoud in het buitenland wordt gehost, heeft de wetgever zich uitgelaten in relatie tot het ontoegankelijkmakingsbevel van artikel 125o Sv:

In 1999:

Nederlandse opsporingsambtenaren mogen op computernetwerken slechts onderzoek doen voor zover de Nederlandse rechtsmacht reikt. Dit betekent dat zij geen onderzoek mogen doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden of wanneer er zodanige aanwijzingen zijn dat er een gerede kans is dat dit het geval is. Aangenomen mag worden dat dit slechts uitzondering lijdt voor zover de opsporingsambtenaar, zoals hierboven aangegeven, als ieder ander mag rondkijken op een openbaar netwerk. Het staat een opsporingsambtenaar dus vrij om met sites waarvan de databestanden zijn opgeslagen op buitenlandse computers, een verbinding te leggen teneinde die sites te bekijken. Wat de opsporingsambtenaar echter níet mag, is op die sites bevoegdheden uitoefenen waarbij inbreuk wordt gemaakt op de rechten van burgers. Voor de voorgestelde maatregel van ontoegankelijkmaking van gegevens betekent dit bijvoorbeeld dat hij niet mag worden toegepast ten aanzien van gegevens waarvan men redelijkerwijs kan vermoeden dat zij zijn opgeslagen in een buitenlandse computer en zich dus aan de Nederlandse rechtsmacht onttrekken.[13]

In 2005:

Toepassing van de bevoegdheid tot ontoegankelijkmaking is derhalve alleen mogelijk ten aanzien van gegevens die zijn opgeslagen in computersystemen die zich bevinden binnen het Nederlandse territorium, op het continentaal plat of aan boord van een vaar- of luchtvaartuig dat onder Nederlandse vlag is geregistreerd. Voor toepassing van de maatregel van ontoegankelijkmaking in computersystemen die zich buiten de Nederlandse

13 *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 36.

rechtsmacht bevinden, zal derhalve een beroep moeten worden gedaan op internationale rechtshulp, ten behoeve waarvan het Cybercrime Verdrag tot stand is gebracht.[14]

51 Uit het standpunt van de wetgever in 1999 volgt dat een bevel tot filteren niet kan worden gegeven voor gegevens in het buitenland. De Nota naar aanleiding van het verslag uit 2005 is iets ruimer geformuleerd, omdat het de mogelijkheid openlaat dat informatie op een buitenlandse computer toch onder de Nederlandse rechtsmacht kan vallen. Daarvoor is dan echter wel vereist dat het aanbod een of meer handelingen behelst (bijvoorbeeld publiceren, voorradig hebben, verspreiden, raadplegen, etc.) die in Nederland strafbaar is volgens de delictsomschrijving van het betreffende strafbare feit. De Nederlandse opsporingsinstanties kunnen niet ten aanzien van iedere website met informatie die naar Nederlandse maatstaven niet in Nederland mag worden aangeboden rechtsmacht hebben en een filterbevel geven. Een dergelijke benadering zou ieder land rechtsmacht verschaffen over het gehele internet. In aansluiting van civielrechtelijke jurisprudentie dient daarvoor sprake te zijn van aanbod, waarvan geoordeeld kan worden dat het specifiek gericht is op Nederland.

52 Een eventuele regeling omtrent verplichte filtering zal dus per strafbaar feit een analyse en opsomming moeten bevatten van de feitelijke omstandigheden waaronder Nederland rechtsmacht toekomt ter zake van een aanbod op een buitenlandse webserver. Daarbij dient te worden aangegeven onder welke omstandigheden in Nederland sprake is van een verboden handeling. Waar daarvan geen sprake is, kan geen filterbevel worden uitgevaardigd. Als raadpleging van bepaalde informatie in Nederland dus niet strafbaar is en de vervaardigings- en verspreidingshandelingen in het buitenland zijn verricht en de website zich niet in het bijzonder mede op Nederland richt, heeft Nederland in beginsel geen rechtsmacht en is voor filtering op last van de Nederlandse autoriteiten geen plaats.

Perspectief van de zender

Artikel 7 Grondwet

53 Artikel 7 van de Grondwet (Gw) bepaalt dat niemand voor het openbaren van gedachten of gevoelens voorafgaand verlof nodig heeft vanwege de inhoud daarvan, en kent daarmee een absoluut verbod op censuur voor alle media.[15]

54 De toelichting op artikel 54a Sr, een wetsbepaling die een basis lijkt te bieden voor een verwijderingsbevel maar zeer omstreden is,[16] onderkent de verplichting van de Staat

[14] *Kamerstukken II* 2004/05, 26 671, nr. 10, p. 13.

[15] De zinsnede "behoudens ieders verantwoordelijkheid volgens de wet" is geen beperking van het censuurverbod, maar betekent dat de strafbare verspreiding van informatie achteraf vervolgd kan worden.

om zich te onthouden van censuur en stelt dat het artikel juist dient ter bescherming van de ontvangstvrijheid:

Artikel 7 van de Grondwet geeft aan de overheid de opdracht de vrijheid van meningsuiting te waarborgen en te stimuleren. Censuur van staatswege dient te worden voorkomen. Artikel 54a beoogt het gevaar in te dammen dat de tussenpersoon, mede gelet op zijn in belang toenemende rol in het proces van gegevensuitwisseling door middel van communicatienetwerken, zich genoodzaakt voelt tot preventieve censuur over te gaan teneinde strafrechtelijke aansprakelijkheid te voorkomen. De regeling dient een onbelemmerde informatie-uitwisseling en daarmee een grondbeginsel van de democratische rechtsstaat.[17]

55 Niettegenstaande deze passage valt moeilijk te ontkennen dat artikel 54a Sr tot gevolg heeft dat informatie op last van de overheid wordt geblokkeerd, en wel vanwege de inhoud van die informatie.

56 Filteren op internet is daarmee in strijd met artikel 7 Gw; een wet die probeert aan filterpraktijken een wettelijke basis te verschaffen is in strijd met de Grondwet, zodat de Staten-Generaal die niet mogen aannemen. Het rapport van Stol c.s. legt bloot dat artikel 54a Sr geen wettelijke basis biedt voor de bestaande praktijk in Nederland, maar gaat er ten onrechte vanuit dat een dergelijk gebrek is te verhelpen.[18]

57 Bij IP- of DNS-filtering is sprake van repressieve censuur, omdat een uiting eerst getoetst wordt en pas dan wordt opgetreden tegen verdere verspreiding. Vanuit het perspectief van de (Nederlandse) consument is echter sprake van preventieve censuur: consultatie van de informatie wordt niet achteraf bestraft maar vooraf verhinderd. Bij *deep packet inspection* is onmiskenbaar sprake van voorafgaande controle op de inhoud van communicatie: indien deze communicatie bepaalde inhoud bevat, wordt die immers geblokkeerd. Dat geldt te meer bij toepassing van DPI op uitgaand verkeer van een internetgebruiker: het wordt hem dan bij voorbaat technisch onmogelijk gemaakt een bepaalde mening te uiten.

58 Het is in de rechtspraak geaccepteerd dat een *rechterlijk* verbod voor de toekomst in bijvoorbeeld perszaken geen verboden censuur vormt, zolang het verbod zorgvuldig is beperkt tot bepaalde, specifieke, onrechtmatig bevonden uitingen (of uitingen van vergelijkbare strekking).[19] Het is in theorie denkbaar dat een filterverplichting zodanig

---

16 M.H.M. Schellekens, B.J. Koops en W.G. Teepe, "Wat niet weg is, is gezien: een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime", Tilburg, november 2007.

17 *Kamerstukken II* 2001-2002, 28 197, nr. 3, p. 63.

18 Zie E.J. Dommering, 'Filteren is gewoon censuur, en daarmee basta', in: *Tijdschrift voor Internetrecht* 2008, nr. 5, p. 125.

19 HR 2 mei 2003, *NJ* 2004, 80 m.nt. EJD (Storms/Niessen).

specifiek wordt geformuleerd dat deze alleen daadwerkelijk illegale informatie raakt. Dan nog biedt de rechtspraak geen enkele basis voor een *bestuurlijk* verbod. Bovenzien zijn de in het voorgaande hoofdstuk beschreven filtertechnieken niet in staat een aldus geformuleerde verplichting na te leven, want raken per definitie meer uitingen dan als illegaal aangemerkte uitingen. Anders gezegd: een van overheidswege opgelegde filterverplichting op het niveau van IP-adres, DNS, URL of pakket is per definitie in strijd met artikel 7 Gw.

59 Ook om een andere reden staat artikel 7 Gw in de weg aan invoering van een filterverplichting, althans met gebruikmaking van de hier besproken technische middelen. De inhoud van een website is per definitie onderhevig aan verandering: de informatieaanbieder kan op ieder moment informatie toevoegen, veranderen of verwijderen. Het gevolg daarvan is dat de (il)legaliteit van een website geen constante is maar gemakkelijk geheel of gedeeltelijk verandert. Een verbod (op doorgifte) van een bepaalde website komt daarom per definitie neer op een vorm van preventieve censuur, zelfs als de website op het moment dat het verbod wordt uitgesproken in zijn geheel illegaal is. Dat geldt in geval XS4ALL als hosting provider informatie van haar server verwijdert, maar geldt in het bijzonder als XS4ALL aan de hand van 'filterlijsten' (lijsten met tientallen of duizenden websites die geblokkeerd moeten worden) IP-adressen, websites of URL's van buiten zou moeten blokkeren. In het volgende hoofdstuk wordt nader ingegaan op de noodzaak van een effectieve klachtprocedure.

60 Artikel 120 Gw verbiedt de rechter om de wet in formele zin aan de Grondwet te toetsen. Het toetsingsverbod geldt niet voor verdragsbepalingen zoals het hierna te bespreken artikel 10 EVRM en EU-recht. Bovendien speelt de Grondwet wel een belangrijke rol in de voorbereiding van wetgeving: de regering wordt geacht geen wetten bij de Staten-Generaal in te dienen – en de gewone wetgever wordt geacht geen wetten aan te nemen – die in strijd zijn met de Grondwet.[20] Anders gezegd: juist omdat rechterlijke toetsing achteraf ontbreekt, dient de wetgever (daarin geadviseerd door de Raad van State) die vooraf uit te voeren. Is een wet eenmaal aangenomen, dan is de rechter vervolgens gehouden deze zo veel mogelijk *grondwetsconform* uit te leggen: indien er verschillende interpretaties van een formeel wettelijk voorschrift mogelijk zijn, moet de rechter kiezen voor de uitleg die in overeenstemming is met de Grondwet.[21] Bovendien kan de rechter wel uitvoeringsmaatregelen (zoals een filterbevel in een specifiek geval) aan de Grondwet toetsen. Artikel 120 Gw is dus geen vrijbrief om wetgeving aan te nemen in strijd met artikel 7 Grondwet en staat ook niet in de weg aan het toetsen van lagere wet- en regelgeving of besluitvorming.

---

20 Zie o.a. Aanwijzingen voor de regelgeving, aanwijzing 18.

21 ABRvS 24 juli 2002, *JB* 2002/272 m.nt. LV (DeNíeuweOmroep), overweging 2.6; M.L.P. van Houten, *Meer zicht op wetgeving* (diss. KUB), Deventer: Tjeenk Willink 1997, p. 46-51; G.J.Th. Belaerts van Blokland, *De onschendbaarheid der wet*, Leiden 1868, p. 47.

Artikel 10 EVRM

61 Ook artikel 10 EVRM beschermt de vrijheid van meningsuiting in ruime zin. Een inbreuk op de vrijheid van meningsuiting is blijkens artikel 10 EVRM toegelaten onder de voorwaarden van artikel 10 lid 2 EVRM: bij de wet voorzien ('prescribed by law' of 'in accordance with the law') en in een democratische samenleving noodzakelijk in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen.

62 Artikel 10 EVRM kent dus geen absoluut verbod op preventieve censuur, maar het EHRM past bij maatregelen van censuur wel de meest stringente toets toe. Artikel 10 EVRM stelt dus op twee manieren grenzen aan de mogelijkheid om een filterverplichting in te voeren. Allereerst moet een dergelijke verplichting zijn gebaseerd op een behoorlijke wettelijke regeling. Ten tweede bevat artikel 10 EVRM een proportionaliteitstoets, die bij censuur strikter is dan bij beperkingen na de eerste publicatie.

– Bij wet voorzien

63 Het is vaste rechtspraak van het EHRM dat het vereiste van een wettelijke basis niet alleen ziet op het bestaan van een wettelijke basis, maar ook eisen stelt aan de inhoud van die bepaling.

The Court points out that the expression "prescribed by law", within the meaning of Article 10 § 2, requires firstly that the impugned measure should have some basis in domestic law; however, it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences, and that it should be compatible with the rule of law (see Kruslin v. France, judgment of 24 April 1990, Series A no. 176-A, p. 20, § 27).[22]

64 Dit vereiste maakt het onmogelijk op dit moment filterwetgeving in te voeren. Bestaande filtertechnieken zijn immers zo weinig precies (ze raken tegelijkertijd te veel als te weinig uitingen, zijn met andere woorden tegelijkertijd *underinclusive* en *overbroad*). Daardoor weet de burger niet weet hij aan toe is, met als gevolg dat hij uitingen ach-

[22] EHRM 17 juli 2001, *NJ* 2002, 444, m.nt. EJD (Ekin), § 44.

terwege zal laten.[23] Filtering raakt immers, zoals in het voorgaande hoofdstuk omschreven, per definitie ook niet-verboden bestaande en toekomstige uitingen (bijvangst of 'overblocking').

65 Niet alleen moet de burger weten waar hij aan toe is, maar de wetgeving zelf dient adequate waarborgen te bevatten tegen misbruik en willekeur.

A law that confers a discretion is not in itself inconsistent with this requirement, provided that the scope of the discretion and the manner of its exercise are indicated with sufficient clarity, having regard to the legitimate aim in question, to give the individual adequate protection against arbitrary interference.[24]

66 Gebrek aan transparantie over de toepassing van een filterbevoegdheid – welke inhoud wordt gefilterd, wie bepaalt welke inhoud wordt verboden, hoe vindt controle en toezicht plaats etc. – zal een filterverplichting dus ook onmiddellijk in strijd doen zijn met artikel 10 EVRM.

– Proportionaliteit

67 Filteren is daarnaast disproportioneel, vooral vanwege de gebrekkige effectiviteit in combinatie met de hoge kosten en schade aan de vrijheid van meningsuiting. Daarnaast is relevant dat filteren de illegale informatie weliswaar moeilijker vindbaar maakt, maar niet doet verdwijnen: de informatie blijft op de server staan, maar op de route ernaartoe wordt een aantal blokkades geplaatst. In de Spycatcher zaak uit 1991, waarin de Engelse regering probeerde een verspreidingsverbod op te leggen aan de memoires van een oud geheim agent die uit de school klapte over de Engelse geheime dienst, nam het EHRM in aanmerking dat het boek al in andere landen op luchthavens was te verkrijgen.[25] Een verspreidingsverbod dat enerzijds veel rechtmatige informatie *tegenhoudt* maar anderzijds de beschikbaarheid van illegale informatie *zelf* niet wezenlijk raakt, zal doorgaans in strijd zijn met artikel 10 EVRM.

68 De exacte invulling van de proportionaliteitstoets is onder meer afhankelijk van de aard van de illegale informatie – hoe minder ernstig het strafbare feit, hoe minder snel de maatregel proportioneel is – en de werking van de specifieke filterverplichting. In zijn algemeenheid kan echter gesteld worden dat de beschikbaarheid van strafbare infor-

---

23 EHRM 17 juli 2001, *NJ* 2002, 444, m.nt. EJD (Ekin); EHRM 25 november 1996, *NJ* 1998, 359 m.nt. EJD (Wingrove); EHRM 26 november 1991, *NJ* 1992, 457, m.nt. EJD (Spycatcher).

24 Zie bijv. EHRM 25 november 1996, *NJ* 1998, 359 (Wingrove), § 40.

25 EHRM 26 november 1991, *NJ* 1992, 457, mnt. EJD (Spycatcher).

matie op het internet in bepaalde gevallen zeker ernstig is, maar dat het bestrijden daarvan via filteren dermate ineffectief is en dermate veel schadelijke neveneffecten heeft, dat het geen proportionele bestrijdingsmaatregel is.

Recht op eerlijke behandeling, onschuldpresumptie

69 Artikel 6 EVRM bepaalt dat een ieder bij het vaststellen van zijn burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging recht heeft op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij de wet is ingesteld. Artikel 6 lid 2 benadrukt de onschuldpresumptie.

70 Of sprake is van een civiele of strafrechtelijke procedure is afhankelijk van de specifieke implementatie van een filterbevoegdheid. Duidelijk is wel dat het afsluiten of blokkeren van een internetverbinding wegens vermeend handelen in strijd met de wet raakt aan de burgerlijke rechten van de informatieaanbieder, zodat een filterbevoegdheid moet voldoen aan alle vereisten van artikel 6 EVRM.

Communicatiegeheim en privacy

71 Bij sommige vormen van filtering, zoals DPI, wordt kennisgenomen van de inhoud van de communicatie en worden verkeers- en persoonsgegevens verwerkt. Dit levert een beperking op van de privacy en het communicatiegeheim van de verzender, welke rechten worden beschermd door de artikelen 8 EVRM, 10 en 13 Grondwet en de Europese privacyrichtlijnen. Als zodanig kan filtering niet worden opgelegd tenzij is voldaan aan de hierboven, ten aanzien van artikel 10 EVRM besproken eisen omtrent de inhoud en kwaliteit van de wettelijke grondslag en de noodzaak en proportionaliteit van de filtermaatregel (zie ook hierna, § 77 e.v.).

Recht op internettoegang

72 De vrijheid om via internet informatie te verzenden en ontvangen is uitgebreid aan de orde geweest bij de totstandkoming van het nieuwe richtlijnenpakket voor de elektronische communicatiesector.[26] De Machtigingsrichtlijn ondergaat geen voor de hier besproken materie relevante wijziging, de Kaderrichtlijn des te meer. Het belangrijkste twistpunt was juist de mate waarin lidstaten internettoegang van consumenten zouden kunnen afsluiten of beperken. De uiteindelijk overeengekomen tekst voor een nieuw artikel 1 lid 3bis van de Kaderrichtlijn luidt als volgt:

---

[26] Richtlijn 2009/140/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/21/EG inzake een gemeenschappelijk regelgevingskader voor elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/19/EG inzake de toegang tot en interconnectie van elektronischecommunicatienetwerken en bijbehorende faciliteiten, en Richtlijn 2002/20/EG betreffende de machtiging voor elektronischecommunicatienetwerken en –diensten.

Maatregelen van de lidstaten betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken eerbiedigen de fundamentele rechten en vrijheden van natuurlijke personen zoals die door het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht worden gewaarborgd.

Maatregelen betreffende toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken die die fundamentele rechten en vrijheden kunnen beperken, mogen alleen worden opgelegd indien zij passend, evenredig en noodzakelijk zijn in een democratische samenleving, en zij worden uitgevoerd met inachtneming van adequate procedurele waarborgen overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden en de algemene beginselen van het Gemeenschapsrecht, waaronder doeltreffende rechtsbescherming en eerlijke rechtsbedeling. Deze maatregelen mogen derhalve alleen worden genomen met inachtneming van het beginsel van het vermoeden van onschuld en het recht op een persoonlijke levenssfeer. Een voorafgaande, eerlijke en onpartijdige procedure wordt gegarandeerd, inclusief het recht van de betrokkene of betrokkenen om te worden gehoord, met dien verstande dat voor naar behoren gestaafde spoedeisende gevallen geëigende voorwaarden en procedurele regelingen gelden overeenkomstig het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden. Het recht op een daadwerkelijke en tijdige beroepsmogelijkheid bij een rechterlijke instantie is gegarandeerd.

73 Gevolg van deze bepaling is dat de toegang van zenders tot hun internetpubliek alleen onder strikte voorwaarden kan worden beperkt. Die voorwaarden volgen grotendeels al uit de artikelen 6, 8 en 10 EVRM maar worden door deze bepaling geëxpliciteerd en uitgewerkt specifiek in de context van internetcommunicatie.[27]

74 Het richtlijnenpakket is op 19 december 2009 in werking getreden en dient uiterlijk 26 mei 2011 geïmplementeerd te zijn in nationale wetgeving. Zoals de tekst zelf aangeeft, gelden de voorgeschreven waarborgen echter reeds op grond van het EVRM en algemene beginselen van gemeenschapsrecht. Een EU-richtlijn kan sowieso het EVRM niet veranderen. Artikelen 4 lid 3 VEU (artikel 10 EG oud) en 288 VWEU (artikel 249 EG oud) houden bovendien in dat "dat de Lid-Staat tot wie de richtlijn is gericht, zich tijdens de in de richtlijn vastgestelde omzettingstermijn dient te onthouden van de vaststelling van bepalingen die de verwezenlijking van het door de richtlijn voorgeschreven resultaat ernstig in het gedrang zouden brengen."[28] Dat geldt, ongeacht of de betrokken

[27] Zie de brief van de Minister van Justitie van 26 januari 2010, *Kamerstukken II* 2009-2010, 29838, nr. 24.
[28] HvJEG 18 december 1997, Inter-Environnement/Wallonië, C-129/96, overweging 45.

bepalingen strekken tot implementatie van de richtlijn[29] en geldt ook voor de nationale rechter.[30]

Perspectief van de ontvanger

75 Artikel 10 EVRM beschermt expliciet ook het recht om inlichtingen te *ontvangen*: de ontvangstvrijheid.[31] Ook vanuit het perspectief van de ontvanger van informatie (in dit geval doorgaans: de klant van de ISP die een pagina probeert op te roepen maar door een filter wordt tegengehouden) moet filteren dus worden beschouwd als een beperking van artikel 10 EVRM.

Recht op internettoegang

76 Hoewel het debat over het nieuwe artikel 1(3)a Kaderrichtlijn vooral gericht was op mogelijkheden voor lidstaten om wetten in te voeren die ertoe leiden dat de verbinding van internetgebruikers kunnen worden *afgesloten* als zij zich schuldig maken aan illegale bestandsuitwisseling, heeft zij evengoed gevolgen voor de mogelijkheid voor Nederland om filterverplichtingen in het leven te roepen. Ook dergelijke verplichtingen zouden immers rechtstreeks raken aan "toegang tot of gebruik van diensten en toepassingen door de eindgebruikers via elektronische communicatienetwerken". De in de nieuwe bepaling geschetste procedurele waarborgen strekken dus ook tot bescherming van potentiële ontvangers van door filtering geraakte informatie.

Persoonlijke levenssfeer en communicatiegeheim

77 De ontvangst van informatie wordt daarnaast ook beschermd door het recht op privacy en het communicatiegeheim. Op nationaal niveau is het recht op bescherming van de persoonlijke levenssfeer neergelegd in artikel 10 en artikel 13, voor zover het gaat om het brief-, telegraaf- en telefoongeheim, van de Grondwet.

78 Daarnaast heeft op grond van artikel 8 lid 1 EVRM een ieder recht op '*respect of his private and family life, his home and correspondence*'. Art. 8 EVRM omvat onder meer een hard recht op respect voor communicatie dat bescherming biedt tegen zowel kennisname en verwerking van de communicatie en verkeersgegevens als het blokkeren van de mogelijkheden tot communicatie.[32] Beperkingen zijn mogelijk, maar moeten voldoen aan de eisen van het tweede lid van art. 8 EVRM. Dat betekent dat ze moeten (i) zijn voorzien bij wet, (ii) noodzakelijk zijn in een democratische samenleving en (iii) een van de in art. 8 lid 2 EVRM genoemde doelen dienen.

---

29 HvJEG 8 mei 2003, ATRAL, C 14/02, overweging 59.

30 HvJEG 4 juli 2006, Adeneler, C-212/04, overweging 123.

31 "Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen." Zie

32 W.A.M. Steenbruggen, *Publieke dimensies van privé-communicatie*, Amsterdam: Otto Cramwinckel 2009, p. 81 e.v.

79 Uit de jurisprudentie van het Europese Hof voor de Rechten van de Mens blijkt dat het Hof bij beperkingen die betrekking hebben op de inhoud van de communicatie, zeer strikte eisen stelt, zowel aan de aan de beperking ten grondslag liggende wetgeving als aan nut, noodzaak en proportionaliteit daarvan.[33]

80 De vertrouwelijkheid van communicatie wordt voorts beschermd door de ePrivacy-richtlijn.[34] Op grond van artikel 5 lid 1 ePrivacy Richtlijnzijn zijn de lidstaten gehouden via hun nationale wetgeving het vertrouwelijke karakter van de communicatie en de daarmee verband houdende verkeersgegevens via openbare communicatienetwerken en via openbare elektronische-communicatiediensten te "*garanderen*". Dit betekent onder meer dat ze geen beperkingen mogen aanbrengen.[35] Uitzonderingen zijn slechts mogelijk, indien wordt voldaan aan de eisen van art. 15 ePrivacyrichtlijn die nagenoeg overeenkomen met de eisen van art. 8 lid 2 EVRM.

81 Filtering is onmiskenbaar een beperking van deze grondrechten, omdat filtering noodzakelijkerwijs gepaard gaat met (heimelijke) kennisname van het communicatie-gedrag van individuen en het genereren van persoonsgebonden verkeersgegevens: dat een bepaalde gebruiker op een bepaald moment heeft geprobeerd een bepaalde, "verboden" bestemming te bereiken of heeft geprobeerd bepaalde, "verboden" inhoud te ontvangen. Afhankelijk van de wijze van implementatie van filteren zullen deze gegevens verder (moeten) worden verwerkt, bijvoorbeeld opgeslagen en/of gedeeld met behoeftestellers.

82 Dat brengt met zich mee dat van overheidswege verplichte filtermaatregelen, indien nut en noodzaak daarvan al kunnen worden vastgesteld, hooguit kunnen worden toegestaan, indien aan de zeer strikte eisen van met name art. 8 lid 2 EVRM is voldaan. Dat betekent onder meer dat de aan de filtering ten grondslag liggende wetgeving zeer duidelijk moet aangeven wie een bevel tot filtering mag geven, wanneer, in welke gevallen, hoe lang en hoe, en dat de wetgeving daarnaast effectieve waarborgen tegen misbruik moet bevatten zoals voorafgaande rechterlijke toetsing en verplichte notificatie.[36] Filtering is een zeer ingrijpende maatregel, zodat de wetgeving ook moet waarborgen dat deze slechts in de *echt noodzakelijke* gevallen kan worden toegepast, zodat de beperking tot een minimum beperkt blijft.[37] Wordt hieraan niet voldaan, dan is een filterverplichting in strijd met de artikelen 8 EVRM en 5 ePrivacyrichtlijn.

---

33 Zie W.A.M. Steenbruggen, Publieke dimensies van privé-communicatie, Amsterdam: Otto Cramwinckel 2009, p. 91 e.v

34 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002, betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie), *PbEG L* 201/37.

35 Steenbruggen 2009, p. 188.

36 Zie bijv. EHRM 29 juni 2006, http://www.echr.coe.int (*Weber en Saravia*); EHRM 1 juli 2008, *EHRC* 2008, 100 (*Liberty*), m.nt. Van der Velde.

37 Vgl. BVerfG 27 februari 2008 (Online-Durchsuchung), Mediaforum 2008-5, p. 223 e.v, m.nt. W.A.M, Steenbruggen.

Perspectief van de tussenpersoon

Richtlijn elektronische handel

83 De artikelen 12 lid 3 en 14 lid 3 van de Richtlijn elektronische handel[38] bepalen dat de uitsluiting van aansprakelijkheid bij mere conduit en hosting "geen afbreuk [doen] aan de mogelijkheid voor een rechtbank of een administratieve autoriteit om in overeenstemming met het rechtsstelsel van de lidstaat te eisen dat de dienstverlener een inbreuk beëindigt of voorkomt." Daarmee is echter niet gezegd dat de Nederlandse wetgever een algemene filterverplichting mag opleggen. Artikel 15 bepaalt immers juist dat lidstaten aan internetaanbieders géén algemene verplichting mogen opleggen op om toe te zien op de informatie die zij doorgeven of opslaan, noch om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.

84 Of een filterverplichting verenigbaar is met het verbod op voorafgaand toezicht, hangt onder meer af van de feitelijke kenmerken en gevolgen van de voorgeschreven filtertechniek en de wijze waarop die volgens de wettelijke filterverplichting wordt toegepast. Blokkades op IP- of DNS-niveau zijn niet goed te rijmen met de geest van de bepaling, maar kunnen mogelijk zodanig vormgegeven worden dat geen algemene controle hoeft te worden uitgeoefend. *Deep packet inspection* lijkt daarentegen duidelijk in strijd met artikel 15, omdat het juist wel algemeen toezicht behelst op *alle* doorgegeven informatie.[39]

85 Artikel 14 lid 3 bepaalt voorts dat de uitsluiting van aansprakelijkheid bij hosting "evenmin afbreuk [doet] aan de mogelijkheid voor lidstaten om procedures vast te stellen om informatie te verwijderen of de toegang daartoe onmogelijk te maken." Dat ziet echter op *notice and take down* procedures van hosting providers, waar het in dezen als gezegd niet om gaat. Als justitie hiermee de informatie aan de bron kan verwijderen, dient zij hier gebruik van te maken en komt men niet toe aan een filterverplichting voor alle access providers.

Machtigingsrichtlijn

86 De Machtigingsrichtlijn[40] beoogt een juridisch kader te scheppen dat de vrijheid van het leveren van elektronische communicatienetwerken en -diensten waarborgt. Het stelt dus absolute grenzen aan de mate waarin lidstaten het vrije verkeer van diensten kun-

---

38 Richtlijn 2000/31/EG van het Europees 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.

39 Zie bijv. K.J. Koelman, 'Online Intermediary Liability', in Hugenholtz, P.B., (red.) *Copyright and Electronic Commerce - Legal Aspects of Electronic Copyright Management* (Information Law Series (no. 8), Kluwer Law International 2000), p. 34.

40 Richtlijn 2002/20/EG van het Europees Parlement en de Raad van 7 maart 2002 betreffende de machtiging voor elektronische communicatie-netwerken en –diensten, *PbEG* L 108/21.

nen beperken. Artikel 3 lid 2 van de Machtigingsrichtlijn bepaalt dat het aanbieden van netwerken en diensten niet aan vergunningen mag worden onderworpen, behalve dan aan een algemene machtiging. Artikel 6 lid 1 van de Machtigingsrichtlijn bepaalt dat deze algemene machtiging alleen aan de voorwaarden kan worden onderworpen die in de bijlage bij deze richtlijn staan.

87 De enige in de bijlage genoemde verplichting die wellicht in aanmerking komt om een filterverplichting mogelijk te maken, is onderdeel 9 van bijlage:[41]

9. Beperkingen in verband met de doorgifte van onwettige inhoud, overeenkomstig Richtlijn 2000/31/EG van het Europees 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(2), en beperkingen in verband met de doorgifte van onwettige inhoud overeenkomstig artikel 2 bis, lid 2, van Richtlijn 89/552/EEG van de Raad van 3 oktober 1989 betreffende de coördinatie van bepaalde wettelijke en bestuursrechtelijke bepalingen in de lidstaten inzake de uitoefening van televisie-omroepactiviteiten(3), gewijzigd bij Richtlijn 97/36/EG van het Europees Parlement en de Raad.

88 Zelfs als een filterverplichting kan worden ontwikkeld die in overeenstemming is met de Richtlijn Elektronische handel, zou een dergelijke verplicht blijkens artikel 6 lid 1 van de Machtigingsrichtlijn alleen kunnen worden opgelegd als deze objectief gerechtvaardigd is in relatie tot het betrokken netwerk of dienst en bovendien niet-discriminerend, proportioneel en transparant is. Dat betekent in elk geval dat een filterverplichting pas kan worden overwogen als deze langs deze maatlat kan worden gerechtvaardigd. Zoals ten aanzien van artikel 10 EVRM toegelicht is een filterverplichting dermate ineffectief, kostbaar en intransparant dat zulks niet het geval is.

89 Hoegenaamd zullen alle kosten ter implementatie en uitvoering van filtering dienen te worden gedragen door de Staat: een filterverplichting op kosten van de Staat is immers even effectief als een filterverplichting op kosten van de aanbieders en behelst een mindere inbreuk op de vrijheid van dienstverlening en vestiging. Filtering op kosten van aanbieders gaat dus verder dan nodig om het beoogde doel te bereiken en is dus niet proportioneel. De verplichting van de Staat om kosten in verband met filtering te betalen, volgt overigens ook uit het beginsel van gelijkheid voor de publieke lasten.

---

41 Onderdeel 11 betreft "Mogelijkheid van legale onderschepping door de bevoegde nationale instanties" en ziet op *aftappen* van telecommunicatieverkeer door de autoriteiten, niet op het *blokkeren* van verkeer.

Tussenconclusie

90 Uit het voorgaande volgt dat Nederland alleen een wettelijke plicht kan invoeren om internetverkeer of via internet aangeboden informatie te (laten) filteren, als dat dient om een strafbaar feit te voorkomen of beëindigen ten aanzien waarvan Nederland rechtsmacht toekomt. De omstandigheden waaronder dat het geval is, verschillen per strafbaar feit want hangen mede af van individuele delictsomschrijvingen. Deze omstandigheden dienen per strafbaar feit zorgvuldig in kaart te worden gebracht en te worden omgezet in eenduidige wettelijke criteria voor de toepassing van een filterbevoegdheid. Het ligt vooralsnog niet voor de hand dat de Nederlandse autoriteiten een filterbevel zullen kunnen richten tegen informatie waarvan weliswaar de openbaarmaking in Nederland strafbaar zou zijn maar die in werkelijkheid is opgeslagen op een buitenlandse server die zich niet specifiek mede op Nederland richt.

91 Zelfs in die gevallen waar Nederland rechtsmacht toekomt, is de juridische ruimte voor een wettelijke filterbevoegdheid uiterst beperkt. Uit het voorgaande volgt namelijk dat filtering, in elk geval via *deep packet inspection*, een vorm van preventieve censuur behelst en om die reden in strijd is met artikel 7 Grondwet is. Zelfs voor zover filtering niet per definitie verboden wordt door de Grondwet, stellen het EVRM-verdrag en diverse EU-richtlijnen strakke grenzen aan de gevallen waarin en de wijze waarop gefilterd kan worden. Die grenzen worden het in volgende hoofdstuk uitgewerkt.

Minimumrandvoorwaarden voor filteren

92 Uit het voorgaande is gebleken dat de invoering van verplichte filtering van internetcontent zowel technisch als juridisch *bad policy* zou zijn. De zorgen die XS4ALL heeft ten aanzien van filteren kunnen tot op zekere hoogte worden ondervangen met stringente waarborgen. Een aantal daarvan wordt hieronder omschreven, zij het 'onder protest' – ook als een dergelijke bevoegdheid wordt voorzien van dergelijke waarborgen en indien deze waarborgen in de praktijk ook stringent worden nageleefd, geldt dat filteren niet goed werkt, eenvoudig is te omzeilen, vooral schade berokkent aan legale informatie en legale gebruikers en indruist tegen elementaire grondrechten.

93 De minimumrandvoorwaarden voor een wettelijke filterbevoegdheid worden gevormd door de besproken verplichtingen op grond van het EVRM, Grondwet en het EU-recht. De waarborgen komen deels vanuit het Europese internemarktrecht (Machtigingsrichtlijn en E-Commerce richtlijn) en strekken tot bescherming van de belangen van *tussenpersonen* zoals XS4ALL.

94 Een handzame samenvatting van de *grondrechtelijke* randvoorwaarden wordt gegeven door het geciteerde nieuwe artikel 1 lid 3bis Kaderrichtlijn: filterverplichtingen zijn alleen denkbaar indien zij passend, evenredig en noodzakelijk zijn in een democrati-

sche samenleving en zij worden uitgevoerd met inachtneming van adequate procedurele waarborgen overeenkomstig het EVRM, waaronder doeltreffende rechtsbescherming en eerlijke rechtsbedeling. Filterverplichtingen mogen derhalve alleen worden genomen met inachtneming van het beginsel van het vermoeden van onschuld en het recht op een persoonlijke levenssfeer. Een voorafgaande, eerlijke en onpartijdige procedure dient te worden gegarandeerd, inclusief het recht van de betrokkene of betrokkenen om te worden gehoord en inclusief een daadwerkelijke en tijdige beroepsmogelijkheid bij een rechterlijke instantie.

95 De vereiste grondrechtelijke waarborgen bij verplichte internetfiltering worden uitgebreid en expliciet omschreven en gedocumenteerd in de recente Aanbeveling van de Raad van Europa over internetfiltering.[42] De aanbeveling raadt onder meer aan dat "Such action by the state should only be taken if the filtering concerns specific and clearly identifiable content, a competent national authority has taken a decision on its illegality and the decision can be reviewed by an independent and impartial tribunal or regulatory body." Nederland heeft zich aan deze aanbeveling te houden.

96 Gezamenlijk bieden deze waarborgen een stringente begrenzing van de toepassingsmogelijkheden voor een filterbevel: in welke gevallen, aan wie, door wie, hoe en met welke rechtsbescherming. Het hiernavolgende vormt daarmee de praktische uitwerking, in de context van een filterbevoegdheid, van de juridische normen en waarborgen zoals in het vorige hoofdstuk geschetst. Die juridische normen zijn daarmee ook de grondslag voor de *noodzakelijkheid* van deze waarborgen: het gaat dus niet om waarborgen die XS4ALL *wenselijk* vindt, maar om waarborgen waartoe Nederland verdragsrechtelijk *verplicht* is als zij een filterbevoegdheid in het leven wil roepen.

In welke gevallen kan een filterbevel worden gegeven?

Teneinde in Nederland kennelijk strafbare uitingsdelicten te beëindigen of voorkomen

97 XS4ALL meent dat het toepassingsbereik van een filterbevoegdheid scherp dient te worden afgebakend, in die zin dat zij uitsluitend wordt ingezet tegen uitingen die strafbaar zijn vanwege de inhoud – uitingsdelicten dus, zoals aanzetting tot terrorisme of kinderpornografie.[43] Kenmerk van deze delicten is inderdaad dat strafbaarheid in beginsel duidelijk uit de inhoud zelf kan worden opgemaakt, dus zonder acht te hoeven slaan op daarbuiten gelegen belangen of omstandigheden die derden betreffen. Dat betekent onder meer dat een filterbevoegdheid in beginsel niet gebruikt kan worden tegen vermeende auteursrechtinbreuk, omdat niet zonder raadpleging van derden kan

---

42 Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters, vastgesteld op 26 maart 2008.

43 A.L.J. Janssens en A.J. Nieuwenhuis, *Uitingsdelicten,* 2e druk, Deventer: Kluwer 2008.

worden vastgesteld of materiaal (nog) auteursrechtelijk beschermd is en, zo ja, of openbaarmaking geschiedt met toestemming van de rechthebbende.

98 Voorop staat dat de regeling een strafvorderlijke bevoegdheid creëert, er moet dus sprake zijn van informatie waarvan het aanbieden of raadplegen ervan in Nederland *strafbaar* is. XS4ALL pleit er daarom voor de hand om in een eventuele wettelijke regeling aan te sluiten bij de formulering van artikel 125o Sv, dat ziet op "gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd". Bovendien dient, als hierboven aangegeven, toepassing van een filterbevel te worden beperkt tot het tegengaan of beëindigen van in Nederland strafbare handelingen.

99 De precieze delictsomschrijvingen van het strafrecht geven vervolgens houvast om te bepalen wat strafbaar is (anders dan de privaatrechtelijke open norm van (onmiskenbare) onrechtmatigheid).[44] Als twijfel bestaat over de strafbaarheid van de daad en (vermeende) dader, beschikt de Officier van Justitie over bevoegdheden om onderzoek te doen naar de omstandigheden die van belang zijn voor de beoordeling daarvan. Desalniettemin kan twijfel blijven bestaan over de strafbaarheid van bepaalde handelingen met betrekking tot informatie. Dat wordt ook onderkend in de recente brief die de Minister van Justitie aan de Tweede Kamer stuurde, met daarin een beleidskader voor rechtshandhaving bij cybercrime en internetgebruik:

[...] in tegenstelling tot kinderpornografische afbeeldingen, is bij terrorismegerelateerde informatie niet altijd klip en klaar dat het om strafbare of onrechtmatige informatie gaat. De bereidheid van internetpartijen om informatie ontoegankelijk te maken geldt alleen ten aanzien van strafbare of onmiskenbaar onrechtmatige informatie. In de beoordeling of bepaalde radicaliserende uitlatingen strafbaar zijn of niet, geldt de huidige jurisprudentie als referentiekader. Zoals eerder vermeld is deze vrij beperkt en contextueel van karakter. Dit heeft effect op de kans van slagen van het ontoegankelijk maken van terroristische uitingen. De vrijheid van meningsuiting zal onder deze omstandigheden prevaleren boven het tegengaan van <<radicaliserende (niet strafbare) boodschappen>>.[45]

100 Een filterbevoegdheid kan dus alleen worden toegepast teneinde in Nederland kennelijk strafbare uitingsdelicten te beëindigen of voorkomen.

Alleen bij ernstige strafbare feiten

101 Het kan niet zo zijn dat een bevel tot ontoegankelijkmaking gegeven kan worden bij welk delict dan ook of bij verdenking van ieder misdrijf met behulp van een geautomatiseerd werk. In het licht van de vergaande inbreuk op grondrechten en gezien de door

44 Schellekens c.s., a.w., p. 24.
45 *Kamerstukken II* 2007/08, 28 684, nr. 133, p. 22, 23.

de verschillende verdragsrechtelijke normen gestelde proportionaliteitseis, moet uitoefening van de bevoegdheid beperkt zijn tot zeer ernstige delicten. Daarbij kan aansluiting worden gezocht bij de toepassingsvoorwaarde voor bevoegd aftappen op grond van artikel 126m Sv: filtering is uitsluitend mogelijk indien dat noodzakelijk is voor het beëindigen of voorkomen van een misdrijf als omschreven in artikel 67 lid 1 Sv, dat gezien zijn aard of de samenhang met andere door verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert.[46]

102 Artikel 67 lid 1 Sv ziet met name op misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld.

Alleen als informatieaanbieder en hosting provider niet aanspreekbaar zijn

103 Een filterbevel is een *ultimum remedium*, dat pas in beeld komt als het werkelijk niet mogelijk is gebleken de beschikbaarheid van de informatie bij de bron aan te pakken, dat wil zeggen de informatieaanbieder zelf of diens hosting provider.

104 Toepassing van een filterbevel dient dus in elk geval achterwege te blijven als sprake is van informatie die wordt aangeboden door een Nederlander of gehost in Nederland. Waar een in Nederland gevestigde partij kan worden aangesproken die eigenhandig de beschikbaarheid van de informatie kan beëindigen, is het disproportioneel om alle andere ISP's, in hun hoedanigheid van aanbieders van mere conduit-diensten, te verplichten tot filtering.

105 Toepassing van een filterbevel dient ook achterwege te blijven als sprake is van informatie die wordt aangeboden of gehost door een inwoner van een land dat is aangesloten bij het Cybercrime verdrag of waarmee Nederland anderszins een rechtshulpverdrag heeft. In beide gevallen dient Nederland in de eerste plaats het land aan te spreken waar de informatie- of hosting aanbieder gevestigd zijn, omdat zij in één keer de beschikbaarheid van de gewraakte informatie voor de hele wereld kunnen beëindigen.

106 Een filterbevel kan dus alleen gericht worden tegen Nederlandse *access providers*, dat wil zeggen aanbieders die een dienst van de informatiemaatschappij leveren bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk.

Proportionaliteit

Meer in het algemeen geldt dat voor filtering geen plaats is, als het strafvorderlijke doel dat met filtering wordt gediend, ook kan worden bereikt op een manier die minder inbreuk maakt op de rechten van internetgebruikers en -providers. Als bijvoorbeeld

[46] Dit sluit aan bij de conclusie in Stol e.a., a.w., p. 117.

justitie de bevoegdheid en de technische middelen heeft de informatie zelf te verwijderen, dient zij dat te doen in plaats van alle ISP's van Nederland te laten filteren, met alle schadelijke gevolgen van dien in termen van kosten en het ook blokkeren van onschuldige informatieverzending en -ontvangst.

Tussenconclusie

107 Een filterbevel kan in elk geval niet gegeven worden als niet is voldaan aan de volgende voorwaarden:

- het bevel is gericht tegen de beschikbaarheid van informatie waarvan de beschikbaarheid vanuit Nederland leidt tot het kennelijk begaan van een of meer ernstige uitingsdelicten ten aanzien waarvan Nederland rechtsmacht heeft;

- het bevel is gericht tegen de beschikbaarheid van informatie waarvan zowel de aanbieder als de hosting provider zijn gevestigd in een land waarmee Nederland geen rechtshulprelatie heeft;

- er bestaan geen middelen om de beschikbaarheid vanuit Nederland te voorkomen die minder inbreuk maken op de rechten van internetgebruikers en –providers.

Aan wie kan een filterbevel worden gegeven?

108 In de voorgaande paragraaf is reeds gebleken dat een filterbevel niet tot Nederlandse hosting providers gericht worden, daarvoor geldt immers de *notice and takedown* (NTD)-procedure. Een filterbevel kan dus alleen gericht worden tegen (Nederlandse) *access providers*, dat wil zeggen aanbieders die een dienst van de informatiemaatschappij leveren bestaande uit het doorgeven van van een ander afkomstige informatie of het verschaffen van toegang tot een communicatienetwerk.

109 Daarbij moet onderscheid worden gemaakt naar de locatie waar het als strafbare aangemerkte materiaal wordt *gehost*. Als die informatie op een Nederlandse server wordt gehost, dient justitie de Nederlandse hosting provider aanspreken tot verwijdering van de informatie.[47] Als strafbare informatie wordt *gehost* op een server in een land dat is aangesloten bij het Cybercrime Verdrag, moet gebruik worden gemaakt van de rechtshulpbepalingen uit dat verdrag.

110 Een filterbevel kan dus slechts worden gericht tot Nederlandse *access providers* met betrekking tot informatie die *gehost* wordt in landen waarmee geen rechtshulpverdrag is gesloten.

---

47 *Kamerstukken II* 2008/09, 28 684, nr. 232.

Wie kan een filterbevel geven?

111 Nu een filterbevel een ernstige inbreuk maakt op grondrechten en de bedrijfsvoering van providers vergaand belast, dient voor de inzet van de bevoegdheid een zwaar regime te gelden dat voorziet in een rechterlijke toets.[48] Dat betekent dat een filterbevel de voorafgaande goedkeuring behoeft van een rechter(-commissaris). Er is geen reden bij een filterbevel een lagere drempel te hanteren dan bij het goedkeuren van een aftapbevel (artikel 126m Sv) of een bevel tot verstrekking van gevoelige verkeersgegevens (artikel 126nf Sv).

Procedure

Voorafgaand aan het uitvaardigen van een filterbevel

112 De uitvoering van een filterbevel moet geregeld worden in een duidelijke, kenbare procedure die een zorgvuldige bevoegdheidsuitoefening waarborgt. De procedure moet specificeren op welke wijze een filterbevel gegeven moet worden en op welke wijze de informatieaanbieder en de ISP gehoord worden. In de woorden van artikel 1 lid 3bis van de nieuwe Kaderrichtlijn: een voorafgaande, eerlijke en onpartijdige procedure dient te worden gegarandeerd, inclusief het recht van de betrokkene of betrokkenen om te worden gehoord.

113 XS4ALL pleit voor een (spoed)procedure bij de rechtbank. In deze procedure is het aan justitie om de rechter ervan te overtuigen dat in het voorliggende geval is voldaan aan alle toepassingsvoorwaarden voor de filterbevoegdheid. In deze procedure zouden zowel de provider(s) tot wie een bevel gericht zal worden als de aanbieder (desgewenst anoniem) de mogelijkheid moeten hebben hun standpunt te bepleiten. Hun commerciële en grondrechtelijke belangen worden immers in vergaande mate geraakt. Nu ook de belangen van informatieontvangers worden geraakt door de vraag of – en zo ja, hoe – een bepaald filterbevel dient te worden uitgevaardigd, dienen organisaties die opkomen voor het collectieve consumentenbelang in de gelegenheid gesteld te worden te worden gehoord.

114 De procedure dient ook te voorzien in notificatie aan de betrokkenen bij de informatieblokkering. Daarbij kan aansluiting gezocht worden bij artikel 125m Sv dat onder meer bepaalt dat wanneer een doorzoeking leidt ontoegankelijkmaking van gegevens, daarvan zo spoedig mogelijk aan de betrokkenen schriftelijk mededeling wordt gedaan.

De inhoud van een filterbevel

115 Het uiteindelijke filterbevel dient precies te omschrijven wat de ISP moet doen – welke informatie op welke wijze geblokkeerd moet worden – en hem een redelijke termijn

[48] Dezelfde conclusie is te vinden in: Schellekens c.s., a.w., p. 44.

geven om dat te doen. Er kan dus nadrukkelijk niet worden volstaan met het in algemene termen opleggen van de verplichting om het ertoe te leiden dat bepaalde informatie in Nederland niet meer opvraagbaar is; aldus zou immers ten onrechte bij de provider de verantwoordelijkheid en het risico worden neergelegd voor de keuze van technische implementatie van filtering in concrete.

116 Het is van cruciaal belang dat een voldoende nauwkeurige afbakening plaatsvindt van hetgeen ontoegankelijk gemaakt moet worden. Een filterbevel moet zien op specifiek aangeduide en als strafbaar gekwalificeerde informatie en zo geformuleerd worden dat bijvangst zo veel mogelijk wordt uitgesloten.

117 Een bevel dient bovendien de informatie te bevatten die de ISP nodig heeft om vast te stellen dat sprake is van een bevoegd gegeven bevel, dat voldoet aan de wettelijke eisen. Een filterbevel zou bijvoorbeeld moeten specificeren waar de betrokken informatie *gehost* wordt, ook opdat voor een ISP kenbaar is dat dit een land is waarmee geen rechtshulpverdrag is gesloten.

118 Tot slot dient een filterbevel informatie te bevatten over beroeps- en herzieningsmogelijkheden (waarover hierna meer), alsmede over de procedures die gelden voor vergoeding van de kosten die de provider moet maken om aan het bevel te voldoen.

Beroep tegen filterbevelen

119 Het systeem dient te voorzien in "een daadwerkelijke en tijdige beroepsmogelijkheid bij een rechterlijke instantie." Deze dienen beschikbaar te zijn voor de informatieaanbieder wiens aanbod strafbaar wordt geacht, maar ook voor consumenten(organisaties) en, niet in de laatste plaats, providers zelf als adressaat van het filterbevel.

120 Er dient sprake te zijn van een volledig beroepsrecht als bedoeld in artikel 4 lid 1 van de Kaderrichtlijn – en dus niet een marginale toetsing. Daarbij dienen alle facetten van de zaak aan de orde te kunnen komen, zoals bijvoorbeeld de vraag of de informatie inderdaad (kennelijk) strafbaar is en of de bevolen filterwijze uitvoerbaar en proportioneel is, mede in het licht van de technische uitvoeringsmoeilijkheden en de bijvangst in termen van onterecht geblokkeerde, rechtmatige content.

121 Bovendien dient het instellen van beroep in beginsel opschortende werking te hebben, zodat een filterbevel pas ten uitvoer gelegd kan worden als het beroep definitief is afgewezen. Een dergelijke werkwijze komt overeen met de recente Franse "three strikes" wet (in de volksmond bekend als HADOPI 2), die erin voorziet dat internetgebruikers kunnen worden afgesloten als zij aanhoudend schuldig maken aan schendingen van het auteursrecht.[49] Een eerste versie van de wet werd door het Franse Conseil Constition-

[49] LOI n° 2009-1311 du 28 octobre 2009 relative à la protection pénale de la propriété littéraire et artistique sur internet, *JORF* n°0251 van 29 oktober 2009 p. 18290.

nel ongrondwettelijke bevonden, juist omdat het voorzag in het afsluiten van internettoegang zonder voorafgaande rechterlijke tussenkomst.[50] In de aangepaste versie is onder meer toegevoegd dat de internetgebruiker pas kan worden afgesloten nadat een daartoe strekkende rechterlijke beslissing gezag van gewijsde heeft.[51]

Herziening, periodiek en op aanvraag

122 De inhoud van een website is per definitie dynamisch: de inhoud ervan kan op ieder moment gewijzigd worden. Het feit dat een website op het tijdstip van aanvragen van een filterbevel inderdaad onmiskenbaar strafbare informatie bevat, betekent niet dat dat voor altijd zo zal zijn. Naast de mogelijkheid voor de informatieaanbieder om in beroep te gaan tegen een filterbevel, dient een filterbevel ook van tijd tot tijd opnieuw bezien te worden.

123 Een filterbevel dient daarom een beperkte geldigheidsduur te hebben van bijvoorbeeld drie of zes maanden, waarna het afloopt tenzij het tijdig wordt verlengd. In die gevallen waarin de informatie in de tussentijd niet is veranderd, kan bij verlenging worden volstaan met een vereenvoudigde procedure (zij het nog steeds met notificatie van belanghebbenden en de mogelijkheid gehoord te worden).

124 Bovendien dienen belanghebbenden op ieder moment te kunnen vragen om intrekking van een filterbevel op grond van de omstandigheid dat de informatie die aanleiding was voor het filterbevel, niet meer op de desbetreffende website staat of niet meer strafbaar is. Zodoende kan een informatieaanbieder die zich geconfronteerd ziet met een filterbevel, zijn website aanpassen en daarmee zekerstellen dat zijn informatieaanbod in Nederland weer toegankelijk is.

Vrijwaring

125 De analyse van de Universiteit van Tilburg van artikel 54a Sr bevat een uitgebreide analyse van de potentiële aansprakelijkheid van ISP's bij zowel een rechtmatig als bij een onrechtmatig gegeven filterbevel. Daarin wordt geconcludeerd dat een ISP zich bij het uitvoeren van een rechtmatig bevel op overmacht kan beroepen. Dat zal in veel gevallen wellicht het geval zijn, maar de gegrondheid van een beroep op overmacht wordt pas in het kader van de procedure vastgesteld aan de hand van de omstandigheden van het geval. Daarmee worden providers nog steeds opgezadeld met risico's en kosten, terwijl zij uitvoering meenden te geven aan een wettelijke verplichting. Dergelijke risico's behoren bij de Staat te rusten. Een uitbreiding van contractuele voorwaar-

50 Conseil Constitutionnel 10 juni 2009 Beslissing No. 2009-580 DC, *Mediaforum* 2009-9, nr. 28.

51 Zie artikel 7: "Lorsque la décision est exécutoire, la peine complémentaire prévue au présent article est portée à la connaissance de la Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet, qui la notifie à la personne dont l'activité est d'offrir un accès à des services de communication au public en ligne afin qu'elle mette en œuvre, dans un délai de quinze jours au plus à compter de la notification, la suspension à l'égard de l'abonné concerné."

den of een exoneratie ondervangt deze eventuele aansprakelijkheid onvoldoende, ook omdat XS4ALL met de informatieaanbieder wiens informatie geblokeerd wordt, doorgaans geen contractuele relatie heeft.[52] Daarom dient een bevel tot ontoegankelijkmaking samen te gaan met het verlenen van een volledige vrijwaring door de Staat.

[52] Schellekens c.s., a.w., p. 31.

Conclusie

126 Uit het voorgaande blijkt dat een verplichting voor internetaanbieders om *deep packet inspection* of andere filtertechnieken in te zetten bij de bestrijding van auteursrechtinbreuk of andere illegale informatie op internet, in praktijk onuitvoerbaar, ineffectief en disproportioneel zal zijn. Er bestaat geen techniek waarmee strafbare informatie gericht geblokkeerd kan worden, zonder dat dit (a) gemakkelijk te omzeilen is voor diegenen die dat willen, (b) leidt tot veel schadelijke bijvangst in termen van onterecht geblokkeerde, niet-illegale informatie en (c) leidt tot aanzienlijke kosten en technische degradatie in de kwaliteit, betrouwbaarheid en veiligheid van de dienstverlening van internetaanbieders.

127 Filteren is dus een ineffectieve, schadelijke en dure vorm van censuur, die raakt aan belangrijke grondrechten van zowel informatieaanbieders als –ontvangers, in het bijzonder rechten op vrijheid van meningsuiting, privacy, communicatiegeheim, een eerlijk proces en internettoegang. Daarnaast raakt een wettelijke filterverplichting aan de rechten en belangen van internetaanbieders, zoals deze zijn verankerd in de Europese Machtigingsrichtlijn en Richtlijn Elektronische handel.

128 In dit position paper zijn zowel de feitelijke als juridische dimensies van filteren geanalyseerd. Daaruit blijkt dat, als de wetgever toch wil kiezen voor een vorm van verplicht filteren, onze verdragsrechtelijke verplichtingen nopen tot een strenge begrenzing en specifieke, vergaande waarborgen. In het laatste hoofdstuk is geanalyseerd welke gevolgen deze verplichtingen hebben voor de inrichting van een wettelijke filterbevoegdheid. Zo kan een filterbevoegdheid alleen worden toegepast tegen buitenlandse websites waarvan zowel de informatieaanbieder als de hosting provider niet via rechtshulpverzoeken kunnen worden aangesproken en alleen worden ingezet tegen zeer ernstige uitingsdelicten waarover Nederland rechtsmacht heeft; kan een filterbevel alleen worden verleend na een voorafgaande rechterlijke toets waarbij alle betrokkenen kunnen worden gehoord; en dienen tegen een filterbevel effectieve beroeps- en herzieningsprocedures open te staan. Uit de Europese proportionaliteitseis volgt bovendien dat alle eenmalige en periodieke technische en administratieve kosten in verband met filtering dienen te worden gedragen door de Staat.

129 Ook als een filterbevoegdheid wordt voorzien van dergelijke stringente waarborgen (en die waarborgen in praktijk worden nageleefd), geldt echter dat filteren niet goed werkt, makkelijk kan worden omzeild, schade berokkent aan legale informatie en inbreuk maakt op elementaire grondrechten.