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