akd

AAN De minister van Justitie en Veiligheid
Postbus 20301
2500 EH DEN HAAG

VAN

TELEFOON
FAX
E-MAIL

BEZOEKADRES

POSTADRES

INTERNET

DATUM 27 november 2018
ONDERWERP Haalbaarheidsstudie bestuursrechtelijke aanpak van kinderporno
UW KENMERK 10100027107
ONS KENMERK 285702

Excellentie,

In dit onderzoek adviseren wij over de vraag of het bestuursrechtelijk handhavend optreden tegen ICT-bedrijven ten einde de verwijdering van kinderporno op het openbare web te bewerkstelligen juridisch haalbaar is en in de praktijk werkbaar is.

---

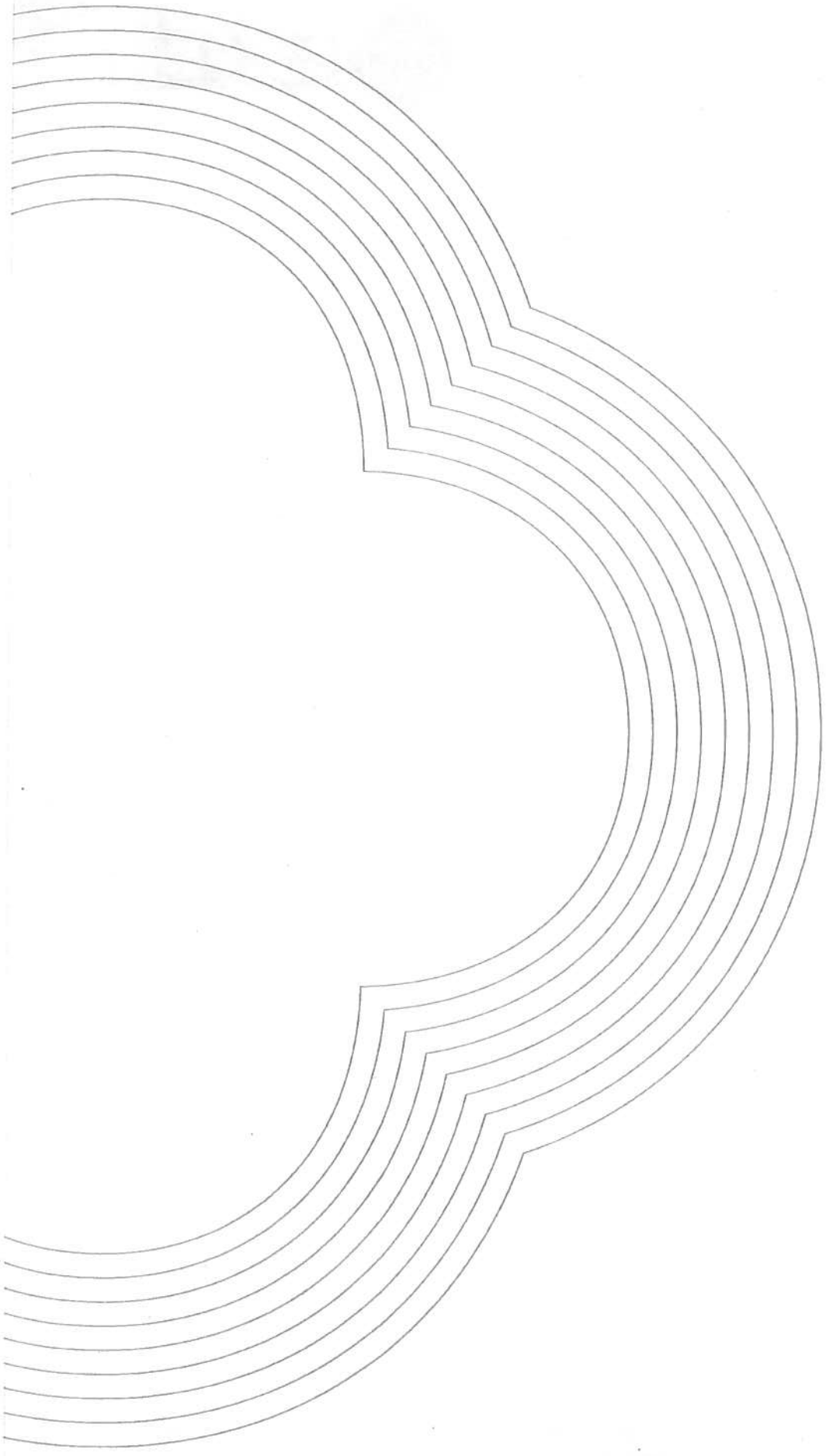
**Managementsamenvatting**

Onze conclusie is dat het mogelijk is om tot een juridisch haalbaar en in de praktijk werkbaar handhavingsinstrumentarium te komen, maar dat het niet haalbaar is om partijen die niet in Nederland zijn gevestigd of in Nederland vermogensbestanddelen hebben te raken op deze manier. Met andere woorden: de aanpak zou op nationaal niveau effect kunnen sorteren, maar kan nooit waterdicht zijn omdat de effectiviteit van het instrumentarium ophoudt bij de Nederlandse landsgrenzen, terwijl het internet daar niet ophoudt.

De aanpak die wij u zouden adviseren is een bestuursrechtelijke normstelling inhoudende dat aan bepaalde ICT-bedrijven die niet of niet voldoende snel na een melding van bijvoorbeeld de politie of het EOKM overgaan tot vrijwillige verwijdering van KP een bindende aanwijzing kan worden opgelegd. Op grond van die aanwijzing wordt het ICT-bedrijf alsnog publiekrechtelijk verplicht om de KP te verwijderen binnen een laatste in de aanwijzing gegeven korte termijn. Deze normstelling zou volgens ons primair moeten worden gesanctioneerd door de inzet van bestuursdwang en/of een bestuurlijke boete. De reden hiervoor is dat met bestuursdwang snel en zonder dat medewerking van de overtreder nodig is fysiek de overtreding worden beëindigd. Van de bestuurlijke boete gaat een belangrijke afschrikwekkende en (bij publicatie daarvan) diffamerende werking uit zodat daarmee een belangrijke bijdrage aan de preventie kan worden geleverd.

---

Dit advies is als volgt opgebouwd. In **onderdeel één** lichten wij de achtergrond voor dit advies toe en gaan wij in op de deelvragen zoals wij die in dit advies beantwoorden. In **onderdeel twee** komt aan de orde of een normstelling gericht aan ICT-bedrijven juridisch haalbaar is, in de praktijk werkbaar is en hoe een eventuele normstelling in hoofdlijnen zou



kunnen gaan luiden. In **onderdeel drie** bespreken wij hoe deze normstelling op een juridisch haalbare en in de praktijk werkbare wijze bestuursrechtelijk kan worden gehandhaafd. In **onderdeel vier** gaan wij in op de mogelijkheden om opgelegde sancties daadwerkelijk uit te voeren (ook over de landsgrenzen). In **onderdeel vijf** sluiten wij af met een conclusie en ons advies aan u.

## 1. Inleiding en achtergronden

1.1. Kinderporno (hierna: '**KP**') is een hardnekkig verschijnsel op het internet. De politie komt websites met KP-materiaal op het spoor door de eigen opsporing van zedenzaken, of door de meldingen via de daarvoor ingestelde meldpunten (het particuliere meldpunt kinderporno op internet en het meldpunt cybercrime van de Nederlandse politie), of door meldingen van politie of overheidsdiensten uit andere landen.[1]

1.2. KP wordt in Nederland op verschillende manieren aangeboden op het openbare internet. In Nederland gevestigde ICT-bedrijven kunnen daar - meestal ongewild en indirect – op verschillende manieren bij betrokken zijn. Gedacht kan daarbij worden aan een in Nederland gevestigde Hosting Service Provider ('**HSP**'). In het verlengde van het concept voor de verordening ter voorkoming van de verspreiding van terroristische online-inhoud[2] (hierna: '**Terrorismeverordening**') verstaan wij daaronder: een aanbieder van diensten van de informatiemaatschappij die eruit bestaan door een aanbieder van inhoud verstrekte informatie op verzoek van die aanbieder van inhoud op te slaan en de opgeslagen informatie aan derden beschikbaar te stellen. Onder de diensten van een HSP kunnen bijvoorbeeld vallen het verhuren van een server of serverruimte waarop websites kunnen worden geplaatst. Naast een HSP kan ook een in Nederland gevestigde Internet Service Provider ('**ISP**') – vaak indirect en ongewild – bij het aanbieden van KP betrokken zijn. Denk in dat verband bijvoorbeeld aan een gebruiker/abonnee van een in Nederland gevestigde ISP die in het netwerk van de ISP een website inricht en beheert. In het kader van dit rapport zal – in het verlengde van de brief aan de minister aan de Tweede Kamer d.d. 7 februari 2018 inzake de aanpak van kindermisbruik – in meer algemene zin over de bij het via het aanbieden van KP op het openbare internet betrokken ICT-bedrijven worden gesproken. Daaronder worden dan in ieder geval een HSP en een ISP begrepen. Niet uitgesloten is echter dat ook andere ICT-bedrijven bij het aanbieden van KP een rol kunnen spelen. In het kader van de normstelling zal een van de te beantwoorden vragen zijn welke ICT-bedrijven specifiek als normadressant zullen moeten worden aangemerkt. Wij hebben in dit rapport primair het oog op be-

[1] Kamerstukken II 2008-2009, 31200 VI, nr. 146.

[2] COM(2018) 640 final 2018/0331(COD)

drijven die diensten aanbieden als tussenpersoon bij het doorgeven en/of opslaan van informatie en niet zozeer op de aanbieders van die informatie zelf. Uiteraard is het ook denkbaar dat er bij het aanbieden van KP via het openbare internet geen in Nederland gevestigd ICT-bedrijf is betrokken, terwijl de websites wel via het internet in Nederland benaderbaar zijn.[3]

1.3. Hoewel het bewust bezitten van KP al strafrechtelijk kan worden aangepakt,[4] is het enkel aanwezig hebben van KP op een server of computer[5] niet strafbaar. Dit betekent dat derden, zoals een in Nederland gevestigd ICT-bedrijf zoals een ISP of HSP, niet strafbaar zijn voor het enkel aanwezig hebben van KP geplaatst op hun server. Het betekent echter ook dat er op dit moment geen publiekrechtelijk afdwingbare wettelijke norm is die een in Nederland gevestigd ICT-bedrijf verplicht om uit eigen beweging KP te verwijderen.[6] Tussenpersonen die (telecommunicatie)diensten op het internet aanbieden (zoals ISP's en HSP's) hebben zich wel gecommitteerd aan de "*Gedragscode Notice-and-Take-Down*" waarin een algemene procedure voor het verwijderen van onrechtmatige content is opgenomen. Dergelijke tussenpersonen verwijderen KP in beginsel vrijwillig naar aanleiding van een melding. Daar speelt ook het eigenbelang van de tussenpersonen (althans voor zover deze tussenpersonen bepaalde diensten verrichten met betrekking tot de opslag van informatie) omdat zij ingevolge artikel 6:196c, lid 3 en 4, BW slechts gevrijwaard zijn voor civiele aansprakelijkheid voor de illegale content indien zij in de in de betreffende artikelleden beschreven gevallen (de nodige maatregelen treffen om) de illegale content te verwijderen of ontoegankelijk te maken.[7] Naar het effect van deze zelfregulering en de prikkel van

[3] Kamerstukken II 2008-2009, 31200 VI, nr. 146.

[4] Artikel 240b Wetboek van Strafrecht.

[5] HR 7 februari 2017, ECLI:NL:HR:2017:167.

[6] Wel is er de mogelijkheid via artikel 54a Wetboek van Strafrecht dat de Officier van Justitie een schriftelijke machtiging vordert van de rechter-commissaris ten einde een 'tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn' te dwingen om alle maatregelen te nemen die redelijkerwijs van hem verlangd kunnen worden om die gegevens ontoegankelijk te maken.

[7] Artikel 6:196c lid 3 heeft betrekking op degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3, bestaande uit het geautomatiseerd, tussentijds en tijdelijk opslaan van van een ander afkomstige informatie voor zover het opslaan enkel geschiedt om het later doorgeven van die informatie aan anderen op hun verzoek doeltreffender te maken. Dergelijke aanbieders zijn slechts van civielrechtelijke aansprakelijkheid gevrijwaard voor de inhoud van de betreffende informatie indien zij prompt de nodige maatregelen neemt om de informatie te verwijderen of de toegang daartoe onmogelijk te maken zodra hij weet dat de informatie is verwijderd van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe onmogelijk is gemaakt, of dat een bevoegde autoriteit heeft bevolen de informatie te verwijderen van de plaats waar deze zich oorspronkelijk in het communicatienetwerk bevond of de toegang daartoe heeft verboden. Artikel 6:196c lid 4 heeft betrekking op degene die diensten van de informatiemaatschappij verricht als bedoeld in artikel 15d lid 3 van Boek 3,

artikel 6:196c BW wordt op dit moment empirisch onderzoek verricht door de TU Delft, maar uit de praktijk komen signalen dat niet altijd adequaat wordt gereageerd op meldingen van KP, met name door zogenaamde 'bad hosters'.

1.4. Omdat de overheid geen instrument heeft om tegen 'bad hosters' op te treden, overweegt u om een wettelijke verplichting te introduceren voor bepaalde ICT-bedrijven strekkende tot het moeten verwijderen of ontoegankelijk maken van KP binnen een bepaalde periode nadat de overheid het bestaan daarvan bij hen heeft gemeld.[8] Deze normstelling zou bestuursrechtelijk moeten worden gehandhaafd.

1.5. Aan AKD is gevraagd om te adviseren over de vraag of een dergelijke bestuursrechtelijk te handhaven normstelling juridisch haalbaar en in de praktijk werkbaar is. Met het team dat binnen uw Ministerie het onderzoek begeleidt is een aantal beperkingen in de advisering besproken.

1.6. Ten eerste is onze adviesopdracht expliciet beperkt tot het bestuderen van de bestuursrechtelijke handhavingsmogelijkheden. Wij zullen dus niet ingaan op eventuele straf- en civielrechtelijke maatregelen die mogelijk zouden kunnen worden getroffen ter handhaving van de normstelling. Ook zullen wij niet stilstaan bij het advies van de Raad van State d.d. 13 juli 2015 (Staatscourant 2015, nr. 30280) omtrent de afweging bij de keuze voor bestuursrechtelijke handhaving in plaats van strafrechtelijke handhaving.

1.7. Ten tweede ziet dit advies op het tegengaan van de aanwezigheid van KP op het openbare web. Het tegengaan van het aanbieden van KP op het TOR-netwerk (ook wel het 'dark-web'), dan wel op andere besloten vormen van communicatie (zoals versleutelde berichten tussen twee personen via berichtendiensten), valt niet binnen de reikwijdte van dit advies.

1.8. Ten derde is besproken dat dit advies niet zal zien op de technische mogelijkheden om KP te verwijderen. Wij mogen aannemen dat het technisch mogelijk is om KP te verwijderen of ontoegankelijk te maken en dat de betreffende ICT-bedrijven dat desgevraagd kunnen (alsook dat de overheid de technische middelen heeft om dat zo nodig af te dwingen). Wij merken ten overvloede op dat de effectiviteit van de handhaving staat of valt met voldoende beschikbaarheid van de benodigde kennis op dit vlak.

---

bestaande uit het op verzoek opslaan van van een ander afkomstige informatie. Dergelijke aanbieders zijn slechts gevrijwaard van civielrechtelijke aansprakelijkheid voor de inhoud van die informatie indien hij zodra hij dat weet of redelijkerwijs behoort te weten, prompt de informatie verwijdert of de toegang daartoe onmogelijk maakt.

[8] Kamerstukken II 2017-2018, 31015, nr. 135, p.8.

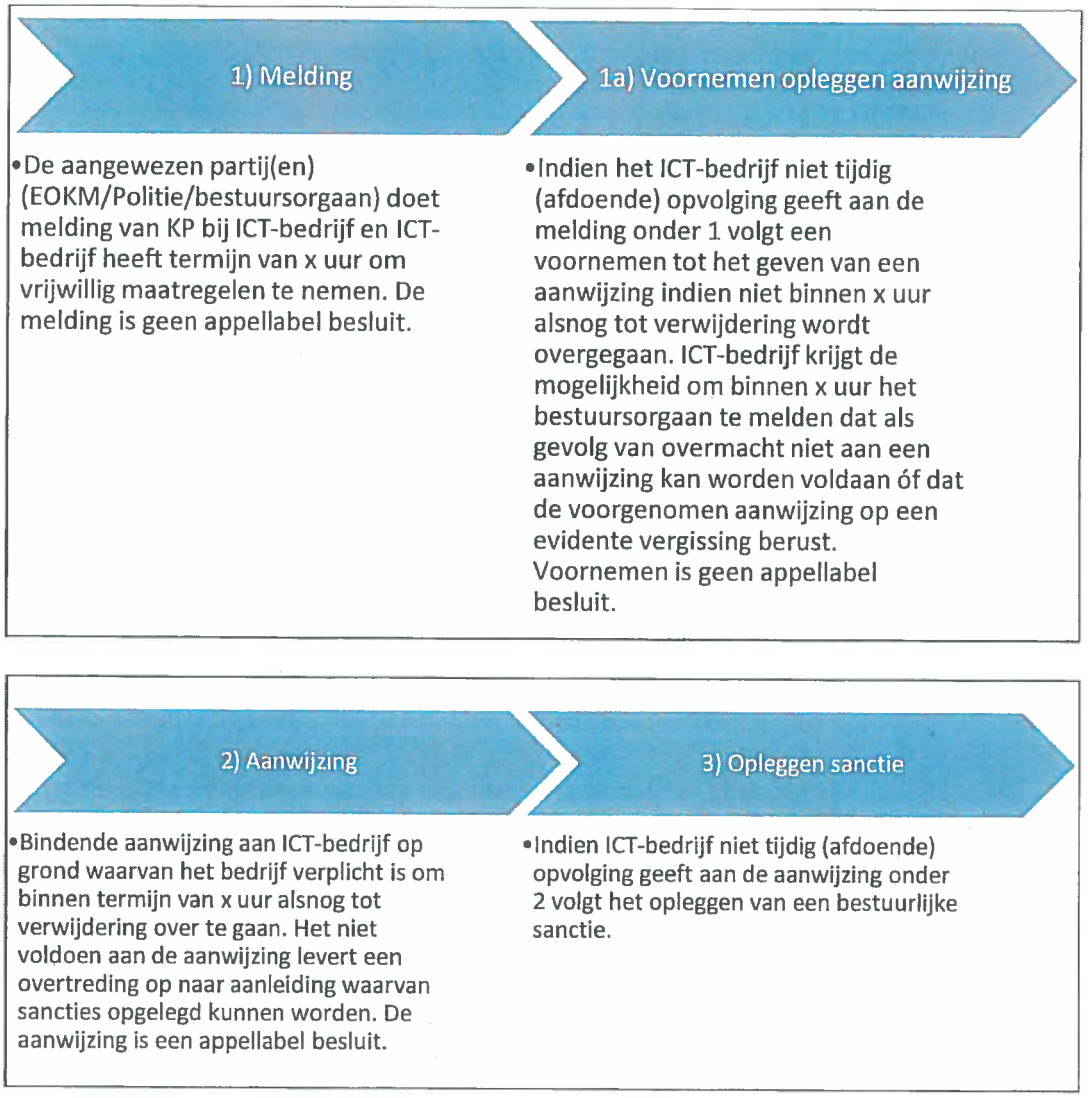
1.9. Ten behoeve van de leesbaarheid van dit advies staan wij wel graag kort stil bij de technische (on)mogelijkheden om verwijdering af te dwingen.

1.10. Het verwijderen of ontoegankelijk maken van KP kan op verschillende manieren. Ten eerste is het mogelijk om KP geheel te verwijderen van een server. Dat kan door de desbetreffende server (bijvoorbeeld) fysiek te verwijderen uit het pand van een ICT-bedrijf, maar het kan ook door op die server de KP te wissen. Ten tweede is het mogelijk om de toegang tot KP te blokkeren en de KP daarmee ontoegankelijk te maken. Dit kan door een reeks verschillende maatregelen. Bijvoorbeeld het blokkeren van een IP-adres of een URL, maar ook door bijvoorbeeld een ISP te instrueren om via het DNS-register een onjuiste routebeschrijving te geven (waarbij het verkeer niet naar de site met KP wordt doorverwezen maar – bijvoorbeeld – naar een site van de Nationale politie of het EOKM). Ten derde is het mogelijk om bepaalde content door een ISP te laten filtreren die voorkomt in een bepaalde databank ('dynamic filtering') en daarmee ontoegankelijk te maken. Dit wordt (bijvoorbeeld) bewerkstelligd met de hashcodesdatabank waarin inmiddels bekende KP-afbeeldingen zijn opgenomen.

1.11. De beperkingen van deze methodes zijn – kort samengevat – de volgende. Ten eerste kan de Nederlandse overheid niet de fysieke verwijdering afdwingen in gevallen waarin de Nederlandse overheid geen rechtsmacht heeft (lees: buiten de Nederlandse landsgrenzen). De eerste optie is dus enkel mogelijk bij in Nederland gevestigde servers of in Nederland bedrijven. Ten tweede zijn alle blokkades en filtreermethodes op de een of andere manier technisch te omzeilen. Bij een IP-blokkade is dat veel eenvoudiger dan (bijvoorbeeld) een DNS-blokkade of een hashcodefilter, maar naar wij begrijpen is het technisch *altijd* mogelijk om een blokkade of filter te omzeilen op het internet.

1.12. Kort samengevat: het is technisch onmogelijk om een waterdicht systeem te ontwerpen. Het technisch hoogst haalbare is dat alle KP die binnen de Nederlandse rechtsmacht valt fysiek wordt verwijderd op servers en dat alle KP die buiten de Nederlandse rechtsmacht valt wordt geblokkeerd of gefiltreerd, met de wetenschap dat die blokkades en filters door kwaadwillenden kunnen worden omzeild. Hierna adviseren wij u of en hoe deze technisch hoogst haalbare doelstelling juridisch kan worden gerealiseerd en wel zodanig dat de aanpak in de praktijk werkbaar is.

Figuur 1


1) Melding
1a) Voornemen opleggen aanwijzing
•De aangewezen partij(en) (EOKM/Politie/bestuursorgaan) doet melding van KP bij ICT-bedrijf en ICT-bedrijf heeft termijn van x uur om vrijwillig maatregelen te nemen. De melding is geen appellabel besluit.
•Indien het ICT-bedrijf niet tijdig (afdoende) opvolging geeft aan de melding onder 1 volgt een voornemen tot het geven van een aanwijzing indien niet binnen x uur alsnog tot verwijdering wordt overgegaan. ICT-bedrijf krijgt de mogelijkheid om binnen x uur het bestuursorgaan te melden dat als gevolg van overmacht niet aan een aanwijzing kan worden voldaan óf dat de voorgenomen aanwijzing op een evidente vergissing berust. Voornemen is geen appellabel besluit.
2) Aanwijzing
3) Opleggen sanctie
•Bindende aanwijzing aan ICT-bedrijf op grond waarvan het bedrijf verplicht is om binnen termijn van x uur alsnog tot verwijdering over te gaan. Het niet voldoen aan de aanwijzing levert een overtreding op naar aanleiding waarvan sancties opgelegd kunnen worden. De aanwijzing is een appellabel besluit.
•Indien ICT-bedrijf niet tijdig (afdoende) opvolging geeft aan de aanwijzing onder 2 volgt het opleggen van een bestuurlijke sanctie.

## 2. Normstelling

2.1. In deze paragraaf beschrijven wij of en op welke wijze normstelling die gericht is op verwijdering (/ontoegankelijk maken) van content die KP bevat (a) juridisch haalbaar is en (b) in de praktijk werkbaar is.

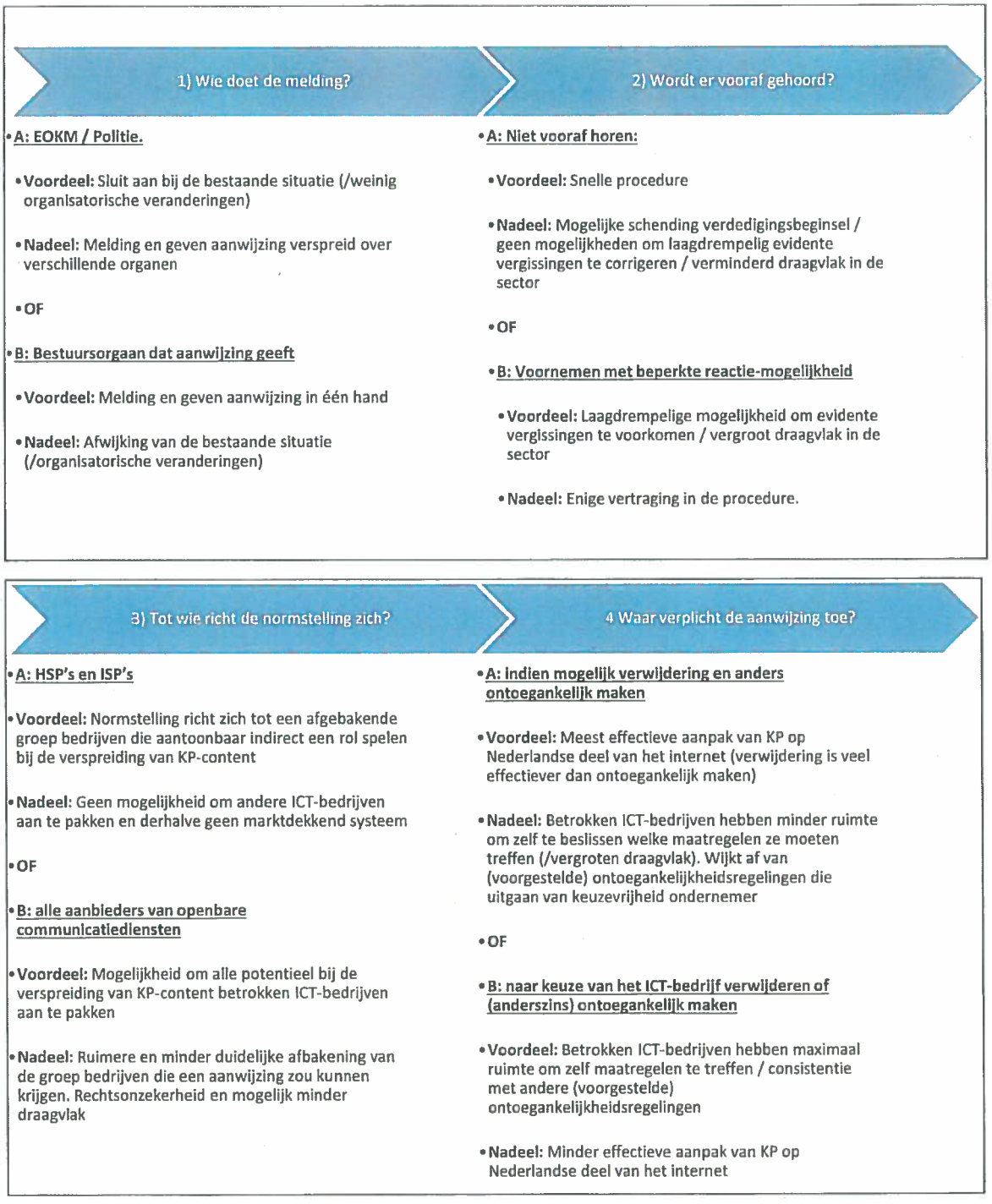
2.2. In het kader van ons onderzoek hebben wij twee stappen gezet. De eerste stap is het formuleren van de voorwaarden waaraan volgens ons voldaan moet zijn om de normstelling juridisch haalbaar en in de praktijk werkbaar te laten zijn. In de tweede stap hebben wij met inachtneming van die voorwaarden gekeken naar de mogelijke inhoud van de beoogde normstelling. Bij deze laatste stap hebben wij zoveel mogelijk aansluiting gezocht bij recente voorstellen voor Europese en nationale regelgeving met betrekking tot het ontoegankelijk maken van illegale content.

Bij onze analyse hebben wij ons gericht op het formuleren van een norm die voorziet in de mogelijkheid om af te kunnen dwingen dat een ICT-bedrijf overgaat tot het verwijderen (/ontoegankelijk maken) van KP indien daar niet of niet voldoende snel vrijwillig tot wordt overgegaan.

Uit de analyse zal volgen dat het wat ons betreft mogelijk is om in normstelling te voorzien die zowel juridisch haalbaar als in de praktijk werkbaar is. De wetgever heeft daarbij volgens ons de vrijheid om binnen bepaalde grenzen op bepaalde punten keuzes te maken. Wij schetsen de grenzen van het speelveld en de punten waarop keuzes gemaakt kunnen worden. Waar mogelijk doen wij daarbij in voorkomend geval suggesties voor die keuzes die naar ons oordeel het beste aan beide doelstellingen (juridisch houdbaar en in de praktijk werkbaar) beantwoorden.

Wij vatten onze bevindingen in de volgende twee figuren samen. **Figuur 1** geeft de verschillende stappen weer die volgens ons onderdeel zouden moeten zijn van een "getrapte normstelling". **Figuur 2** geeft de in verband met deze normstelling te maken belangrijkste inhoudelijke keuzes weer, inclusief een inventarisatie van de voor- en nadelen van bepaalde keuzes.

Figuur 2


1) Wie doet de melding?
2) Wordt er vooraf gehoord?
A: EOKM / Politie.
Voordeel: Sluit aan bij de bestaande situatie (/weinig organisatorische veranderingen)
Nadeel: Melding en geven aanwijzing verspreid over verschillende organen
OF
B: Bestuursorgaan dat aanwijzing geeft
Voordeel: Melding en geven aanwijzing in één hand
Nadeel: Afwijking van de bestaande situatie (/organisatorische veranderingen)
A: Niet vooraf horen:
Voordeel: Snelle procedure
Nadeel: Mogelijke schending verdedigingsbeginsel / geen mogelijkheden om laagdrempelig evidente vergissingen te corrigeren / verminderd draagvlak in de sector
OF
B: Voornemen met beperkte reactie-mogelijkheid
Voordeel: Laagdrempelige mogelijkheid om evidente vergissingen te voorkomen / vergroot draagvlak in de sector
Nadeel: Enige vertraging in de procedure.
3) Tot wie richt de normstelling zich?
4 Waar verplicht de aanwijzing toe?
A: HSP's en ISP's
Voordeel: Normstelling richt zich tot een afgebakende groep bedrijven die aantoonbaar indirect een rol spelen bij de verspreiding van KP-content
Nadeel: Geen mogelijkheid om andere ICT-bedrijven aan te pakken en derhalve geen marktdekkend systeem
OF
B: alle aanbieders van openbare communicatiediensten
Voordeel: Mogelijkheid om alle potentieel bij de verspreiding van KP-content betrokken ICT-bedrijven aan te pakken
Nadeel: Ruimere en minder duidelijke afbakening van de groep bedrijven die een aanwijzing zou kunnen krijgen. Rechtsonzekerheid en mogelijk minder draagvlak
A: Indien mogelijk verwijdering en anders ontoegankelijk maken
Voordeel: Meest effectieve aanpak van KP op Nederlandse deel van het internet (verwijdering is veel effectiever dan ontoegankelijk maken)
Nadeel: Betrokken ICT-bedrijven hebben minder ruimte om zelf te beslissen welke maatregelen ze moeten treffen (/vergroten draagvlak). Wijkt af van (voorgestelde) ontoegankelijkheidsregelingen die uitgaan van keuzevrijheid ondernemer
OF
B: naar keuze van het ICT-bedrijf verwijderen of (anderszins) ontoegankelijk maken
Voordeel: Betrokken ICT-bedrijven hebben maximaal ruimte om zelf maatregelen te treffen / consistentie met andere (voorgestelde) ontoegankelijkheidsregelingen
Nadeel: Minder effectieve aanpak van KP op Nederlandse deel van het internet

**Stap 1: de voorwaarden waaraan de betreffende normstelling moet voldoen om juridisch haalbaar en in de praktijk werkbaar te zijn**

**Juridisch houdbaar**

2.3. Onder normstelling die juridisch houdbaar is verstaan wij normstelling die enerzijds de constitutionele toetsing die de Afdeling advisering van de Raad van State in het kader van de advisering over wetsvoorstellen hanteert[9] en die anderzijds de toetsing van wetten in formele zin door de rechter zou moeten kunnen doorstaan. Wij hebben daarom die voorwaarden geformuleerd die specifiek nodig zijn om de normstelling te kunnen laten voldoen aan de (relevante) bepalingen uit de Grondwet, het Statuut, het Unierecht en de eenieder verbindende bepalingen uit verdragen.[10] De geformuleerde voorwaarden vallen in twee categorieën uiteen: voorwaarden om de inbreuken op de aan de orde zijnde grondrechten te kunnen rechtvaardigen enerzijds (**stap 1a**) en voorwaarden om de normstelling aan de (overige) relevante bepalingen uit het Unierecht te laten voldoen anderzijds (**stap 1b**). De vraag of een bepaalde norm uiteindelijk de toetsing door de Afdeling advisering en eventueel van de rechter kan doorstaan, hangt uiteraard in belangrijke mate af van de precieze formulering van de norm en de daarbij behorende toelichting. Dit rapport houdt echter geen advies in over de formulering van de norm noch over de inhoud van de daarbij behorende toelichting.

**Stap 1a: voorwaarden om de inbreuken op grondrechten te kunnen rechtvaardigen**

*Welke grondrechten spelen een rol?*

2.4. In het kader van de beoogde normstelling zijn de navolgende grondrechten specifiek van belang. Wij bespreken de van toepassing zijnde grondrechten vanuit het perspectief van de verschillende bij KP betrokken actoren (zoals ook onderscheiden in de meest recente brieven aan de Tweede Kamer).

2.5. Allereerst zijn van uit het perspectief van het slachtoffer het recht op eerbiediging van de persoonlijke integriteit (onder meer art. 2 en 3 EVRM) en het recht

[9] B.P. Vermeulen & H.J.Th.M. van Roosmalen, De constitutionele toetsing door de Raad van State, RegelMaat 2012 (27) 4.

[10] De toetsing van voorgestelde wetgeving door de Afdeling advisering van de Raad van State omvat uitdrukkelijk meer aspecten dan uitsluitend een constitutionele toetsing. Andere aspecten die doorgaans in de advisering door de Afdeling een rol spelen blijven in dit rapport buiten beschouwing.

op eerbiediging van het privéleven van belang. Door het Europees Hof van de Rechten van de Mens (hierna: EHRM) is onder voorwaarden aangenomen dat er op de verdragsstaten positieve verplichtingen rusten om te voorzien in adequate wettelijke maatregelen om misbruik van kinderen te voorkomen en slachtoffers van kindermisbruik te beschermen.[11] Bij de huidige stand van de rechtspraak van het EHRM lijkt er overigens geen dwingende verplichting op Nederland te rusten om te voorzien in wettelijke voorschriften die internetbedrijven verplichten om illegale content te verwijderen c.q. ontoegankelijk te maken. Wel onderstreept de rechtspraak van het EHRM het belang van het treffen van adequate wettelijke maatregelen. In zoverre is de beoogde wetgeving in het kader van de grondrechtenbescherming die aan (potentiële) slachtoffers van kindermisbruik toekomt een logische stap. In de toelichting op de beoogde normstelling zou dit kunnen worden verduidelijkt door toe te lichten hoe het (snel) verwijderen (/ontoegankelijk maken) van KP misbruik van kinderen kan voorkomen en slachtoffers van dergelijk misbruik kan beschermen. Bovendien geeft Nederland met de beoogde wetgeving verdere invulling aan de verplichting op grond van Richtlijn 2011/93/EU (bestrijden seksueel misbruik en seksuele uitbuiting, hierna: **'Richtlijn KP'**) tot het nemen van maatregelen om websites die KP bevatten of verspreiden die op het Nederlandse grondgebied worden gehost te verwijderen.[12] De Europese Commissie heeft in haar evaluatieverslag van de tenuitvoerlegging van de betreffende Richtlijn aangegeven dat artikel 25 van de Richtlijn ondanks de reeds gepleegde belangrijke inspanningen van de lidstaten nog meer potentieel heeft. In dat verband is als een van de belangrijke opgaven de zorg voor de onverwijlde verwijdering van illegale content genoemd.[13]

2.6. Vanuit het perspectief van de dader (in deze context vooral degene die het materiaal plaatst, verspreidt of bekijkt/downloadt) is primair de vrijheid van meningsuiting (artikel 7 Grondwet, artikel 10 EVRM en artikel 11 van het Handvest van de grondrechten van de Europese Unie, hierna **'Handvest EU'**) van belang en onder omstandigheden het recht op eerbiediging van het privéleven (artikel 8 EVRM en artikel 7 EU Handvest). Wij leiden uit de rechtspraak van het EHRM af dat – op dat punt overigens in afwijking van bijvoorbeeld de Verenigde Staten[14] en in afwijking van de opvatting van het Europees parlement en de Raad dienaangaande[15] – de verspreiding en het bezit van KP vallen onder de werkings-

[11] EHRM 2 december 2008, (K.U. vs. Finland), 2872/02 en EHRM 12 november 2013 (Söderman vs. Sweden), 5786/08.

[12] Artikel 25, eerste lid, Richtlijn 2011/93/EU, P.bl. 335/1.

[13] COM/2016/0872 final.

[14] U.S. Supreme Court New York v.s. Ferber, 458 U.S. 747 (1982).

[15] Zie considerans punt 46, Richtlijn 2011/92/EU.

sfeer van de vrijheid van meningsuiting[16] en dat het overheidsoptreden dat daarop een inbreuk maakt moet voldoen aan de eisen uit artikel 10 EVRM.[17]

Deze benadering is ook in lijn met de regeling van de vrijheid van meningsuiting in artikel 7 van de Grondwet. Het betreffende artikel verbiedt iedere vorm van preventieve inmenging door de overheid in de meningsuiting (voor zover het de openbaarmaking betreft) op grond van de inhoud van de geuite mening. Slechts repressieve beperkingen van inhoudelijke aard zijn – onder bepaalde strikte voorwaarden – toegestaan. Het zou op gespannen voet met artikel 7 van de Grondwet staan indien het plaatsen of verspreiden van KP op voorhand van het beschermingsbereik van dat artikel zou worden uitgezonderd. Feitelijk zou dat immers neerkomen op een preventieve beperking van de vrijheid van meningsuiting op grond van de inhoud van de mededeling. De beoogde normstelling zal tevens aan het bepaalde in artikel 7 van de Grondwet dienen te voldoen.

De beoogde wetgeving lijkt, vanuit het perspectief van de dader, op het eerste gezicht geen inbreuk in te houden op artikel 8 EVRM. In de digitale context vallen met name de bescherming van persoonlijke data (zoals gerichte communicatie en metadata met betrekking tot persoonlijk internetgebruik) enerzijds en het recht om onder omstandigheden anoniem gebruik te kunnen maken van het internet anderzijds onder de werkingssfeer van artikel 8 EVRM. Het ontoegankelijk maken van KP-websites/-content houdt in principe geen aantasting van de persoonlijke data van de dader in en evenmin een inbreuk op zijn of haar anonimiteit op het internet.[18]

2.7. Vanuit het perspectief van het ICT-bedrijf lijkt een beperking van de vrijheid van meningsuiting uitsluitend aan de orde te kunnen zijn indien het bedrijf ten aanzien van die content niet uitsluitend handelt als tussenpersoon die diensten be-

[16] EHRM 10 mei 2011 (Karttunen v Finland), 1685/10. Die uitspraak is bovendien in lijn met vaste rechtspraak van het EHRM op grond waarvan iedereen recht heeft om informatie te ontvangen en te verzamelen, ongeacht het doel van of de rol die een persoon speelt bij de uitoefening van het recht van vrijheid van meningsuiting (zie bijvoorbeeld EHRM 1 december 2015 (Cengiz e.a. v Turkije), 48226/10 en 14027/11).

[17] Enige voorzichtigheid is dienaangaande overigens geboden. Het betrof een zaak waarin een Finse onderdaan strafrechtelijk was vervolgd (en schuldig bevonden) in verband met – kort gezegd – het verspreiden van KP (overigens om aan de kaak te stellen dat KP veel te makkelijk toegankelijk is). Het EHRM oordeelde dat de betreffende veroordeling een beperking inhield van de vrijheid van meningsuiting en daarom in overeenstemming diende te zijn met het bepaalde in artikel 10 EVRM. Niet geheel is uitgesloten dat het Hof in de betreffende zaak mede gewicht heeft toegekend aan het motief van de verspreider van KP en gelet daarop meende dat de opgelegde sanctie een beperking van de vrijheid van meningsuiting opleverde en daaruit niet mag worden afgeleid dat de verspreiding van KP onder alle gevallen kan worden beschouwd als een meningsuiting die binnen het beschermingsbereik van artikel 10 EVRM valt.

[18] EHRM 24 april 2018 (Benedik v. Slovenië), 62357/14.

staande uit het doorgeven of opslaan van gegevens verricht, maar ook zelf een bepaalde inhoudelijke rol met betrekking tot de content vervult.[19] Wel houdt de beoogde normstelling een beperking in van de vrijheid van ondernemerschap zoals bedoeld in artikel 16 Handvest EU.[20]

2.8. Op deze plaats maken wij volledigheidshalve nog een opmerking over het van toepassing zijn van (bepaalde grondrechten uit) het Handvest EU in relatie tot de beoogde normstelling. De bepalingen uit het Handvest zijn uitsluitend tot de Lidstaten gericht voor zover zij het recht van de Unie ten uitvoer brengen.[21] Hoewel daar enige twijfel over mogelijk is, gaan wij er in het kader van dit rapport van uit dat in verband met de beoogde normstelling betekenis toekomt aan het Handvest EU. Daarbij hebben wij ten eerste betrokken dat de rechtspraak van het HvJ EU over de vraag wanneer een nationale regeling (nog) onder de werkingssfeer van het Unierecht valt, nog niet volledig uitgekristalliseerd is.[22] Bovendien bestaat er voor wat betreft de verwijdering van webpagina's die KP bevatten en verspreiden en die op het grondgebied van de Lidstaat worden gehost, op grond van de Richtlijn 2011/92/EU een verplichting om de nodige maatregelen te nemen om die websites onverwijld te verwijderen. Gesteld kan dan ook worden dat met de beoogde normstelling (mede) Unierecht ten uitvoer wordt gebracht. De Europese Commissie gaat er – tot slot – in de recente 'aanbeveling over maatregelen om illegale online-inhoud effectief te bestrijden' [23]van uit dat bij het treffen van dergelijke maatregelen de grondrechten uit het Handvest EU in acht dienen te worden genomen.[24]

*Voorwaarden om de beperkingen van de aan de orde zijnde grondrechten te kunnen rechtvaardigen*

2.9. Kort en goed zal de beoogde normstelling met name een inbreuk opleveren van de vrijheid van meningsuiting (voor de dader en – onder omstandigheden – de internetgebruiker) en de vrijheid van ondernemerschap (voor het ICT-bedrijf). De betreffende grondrechten gelden evenwel niet absoluut. Onder geclausuleerde omstandigheden is het gerechtvaardigd beperkingen aan te brengen.

2.10. Van belang is overigens te beseffen dat de hiervoor genoemde grondrechten bij het opleggen van een maatregel strekkende tot het verwijderen of ontoeganke-

[19] EHRM 16 juni 2015 (Delfi as v Estland), 64569/09.

[20] Zie ook: HvJ EU 27-03-2014, ECLI:NL:XX:2014:132, m.nt. S. Kulk (UPC Telekabel Wien/Constantin).

[21] Artikel 51, eerste lid, Handvest EU.

[22] Illustratief in dat verband is de conclusie van AG Bobek in de Ispas-zaak 7 september 2017, C-298/16.

[23] Aanbeveling (EU) 2018/334 van de Commissie d.d. 1 maart 2018.

[24] Considerans, overweging 13.

lijk maken van een KP-website gelijktijdig in het geding zijn. Dat betekent dat het juiste evenwicht moet worden gevonden tussen enerzijds het belang van bescherming van de (potentiële) slachtoffers van KP enerzijds en de vrijheid van meningsuiting (van internetgebruikers en daders) en de vrijheid van ondernemerschap (van ICT-bedrijven) anderzijds.[25]

*Beperkingen vrijheid van meningsuiting*

2.11. Voor zover het gaat om de vrijheid van meningsuiting als bedoeld in artikel 10 EVRM is het aanbrengen van beperkingen gerechtvaardigd indien de beperking bij wet is voorzien en in een democratische samenleving noodzakelijk (proportioneel en subsidiair) is in het belang van onder meer het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid en de goede zeden, de bescherming van de goede naam of de rechten van anderen of om de verspreiding van vertrouwelijke mededelingen te voorkomen.

2.12. De commissie modernisering opsporingsonderzoek in het digitale tijdperk heeft er in een recent rapport op gewezen dat EHRM-rechtspraak beperkt bruikbaar zou zijn om te dienen als normatief kader voor de toekomstige regeling van opsporingsbevoegdheden. De commissie noemt daar twee redenen voor. Ten eerste het sterk casuïstische karakter van de uitspraken van het EHRM, in die zin dat het oordeel of er sprake is van een inbreuk afhangt van alle specifieke feiten en omstandigheden van het geval, met inachtneming van de nationale context en het hele stelsel van waarborgen in de nationale wetgeving. Ten tweede de omstandigheid dat uitspraken van het EHRM met betrekking tot digitale opsporingsbevoegdheden (gelet op de lange doorlooptijd van de nationale procedure en de procedure ten overstaan van het Hof) doorgaans betrekking hebben op activiteiten die een jaar of vijf voor de uitspraak plaatsvinden.[26] In het verlengde van de bevindingen van de commissie hebben wij er voor gekozen om ons bij het beantwoorden van de vraag onder welke voorwaarden een inbreuk op de vrijheid van meningsuiting door middel van de beoogde KP-wetgeving is toegestaan primair te baseren op algemene uitgangspunten in plaats van aansluiting te zoeken bij een of meer specifieke uitspraken van het EHRM.

2.13. Voor wat betreft de algemene uitgangspunten achten wij in het bijzonder de zogenoemde 'concurring opinion' van rechter Pinto de Albuquerque in de zaak Yil-

[25] Zie voor deze benadering (in een IE-context): HvJEU 27 maart 2014, C-314/12, ECLI:EU:C:2014:192, *RvdW* 2014/744, *IER* 2014/45 m.nt. S. Kulk, *EHRC* 2014/138 m.nt. C. Mak, JHG 2015/41 m.nt. S.A. de Vries (*Telekabel Wien*).

[26] Commissie modernisering opsporingsonderzoek in het digitale tijdperk, Regulering van opsporingsbevoegdheden in een digitale omgeving, s.l. 2018, p. 33-35.

dirim/Turkije[27] van belang. In deze concurring opinion heeft de betreffende rechter een aantal minimumcriteria geformuleerd waaraan wetgeving omtrent het ontoegankelijk maken van delen van het internet zou moeten voldoen om "EVRM-proof" te zijn. De criteria zijn gebaseerd op een analyse van relevante internationaalrechtelijke documenten.[28] In de opinion worden de volgende 11 criteria genoemd, waarbij het van belang is er op te wijzen dat de criteria primair betrekking hebben op het ontoegankelijk maken van een website en niet op de verwijdering daarvan:

(a) Een definitie van de categorieën (rechts)personen waarop de maatregelen betrekking kunnen hebben;
(b) Een omschrijving van de mogelijk te treffen maatregelen strekkende tot het ontoegankelijk maken van delen van het internet (bijvoorbeeld het blokkeren van volledige websites of van IP-adressen);
(c) Een bepaling van de territoriale reikwijdte van de maatregelen;
(d) Een limitering van de duur van de maatregel[29];
(e) Een indicatie van de belangen die de maatregel rechtvaardigt;
(f) Inachtneming van het proportionaliteitsvereiste (een fair balance tussen de belangen die de maatregelen rechtvaardigen en het effect van de maatregel op de vrijheid van meningsuiting);
(g) Voldoen aan het noodzakelijkheidsvereiste (is de maatregel noodzakelijk om het beoogde doel te bereiken en gaat de maatregel niet verder dan strikt noodzakelijk);
(h) Benoemen van de autoriteiten die bevoegd zijn om de maatregel op te leggen;
(i) Een procedure die moet worden gevolgd bij het opleggen van een maatregel en die mede een beoordeling omvat door de bevoegde autoriteit van een verzoek tot het treffen van de maatregel en – voor zover de aan de orde zijnde belangen zich daar niet tegen verzetten – het verkrijgen van een zienswijze van de door de maatregel getroffen personen;
(j) Bekendmaking van de maatregel (en de gronden daarvoor) aan de personen die daardoor worden geraakt en
(k) Een juridische beroepsprocedure tegen de maatregel.

2.14. Artikel 7 Grondwet voorziet in de mogelijkheid om repressieve beperkingen op de vrijheid van meningsuiting aan te brengen, maar stelt dienaangaande geen inhoudelijke eisen. Wel geldt – voor zover het gaat om het kernrecht van open-

[27] EHRM 18 december 2012, 3111/10.

[28] Welke documenten naar ons oordeel nog steeds relevantie hebben.

[29] Omdat de beoogde normering tot doel heeft te komen tot definitieve verwijdering respectievelijk ontoegankelijk maken, blijft deze voorwaarde in onze rapportage verder buiten beschouwing.

baren van gedachten en gevoelens – de eis dat de beperkingen bij wet in formele zin geregeld dienen te worden.

*Beperkingen vrijheid van ondernemerschap*

2.15. Het grondrecht van vrijheid van ondernemerschap dient eveneens in de te maken afwegingen te worden betrokken. Dit grondrecht omvat met name het recht voor elke onderneming om, binnen de grenzen van de aansprakelijkheid voor eigen handelingen, vrij te beschikken over de haar ten dienste staande economische, technische en financiële middelen.[30] Aan dat grondrecht komt wat ons betreft in het kader van de beoogde normering meer gewicht toe omdat de betreffende internetbedrijven (doorgaans) niet verwijtbaar hebben gehandeld met betrekking tot de inhoud van de illegale content.

2.16. De in het Handvest EU gewaarborgde vrijheid van ondernemerschap is niet onbegrensd en laat aan de overheid de ruimte om in het algemeen belang beperkingen aan een economische activiteit te stellen. Het stellen van dergelijke beperkingen is mogelijk indien deze bij wet zijn gesteld, geen afbreuk doen aan de wezenlijke inhoud van de vrijheid van ondernemerschap en met inachtneming van het evenredigheidsbeginsel noodzakelijk zijn en daadwerkelijk beantwoorden aan de door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen.[31] Uit de rechtspraak van het HvJEU blijkt dat er bij maatregelen ter bestrijding van illegale content sprake is van een botsing van verschillende grondrechten (in IE-zaken bijvoorbeeld het recht op eigendom, de vrijheid van meningsuiting en de vrijheid van ondernemerschap). Uit de rechtspraak volgt dat van geval tot geval een evenwicht tussen de aan de orde zijnde grondrechten gevonden zal moeten worden. [32]

2.17. De vrijheid van ondernemerschap in relatie tot maatregelen om websites ontoegankelijk te maken is in de rechtspraak van het HvJ EU en de Hoge Raad vooral aan de orde geweest in relatie tot maatregelen ter bestrijding van IE-inbreuken. Toegespitst op voornoemde IE-zaken is volgens het HvJ EU het vereiste evenwicht bereikt indien aan de volgende drie voorwaarden wordt voldaan[33]:

(a) De dienstverrichter moet de technische maatregelen kunnen kiezen om

[30] Onder meer: HvJEU 30 juni 2016, C-134 / 15 (Lidl).

[31] HvJEU 22 januari 2013, C-283/11 (Sky Österreich).

[32] HvJEU 27 maart 2014, C-314/12, ECLI:EU:C:2014:192, *RvdW* 2014/744, *IER* 2014/45 m.nt. S. Kulk, *EHRC* 2014/138 m.nt. C. Mak, JHG 2015/41 m.nt. S.A. de Vries (*Telekabel Wien*).

[33] Zie ook: conclusie AG Van Peursem d.d. 16 maart 2018, ECLI:NL:PHR:2018:202, 7.6 – 7.9.

aan de maatregel te kunnen voldoen en de vrijheid hebben om niet aan de maatregel te hoeven voldoen indien kan worden aangetoond dat hij reeds zelf alle redelijkerwijs te treffen maatregelen heeft genomen (waarmee is verzekerd dat de vrijheid van ondernemerschap niet in de kern wordt aangetast);

(b) De door de dienstverrichter getroffen maatregelen moeten de internetgebruikers niet nodeloos de mogelijkheid ontnemen om op een rechtmatige wijze toegang tot informatie te verkrijgen en

(c) De maatregel moet tot doel hebben de inbreuk op auteursrechten te beëindigen en te voorkomen en redelijkerwijs doeltreffend zijn om dat doel te bereiken.

**Stap 1b: voorwaarden om aan (de overige) bepalingen uit het Unierecht te voldoen**

2.18. Ten eerste is van belang de Richtlijn kindermisbruik. Artikel 25 lid 1 van die richtlijn schrijft voor dat Lidstaten maatregelen nemen om onverwijlde verwijdering te bewerkstelligen van websites die KP bevatten of verspreiden en die op hun grondgebied worden gehost. Tevens moeten maatregelen worden genomen om de verwijdering van websites die niet vanaf hun grondgebied worden gehost verwijderd te krijgen. Op grond van artikel 25 lid 2 van de Richtlijn Kindermisbruik kunnen Lidstaten tevens maatregelen nemen om ervoor te zorgen dat websites worden geblokkeerd voor internetgebruikers op hun grondgebied. Dergelijke maatregelen moeten via een transparante procedure worden vastgesteld en voldoende waarborgen bieden, met name om er zeker van te zijn dat de beperking niet verder gaat dan nodig/proportioneel is, dat gebruikers worden geïnformeerd over de reden van deze beperking en dat is voorzien in de mogelijkheid van een rechtsmiddel. Zien wij het goed dan schrijft – afgaande op de tekst en de considerans daarvan – de Richtlijn kindermisbruik de bovenstaande waarborgen overigens niet voor met betrekking tot maatregelen die voorzien in verwijdering van KP.

2.19. Ten tweede is de Richtlijn 2000/31/EG inzake elektronische handel (hierna: Richtlijn elektronische handel) van belang. Voor zover hier van belang regelt de betreffende richtlijn dat de Lidstaten ervoor dienen te zorgen dat een dienstverlener die bepaalde specifieke diensten van een informatiemaatschappij aanbiedt niet aansprakelijk kan worden gehouden, mits aan een aantal in de richtlijn geformuleerde voorwaarden wordt voldaan. Deze bepalingen laten echter steeds onverlet de mogelijkheid voor een rechtbank of een administratieve autoriteit om te eisen dat de dienstverlener een inbreuk beëindigt of voorkomt.[34] De

[34] Artikel 12-14 Richtlijn 2000/31/EG

Richtlijn elektronische handel bevat voorts een verbod voor de Lidstaten om aan de dienstverleners een algemene verplichting op te leggen om toe te zien op de informatie die zij doorgeven of opslaan of om actief te zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.[35] In beginsel is het op grond van de richtlijn verboden om de diensten van een informatiemaatschappij die vanuit een andere lidstaat worden verricht te beperken. De richtlijn voorziet evenwel in mogelijkheden om daarvan af te wijken en bijvoorbeeld in het kader van de handhaving van de openbare orde (waar de bestrijding van online KP onder valt[36]) maatregelen te treffen. Voorwaarden voor het treffen van dergelijke maatregelen zijn wel dat enerzijds de maatregelen evenredig moeten zijn om de beoogde doelstelling te bereiken en anderzijds de betrokken Lidstaat (in beginsel) zelf moet zijn verzocht maatregelen te treffen.

**Stap 1b: praktisch werkbaar**

2.20. In deze paragraaf brengen we de voorwaarden in beeld die van belang zijn om ervoor te zorgen dat de beoogde normstelling ook praktisch werkbaar is. In grote lijnen verstaan wij daaronder normstelling die in voldoende mate beantwoordt aan de relevante beleidsdoelstellingen enerzijds en die voor de praktijk (handhavende instanties, ICT-bedrijven etc.) hanteerbaar is anderzijds.

2.21. Volgens ons moet de beoogde normstelling aan (in ieder geval) de volgende voorwaarden voldoen om praktisch werkbaar te zijn:

(a) Er moet zoveel mogelijk sprake zijn van een sluitend marktdekkend systeem waarbij voor alle economische actoren die indirect een faciliterende rol vervullen in het netwerk van online seksueel kindermisbruik eenzelfde normering geldt;
(b) Het systeem moet dienen als slot op de deur bedoeld voor die ICT-bedrijven die niet of in mindere mate meewerken met het – al dan niet met toepassing van de door de sector zelf vastgestelde Notice and take-down procedure – op melding van (in de huidige situatie) de politie of het EOKM verwijderen van KP.[37] Gelet op de belangrijke rol die andere zogenoemde "betrouwbare flaggers" spelen bij het doen van meldingen van

[35] Artikel 15 lid 1.

[36] Dit leiden wij af uit artikel 3, vierde lid aanhef en onder a sub i waarin openbare orde is gepreciseerd en waaruit volgt dat onder openbare orde in ieder geval wordt verstaan: de preventie van, het onderzoek naar, de opsporing en de vervolging van strafbare feiten, waaronder de bescherming van minderjarigen en de bestrijding van het aanzetten tot haat wegens ras, geslacht, godsdienst of nationaliteit en van schendingen van de menselijke waardigheid ten aanzien van individuen.

[37] Tweede Kamer, vergaderjaar 2017-2018, 31 015, nr. 135, p. 8 en 9.

KP[38] zou tevens overwogen kunnen worden om de normstelling tevens te hanteren als slot op de deur voor het niet (voldoende) prioritair afhandelen door ICT-bedrijven van meldingen van dergelijke partijen;

(c) De normstelling dient geen afbreuk te doen aan de rol van en de samenwerking met de strafrechtelijke keten (politie en justitie), hetgeen onder meer zal moeten inhouden dat de autoriteit die om verwijdering verzoekt moet kunnen bepalen dat het betrokken ICT-bedrijf de aanbieder van de inhoud van het te verwijderen materiaal niet van de verwijdering op de hoogte stelt (zolang dit noodzakelijk is in het kader van het onderzoek naar strafbare feiten)[39] respectievelijk dat zij het maken van een kopie dienen toe te staan;

(d) De normstelling dient ten minste betrekking te hebben op HSP's, gelet op de cruciale rol die zij vervullen bij de bestrijding van illegale online-inhoud[40];

(e) De normstelling dient te onderkennen dat verwijdering van KP doeltreffender is dan blokkering (aangezien door blokkering de inhoud niet wordt verwijderd en blokkeringen omzeild kunnen worden);

(f) De normstelling dient te voorzien in (de bepaling van) een termijn omtrent het ontoegankelijk maken van KP die enerzijds beantwoordt aan het belang van een zo snel mogelijke verwijdering en anderzijds – gelet onder meer op de huidige stand van de techniek – geen onevenredige inspanningen van de betrokken ICT-bedrijven vergt en

(g) De normstelling dient, waar mogelijk, aansluiting te zoeken bij de reeds door de branche vastgestelde 'Gedragscode Notice-and-take-down' (zie ook aanwijzing 2.5 van de Aanwijzingen voor de regelgeving).

**Stap 2: een voorstel voor normstelling die voldoet aan de geformuleerde voorwaarden**

Inleiding

*Keuze voor een smal of een breed spoor?*

2.22. Een eerste keuze die moet worden gemaakt betreft de wijze van normeren. Wij onderscheiden daarbij een smal en een breed spoor. Het smalle spoor gaat ervan uit dat de maatregelen die de ICT-bedrijven zelf hebben genomen (onder meer de Notice-and-take-down procedure) in principe afdoende functioneren,

[38] Aanbeveling (EU) 2018/334 van de Commissie d.d. 1 maart 2018, Publicatieblad L63/50, overweging 29.

[39] Tweede Kamer, vergaderjaar 2017-2018, 31 015, nr. 135, p. 9 en Aanbeveling (EU) 2018/334 van de Commissie d.d. 1 maart 2018, Publicatieblad L63/50, overweging 21.

[40] Aanbeveling (EU) 2018/334 van de Commissie d.d. 1 maart 2018, Publicatieblad L63/50, overweging 15.

maar dat *aanvullend* een slot op de deur noodzakelijk is voor het geval bepaalde bedrijven onvoldoende doen om KP-content te verwijderen of ontoegankelijk te maken. Binnen het smalle spoor voorzien wij de introductie van een norm die inhoudt dat ICT-bedrijven door middel van een aanwijzing verplicht kunnen worden om bepaalde KP-content te verwijderen of in voorkomend geval anderszins ontoegankelijk te maken. Indien de betreffende aanwijzing niet wordt opgevolgd levert dat een overtreding op naar aanleiding waarvan bestuurlijke sancties opgelegd kunnen worden. Het brede spoor neemt tot uitgangspunt dat de zelfregulering omtrent de aanpak van KP-content op dit moment onvoldoende functioneert en dat publiekrechtelijke normering noodzakelijk is om alsnog tot de vereiste inzet van ICT-bedrijven te komen. Binnen het brede spoor zou meer specifiek gekozen kunnen worden voor de introductie van verschillende zorgplichten voor ICT-bedrijven, zoals een zorgplicht om te voorzien in een adequate maatregelen om de verspreiding van KP-content zoveel mogelijk te voorkomen.[41]

2.23. Wij kunnen ons bij de huidige stand van zaken voorstellen dat in eerste instantie voor het smalle spoor wordt gekozen. In de brief van de minister aan de Tweede Kamer d.d. 7 februari 2018 inzake de aanpak van kindermishandeling wordt opgemerkt dat het overgrote deel van de ICT-bedrijven KP-content actief verwijdert nadat een melding van de politie of het EOKM is ontvangen, maar dat een slot op de deur mist voor een kleine groep ICT-bedrijven die niet (of verminderd) meewerken. Bij die stand van zaken lijkt het introduceren van een bredere normstelling om de verwijdering van KP-content sector-breed te reguleren op dit moment niet zonder meer opportuun. Wij wijzen er echter wel op dat dit anders zou kunnen komen te liggen indien uit het onderzoek van de TU Delft zou blijken dat de Notice-and-Take down-procedure onvoldoende werkt of dat anderszins blijkt dat ICT-bedrijven zich minder goed inspannen om KP (snel) verwijderd te krijgen. Indien er overigens uiteindelijk een bredere normstelling zou worden overwogen, is het van belang dat daarbij de grenzen die uit de Richtlijn elektronische handel volgen in acht worden genomen. Een zorgplicht kan bijvoorbeeld op grond van die richtlijn niet zover gaan dat er op het ICT-bedrijf in feite een verplichting komt te rusten die feitelijk neerkomt op het actief zoeken naar feiten of omstandigheden die op onwettige activiteiten duiden.[42]

2.24. In het navolgende zullen wij ons verder beperken tot het smalle spoor en ons richten op normering die is gericht op de introductie van een aanwijzingsbevoegdheid op grond waarvan ICT-bedrijven verplicht kunnen worden om KP te verwijderen (/ontoegankelijk te maken).

[41] Vergelijk artikel 3 van het concept van de Terrorismeverordening.

[42] Artikel 15 lid 1 van de Richtlijn elektronische handel.

*Recente voorstellen tot normering van het ontoegankelijk maken van illegale content*

2.25. In het navolgende zullen wij een voorstel (op hoofdlijnen) doen voor een normstelling die aan de hiervoor geformuleerde voorwaarden voldoet. Waar mogelijk hebben we daarbij geprobeerd om aansluiting te zoeken bij twee recente voorstellen voor regelgeving die eveneens – zij het in een andere context – strekken tot het ontoegankelijk maken van bepaalde illegale onlinecontent. Enerzijds gaat het om een voorstel tot wijziging van de Wet op de kansspelen (hierna: Wok) om een bindende aanwijzing te kunnen geven aan bepaalde ICT-bedrijven om internetverkeer te blokkeren dat wordt gebruikt voor het organiseren van illegale kansspelen.[43] Anderzijds gaat het om een voorstel van de Europese Commissie voor een Verordening voor de aanpak van illegale terroristische content.[44] Hierna worden eerst deze beide voorstellen kort besproken. Daarna bespreken we de onderwerpen die in het kader van de beoogde normstelling nadere invulling behoeven en de keuzes die dienaangaande gemaakt zouden moeten worden.

2.26. De voorgestelde normstelling in het kader van de Wok komt in het kort op het volgende neer. De Kansspelautoriteit wordt de bevoegdheid toegekend om een bindende aanwijzing te geven aan onder meer degene die illegale kansspelen bevordert of daartoe de middelen verschaft. Een dergelijke aanwijzing kan onder meer inhouden dat een aanbieder van een openbare elektronische communicatiedienst wordt verplicht om bepaalde gegevens ontoegankelijk te maken voor zover dit nodig is voor de beëindiging of het voorkomen van bepaalde overtredingen van de Wok. Onder het ontoegankelijk maken wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van een geautomatiseerd werk of derden verder kennis kunnen nemen van de betreffende gegevens, waaronder begrepen het verwijderen van die gegevens. Onder het ontoegankelijk maken als bedoeld in een dergelijke aanwijzing wordt uitdrukkelijk niet het verstoren van het internetverkeer verstaan. Alvorens een aanwijzing kan worden gegeven behoeft de Kansspelautoriteit de toestemming van de rechtercommissaris. Degene die een aanwijzing krijgt is – tot slot – gehouden dienovereenkomstig te handelen. Het negeren van een aanwijzing houdt een overtreding in waartegen door de Kansspelautoriteit handhavend opgetreden kan worden.

[43] Eerste Kamer 2015-2016, 33 996, A, artikel 34n.

[44] COM(2018) 640 final.

2.27. De voorgestelde normstelling in de beoogde Terrorismeverordening ziet er – voor zover hier van belang – op grote lijnen als volgt uit. Op hostingproviders komt een zorgplicht te rusten die inhoudt dat zij de redelijkerwijs noodzakelijke maatregelen dienen te treffen om – met inachtneming van de aan de orde zijnde fundamentele rechten van de gebruikers van hun diensten – de verspreiding van terroristische content zoveel mogelijk te voorkomen en hun gebruikers zoveel mogelijk te beschermen tegen dergelijke content. Verder voorziet de voorgestelde verordening in de bevoegdheid voor de autoriteiten om een verwijderingsbevel uit te vaardigen om de hostingprovider te verplichten om de terroristische content te verwijderen of ontoegankelijk te maken. De provider die een dergelijk bevel krijgt heeft de verplichting om daar binnen een uur aan te voldoen. De verordening schrijft een aantal elementen voor die verplicht in een dergelijk bevel opgenomen dienen te worden, waaronder een omschrijving van de reden voor het bevel en informatie om de provider in staat te stellen de betreffende content te kunnen identificeren. Op verzoek van de betrokken providers zijn de bevoegde autoriteiten verplicht om het bevel nader te onderbouwen. De Verordening voorziet voorts in specifieke bekendmakingsregels die moeten bevorderen dat de betreffende providers prompt kennis kunnen nemen van het betreffende bevel. Tot slot voorziet de verordening in de mogelijkheden voor providers om naar aanleiding van een bevel te kunnen melden dat vanwege evidente redenen (zoals overmacht of een kennelijke onjuistheid in een bevel) niet aan het gegeven bevel kan worden voldaan.

2.28. In het navolgende bezien we op basis van de verschillende hiervoor geformuleerde voorwaarden voor een normstelling die juridisch haalbaar en praktisch werkbaar is wat de contouren van de toekomstige normstelling zou kunnen zijn en welke keuzes in dat verband gemaakt moeten worden.

<u>In het kader van de normstelling te maken keuzes</u>

*1) Categorieën van (rechts)personen waarop de maatregelen betrekking kunnen hebben*

2.29. Er dient een keuze gemaakt te worden tussen een ruimere of smallere groep (rechts)personen die met een maatregel geconfronteerd kunnen worden. De voorgestelde regeling in de Wok maakt het mogelijk een aanwijzing te geven aan aanbieders van openbare communicatiediensten in het algemeen en is daarom ruimer dan de voorgestelde verordening waarin het verwijderingsbevel uitsluitend aan hostingproviders gericht kan worden. Uit openbare bron blijkt dat in ieder geval hostingproviders een cruciale (indirecte) rol spelen bij de verspreiding (en dus ook bij de voorkoming daarvan) van KP. In Nederland gevestigde HSP's dienen naar ons oordeel dan ook in ieder geval onder de normstel-

ling te vallen. Het introduceren van een norm die zich uitsluitend tot HSP's richt is, denken wij, echter te beperkt om het doel van de normering (lees: het zoveel mogelijk verwijderen van KP van het Nederlandse deel van het internet) in voldoende mate te verwezenlijken. In dat verband is onder meer van belang dat veel HSP's niet in Nederland zijn gevestigd. In ieder geval moet het in dat geval ook mogelijk zijn om aan een ISP een maatregel op te leggen. Wij hebben er geen inzicht in of en in hoeverre ook andere ICT-bedrijven een (belangrijke) rol spelen bij de verspreiding van KP en daarom in de normstelling betrokken zouden moeten worden. Indien en voor zover ook dergelijke bedrijven aantoonbaar een belangrijke rol kunnen vervullen bij de verspreiding van KP kunnen wij ons voorstellen dat voor een ruimere regeling wordt gekozen, bijvoorbeeld in lijn met de voorgestelde regeling uit de Wok. Indien de bijdrage van anderen dan HSP's en ISP's beperkt is kunnen wij ons – mede in aanmerking nemend het proportionaliteitsbeginsel en de vrijheid van ondernemerschap – voorstellen dat een regeling (in eerste instantie) wordt beperkt tot HSP's en ISP's. Mogelijk zou overigens nog een tussenvariant kunnen worden gekozen waarbij in de wettelijke regeling wordt bepaald dat een aanwijzing in ieder geval gegeven kan worden aan HSP's en ISP's, alsmede aan daartoe bij algemene maatregel van bestuur aan te wijzen andere categorieën van aanbieders van openbare elektronische communicatiediensten. In het kader van de uiteindelijke normstelling is een specifiek punt van aandacht de definiëring van de categorieën ICT-bedrijven die onder de norm komen te vallen. Denk daarbij aan voldoende duidelijke definities van wat in het kader van de normstelling onder een HSP of ISP wordt verstaan.

*2) Beschrijving van de (categorieën van) te nemen maatregelen*

2.30. De (mogelijk) door de betreffende ICT-bedrijven te nemen maatregelen dienen in het kader van de normstelling te worden omschreven. Hierbij zal een keuze gemaakt moeten worden met betrekking tot de mate van vrijheid die nog aan ICT-bedrijven wordt gelaten om het met de aanwijzing beoogde doel te bereiken.

2.31. Een eerste keuze die moet worden gemaakt is of de aanwijzing voor de betrokken ICT-bedrijven een resultaats- dan wel inspanningsverplichting moet inhouden. In het eerste geval is het bedrijf gehouden om de verwijdering (of in voorkomend geval: het ontoegankelijk maken) van de KP-content te bewerkstelligen, waarbij aan het bedrijf een sanctie kan worden opgelegd indien dat niet lukt. In het tweede geval houdt de aanwijzing in dat alle maatregelen dienen te worden genomen die redelijkerwijs van het ICT-bedrijf gevergd kunnen worden om de KP-content te verwijderen respectievelijk ontoegankelijk te maken.

2.32. Zowel de Wok als de Terrorismeverordening gaan in feite uit van een resultaatsverplichting.[45] Wij zien geen redenen om daar in de beoogde normstelling niet tevens van uit te gaan. Wij wijzen er daarbij ten eerste op dat wat ons betreft de Richtlijn elektronische handel niet aan het opleggen van een resultaatsverplichting in de weg staat. In de richtlijn is benadrukt dat de daarin opgenomen vrijwaringsregelingen geen afbreuk doen aan de bevoegdheid van de Lidstaten om dienstverleners te verplichten bepaalde inbreuken te beëindigen[46] (waaronder expliciet ook de verplichting tot verwijdering wordt verstaan[47]). Ook het arrest van het HvJEU inzake Telekabel/Wien biedt ruimte voor het opleggen van een resultaatsverplichting. In dat arrest (dat overigens in een IE-context is gewezen) is overwogen dat een aanbieder aan zijn aansprakelijkheid moet kunnen ontkomen door aan te tonen dat hij alle redelijkerwijs van hem te vergen maatregelen heeft getroffen. Uit het arrest blijkt dat dit betekent dat een ICT-bedrijf de oplegging van een sanctie moet kunnen voorkomen in verband met het niet voldoen aan het gegeven bevel indien hij kan aantonen alle redelijkerwijs van hem te verlangen maatregelen te hebben getroffen. Het bevel zelf mag echter wel in een resultaatsverplichting voorzien. Wij menen dan ook dat het mogelijk is om een aanwijzing te geven die voor het ICT-bedrijf voorziet in een resultaatsverplichting om de KP-content te verwijderen/ontoegankelijk te maken. Wel menen wij dat bij het niet bereiken van een resultaat van het opleggen van een sanctie zou moeten kunnen worden afgezien indien het ICT-bedrijf aannemelijk kan maken dat hij alle maatregelen heeft genomen die redelijkerwijs van hem gevergd kunnen worden (maar dit zonder succes is gebleven).

2.33. Een tweede keuze die moet worden gemaakt is of aan de ICT-bedrijven zelf de vrijheid wordt gelaten om te kiezen welke maatregelen zij treffen om de content ontoegankelijk te maken (waarbij verwijdering een van de opties is) of dat het mogelijk moet zijn om een ICT-bedrijf te verplichten om de KP-content te verwijderen (en dat dus niet met een andere vorm van ontoegankelijk maken kan worden volstaan).

2.34. Voorop moet worden gesteld dat het bestuursorgaan in ieder geval bevoegd moet zijn om niet alleen een aanwijzing te geven om content te verwijderen maar ook om een ICT-bedrijf te verplichten de content anderszins ontoegankelijk te maken. Er zijn immers situaties denkbaar waarin – bijvoorbeeld vanwege

[45] De Terrorismeverordening voorziet in een verplichting om indien een verwijderingsbevel wordt gegeven tot verwijdering c.q. het ontoegankelijk maken van de content over te gaan (artikel 4 lid 2), zij het dat de HSP's geclausuleerde mogelijkheden hebben om de autoriteiten erop te wijzen dat als gevolg van overmacht niet aan het bevel kan worden voldaan.

[46] Artikel 12-14 van de Richtlijn elektronische handel.

[47] Considerans punt 45 van de Richtlijn elektronische handel.

het niet fysiek aanwezig zijn van de server in Nederland – verwijdering niet mogelijk is. In dergelijke gevallen moet op andere vormen van het ontoegankelijk maken van content kunnen worden teruggevallen.

2.35. Het verplicht voorschrijven van verwijdering van de content draagt het beste bij aan de effectieve aanpak van KP en sluit bovendien aan bij de gedragscode van de branche die ook van verwijdering uitgaat. De Richtlijn kindermisbruik verplicht de Lidstaten bovendien om maatregelen te treffen om de verwijdering van KP-websites die op hun grondgebied gehost worden te verwijderen.

Wij menen dat het niet alleen wenselijk is om een ICT-bedrijf er specifiek toe te verplichten de KP-content te verwijderen, maar dat het juridisch ook mogelijk is om een dergelijke aanwijzing te geven. Ter toelichting het volgende. In het hiervoor meermaals aangehaalde *Telekabel Wien-arrest* is geoordeeld dat de betreffende blokkeringsmaatregel niet in strijd was met de vrijheid van ondernemerschap mede omdat de ondernemer vrij was om zelf de maatregelen te bepalen waarmee aan het bevel tot het ontoegankelijk maken zou worden voldaan. Bovendien is in dat arrest geoordeeld dat het ook in overeenstemming kan zijn met het evenredigheidsbeginsel indien de getroffen maatregelen de toegang niet verhinderen, maar slechts bemoeilijken. Wij menen dat het arrest er echter niet aan in de weg staat dat aan een ICT-bedrijf de verplichting wordt opgelegd om KP-content te verwijderen. In dat verband is ten eerste van belang dat het evenredigheidsbeginsel vergt dat een bepaalde maatregel niet verder gaat dan geschikt en noodzakelijk voor de verwezenlijking van de legitieme doelstellingen die met de betrokken regeling worden nagestreefd. Duidelijk is dat in voorkomend geval verwijdering veel effectiever is om KP-content van het openbare internet te laten verdwijnen dan het op een andere manier ontoegankelijk maken van die content. In zoverre kan gesteld worden dat – indien mogelijk – verwijdering het meest geschikt en noodzakelijk is om de met de normstelling nagestreefde doelen te kunnen bereiken. Daar komt bij dat het illegale karakter van (het plaatsen en raadplegen van) KP-content van een andere orde is dan het plaatsen of raadplegen van (bijvoorbeeld) films ten aanzien waarvan bepaalde partijen IE-rechten kunnen doen gelden en waarbij het bevel ertoe strekt verdere IE-inbreuken te voorkomen. Ons is verder niet gebleken dat verwijdering van KP-content voor de ICT-bedrijven tot onaanvaardbare offers leidt om welke reden het toch aan die bedrijven zou moeten worden gelaten om zelf de modaliteit van het ontoegankelijk maken van de content te bepalen. In dat verband herhalen wij dat de sector in de Notice-and-take down-procedure zelf voor verwijdering heeft gekozen en dit dus kennelijk zelf als een bedrijfseconomisch haalbare maatregel beschouwt.

2.36. Overigens is een nadeel van het verplicht verwijderen (derhalve met uitsluiting van andere vormen van ontoegankelijk maken) van content dat daarmee wordt afgeweken van andere (voorstellen tot) regelingen die voorzien in het ontoegankelijk maken van illegale content. Zowel het voorstel tot wijziging van de Wok als het voorstel voor de Terrorismeverordening[48] laten het aan de beoordeling van het ICT-bedrijf om te bepalen of voor verwijdering of (een andere vorm van) het ontoegankelijk maken wordt gekozen. Hetzelfde geldt voor het strafrechtelijke bevel als bedoeld in artikel 54a Sr dat zich eveneens richt op het ontoegankelijk maken, zonder daarbij het bedrijf tot verwijdering te verplichten. Uit een oogpunt van consistentie zou derhalve kunnen worden overwogen om ook in dit geval aan het ICT-bedrijf de vrijheid te laten om zelf de wijze van het ontoegankelijk maken te bepalen. In ieder geval menen wij dat het aanbeveling verdient om indien er voor verplichte verwijdering wordt gekozen (wat wij ons overigens kunnen voorstellen) in de memorie van toelichting wordt gemotiveerd waarom dienaangaande wordt afgeweken van de hiervoor genoemde (voorstellen voor) regelgeving.

*3) Invulling van het proportionaliteits- en subsidiariteitsbeginsel*

2.37. Bij de voorgestelde regeling in de Wok is beoogd invulling te geven aan het proportionaliteits- en subsidiariteitsbeginsel door (onder meer) i) de aanwijzingsbevoegdheid vorm te geven als een discretionaire bevoegdheid, ii) in de wettelijke regeling voldoende ruimte voor het bieden van maatwerk in het individuele geval te laten (bijvoorbeeld door te bepalen dat in de aanwijzing zelf een redelijke termijn dient te worden opgenomen waarbinnen aan de aanwijzing moet worden voldaan) en iii) door de aanwijzing vorm te geven als een Awb-besluit (met als gevolg de toepasselijkheid van de algemene beginselen van behoorlijk bestuur en de in de Awb voorgeschreven procedures). In algemene zin menen wij dat dit een adequate manier is om te (kunnen) borgen dat de maatregel in het individuele geval steeds aan de vereisten van proportionaliteit en subsidiariteit voldoet.

2.38. Het systeem zoals voorgesteld in de concept Terrorismeverordening is in vergelijking met het voorgestelde systeem uit de Wok meer rigide. De verschillen bestaan er ten opzichte van de Wok-regeling met name uit dat wordt gewerkt met een zeer korte en bovendien gefixeerde termijn voor het ontoegankelijk maken (maximaal 1 uur), terwijl op onder meer het punt van de bekendmaking lijkt te worden voorzien in (deels) van de Awb afwijkende regels. De zeer korte termijn van 1 uur is gekozen in verband met de gebleken zeer hoge verspreidingssnelheid van terroristische content.

[48] Vergelijk considerans, overweging 13.

2.39. Het is uiteindelijk aan de wetgever om een keuze te maken over de precieze vormgeving van het aanwijzingssysteem. Wij kunnen ons daarbij voorstellen dat de keuze die gemaakt wordt ter waarborging van het proportionaliteits- en subsidiariteitsbeginsel uiteindelijk het midden houdt tussen het Wok-systeem en het systeem uit de voorgestelde Terrorismeverordening. Daarmee zou enerzijds worden onderkend dat de adequate aanpak van KP op sommige punten een meer voortvarende aanpak vergt dan de aanpak van – kort gezegd – illegale goksites. Anderzijds wordt daarmee, denken wij, tevens onderkend dat ook bij een voortvarende aanpak van KP zal moeten worden voorzien in voldoende waarborgen om ervoor te zorgen dat in het individuele geval aan (onder meer) de eisen van proportionaliteit en subsidiariteit wordt voldaan.

2.40. Meer specifiek kunnen wij ons daarbij ten eerste voorstellen dat de aanwijzingsbevoegdheid als een discretionaire bevoegdheid wordt vormgegeven ('kan'-bepaling), zodat aan het bevoegde orgaan ruimte wordt gelaten om – met inachtneming van de algemene beginselen van behoorlijk bestuur – steeds een nadere afweging te maken met betrekking tot de vraag of een aanwijzing gegeven dient te worden. Verder kunnen wij ons voorstellen dat in de normering wordt bepaald dat aan de aanwijzing binnen een gefixeerd aantal uren gevolg dient te worden gegeven, tenzij er in het aanwijzingsbesluit is voorzien in een andere termijn. De te hanteren standaardtermijn dient geschikt en noodzakelijk te zijn om de met de normstelling beoogde doelen te bereiken. Naarmate de verspreidingssnelheid van KP-content hoger is, rechtvaardigt dit een kortere termijn. Hetzelfde geldt naarmate de kans dat derden onbedoeld kennisnemen van de KP-content groter is. De duur van de (gefixeerde) termijn kan wat ons betreft overigens mede afgestemd worden op de tijd die ICT-bedrijven wordt gegund om vrijwillig aan de melding te voldoen. Naarmate die termijn langer is kan de aan de aanwijzing te verbinden termijn korter zijn (en vice versa).

2.41. Doordat de bestuursrechtelijke aanwijzing een besluit als bedoeld in de Awb inhoudt zijn daarop (ook) de relevante bepalingen uit de Awb van toepassing, inclusief de daaraan voor de ICT-bedrijven verbonden waarborgen. Wel kunnen wij ons voorstellen dat in het kader van de normering in het belang van de effectiviteit wordt bezien of er op punten aanleiding bestaat van een of meerdere bepalingen uit de Awb af te wijken. Wij kunnen ons bijvoorbeeld – gelet op het belang van een zo spoedig mogelijke verwijdering/ontoegankelijk making – voorstellen dat bij een aanwijzing in eerste instantie met een beperkte (kern)motivering kan worden volstaan (die in een later stadium nader kan worden uitgewerkt).[49] Verder kunnen wij ons voorstellen dat wordt voorzien in een

[49] Weliswaar voorziet artikel 3:47, derde lid, van de Awb in de mogelijkheid om in verband met de vereiste spoed de

specifieke (snelle) wijze van bekendmaking.[50]

*4) Vormgeving van de procedure voorafgaand aan de te geven aanwijzing/rechtsbescherming nadat de aanwijzing is gegeven*

2.42. Ook op het punt van de vormgeving van de aan de aanwijzing voorafgaande procedure constateren wij grote verschillen tussen het voorgestelde systeem in de Wok en de voorgestelde Terrorismeverordening. Het systeem in de Wok gaat ervan uit dat voorafgaand aan de aanwijzing de aanbieder om een zienswijze dient te worden gevraagd enerzijds en dat een voorafgaande machtiging van de rechter-commissaris is vereist anderzijds. De conceptverordening lijkt geen specifieke voorschriften te geven omtrent de voorbereiding van het bevel en dit in belangrijke mate aan de Lidstaten over te laten.

2.43. Het is ontegenzeggelijk zo dat het voorafgaand aan het besluit verplicht vragen van de zienswijze van de betrokkene en het voorschrijven van een voorafgaande machtiging van de rechter-commissaris belangrijke waarborgen opleveren voor de ICT-bedrijven. In die zin kunnen wij ons voorstellen dat die waarborgen een plaats krijgen in de normering. Daar staat tegenover dat de effectieve aanpak van KP is gediend met een zo spoedig mogelijke verwijdering van KP-content en dat de hiervoor genoemde waarborgen tot gevolg (zullen) hebben dat die verwijdering vertraging oploopt door te voorzien in dergelijke waarborgen.

2.44. In het kader van de vormgeving van de procedure is het verdedigingsbeginsel van belang dat een algemeen beginsel van het Unierecht vormt. Dit beginsel is van toepassing als een bepaald besluit binnen het toepassingsbereik van het Unierecht valt. Omdat gelet op de Richtlijn kindermisbruik niet is uit te sluiten dat een verwijderingsbevel binnen het toepassingsbereik van het Unierecht valt (zie hiervoor), bespreken wij in dit rapport in hoeverre het betreffende beginsel ertoe verplicht om een ICT-bedrijf voorafgaande aan de aanwijzing te horen. Het verdedigingsbeginsel omvat onder meer het recht voor eenieder om gehoord te worden voordat jegens hem een voor hem nadelige individuele maatregel wordt

---

motivering niet aanstonds bij de bekendmaking van het besluit te vermelden, maar dat artikellid lijkt ons niet de bevoegdheid te geven om structureel bij besluiten zoals hier aan de orde de motivering eerst op een later tijdstip te vermelden. Indien een dergelijke structurele afwijking is beoogd, behoeft dit een specifieke wettelijke grondslag.

[50] De Awb gaat er in haar huidige vorm vanuit dat bekendmaking van een aan één of meer geadresseerden gericht besluit (zoals de beoogde aanwijzing) dient te geschieden door uitreiking of toezending aan de geadresseerde. Toezending kan daarbij uitsluitend elektronisch geschieden indien de ontvanger voorafgaande kenbaar heeft gemaakt langs deze weg voldoende bereikbaar te zijn. Vergelijk artikel 3:41 en 2:14 Awb. Wij denken dat het noodzakelijk is om ten aanzien van de beoogde aanwijzing (en de eventueel daaropvolgende sanctiebesluiten) te bepalen dat deze steeds (op een bepaalde) elektronische wijze bekendgemaakt dienen te worden.

genomen.[51] Op grond van het verdedigingsbeginsel dient een ICT-bedrijf dus gehoord te worden voordat er aan hem een aanwijzing wordt gegeven. Op dat beginsel zijn onder omstandigheden echter uitzonderingen mogelijk, mits deze werkelijk beantwoorden aan de doeleinden van algemeen belang die met de betrokken maatregel worden nagestreefd en die, het nagestreefde doel in aanmerking nemend, het verdedigingsbeginsel niet in de kern aantasten.[52] Onder bijzondere omstandigheden is het door het HvJEU aanvaard (bijvoorbeeld in het kader van de bestrijding van mond-en-klauwzeer) dat het afdoende kan zijn indien het betrokken bedrijf uitsluitend de mogelijkheid heeft om de maatregel achteraf aan de rechter voor te leggen zonder dat de mogelijkheid is geboden om voorafgaand te worden gehoord.[53] Dergelijke uitzonderingen dienen echter wel draagkrachtig gemotiveerd te worden. Indien de wetgever meent dat de bestrijding van KP-content zich niet verdraagt met het vooraf horen van het betrokken ICT-bedrijf, zal de wetgever deze keuze derhalve goed dienen te motiveren. Wij kunnen ons daarbij voorstellen dat die motivering in voorkomend geval inhoudt dat de verwijdering van KP-content voortvarend dient te geschieden en dat het vooraf horen van het betrokken bedrijf daarbij tot onaanvaardbare vertraging zou leiden.

2.45. Overigens kunnen we ons voorstellen dat de aanwijzing vooraf wordt gegaan door een voornemen. Ten aanzien van dat voornemen kan dan worden voorzien in een beperkte zienswijzemogelijkheid, bijvoorbeeld beperkt tot de mogelijkheid om aan te geven dat als gevolg van overmacht of feitelijke onmogelijkheid[54] niet aan de voorgenomen aanwijzing kan worden voldaan en de mogelijkheid om aan te voeren dat de voorgenomen aanwijzing op een evidente fout berust. Op die manier wordt weliswaar het betrokken ICT-bedrijf niet een volledig "hoorrecht" geboden, maar beantwoordt de procedure naar onze inschatting wel aan de kern van het verdedigingsbeginsel, namelijk het hebben van de mogelijkheid om een vergissing te corrigeren of individuele omstandigheden aan te voeren die ervoor pleiten dat een bepaald besluit (niet) wordt genomen.[55] Wij menen dat het voorafgaand vragen van een zienswijze van het betrokken ICT-bedrijf eveneens een positieve bijdrage kan leveren aan het draagvlak binnen de sector voor de beoogde normstelling.

2.46. Wij menen dat het op grond van de van toepassing zijnde grondrechten niet zonder meer verplicht is te voorzien in voorafgaande rechterlijke toetsing. Wij

[51] HvJEU 3 juli 2014, C-129 / 13 (Kamino).

[52] HvJEU 3 juli 2014, C-129 / 13 (Kamino).

[53] HvJEU 15 juni 2006, C-28 / 05 (EU Dokters e.a.).

[54] Deze categorieën zijn ontleend aan het voorstel voor de Terrorismeverordening.

[55] HvJEU 21 december 2011, C-27 / 09 P (Frankrijk / People's Mojahedin Organization of Iran).

menen dat het ook op dit punt aankomt op een zorgvuldige afweging door de wetgever van enerzijds het belang dat is gediend met een snelle aanpak van KP en anderzijds het belang dat is gediend met een zorgvuldige voorbereiding van het aanwijzingsbesluit.

2.47. Wij zien het voor ons dat de aanwijzing wordt vormgegeven als een Awb-besluit waartegen rechtsbescherming bij de bestuursrechter openstaat. Omdat het aanwenden van rechtsmiddelen geen schorsende werking heeft (artikel 6:16 Awb) hoeft de bestuursrechtelijke rechtsbescherming geen afbreuk te doen aan de snelle effectuering van maatregelen tot het ontoegankelijk maken van KP.

2.48. Om de betrokken belanghebbenden daadwerkelijk een doeltreffende voorziening in rechte te bieden, is het van belang om een voorziening te treffen indien een aanwijzing wordt gegeven die strekt tot verwijdering van KP-content. In de gerechtelijke procedure dient immers getoetst te kunnen worden of de aanwijzing terecht is gegeven in welk kader ook de inhoud van de content aan de orde gesteld dient te kunnen worden. Dat betekent dat er op enigerlei wijze voorzien dient te worden in het maken van een "kopie" van de content om die in de procedure aan de orde te kunnen stellen.

Voorkomen moet zoveel mogelijk worden dat er sprake is van ketens van elkaar snel opvolgende seriële besluiten (aanwijzing, sanctie 1, sanctie 2) waarbij tegen ieder separaat besluit apart bezwaar en beroep kan worden aangetekend. Dit zou kunnen worden ondervangen door te bepalen dat het bezwaar of beroep tegen het aanwijzingsbesluit zich mede uitstrekt over de eventueel daaropvolgende sanctiebesluiten (naar analogie met bijvoorbeeld artikel 5:39 van de Awb).

5) *Overige in het kader van de normstelling te betrekken omstandigheden*

2.49. De beoogde normstelling strekt ertoe dat (bepaalde) ICT-bedrijven verplicht moeten kunnen worden om KP te verwijderen/ontoegankelijk te maken indien deze bedrijven geen, althans onvoldoende, opvolging geven aan een melding. Dit systeem zou op twee manieren kunnen worden vormgegeven.

De eerste mogelijkheid is dat de meldingen – zoals ook thans al het geval is – door de politie of het EOKM worden gedaan en dat indien die melding niet (afdoende) wordt opgevolgd er door het bevoegde bestuursorgaan een aanwijzing kan worden gegeven. Dit zou in de normstelling tot uitdrukking gebracht kunnen worden door te bepalen dat de bevoegde autoriteit een aanwijzing kan geven aan een ICT-bedrijf niet binnen een bepaalde termijn opvolging heeft gegeven aan een melding van KP van een of meerdere in de normstelling specifiek ge-

noemde melders. In het kader van de normstelling dient een keuze te worden gemaakt omtrent de partijen waarvan de wetgever vindt dat daarvan afkomstige meldingen (mits juist) opgevolgd dienen te worden door de ICT-bedrijven. In dat verband zou in ieder geval aansluiting gezocht kunnen worden bij de gedragscode van de branche waarin tot uitdrukking is gebracht dat aan meldingen van een controle- of opsporingsinstantie respectievelijk de officier van justitie extra groot gewicht toekomt. Om de aanwijzingsbevoegdheid effectief te laten zijn is het belangrijk dat het bestuursorgaan dat bevoegd is om een aanwijzing te geven kennis draagt van de door de aangewezen melders gedane meldingen, het tijdstip daarvan en van de opvolging die daaraan door het betreffende ICT-bedrijf (wel of niet) is gegeven. Immers is het uitsluitend op die manier mogelijk om te monitoren of een ICT-bedrijf een melding heeft gehad en (afdoende) opvolging geeft aan die melding. Wij geven daarom in overweging ook dat aspect in de normstelling te betrekken.

Een tweede mogelijkheid is dat het tot de aanwijzing bevoegde bestuursorgaan (ook) zelf de voorafgaande melding doet. Dit zou in de normstelling tot uitdrukking gebracht kunnen worden door te bepalen dat het bestuursorgaan een aanwijzing kan geven aan een ICT-bedrijf indien dat bedrijf niet binnen een bepaalde termijn opvolging heeft gegeven aan een voorafgaande melding door dat bestuursorgaan van KP. Indien voor dit systeem zou worden gekozen is voorstelbaar dat de melding wordt gecombineerd met een voornemen tot het opleggen van een aanwijzing (inclusief de hiervoor geschetste mogelijkheid voor het ICT-bedrijf om dienaangaande een – beperkte – zienswijze te geven). Voordeel van dit systeem is dat het doen van de melding, de monitoring van de opvolging van de melding en het opleggen en handhaven van een aanwijzing in één hand zijn wat de effectieve aanpak van de verwijdering van KP-content bevordert.

2.50. Om geen afbreuk te doen aan de opsporing van de met de KP-content samenhangende strafbare feiten moet in de normstelling (al dan niet over de band van de te geven aanwijzing) worden geregeld dat de ICT-bedrijven die ingevolge een aanwijzing gehouden zijn om bepaalde KP ontoegankelijk te maken gehouden zijn om dienaangaande geen mededeling te doen aan degene die de content heeft geplaatst en/of verplicht zijn medewerking te verlenen aan het maken van een "kopie" van de betreffende content.

2.51. In het kader van de normstelling dient – tot slot – een partij te worden aangewezen die bevoegd is tot het geven van de betreffende aanwijzing. Wij menen dat de uitvoering van de betreffende taak niet zonder meer zodanig is dat daar een nieuwe toezichthouder voor zou moeten worden gecreëerd. Het komt ons daarentegen als het meest logisch voor indien de taak wordt belegd bij een reeds bestaand zelfstandig bestuursorgaan dat het best is geëquipeerd om de

betreffende taak uit te voeren. Op dit moment is de ACM onder meer belast met de handhaving van de Telecommunicatiewet. Tegen die achtergrond is voorstelbaar dat ook de uitoefening van de beoogde aanwijzingsbevoegdheid bij de ACM wordt belegd. Een en ander zal overigens wel mede afhangen van de keuze voor een stelsel met of zonder meldingsbevoegdheid van het bevoegde orgaan. Indien het bestuursorgaan ook zou worden belast met het doen van meldingen (op basis van onder meer internetanalyses) en het monitoren van de opvolging van die meldingen, is er immers sprake van een andere vereiste expertise (onder meer het beoordelen of er sprake is van KP) en bijbehorende personele bezetting dan in de variant waarin de meldingen door het EOKM/de politie worden gedaan.

## 3. Handhaving

3.1. Een norm die niet voldoende handhaafbaar is, moet niet in het leven worden geroepen.[56] In dit onderdeel onderzoeken wij daarom of de handhaving van de voorgestelde normstelling juridisch haalbaar en in de praktijk werkbaar is. Dit doen wij aan de hand van aantal criteria waar handhaving in onze optiek aan moet voldoen:

**Effectief**: handhaving moet doeltreffend zijn. De voorgestelde norm heeft een doel. Dat doel is primair om af te dwingen dat KP zo snel mogelijk wordt verwijderd of (als dat niet kan) ontoegankelijk wordt gemaakt. Relevante secundaire doelen zijn: preventie (voorkomen dat de overtreding wordt herhaald) en bestraffen van de overtreding (vergelding).[57] Handhaving moet kunnen bewerkstelligen dat dit geschiedt.

**Evenredig**: er moet een redelijk evenwicht worden gezocht tussen de betrokken belangen. Onder redelijk evenwicht verstaan wij een objectief te rechtvaardigen evenwicht. In dit geval betrekken wij enerzijds de belangen van de betrokken ICT-bedrijven (zoals ISP's en HSP's) en de belangen van individuele gebruikers van het internet en anderzijds het algemene belang gemoeid met het verwijderen van KP. Wij verwijzen hiervoor naar de evenredigheidsafweging die wordt verricht in het kader van de normstelling (zie onderdeel 2).

[56] Zie ook Aanwijzing 2.7 van de Aanwijzingen voor de regelgeving: "*1. Tot het tot stand brengen van een regeling wordt niet besloten dan nadat is nagegaan of in voldoende mate handhaving te realiseren valt.*"

[57] N. Struiksma, J. de Ridder, H.B. Winter, 'De effectiviteit van bestuurlijke en strafrechtelijke milieuhandhaving', (WODC, 2007), p. 35.

**Praktisch**: het handhavingsrecht moet zo veel mogelijk eenvoudig (toegankelijk) en duidelijk (rechtszeker) zijn. Daarnaast moet het ook mogelijk zijn om de op te leggen sanctie daadwerkelijk uit te voeren. Het heeft immers weinig zin om bijvoorbeeld bestuursdwang aan te zeggen als het niet mogelijk is voor de overheid om zelf de overtreding te beëindigen. Dat komt de geloofwaardigheid van de overheid niet ten goede.

3.2. Hierna bespreken wij (onder i) welke bestuursrechtelijke sancties er zijn. Daarna gaan wij in op de vraag welke van deze sancties in dit geval het overwegen waard zijn (onder ii). Vervolgens gaan wij in op de vraag of de sancties ten uitvoer kunnen worden gelegd (onder iii), waarna wij de mogelijke sancties tegen elkaar afwegen en u adviseren welk instrumentarium hier voor de hand ligt.

**(i) Welke bestuursrechtelijke sancties zijn er?**

3.3. Het bestuursrecht biedt een breed scala aan bestuurlijke sancties[58] die kunnen worden ingezet ter handhaving van de normstelling. In de Aanwijzingen voor de regelgeving worden de volgende sancties genoemd: intrekken of schorsen van een beschikking, opleggen van een last onder bestuursdwang, opleggen van een last onder dwangsom of opleggen van een bestuurlijke boete.[59] Daarnaast is er nog de (aanvullende) mogelijkheid van 'naming and shaming' – het actief openbaar maken van een sanctiebesluit (of van het feit dat een bepaald sanctiebesluit is opgelegd) op grond van artikel 8 van de Wet openbaarheid van bestuur of een andere specifieke in het leven geroepen wettelijk grondslag (zoals in de Wet op het financieel toezicht). Tot slot zou nog gedacht kunnen worden aan het toepassen van een 'beroepsverbod' zoals bijvoorbeeld opgenomen in artikel 15.2a Telecommunicatiewet in (ernstige) gevallen.

3.4. **De bestuurlijke boete**: de bestuurlijke boete is een bestraffende sanctie inhoudende dat de overtreder onvoorwaardelijk wordt verplicht om een geldbedrag te betalen.[60] Het bestraffende karakter houdt in dat de boete het oogmerk heeft de overtreder leed toe te voegen.[61] Het oogmerk van een bestuurlijke boe-

[58] Zie artikel 5:2, lid 1, onder a, Awb: "*bestuurlijke sanctie: een door een bestuursorgaan wegens een overtreding opgelegde verplichting of onthouden aanspraak*".

[59] Zie aanwijzing 5.40: "*Als bestuurlijke sancties worden met name de volgende mogelijkheden overwogen: Intrekken of schorsen van een beschikking, opleggen van een last onder bestuursdwang, opleggen van een last onder dwangsom of opleggen van een bestuurlijke boete*"

[60] Zie artikel 5:40, lid 1, Awb: "*Onder bestuurlijke boete wordt verstaan: de bestraffende sanctie, inhoudende een onvoorwaardelijke verplichting tot betaling van een geldsom.*"

[61] Zie artikel 5:2, lid 1, onder c, Awb: "*bestraffende sanctie: een bestuurlijke sanctie voor zover deze beoogt de overtreder leed toe te voegen.*"

te is dus niet zozeer om een reeds begane overtreding alsnog ongedaan te maken (de overtreding te 'herstellen'), maar om de overtreder te bestraffen ten einde te voorkomen dat hij nogmaals de fout in gaat (specifieke preventie) en een voorbeeld te stellen voor anderen (generale preventie). De bestuurlijke boete is in titel 5.4 van de Awb geregeld. De bestuurlijke boete geldt als een zogenaamde *'criminal charge'* in de zin van artikel 6 EVRM, zodat bij de bestuurlijke boete op grond van artikel 6 EVRM dezelfde waarborgen gelden als bij strafrechtelijke handhaving.

3.5. **De last onder dwangsom**: de last onder dwangsom is een herstellende sanctie[62] waarbij het oogmerk is om de overtreder te bewegen om een overtreding ongedaan te maken of om herhaling van de overtreding te voorkomen.[63] Bij een last onder dwangsom krijgt de overtreder de gelegenheid om de overtreding ongedaan te maken of te voorkomen. Doet hij dat niet (tijdig), dan verbeurt hij de aan de last verbonden dwangsom en is hij verplicht om die te betalen. De last onder dwangsom is volgens de Nederlandse rechter geen *'criminal charge'* in de zin van artikel 6 EVRM, zodat de waarborgen op grond van artikel 6 EVRM niet van toepassing zijn.[64]

3.6. **De last onder bestuursdwang**: de last onder bestuursdwang is een herstellende sanctie waarbij het oogmerk is om de overtreder te bewegen om een overtreding ongedaan te maken of om herhaling van de overtreding te voorkomen. Bij een last onder bestuursdwang krijgt de overtreder de gelegenheid om de overtreding ongedaan te maken of te voorkomen. Doet hij dat niet (tijdig), dan kan de overheid door feitelijk handelen de last ten uitvoer te leggen ten einde de overtreding zelf op te heffen (in beginsel op kosten van de overtreder). De last onder bestuursdwang is volgens de Nederlandse rechter geen *'criminal charge'* in de zin van artikel 6 EVRM, zodat de waarborgen op grond van artikel 6 EVRM niet van toepassing zijn.[65]

3.7. **De intrekking of schorsing van beschikkingen**: het intrekken of schorsen van beschikkingen houdt in dat de overheid als reactie op een overtreding een voor de overtreder geldende (begunstigende) beschikking intrekt. Te denken

[62] Zie artikel 5:2, lid 1, onder b, Awb: *"herstelsanctie: een bestuurlijke sanctie die strekt tot het geheel of gedeeltelijk ongedaan maken of beëindigen van een overtreding, tot het voorkomen van herhaling van een overtreding, dan wel tot het wegnemen of beperken van de gevolgen van een overtreding"*.

[63] Zie artikel 5:32, lid 1, Awb: *"Onder last onder dwangsom wordt verstaan: de herstelsanctie, inhoudende: a. een last tot geheel of gedeeltelijk herstel van de overtreding, en b. de verplichting tot betaling van een geldsom indien de last niet of niet tijdig wordt uitgevoerd"*.

[64] ABRvS 31 mei 2017, ECLI:NL:RVS:2017:1444.

[65] ABRvS 10 maart 2017, ECLI:NL:RVS:2017:634.

valt aan het intrekken van een Drank- en Horecawet vergunning als een café-eigenaar zich niet aan die wet houdt. Afhankelijk van de omstandigheden kan een intrekking door de Nederlandse rechter als punitief of herstellend worden aangemerkt.

3.8. **Naming and shaming**: als zodanig is 'naming and shaming' doorgaans geen zelfstandige bestuurlijke sanctie. Het betreft het openbaren van het feit dat de overheid een bepaald (rechts)persoon een bestuurlijke sanctie heeft opgelegd. Hiervoor is geen aparte wettelijke bevoegdheid nodig nu bestuursorganen op grond van artikel 8 Wet openbaarheid van bestuur in beginsel de mogelijkheid hebben om uit eigen beweging informatie openbaar te maken. "Naming and shaming" kan onder omstandigheden wel kwalificeren als een aparte bestuurlijke sanctie, maar indien de sanctie terecht is opgelegd, dan is doorgaans de conclusie van de bestuursrechter dat er ook geen bezwaar bestaat tegen het 'namen and shamen'. Bijvoorbeeld als het openbaarmaken van de overtreding de enige sanctie is die is of kan worden opgelegd.

3.9. **Beroepsverbod**: een bijzondere herstelsanctie is tot slot nog het 'beroepsverbod' in artikel 15.2a Telecommunicatiewet. Hierin is opgenomen dat de Minister van Economische Zaken onder omstandigheden een aanbieder van elektronische communicatiediensten kan verbieden voor een (redelijke) termijn nog langer die diensten aan te bieden. Dit kan bij "*ernstig en herhaaldelijk niet-nakomen van de verplichtingen* [in de Telecommunicatiewet] en als eerdere handhavings*maatregelen tot naleving van de bedoelde verplichtingen hebben gefaald*". In de rechtspraak hebben wij geen geval aangetroffen waarin daadwerkelijk gebruik is gemaakt van deze bevoegdheid, zodat niet duidelijk is of de maatregel kwalificeert als herstellend of bestraffend. Wij zouden menen dat het beroepsverbod in beginsel herstellend is (omdat het beoogt een verdere overtreding te voorkomen), maar kunnen niet uitsluiten dat de maatregel onder omstandigheden toch bestraffend van aard zal zijn.

**(ii) Welke sancties zijn geschikt om in dit geval te overwegen?**

3.10. Wij stellen voorop dat intrekking van een begunstigende beschikking in dit geval geen reële optie is. In het geval van ISP's en HSP's zijn er geen toestemmingen van overheidswege noodzakelijk om de dienst te kunnen leveren. Weliswaar is de kans zeer groot dat in Nederland gevestigde ISP's en HSP's op enigerlei wijze een begunstigende beschikking van een Nederlands bestuursorgaan ontvangen (denk bijvoorbeeld aan een belastingteruggaaf), maar niet alle ISP's en HSP's zullen dezelfde begunstigende beschikking ontvangen en geen van de begunstigende beschikkingen houdt direct verband met de mogelijkheid om in Nederland als ISP of HSP te kunnen werken.

3.11. Verder is 'Naming and shaming' in beginsel geen zelfstandige bestuurlijke sanctie. Het betreft meestal het openbaar maken van het feit dat er een andere sanctie is opgelegd. Daar zijn uitzonderingen op, zoals bijvoorbeeld artikel 80 Wet marktordening gezondheidszorg ('Wmg'). In dat artikel wordt het mogelijk gemaakt om aan het publiek kennis te geven van het feit dat de Nederlandse Zorgautoriteit van oordeel is dat een zorgaanbieder of ziektekostenverzekeraar zich niet aan de Wmg houdt. Het doel van het openbaar maken is in dat geval veelal om het publiek te waarschuwen voor malafide contractspartijen (/malafide praktijken). Dat lijkt in het geval van KP niet of minder aan de orde te zijn. Bij KP komt het ons voor dat 'naming and shaming' veelal een aanvullende werking zal hebben, om een andere sanctie kracht bij te zetten. Met andere woorden: dat in het kader van de handhaving wordt gekozen voor het verplicht openbaar maken van besluiten waarbij het niet (tijdig) verwijderen van KP wordt gesanctioneerd. Omdat 'naming and shaming' in onze optiek in dit geval een aanvullende werking zal hebben laten wij deze bij de keuze van de *primaire* sanctie buiten beschouwing.

3.12. Een beroepsverbod zoals bijvoorbeeld opgenomen in artikel 15.2a Telecommunicatiewet is een interessante mogelijkheid bij hardnekkige en herhaaldelijke overtreders. Gelet op de ingrijpende gevolgen daarvan en het feit dat andere middelen dan reeds geen effect moeten hebben gesorteerd, lijkt het beroepsverbod ons een laatste redmiddel en niet een primair sanctiemiddel. Het beroepsverbod beschouwen wij (net als het strafrecht) als een mogelijke stok achter de deur voor de extreme gevallen en is dus het overwegen waard als aanvullende maatregel. Omdat het beroepsverbod in onze optiek in dit geval een aanvullende werking zal hebben laten wij deze bij de keuze van de *primaire* sanctie buiten beschouwing.

3.13. Er resteren dan nog drie mogelijke bestuurlijke sancties in dit geval als primaire sanctie: de bestuurlijke boete, de last onder dwangsom en de last onder bestuursdwang.

*(a) De bestuurlijke boete*

3.14. De bestuurlijke boete is eenvoudig en effectief. Een voordeel is dat de bestuurlijke boete als straf heeft te gelden zodat het een nadrukkelijke afwijzing van het gedrag van de overtreder met zich meebrengt. Dat heeft een symbolische waarde. Zeker in combinatie met de mogelijkheid van 'naming and shaming' kan een bestuurlijke boete dus de naleving van de normstelling sterk bevorderen.

3.15. Het nadeel van de bestuurlijke boete is dat deze niet bewerkstelligt dat de ten onrechte toegankelijk gehouden KP alsnog (spoedig) ontoegankelijk wordt gemaakt. Immers kan een bestuurlijke boete nog steeds aan de overtreder worden opgelegd nadat deze in een later stadium alsnog de KP vrijwillig verwijdert.

*(b) De last onder dwangsom*

3.16. De last onder dwangsom is doorgaans een uitstekend handhavingsinstrument. Het is eenvoudig en effectief, leidt vaak tot herstel van de situatie, terwijl de uitvoering ook nog eens lage kosten voor de overheid met zich meebrengt.

3.17. In dit geval is de last onder dwangsom naar ons oordeel echter niet geschikt voor de handhaving van de normstelling. Dat komt omdat de last onder dwangsom niet goed werkt in spoedeisende gevallen. De reden daarvoor is ten eerste dat de bekendmakingsvereisten in de Awb een deel van het voordeel van de last onder dwangsom (lage kosten) in spoedeisende gevallen te niet doet. Ten tweede moet bij een last onder dwangsom een begunstigingstermijn worden geboden aan de overtreder – daarmee wordt het feitelijk verwijderen van de KP vertraagd. Ten derde staat de inzet van de last onder dwangsom in spoedeisende situaties op gespannen voet met artikel 5:32, lid 2, Awb.

3.18. Bij alle besluiten is vereist dat deze bekend worden gemaakt voordat het besluit in werking treedt (zie artikel 3:40 Awb). Dat doet men doorgaans door verzending per post (zie artikel 3:41, lid 1, Awb). Dat is te langzaam in het geval van KP. Het alternatief voor verzending is (i) het besluit door uitreiking bekend te maken of (ii) digitale toezending. Het besluit fysiek uitreiken doet een belangrijk voordeel van de last onder dwangsom teniet, namelijk dat deze relatief lage uitvoeringskosten met zich meebrengt. Immers, in dat geval zal een toezichthouder fysiek naar het adres van het betreffende ICT-bedrijf moeten gaan en in persoon het besluit uitreiken. Het besluit digitaal toezenden is aanzienlijk sneller, maar dat kan volgens artikel 2:14, lid 1, Awb alleen als de geadresseerde van dat besluit "*kenbaar heeft gemaakt dat hij langs deze weg voldoende bereikbaar is*". In de Awb is het initiatief daartoe bij de geadresseerde van het besluit gelegd, zodat als deze weg verplicht moet worden gesteld in het geval van KP omwille van de snelheid daar aanvullende wetgeving voor nodig is die ook wezenlijk afwijkt van de Awb.[66]

3.19. Daarnaast vereist de last onder dwangsom dat er na oplegging van de last een termijn wordt gegund aan de overtreder om de overtreding te beëindigen. Die

[66] Wij wijzen erop dat dit ook het geval zal zijn na de inwerkingtreding van de Wet modernisering elektronisch bestuurlijk verkeer die zich thans nog in de consultatiefase bevindt.

termijn mag niet wezenlijk langer of korter zijn dan nodig is om de overtreding feitelijk te beëindigen.[67] Anders zou de last onder dwangsom immers feitelijk neerkomen op een boete. Dit betekent echter wel dat, indien bijvoorbeeld wordt gekozen voor de norm dat KP binnen 24 uur verwijderd moet worden, de overtreder na de bekendmaking van de last onder dwangsom daarbovenop een redelijke termijn moet krijgen om de content te verwijderen. Zelfs al is de gegeven begunstigingstermijn dan maar 24 uur, dan nog betekent dit feitelijk dat de tijd tussen de melding en verwijdering met 100% wordt vertraagd ten opzichte van de norm.

3.20. Tot slot is in artikel 5:32, lid 2, Awb bepaald dat niet voor de inzet van een last onder dwangsom wordt gekozen indien het belang dat het betrokken voorschrift beoogt te beschermen zich daartegen verzet. In de wetsgeschiedenis is daarover opgemerkt dat het met name gaat om gevallen waarin "*niet het risico mag worden gelopen dat de overtreding ondanks de last onder dwangsom nog zou worden voortgezet of herhaald zou worden*".[68] Hoewel in dat kader met name is gedacht aan ernstige milieuovertredingen, wijzen wij erop dat het online blijven van KP in de beleving van velen in dezelfde categorie valt: overtredingen die koste wat kost zo snel mogelijk beëindigd moeten worden. Wij zijn dan ook van mening dat de last onder dwangsom reeds daarom geen geschikte bestuurlijke sanctie is gelet op de gewenste normstelling (binnen korte termijn na melding KP verwijderen) en het belang dat wordt gehecht aan het daadwerkelijk beëindigen van de overtreding.

*(c) De last onder bestuursdwang*

3.21. De last onder bestuursdwang houdt heel simpel samengevat in dat als het betrokken ICT-bedrijf (bijvoorbeeld een ISP of HSP) niet zelf alsnog de KP verwijderen en/of ontoegankelijk maken, de overheid dat dan zelf zal doen. De overheid zal dan 'onder toepassing van bestuursdwang' zich feitelijk toegang verschaffen tot de systemen van het bedrijf om de KP ontoegankelijk te maken.

3.22. De problemen die zich bij de last onder bestuursdwang voordoen omtrent de bekendmaking en de begunstigingstermijn zijn in beginsel dezelfde als bij de last onder dwangsom, maar bij de last onder bestuursdwang kunnen die problemen goed worden ondervangen. Dat komt omdat (voor wat betreft de bekendmaking) de toepassing van bestuursdwang vergt dat de toezichthouder zelf toch al feitelijk ter plaatse zal moeten gaan om de toegang tot KP onmogelijk te maken. Uitreiking in persoon is dan weinig bezwaarlijk. Bij bestuursdwang is

[67] ABRvS 4 juli 2018, ECLI:NL:RVS:2018:2196.

[68] Kamerstukken II, 1994-1995, 23 780, nr. 8, onder 6.100.

overigens ook vereist dat de last bekend wordt gemaakt aan de rechthebbende op de zaak (zie artikel 5:24, lid 3, Awb). Dat is echter geen onoverkomelijk probleem nu de bestuursrechter heeft geoordeeld dat het niet bekendmaken aan de rechthebbende op de zaak niet in de weg staat aan de rechtsgeldigheid en inwerkingtreding van de last voor zover wel aan de overtreder bekend gemaakt.[69]

3.23. Voor wat betreft de begunstigingstermijn voorziet de Awb in een mogelijkheid om die bij bestuursdwang achterwege te laten in spoedeisende situaties (zie artikel 5:31, lid 1, Awb). Wij vinden het verdedigbaar dat gelet op de aard van de materie de verwijdering van KP altijd spoedeisend van aard zal zijn zodat een begunstigingstermijn achterwege kan blijven. Het verdient echter vanuit rechtstatelijk perspectief dit standaard spoedeisende karakter vast te leggen bij wet – ook om twijfel hierover te voorkomen.[70] Het spoedeisende karakter heeft overigens als bijkomend voordeel dat bij de voorbereiding van het besluit niet aan de hoorplicht in artikel 4:8 Awb hoeft te worden voldaan (zie artikel 4:11, onder a, Awb), hetgeen overigens onverlet laat dat het Unierechtelijke verdedigingsbeginsel in het kader van de beoogde normstelling een eigenstandige afweging vergt (vergelijk hoofdstuk 2).

3.24. Een nadeel van bestuursdwang is wel dat bestuursdwang niet buiten de territoriale grenzen van Nederland kan worden toegepast. Hier komen wij nog in hoofdstuk 4 op terug.

**(iii) Welke bestuurlijke sanctie(s) raden wij aan?**

3.25. Handhaving heeft in dit geval uiteindelijk als doel om de KP zo snel mogelijk van het openbare internet te verwijderen. Bestuursdwang bereikt dat doel het beste en is daardoor het meest effectief. Bovendien is bestuursdwang praktisch en is de inzet ervan in de regel als evenredig te noemen.

3.26. De last onder dwangsom is voor deze situatie op zich ook bruikbaar, maar volgens ons wel onpraktisch en niet voldoende effectief vanwege de noodzaak om (onder meer) een begunstigingstermijn te geven en daarmee optredende vertraging. Bovendien is niet zeker dat de KP dan ook daadwerkelijk ontoegankelijk wordt gemaakt (lees: dat de overtreding wordt beëindigd).

3.27. De bestuurlijke boete is volgens ons maar beperkt effectief omdat het niet afdwingt dat de KP alsnog wordt verwijderd, maar de overtreder bestraft voor het

[69] Zie onder meer ABRvS 2 augustus 2006, ECLI:NL:RVS:2006:AY5495 en ABRvS 30 november 2016, ECLI:NL:RVS:2016:3167.

[70] Vergelijk artikel 15.2 lid 4 en 5 Telecommunicatiewet.

niet tijdig verwijderd hebben van de KP. De bestuurlijke boete heeft wel als voordeel dat het een belangrijke signaalfunctie kan hebben in zoverre dat het een duidelijke afkeuring is van het gedrag van het betreffende ICT-bedrijf. In zoverre zien wij wel nut in de bestuurlijke boete als handhavingsinstrument in dit geval.

3.28. Onze bevindingen overziend komen wij tot de volgende samenvattende tabel over de inzet van bestuurlijke sancties.

| | Straf? | Effectief? | Evenredig? | Praktisch? |
|---|---|---|---|---|
| **Bestuurlijke boete** | Ja | Beperkt | Ja | Ja |
| **Last onder dwangsom** | Nee | Beperkt | Ja | Nee |
| **Last onder bestuursdwang** | Nee | Ja | Ja | Ja |

3.29. Gelet op het voorgaande lijkt het ons voor de hand te liggen om te kiezen voor de toepassing van bestuursdwang als primair handhavingsinstrument.

3.30. Daarnaast lijkt het ons aanbevelenswaardig om een toezichthouder[71] ook de mogelijkheid te geven om een bestuurlijke boete op te leggen wegens het (al dan niet herhaaldelijk) niet-tijdig ontoegankelijk maken van KP (lees: het niet voldoen aan daartoe gegeven aanwijzingen). De combinatie van het opleggen van een herstelsanctie en een bestraffende sanctie is naar de huidige stand van het recht in het Nederlandse bestuursrecht gewoon toegestaan,[72] maar daarbij dient wel een beoordeling te worden gemaakt van de evenredigheid van het gehele 'pakket' aan maatregelen in het concrete geval.[73]

3.31. Mocht het wenselijk worden geacht om een nog steviger handhavingsinstrumentarium in te zetten, dan zien wij nog drie mogelijkheden daartoe.

[71] Met het begrip toezichthouder doelen wij niet alleen op de toezichthouder op grond van artikel 5:11 Awb, maar ook op de instantie die belast is met het toezicht op de naleving in zijn geheel.

[72] Zie A.B. Blomberg, 'Cumulatie van sancties', JBplus 2001/1.

[73] ABRvS 29 juni 2016, ECLI:NL:RVS:2016:1803.

3.32. Ten eerste door het 'naming and shaming' instrument in te zetten als aanvullende sanctie. Hierbij wordt het sanctiebesluit altijd gepubliceerd door de toezichthouder. Hier is in beginsel geen specifiek wettelijk voorschrift voor vereist, tenzij de wens bestaat om de toezichthouder te verplichten om altijd het sanctiebesluit volledig openbaar te maken. Ten tweede door overtreding van de normstelling in de Wet Economische Delicten op te nemen. Het verwijzen naar de normstelling in de Wet Economische Delicten (hierna: 'WED') als overtreding of misdrijf (doorgaans is de kwalificatie als overtreding of misdrijf in de WED afhankelijk van de vraag of er opzet in het spel is), maakt het eenvoudig om bij zeer ernstige schendingen zo nodig op te schalen naar het strafrecht. Ten derde om de Minister de bevoegdheid te geven om bij herhaaldelijke en ernstige overtredingen (een beroepsverbod als bedoeld in) artikel 15.2a, lid 1, Telecommunicatiewet toe te passen en het ICT-bedrijf te verbieden om voor een bepaalde termijn nog diensten aan te bieden.

3.33. Wij wijzen er wel op dat de evenredigheid van sanctiepakketten nadrukkelijk de aandacht van de rechterlijke macht lijkt te hebben. Bovendien kan het inzetten van al deze bevoegdheden tegelijkertijd vanwege dezelfde overtreding een onevenredig karakter hebben (naast het feit dat een bestuurlijke boete en strafvervolging niet mogen plaatsvinden vanwege één en dezelfde overtreding). Het lijkt ons dus dat in het concrete geval uiteindelijk een evenredige keuze moet worden gemaakt door de toezichthouder welk(e) sanctie instrument(en) zal (zullen) worden ingezet.

**4. Kunnen deze sancties altijd ten uitvoer worden gelegd?**

4.1. Een belangrijke factor om nog mee te wegen is de vraag of de sancties altijd ten uitvoer kunnen worden gelegd. Het internet eindigt namelijk niet bij onze landsgrenzen. De rechtsmacht van de Nederlandse Staat wel. Dat vormt een probleem bij het formuleren van een juridisch haalbare en in de praktijk werkbare aanpak van KP omdat de Nederlandse overheid wel de in Nederland gevestigde ICT-bedrijven kan raken, maar in het buitenland gevestigde aanbieders niet.

4.2. Voor de toepassing van bestuursdwang is het evident waarom het effectueren van de sanctie niet mogelijk is over de Nederlandse grenzen. Toezichthouders van de Nederlandse overheid kunnen uiteraard niet in een ander land een server fysiek mee gaan nemen. De toepassing van bestuursdwang kan dan ook alleen binnen de Nederlandse territoriale grenzen. Hieruit vloeit voort dat de Nederlandse overheid KP niet kan verwijderen van een server als de server waarop de KP zich bevindt niet fysiek in Nederland staat.

4.3. Bij bestuurlijke sancties waaruit een bestuursrechtelijke geldschuld voortvloeit (zoals de last onder dwangsom en de bestuurlijke boete) ligt het een en ander genuanceerder. Ten eerste kan een geldelijke sanctie op zich worden opgelegd aan een buitenlandse vennootschap die niet fysiek in Nederland aanwezig is, maar wel activiteiten verricht in Nederland (zo lang de handhaving zich maar richt op de activiteiten in Nederland).[74] Ten tweede zijn er verdragen (bijvoorbeeld Europese) die het onder bepaalde omstandigheden mogelijk maken om geldelijke sancties ten uitvoer te leggen buiten de Nederlandse territoriale grenzen. Wij hebben in dat kader onderzocht of, en zo ja in hoeverre, geldschulden die voortvloeien uit bestuurlijke sancties over de Nederlandse grenzen heen zouden kunnen worden ingevorderd (onder i.).

4.4. Omdat die mogelijkheden afwezig lijken te zijn, hebben wij gezocht naar alternatieven om in het buitenland gevestigde ICT-bedrijven te raken met Nederlandse bestuurlijke sancties (onderdeel ii.). In dat kader hebben wij onderzocht of het mogelijk is om geldschulden die voortvloeien uit bestuurlijke sancties te effectueren op tegoeden van buitenlandse (rechts)personen die slechts kortstondig in Nederland zijn.[75]

**(i) Innen geldschulden uit sancties in het buitenland**

4.5. Een bestuursrechtelijke geldschuld kan in Nederland worden geïnd op basis van een dwangbevel (een executoriale titel – zie artikel 4:116 Awb). Om in het buitenland deze schulden te kunnen innen dient een dwangbevel in dat land erkend te worden. Zowel binnen de EU als internationaal zijn daar echter op basis van de huidige wet- en regelgeving geen mogelijkheden toe.

*EU: EEX-Verordening*

4.6. Binnen de Europese Unie kennen we de EEX-verordening[76] voor de erkenning

[74] CBb 10 januari 2018, ECLI:NL:CBB:2018:2. Zie ook ABRvS 17 januari 2018, ECLI:NL:RVS:2018:155 waaruit blijkt dat het gevestigd zijn in Antigua en Barbados niet in de weg staat aan beboeting door de Kansspelautoriteit indien de gokdiensten via het internet aan Nederlandse gebruikers worden aangeboden.

[75] Als bedoeld in de motie Groothuizen / Van Oosten, Kamerstukken II 2017-2018, 31015, nr. 143: "*roept de regering op bij het uitwerken van dit bestuursrechtelijke instrumentarium aandacht te besteden aan dit probleem om te voorkomen dat het bestuurlijke instrumentarium onvoldoende effect sorteert, en daarbij in ieder geval te onderzoeken of er enige vorm van beslag kan worden gelegd op tegoeden als deze via Nederlandse betaalinstellingen lopen en te onderzoeken of er een lijst met instellingen kan worden gemaakt van wie de hiervoor bedoelde tegoeden dienen te worden beslagen*".

[76] Verordening 1215/2012 van 12 december 2012 betreffende de rechterlijke bevoegdheid, de erkenning en de tenuitvoerlegging van beslissingen in burgerlijke en handelszaken.

van gerechtelijke uitspraken. De EEX-verordening heeft geen betrekking op administratiefrechtelijke zaken.[77] Daarbij beslissend is of een overheidsinstantie krachtens overheidsbevoegdheid handelt.[78] Dit geldt vooral indien de overheidsinstantie gebruik maakt van een eigen recht (dat niet door particulieren kan worden ingeroepen) dat te herleiden is tot publiekrechtelijke regels. Voorbeelden zijn het opleggen van uit publiekrechtelijke regelgeving verschuldigde administratiefrechtelijke/strafrechtelijke boetes[79], bestuursrechtelijke dwangsom[80], belastingaanspraken c.q. sociale zekerheidsaanspraken. In de literatuur wordt deze scherpe afbakening bevestigd.[81] Uit de rechtspraak komt duidelijk een beeld naar voren dat slechts van een burgerlijke of handelszaak sprake is indien de positie van de overheidsinstantie te vergelijken is met die van een particulier en dus een vorderingsrecht geldend maakt dat voortvloeit uit een privaatrechtelijke grondslag. Kortom: in deze zien we geen ruimte voor een erkenning op basis van de EEX-Verordening.

*EU: EET*

4.7. In een civiele procedure kan een partij de rechtbank verzoeken om een waarmerking van het vonnis als Europese Executoriale Titel ('EET') als bedoeld in Verordening (EG) 805/2004. Ook deze verordening is alleen van toepassing op burgerlijke en handelszaken. In het bijzonder heeft zij geen betrekking op bestuursrechtelijke zaken.[82] Voor de uitleg van deze begrippen dient aangesloten te worden bij de uitleg van de EEX-Verordening.[83] Ook dit biedt geen soelaas.

*EU: Kaderbesluit*

4.8. Voor de erkenning van geldelijke sancties geldt er een specifiek regime binnen de EU. Dit is vastgelegd in het Kaderbesluit.[84] Een geldelijke sanctie is onder meer een verplichting tot betaling van een geldsom die in geval van veroorde-

[77] Artikel 1, lid 1, EEX-Vo.

[78] HvJ EG 14 oktober 1976, zaak 29/76, NJ 1982, 95 m. nt. Schultsz. Deze uitspraak is vervolgens bevestigd in latere rechtspraak van het HvJ EG: HvJ EG HvJ EG 15 mei 2003, zaak C-266/01, NJ 2005, 65; HvJ EG 15 februari 2007, zaak C-292/05, NJ 2008, 618.

[79] Gerechtshof 's-Gravenhage, NIPR 2000, 206.

[80] Conclusie A-G Bloembergen bij HR 22 oktober 1993, NJ 1995, 717 m.nt. MS, nr. 5.3.

[81] Magnus/Mankowski, Brussels I Regulation, München: Sellier 2007, p. 51-56; Th. Rauscher, Europaïsches Zivilprozessrecht, Sellier: 2003, p. 48-50; P. Vlas, Groene Losbladige Kluwer, Burgerlijke Rechtsvordering: Verdragen & Verordeningen, Deventer: Kluwer 2013, art. 1 EEX-Vo.

[82] Artikel 2 Verordening (EG) 805/2004.

[83] Rechtbank Den Haag 16 maart 2016, ECLI:NL:RBDHA:2016:2684, r.o. 4.17 en 4.18.

[84] Kaderbesluit 2005/214/JBZ inzake de toepassing van het beginsel van wederzijdse erkenning op geldelijke sancties, zoals gewijzigd bij het Kaderbesluit 2009/299/JBZ.

ling wegens een strafbaar feit bij beslissing is opgelegd.[85] Daaronder valt ook de bestuurlijke boete op grond van de Awb, aldus de Afdeling.[86] Een last onder dwangsom valt ons inziens daar niet onder nu het geen veroordeling wegens een strafbaar feit inhoudt.

4.9. Het Kaderbesluit is in Nederland (onvolledig – aldus de Afdeling[87]) geïmplementeerd in de Wet wederzijdse erkenning en tenuitvoerlegging geldelijke sancties en beslissingen tot confiscatie. Artikel 10 van deze wet bepaalt dat vatbaar voor erkenning en tenuitvoerlegging in een andere lidstaat van de Europese Unie zijn beslissingen, houdende een in Nederland:

a. bij rechterlijke uitspraak opgelegde geldboete;
b. bij rechterlijke uitspraak opgelegde verplichting tot betaling aan de staat van een geldsom ten behoeve van het slachtoffer;
c. door de bevoegde autoriteiten bij beschikking opgelegde administratieve sanctie als bedoeld in artikel 2 van de Wet administratiefrechtelijke handhaving verkeersvoorschriften;
d. genomen beslissing tot confiscatie, betreffende een geldbedrag;
e. genomen beslissing tot confiscatie, betreffende een specifiek voorwerp;
f. door de bevoegde autoriteiten bij beschikking opgelegde bestuurlijke boete als bedoeld in artikel 10:5 van de Arbeidstijdenwet voor zover het overtredingen betreft van hoofdstuk 2 van het Arbeidstijdenbesluit vervoer.

4.10. Een bestuursrechtelijke geldschuld kan zijn ontstaan door een bestuurlijke boete. Kenmerkend voor een bestuurlijke boete is dat die door het bestuur wordt opgelegd en na heroverweging al dan niet geheel of gedeeltelijk wordt gehandhaafd in het besluit op bezwaar. De rechter kan als het beroep daartegen gegrond is, dat besluit op bezwaar weliswaar vernietigen en de oplegging van de boete herroepen, maar die bevoegdheid kan niet worden gekwalificeerd als een beslissing zoals genoemd in voornoemd artikel onder categorie a.[88] De andere categorieën bieden ook geen soelaas.

4.11. Er is een wetswijziging op komst. De wetgever wil dat ook bij beschikking opgelegde geldboetes erkend kunnen worden.[89] De daartoe benodigde wetswijziging is aangenomen en in 2017 in het Staatsblad gepubliceerd, de wetswijziging is echter nog niet in werking getreden. Het is echter de vraag of de toevoeging 'beschikking' ook ziet op bestuurlijke boeten als bedoeld in de Awb. Uit de Me-

[85] Artikel 1.b. Kaderbesluit.

[86] ABRvS 3 december 2014, ECLI:NL:RVS:2014:4346.

[87] ABRvS 3 december 2014, ECLI:NL:RVS:2014:4346.

[88] Ibidem.

[89] Staatsblad 2017, nr. 82.

morie van Toelichting volgt dat de wetgever specifiek doelt op strafbeschikkingen.[90] Deze dienen ook voor erkenning en tenuitvoerlegging in een andere lidstaat vatbaar te zijn. Dit past in de ontwikkeling van de jurisprudentie van de afgelopen jaren. In de Baláz uitspraak[91] oordeelde het Europese Hof dat een beslissing van elke rechterlijke instantie die een procedure toepast die aan de wezenlijke kenmerken van een strafrechtelijke procedure voldoet onder de werking van het Kaderbesluit valt, zonder dat echter is vereist dat deze rechter uitsluitend in strafzaken bevoegd is. Daarbij moeten verschillende objectieve factoren in ogenschouw worden genomen die het orgaan en de werking ervan kenmerken. In het arrest noemt het Hof als factoren dat het beroep schorsende werking heeft, de rechter volle rechtsmacht heeft en de rechter een procedure van strafrechtelijke aard toepast waarin de in strafzaken gepaste procedurele waarborgen gelden. Het moet echter wel nog steeds gaan om boetes die onder het bereik van het Kaderbesluit vallen.

4.12. Naar het oordeel van de Afdeling van 3 december 2014[92] voldoet de bestuursrechtelijke procedure in boetezaken (het ging in deze om een overtreding van de Arbeidstijdenwet) aan de wezenlijke kenmerken van een strafrechtelijke procedure als door het Hof van Justitie geformuleerd. De bestuursrechter beschikt over volle rechtsmacht. Hij kan over zowel de rechtsvragen als de feitelijke vragen oordelen, als ook over de evenredigheid van de boete in relatie tot de overtreding. Daarnaast gelden in boetezaken als de onderhavige de in strafzaken gepaste procedurele waarborgen (alleen een boete opleggen voor zover de overtreding aan de overtreder kan worden verweten, dient bij de bepaling van de hoogte van de boete rekening te worden gehouden met de bijzondere omstandigheden van het geval, de partij aan wie de boete is opgelegd is niet verplicht omtrent de overtredingen verklaringen af te leggen etc.). De omstandigheid dat artikel 6:16 van de Awb een verzoek om voorlopige voorziening vergt om schorsende werking van het besluit te bereiken, brengt volgens de Afdeling niet met zich dat de bestuursrechtelijke boteprocedure niet aan de voorwaarden voor toepasbaarheid van het Kaderbesluit voldoet, nu het arrest niet voorschrijft dat aan alle genoemde factoren cumulatief moet zijn voldaan. Volgens de Afdeling valt deze bestuurlijke boete onder het toepassingsbereik van het Kaderbesluit. De Afdeling oordeelde echter dat de door de minister opgelegde boete buiten

[90] Kamerstukken II 2013-2014, 34086, nr. 3, p. 135:*" Met de wijzigingen van onderdelen a en b van het eerste lid van artikel 10 van de Wet wederzijdse erkenning en tenuitvoerlegging geldelijke sancties en beslissingen tot confiscatie wordt verduidelijkt dat ook strafbeschikkingen voor erkenning en tenuitvoerlegging in een andere lidstaat vatbaar zijn. De wijzigingen van het tweede lid van artikel 10 vloeien voort uit de nieuwe verdeling van verantwoordelijkheden in de tenuitvoerlegging tussen openbaar ministerie en Minister."*

[91] HvJ EU 14 november 2013, C-60/12, ECLI:EU:C:2013:733 (Baláz).

[92] Afdeling bestuursrechtspraak 3 december 2014, ECLI:NL:RVS:2014:4346.

het bereik van de Wet Wederzijdse erkenning viel, nu de boete niet onder één van de destijds in de wet genoemde categorieën viel. Naar aanleiding van deze uitspraak is de Wet wederzijdse erkenning aangevuld met categorie sub f.

4.13. Kortom: als een bestuursrechtelijke geldschuld is gebaseerd op een bestuurlijke boete kan deze onder het bereik van het Kaderbesluit vallen. Voor erkenning is echter noodzakelijk dat de boete ook onder het bereik van de Wet wederzijdse erkenningen valt. In de huidige situatie achten wij dat niet het geval voor wat betreft KP. Wij geven in overweging om artikel 10 van de Wet wederzijdse erkenning aan te vullen met een nieuwe categorie, waarbij uiteraard niet de door het Hof van Justitie gestelde grenzen omtrent de uitleg van het Kaderbesluit moeten worden overschreden.

*EU: Richtlijn 2010/24/EU*

4.14. Deze richtlijn betreft de wederzijdse bijstand inzake de invordering van schuldvorderingen die voortvloeien uit belastingen, rechten en andere maatregelen. De bestuursrechtelijke geldschulden vallen buiten de materiële reikwijdte van deze richtlijn.

*Buiten de EU*

4.15. Of een bestuurlijke geldschuld buiten de Europese Unie wordt erkend zal afhangen van het nationale recht van dat desbetreffende land (inclusief de eventueel door het land afgesloten verdragen). Een bekend verdrag is het Verdrag betreffende de erkenning en de tenuitvoerlegging van buitenlandse vonnissen in burgerlijke en handelszaken. Het materiële toepassingsgebied komt grosso modo overeen met dat van de EEX-Verordening. De bestuursrechtelijke geldschulden vallen ook buiten het toepassingsbereik van dit Verdrag. Er zijn naar ons weten geen verdragen die betrekking hebben op bestuursrechtelijke geldschulden. Zoals hiervoor al aangegeven zal het dan van het recht van dat land afhangen of een bestuursrechtelijke geldschuld wordt erkend.

**(ii) Beslag op banktegoeden die kortstondig in Nederland zijn**

4.16. Een alternatief om ICT-bedrijven te kunnen raken die in het buitenland zijn gevestigd is door vermogensbestanddelen die zich in Nederland bevinden te raken. Het gaat dan met name om tegoeden die kortstondig in Nederland zijn omdat deze tegoeden via Nederlandse betaaldiensten of banken verlopen. De Tweede Kamer heeft u opgeroepen om de mogelijkheden om hier beslag op te leggen in het geval van KP te onderzoeken en te betrekken in uw afwegingen.[93]

[93] Motie Groothuizen/Van Oosten, Kamerstukken II 2017-2018, 31015, nr. 143.

4.17. Op grond van artikel 765 Rv kan ten aanzien van de schuldenaar zonder bekende woonplaats in Nederland elke vorm van conservatoir beslag worden toegepast (vreemdelingenbeslag). Een beslagverlof heeft echter, gelet op de territoriale werking van het conservatoire beslag, in beginsel alleen betrekking op zaken die zich in Nederland bevinden of geldvorderingen die in Nederland betaalbaar zijn. Een uitzondering daarop is het Europees bankbeslag. Deze mogelijkheid bestaat echter alleen bij geldelijke vorderingen in burgerlijke en handelszaken in grensoverschrijdend verband. Zij heeft in het bijzonder geen betrekking op bestuursrechtelijke zaken.[94]

4.18. Een andere uitzondering is wanneer een (ook) in Nederland gevestigde bank ook tegoeden voor een klant aanhoudt in het buitenland. Indien de rechtsverhouding tussen de bank en de beslagene meebrengt dat de beslagene ook in Nederland aanspraak heeft op betaling van de in het buitenland geadministreerde tegoeden, kunnen die tegoeden ook onder het beslag vallen,[95] mits (a) het beslag in het buitenland wordt erkend (b) in het verzoekschrift is gemeld in welk land en bij welk kantoor tegoeden van de beslagene aanwezig zijn.[96]

4.19. De vraag is ook of het mogelijk of praktisch werkbaar is om beslag te leggen op tegoeden die slechts (zeer) kortstondig in Nederland staan. Als de buitenlandse rechtspersoon een bankrekening in Nederland aanhoudt kan op het saldo van deze bankrekening beslag worden gelegd. Let wel dat het beslag alleen het saldo treft wat op dat moment aanwezig is. Als er één minuut na beslaglegging een aanzienlijke som geld op deze rekening wordt gestort valt dat niet onder het beslag. Wellicht dat in samenspraak met politie nader inzicht verkregen kan worden in wanneer er bedragen op de rekening worden gestort. De deurwaarder kan dan geïnstrueerd worden om exact op die momenten beslag te leggen. Praktisch gezien is dat niet eenvoudig.

4.20. Het is ook mogelijk om beslag te leggen onder een derde op alles wat die partij aan de buitenlandse rechtspersoon verschuldigd is. Dit beslag treft niet alleen de op dat moment aanwezige vorderingen van de buitenlandse rechtspersoon op de derde, maar ook de vorderingen die de beslagene op de derde uit een ten tijde van het beslag reeds bestaande rechtsverhouding rechtstreeks zal verkrijgen

[94] Artikel 2, lid 1, Verordening (EU) nr. 655/2014 van het Europees Parlement en de Raad van 15 mei 2014 tot vaststelling van een procedure betreffende het Europees bevel tot conservatoir beslag op bankrekeningen om de grensoverschrijdende inning van schuldvorderingen in burgerlijke en handelszaken te vergemakkelijken.

[95] Gerechtshof Amsterdam 10 april 2012, ECLI:NL:GHAMS:2012:BW3378 en Gerechtshof Amsterdam 8 september 2017, ECLI:NL:GHAMS:2017:7730.

[96] Beslagsyllabus, p. 49.

(art. 475 Rv). Om dit beslag te kunnen leggen moet de naam van de derde bekend zijn. Het is praktisch lastig om vast te stellen op wie in Nederland het buitenlandse ICT-bedrijf een vordering heeft zodat ook deze vorm praktisch moeilijk uitvoerbaar is.

4.21. Er kan onzes inziens beslag gelegd worden onder een Collecterende Payment Service Provider: deze partijen incasseren direct van de klant en storten de omzet door aan ondernemer met aftrek van de kosten voor de betaling. Een Collecterende Payment Service Provider houdt voor korte tijd de gelden. De vraag is echter of het beslag ook de toekomstige vorderingen treft of alleen het op het moment van beslaglegging aanwezige saldo. Wij menen dat het laatste het geval is. De latere creditbedragen vloeien niet voort uit de beslagen rechtsverhouding tussen de Payment Provider en de beslagene, maar het gaat juist om geldbedragen die de Payment Provider ingevolge andere rechtshandelingen ten behoeve van de beslagene onder zich krijgt. Het gaat om rechtshandelingen tussen de beslagene en vierden, die geheel los staan van de verhouding tussen de Payment Provider en de derde.[97]

4.22. Kortom: technisch en juridisch is het mogelijk om te voldoen aan de (aangehouden) motie Groothuizen/Van Oosten. Het is echter praktisch nagenoeg onwerkbaar. Het is namelijk niet mogelijk om een doorlopend beslag te leggen waarbij alle tegoeden van een (rechts)persoon die via Nederland lopen worden beslagen. Dit betekent dat telkens gericht beslag moet worden gelegd op het moment dat er een vermoeden is dat er een tegoed van die (rechts)persoon via Nederland loopt. Wij zien niet in hoe die informatie tijdig genoeg beschikbaar zou kunnen zijn om de overheid effectief in staat te stellen om beslag te leggen op die tegoeden. Indien het gewenst is om dergelijke maatregelen te treffen, is bovendien een ingrijpende wetswijziging ten aanzien van het beslagrecht en nader onderzoek naar de wenselijkheid daarvan noodzakelijk.

**(iii) Afsluitende opmerkingen**

4.23. De aanpak van KP lijkt niet effectief mogelijk voor zover het betreft de verwijdering en het ontoegankelijk maken van KP ten aanzien waarvan geen van de betrokken ICT-bedrijven in Nederland is gevestigd. Dat zou de vraag kunnen opwerpen in hoeverre de introductie van een bestuursrechtelijk instrumentarium gericht op de aanpak van KP op het Nederlandse deel van het internet – gelet op het internationale karakter van KP – dan wel zinvol is. Wij menen echter dat een dergelijk instrumentarium wel degelijk toegevoegde waarde heeft. In dat verband is onder meer van belang dat de Europese Commissie in het belang van

[97] Zie Groene Serie Burgerlijke Rechtsvordering, art. 475 Rv, aant. 7.2.

de bestrijding van KP de Lidstaten heeft opgeroepen om binnen hun eigen jurisdictie meer maatregelen te treffen om KP te verwijderen. Nederland geeft met de introductie van het beoogde bestuursrechtelijke instrument gehoor aan die oproep. Bovendien wordt met de introductie van het instrumentarium de ruimte voor in Nederland gevestigde ICT-bedrijven nog verder beperkt om niet mee te werken aan de (prompte) verwijdering van KP. In zoverre draagt het instrument bij aan het verder veilig maken van het Nederlandse gedeelte van het internet. Uiteraard laat de introductie van een nationaalrechtelijk instrumentarium het onverlet dat het aan te bevelen is om in samenspraak met andere landen ook de internationale aanpak van KP te intensiveren. Het te introduceren instrumentarium zou daarbij mogelijk (ook) een rol kunnen vervullen als voorbeeld voor de wijze waarop de effectieve aanpak van KP vorm kan worden gegeven.

## 5. Conclusie

U heeft ons gevraagd te adviseren over de mogelijkheden van een bestuursrechtelijke aanpak van de verwijdering van KP op het internet. U heeft ons meer specifiek gevraagd te adviseren omtrent een aanpak die in onze ogen zowel juridisch houdbaar als praktisch werkbaar is.

Om een bestuursrechtelijke aanpak van KP mogelijk te maken zal allereerst voorzien dienen te worden in een te handhaven norm. Bij het formuleren van zo'n norm zou (in theorie) gekozen kunnen worden voor een algemene publiekrechtelijke normering van de aanpak van KP die (deels) in de plaats komt van de binnen de sector (van tussenpersonen die zich bezighouden met het doorgeven en/of opslaan van gegevens op het internet) bestaande zelfregulering. Bij een dergelijk publiekrechtelijk stelsel zou gedacht kunnen worden aan bijvoorbeeld het introduceren van een zorgplicht voor bepaalde soorten bedrijven om alle redelijkerwijs mogelijke maatregelen te nemen om de verspreiding van KP tegen te gaan en om de gebruikers tegen KP te beschermen. Een dergelijke zorgplicht kan vervolgens via verschillende bestuursrechtelijke instrumenten gehandhaafd worden. Een dergelijk meeromvattend systeem lijkt vooral aangewezen indien geconcludeerd zou moeten worden dat de bestaande zelfregulering onvoldoende werkt en niet of onvoldoende leidt tot de daadwerkelijke verwijdering van KP door de sector. Voor zover wij het echter begrijpen functioneert de bestaande zelfregulering op zichzelf naar behoren, maar is er geen sprake van een sluitend stelsel. Dit laatste wordt veroorzaakt door een aantal onwelwillende partijen. In dat licht wordt de noodzaak van een "slot op de deur" gevoeld. Bij die stand van zaken lijkt een beperkt doch doeltreffend bestuursrechtelijk kader dat kan dienen als slot op de deur om de rotte appels aan te kunnen pakken te verkiezen boven een meer breed systeem.

In ons rapport hebben wij de voorwaarden in beeld gebracht waaraan normstelling volgens ons zou moeten voldoen om juridisch haalbaar en praktisch werkbaar te zijn. Op grond van de door ons benoemde voorwaarden kunnen wij ons voorstellen dat de beoogde normstel-

ling in grote lijnen de volgende kenmerken zou kunnen hebben:

1. Er wordt een bestuursorgaan aangewezen dat bevoegd is om een bindende aanwijzing te geven.
2. De bevoegdheid tot het geven van een aanwijzing bestaat indien een aangewezen ICT-bedrijf niet binnen een bepaalde (maximale) termijn (van bijvoorbeeld 12 uur) na ontvangst van een KP-melding door daartoe aangewezen organisaties (bijvoorbeeld politie/EOKM) tot verwijdering van de betreffende KP is overgegaan of, indien dat niet mogelijk is, tot het ontoegankelijk maken daarvan.
3. De aanwijzing kan worden gegeven aan in de normstelling aangewezen categorieën van ICT-bedrijven, waaronder bij de huidige stand van zaken in ieder geval hosting- en serviceproviders lijken te moeten vallen. Het is zaak om de categorieën van bedrijven die onder de normstelling vallen voldoende precies te definiëren.
4. Het bestuursorgaan beschikt over een discretionaire bevoegdheid om een aanwijzing te geven. Het geven van een aanwijzing is dus geen automatisme maar vergt van geval tot geval een afweging van de betrokken belangen.
5. De aanwijzing kan inhouden dat het betreffende ICT-bedrijf verplicht wordt om tot verwijdering van de betreffende KP-content over te gaan. Het geven van een dergelijke aanwijzing ligt in de rede indien de betreffende server zich in Nederland bevindt en het dus fysiek mogelijk is om tot verwijdering over te gaan. Een aanwijzing kan indien verwijdering onmogelijk is in plaats daarvan inhouden dat de KP op een andere manier ontoegankelijk moet worden gemaakt (blokkeren).
6. De aanwijzing wordt vormgegeven als een resultaatsverplichting. Na ommekomst van de in de aanwijzing opgenomen termijn dient de KP verwijderd te zijn of in voorkomend geval ontoegankelijk te zijn gemaakt.
7. De aanwijzing dient binnen een in de normstelling opgenomen gefixeerde (korte) termijn te zijn opgevolgd, waarbij de normstelling ruimte moet laten om in de aanwijzing een afwijkende termijn op te nemen.
8. De aanwijzing wordt standaard op een specifiek daartoe aangewezen wijze langs elektronische wijze bekendgemaakt. De aanwijzing mag summier gemotiveerd worden indien erin is voorzien dat binnen een bepaalde termijn en op verzoek van het ICT-bedrijf alsnog in een aanvullende motivering wordt voorzien.
9. Te overwegen valt om de aanwijzing vooraf te laten gaan door een voornemen. Ten aanzien van het voornemen zou voorzien kunnen worden in een beperkte zienswijzemogelijkheid voor het ICT-bedrijf. Gedacht zou kunnen worden aan de mogelijkheid om binnen een termijn van bijvoorbeeld 2 uur aan te geven dat er sprake is van overmacht waardoor niet aan een eventuele aanwijzing voldaan kan worden of dat de voorgenomen aanwijzing op een evidente vergissing berust.
10. De aanwijzing levert een appellabel besluit als bedoeld in de Awb op.
11. Om een onnodige stapeling van bestuursrechtelijke procedures te voorkomen zou kunnen worden bepaald dat bezwaar en beroep tegen de aanwijzing zich mede uitstrekt over eventuele daaropvolgende sanctiebesluiten.

12. De normstelling houdt de verplichting in om aan de aanwijzing te voldoen. Het niet voldoen aan de aanwijzing kwalificeert dan als een overtreding naar aanleiding waarvan het bestuursrechtelijke sanctie-instrumentarium ingezet kan worden.

Voor wat betreft de handhaving van de betreffende normstelling hebben wij de verschillende bestaande bestuursrechtelijke sancties in beeld gebracht en hebben wij de daaraan in dit geval verbonden voor- en nadelen tegen elkaar afgewogen. Kort en goed hebben wij daarbij een onderscheid gemaakt tussen in Nederland gevestigde ICT-bedrijven en ICT-bedrijven die in het buitenland zijn gevestigd en in Nederland actief zijn.

Voor wat betreft de in Nederland gevestigde ICT-bedrijven zijn wij tot de conclusie gekomen dat als primaire sanctie de last onder bestuursdwang de meest geschikte sanctie lijkt. In dat verband is specifiek van belang dat die sanctie de mogelijkheid biedt dat de overheid zonder nadere begunstigingstermijn zelf (fysiek) de aan de orde zijnde overtreding beëindigt. Op die manier kan de sanctie eraan bijdragen om snel en zonder dat de verdere medewerking van de overtreder nodig is tot verwijdering van de betreffende KP over te gaan. Te overwegen valt om het bestuursorgaan tevens de bevoegdheid te geven om (al dan niet in combinatie met een last onder bestuursdwang) een bestuurlijke boete op te leggen. Een dergelijke boete kan namelijk een afschrikwekkend en/of diffamerend effect hebben en daarom een preventieve werking hebben. Indien een meer omvattend sanctiepakket zou worden overwogen kunnen wij ons voorstellen dat aanvullend nog wordt voorzien in het openbaar maken van de opgelegde sanctiebesluiten en (in de meest ernstige gevallen) het toepassen van een beroepsverbod. Bij het introduceren van een dergelijk meeromvattend sanctiestelsel is de evenredigheid van een dergelijk stelsel in abstracto en de toepassing die aan dat systeem in het individuele geval wordt gegeven een extra punt van aandacht.

Voor wat betreft de handhaving van buiten Nederland gevestigde ICT-bedrijven die in Nederland actief zijn, geldt het volgende. De last onder bestuursdwang is hier geen geschikte sanctie omdat Nederland geen bestuursdwang buiten de eigen landsgrenzen kan toepassen. Dat betekent dat de minder geschikte sancties van de last onder dwangsom en (vooral) de bestuurlijke boete resteren. Dergelijke sancties zullen niet direct leiden tot het verwijderen van de betreffende KP. Indien de overtreding niet wordt beëindigd ontstaat er voor de overtreder een bestuurlijke geldschuld. De mogelijkheden voor de Nederlandse overheid om zich te verhalen op de vermogensbestanddelen van het betreffende ICT-bedrijf. Voor verhaal in het buitenland is daartoe erkenning van de betreffende bestuurlijke geldschuld vereist. Bij de huidige stand van de regelgeving zien wij binnen noch buiten de EU-mogelijkheden om (de geldschulden voortvloeiend uit) bestuurlijke sancties erkend te krijgen. Wel geven wij in overweging om de Wet wederzijdse erkenning zodanig aan te passen dat in ieder geval bestuurlijke boetes binnen de EU erkend kunnen gaan worden.

Voor zover het betreffende ICT-bedrijf binnen Nederland al over vermogensbestanddelen beschikt, zal het in veel gevallen praktisch gezien erg complex zijn om daar effectief beslag op te doen leggen. Het zal immers veelal gaan om aanspraken jegens of betalingen van derden waarvan het bestaan niet bekend is of moeilijk te achterhalen zal zijn of (voor zover het tegoeden betreft) die slechts een ondeelbaar moment in Nederland zullen zijn.

Hoogachtend,