Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime

M.H.M. Schellekens
B.J. Koops
W.G. Teepe

Universiteit van Tilburg
TILT – Centrum voor Recht, Technologie en Samenleving
Cycris – Center for Cybercrime Studies
Postbus 90153
5000 LE Tilburg
e.j.koops@uvt.nl
m.h.m.schellekens@uvt.nl
w.teepe@cs.ru.nl

november 2007

Voorwoord

Dit onderzoek is uitgevoerd ten behoeve van het NICC (Nationale Infrastructuur Cyber Crime), i.e. een publiek-privaat samenwerkingsverband dat zich bezighoudt met de bestrijding van criminaliteit waarmee het bedrijfsleven in Nederland wordt geconfronteerd.

De auteurs willen graag dhr. August Nieland van de Directie Wetgeving van het Ministerie van Justitie en dhr. Bart den Hartigh van het Landelijk Parket bedanken voor de waardevolle input die zij voor dit onderzoek hebben geleverd. Tevens mag Prof. Bart Jacobs van de RU niet onvermeld blijven. De auteurs bedanken hem onder andere voor zijn zeer nuttige commentaren op eerdere versies van dit rapport.

Het onderzoek is afgesloten op 14 augustus 2007. De rapportage is afgerond op 30 november 2007.

Inhoudsopgave

Afkortingen

BVD	Binnenlandse VeiligheidsDienst
DNS	Domain Name System
gvo	gerechtelijk vooronderzoek
Gw	Grondwet
IP	Internet Protocol
ISP	Internet Service Provider
NTD	Notice and Take Down
OvJ	Officier van Justitie
PbEG	Publicatieblad van de Europese Gemeenschappen
r-c	rechter-commissaris in strafzaken
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering
Trb.	Tractatenblad
URL	Uniform Resource Locator

1. Inleiding

Directe aanleiding voor dit onderzoek vormt het regeerakkoord uit 2007, waarin de regering de volgende intentie uitspreekt:

> Teneinde radicaliserende boodschappen en voorlichting over de middelen van terreur te bestrijden, wordt voorzien in de mogelijkheid om het doorgeven van boodschappen door 'internet-providers' te verbieden.[1]

De intentie neergelegd in het regeerakkoord geeft aanleiding te bezien of er juridische instrumenten bestaan om internetaanbieders te verbieden haatzaai-informatie door te geven. Op dit moment bestaat er geen verbod voor ISP's om van derden afkomstige haatzaai-informatie via het Internet door te geven, behoudens bijzondere omstandigheden. In het bijzonder zijn zij niet verplicht het informatieaanbod dat op hun servers is opgeslagen of via hun systemen wordt door gegeven pro-actief te controleren op de aanwezigheid van haatzaai-informatie. Het is ook niet mogelijk een dergelijke monitorplicht in de Nederlandse wetgeving op te nemen. Art. 15 van de Europese Richtlijn inzake elektronische handel staat daaraan in de weg.[2]

Een juridisch gezien beter begaanbare weg is ISP's te wijzen op de aanwezigheid van bepaalde concrete, strafbare informatieaanboden in hun systemen om hen dusdoende te bewegen dat informatieaanbod ontoegankelijk te maken.[3] Gegeven deze insteek komt art. 54a Sr in beeld. Deze bepaling is ingevoerd in het Wetboek van Strafrecht (Sr) ter implementatie van de Richtlijn inzake elektronische handel en suggereert in zeker opzicht dat de Officier van Justitie de bevoegdheid heeft een ISP te bevelen dat hij concreet aangeduide haatzaai-informatie of andere strafbare informatieaanboden ontoegankelijk maakt.

De ratio van genoemde bepaling is tweeledig. Enerzijds voorziet de bepaling erin dat de ISP die het bevel tot ontoegankelijkmaking opvolgt niet vervolgbaar is voor (medeplichtigheid aan) het onderliggende strafbare feit, bijvoorbeeld de openbaarmaking van haatzaai-informatie. ISP's kunnen zich aldus volledig richten op de ontwikkeling van het Internet als hoeksteen van de informatie-samenleving zonder zich overmatig te hoeven bekommeren om hun eventuele aansprakelijkheid voor doorgegeven inhoud. Anderzijds dient art. 54a Sr de vrijheid van meningsuiting. Art. 54a Sr neemt het inhoudelijke oordeel over de strafbaarheid van een informatieaanbod uit handen van de ISP en legt het in handen van de rechter-commissaris (r-c) en de Officier van Justitie (OvJ). Daarmee wordt voorkomen dat een ISP uit vrees voor eigen aansprakelijkheid al te voortvarend te werk zou gaan bij het ontoegankelijk maken van informatieaanboden die in de ogen van de ISP wel eens strafrechtelijk bedenkelijk zouden kunnen zijn. De vrijheid van meningsuiting is een leidend beginsel bij deze regeling:

> Artikel 7 van de Grondwet geeft aan de overheid de opdracht de vrijheid van meningsuiting te waarborgen en te stimuleren. Censuur van staatswege dient te worden voorkomen. Artikel 54a beoogt het gevaar in te dammen dat de tussenpersoon, mede gelet op zijn in belang toenemende rol in het proces van gegevensuitwisseling door middel van communicatienetwerken, zich genoodzaakt voelt tot preventieve censuur over te gaan teneinde strafrechtelijke aansprakelijkheid te voorkomen. De regeling dient een onbelemmerde informatie-uitwisseling en daarmee een grondbeginsel van de democratische rechtsstaat.[4]

---

[1] http://www.avs.nl/upload_mm//51683/e/d/3/regeerakkoord_2007.pdf

[2] Richtlijn 2000/31/EG, *PbEG* L 178. Overweging 48 van de richtlijn zet de deur op een kier om Internetaanbieders specifieke zorgvuldigheisplichten op te leggen. Gegeven art. 15 van de richtlijn zal de mogelijkheid die overweging 48 opent uiterst beperkt moeten worden geinterpreteerd.

[3] Vergelijk ook *Kamerstukken II* 2004-2005, 29 754, nr. 5, p. 15.

[4] *Kamerstukken II* 2001-2002, 28 197, nr. 3, p. 63.

De betrokkenheid van r-c en OvJ is bedoeld als een waarborg dat uitsluitend 'echt' strafbare informatieaanboden ontoegankelijk worden gemaakt. In de praktijk blijkt overigens dat vooralsnog van de bepaling geen of nauwelijks gebruik wordt gemaakt.[5]

Het idee dat art. 54a Sr een instrument zou kunnen zijn ter verwezenlijking van de doelstelling als verwoord in het regeerakkoord stelt de bepaling in een nieuw licht. Niet de aansprakelijkheid van de ISP of de vrijheid van meningsuiting staat voorop, maar de bevelsbevoegdheid die kan worden gebruikt voor een 'grote schoonmaak' van het Internet. Het regeerakkord zou mee kunnen brengen dat de bevelsbevoegdheid structureel wordt ingezet om bepaalde informatie van het Internet te weren. Dat leidt tot twee vragen die tezamen de probleemstelling vormen van dit onderzoek:

1. Is art. 54a Sr een geschikt instrument om haatzaai-informatie en andere strafbare informatieaanboden van het Internet te weren?
2. Wat voor procedure is er nodig om het proces van *notice-and-take-down* efficiënt en juridisch verantwoord te laten verlopen?[6]

Dit onderzoek is een eerste stap in een drieledig onderzoek. Dit deel richt zich met genoemde vraagstelling op de juridische vragen die toepassing van art. 54a Sr in het licht van notice and take-down oproept. De daadwerkelijke inrichting van een *notice-and-take-down*procedure zal het voorwerp vormen van de twee vervolgstappen in het onderzoek.

In dit onderzoek wordt allereerst aandacht besteed aan enige juridische achtergronden van strafbare informatieaanboden op het Internet en de verantwoordelijkheid van de Internetaanbieder daarin. Daarbij wordt tevens bezien wat de Internetaanbieder in technisch opzicht kan doen ter beperking van strafbare informatieaanboden en waar de grenzen van zijn mogelijkheden liggen. Na het 'voorwerk' worden de juridische vragen aangesneden. Achtereenvolgens komen aan de orde: de grondslag voor de bevelsbevoegdheid (Hfst. 3), materiële en procedurele juridische vragen (Hfst. 4), jurisdictievragen (Hfst. 5) en praktische vragen (Hfst. 6). Hoofdstuk 7 bevat, naast de conclusies, enkele aanbevelingen.

Voor de beantwoording van de juridische deelvragen worden afhankelijk van de mate waarin de desbetreffende deelvraag zich daarvoor leent verschillende methoden gebruikt. De in aanmerking genomen methoden zijn:

- wetshistorische analyse, waarbij naast de nationale wetsgeschiedenis met name ook de Europese Richtlijn inzake elektronische handel betrokken wordt, ter implementatie waarvan art. 54a in het Nederlandse Wetboek van Strafrecht is opgenomen.
- Horizontale vergelijking met vergelijkbare vragen in het privaatrecht. Ook in de privaatrechtelijke context doet zich de vraag voor of een Internetprovider gehouden is materiaal offline te halen. Met inachtneming van de noodzakelijke verschillen die er tussen privaat- en strafrecht bestaan en tussen de typen inhoud die civiel- dan wel strafrechtelijk aan de orde worden gesteld, zijn oplossingrichtingen en argumenten te distilleren uit de civielrechtelijke rechtspraak, die een hogere vlucht heeft genomen dan de strafrechtelijke.
- Wetsystematische vergelijking. Art. 54a Sr maakt deel uit van een Wetboek dat systematisch is opgezet en waarin termen in dezelfde betekenis worden gebruikt.
- Vanwege het ontbreken van jurisprudentie over art. 54a Sr zelf, zal strafrechtelijk jurisprudentieonderzoek geen zelfstandige onderzoeksmethode zijn.

[5] Mondelinge mededeling A. Nieland (Directie wetgeving, Ministerie van Justitie) op 26 juni 2007.
[6] Vgl. *Kamerstukken II* 2001-2002, 28 197, nr. 3, p. 26: De richtlijn roept de lidstaten op om aan te moedigen dat op basis van vrijwillige overeenkomsten tussen alle betrokken partijen de uitwerking ter hand wordt genomen van snelle, betrouwbare mechanismen om onwettige informatie te verwijderen en ontoegankelijk te maken (preambule 40).

Voor wat betreft de technische vragen vindt een marginale toets plaats, die ten doel heeft duidelijk te maken of de maatregelen die op juridische gronden aan de Internetaanbieder worden opgedragen technisch uitvoerbaar cq. haalbaar zijn.

2. Achtergronden van ontoegankelijkmaking

2.1. Juridische achtergronden

2.1.1. De betrokken actoren

Bij het aanbieden van informatie op het Internet en het eventuele ontoegankelijk maken van de desbetreffende informatie zijn vele partijen betrokken. In de eerste plaats is er degene die de informatie op het Internet aanbiedt, zoals de houder van een webpagina. Deze actor wordt in dit rapport de inhoudsaanbieder genoemd. Het informatieaanbod van de inhoudsaanbieder is toegankelijk voor andere Internetgebruikers door tussenkomst van een groot aantal Internetaanbieders, die de technische infrastructuur verzorgen. De Internetaanbieders worden in dit rapport ook wel aangeduid met de Engelstalige afkorting ISP, hetgeen staat voor 'Internet Service Provider'. Met het gebruik van de ene of de andere term is geen betekenisverschil bedoeld; beide termen worden door elkaar gebruikt. Derden kunnen bezwaar hebben tegen een informatieaanbod van een inhoudsaanbieder, bijvoorbeeld omdat zij constateren dat er inbreuk wordt gemaakt op hun intellectuele eigendomsrechten of dat een webpagina haatzaai-informatie bevat. Indien een derde zijn bezwaar vervat in een notificatie die hij naar de ISP of een meldpunt voor Internet-informatie stuurt, noemen we de derde een notificeerder. Indien het informatieaanbod waartegen bezwaar bestaat in strafrechtelijke zin 'verdacht' is kan een Officier van Justitie (OvJ) een opsporingsonderzoek met betrekking tot het betreffende informatieaanbod ondernemen. Indien tijdens een opsporingsonderzoek vergaande – bijvoorbeeld op grondrechten inbreuk makende – opsporingshandelingen verricht moeten worden dan vereist de wet vaak dat een rechter-commissaris in strafzaken betrokken wordt bij de uitoefening van die strafvorderlijke bevoegdheden. Deze functionaris wordt in dit rapport aangeduid als de 'rechter-commissaris' of afgekort als 'r-c'.

2.1.2. Strafbare feiten op het Internet

Op of met behulp van het Internet kunnen velerlei strafbare feiten gepleegd worden. Zo kunnen bijvoorbeeld via het Internet virussen verspreid worden, of e-mail berichten die onderweg zijn zouden door onbevoegden gelezen kunnen worden. In dit rapport gaat het echter om het openbaar aanbieden van informatie op het Internet welk aanbod op enigerlei grond strafrechtelijk niet oirbaar is. Voorbeelden zijn het aanbieden van opruiende uitingen, auteursrechtinbreuken, smaad of oplichtingspagina's. De belangen die via de afzonderlijke strafbepalingen beschermd worden lopen zeer uiteen. Opruiing is strafbaar ter bescherming van de (openbare) orde, auteursrechtinbreuk voornamelijk ter bescherming van de economische belangen van de rechthebbende, smaad ter bescherming van de eer of goede naam van het slachtoffer, en oplichting ter bescherming van economische belangen van de opgelichte.

In dit rapport wordt meer dan eens gesproken over haatzaaien. De strafbaarstelling die dit het dichtst benadert is art. 137d Sr: het aanzetten tot haat, discriminatie of geweld tegen personen wegens hun ras, religie, geslacht, sexuele geaardheid of handicap. Daarnaast is er nog een aantal strafbepalingen die een aanvullende rol zouden kunnen spelen bij het aanpakken van haatzaai-pagina's:

1. opruiing: het oproepen tot het plegen van misdrijven of geweld (art. 131 Sr);
2. belediging van een bevolkingsgroep wegens ras, religie, sexuele geaardheid of handicap (art. 137c Sr, zie ook art. 137e, 137f Sr);
3. smalende godslastering (art. 147,147a Sr).

Degene die de informatie op het Internet aanbiedt kan in het algemeen als de pleger van de desbetreffende feiten gezien worden. Om de informatie op het Internet aan te kunnen bieden

heeft de inhoudsaanbieder de technische hulp nodig van Internetaanbieders die hetzij de serverruimte aanbieden waarop de gegevens geherbergd worden, hetzij de verbindingsfaciliteiten aanbieden waarmee de gegevens getransporteerd kunnen worden. Door de positie die ze innemen zijn Internetaanbieders vaak in staat de gegevens die deel uitmaken van een informatieaanbod op het Internet ontoegankelijk te maken en zo wellicht het informatieaanbod zelf te beëindigen.

2.1.3. De aansprakelijkheid van de Internetaanbieder

Kan het niet-gebruiken van de middelen die een Internetaanbieder heeft om in te grijpen in een strafbaar informatieaanbod leiden tot mede-aansprakelijkheid van de Internetaanbieder voor een strafbaar informatieaanbod? In het strafrecht kan naast de eigenlijke pleger van een strafbaar feit ook degene die medeplichtig is aan het feit gestraft worden (art. 48 Sr):

> Als medeplichtigen van een misdrijf worden gestraft:
> 1°. zij die opzettelijk behulpzaam zijn bij het plegen van het misdrijf;
> 2°. zij die opzettelijk gelegenheid, middelen of inlichtingen verschaffen tot het plegen van het misdrijf.

Zoals uit de tekst van het wetsartikel blijkt is de medeplichtige aan een strafbaar feit slechts strafbaar als hij opzettelijk heeft gehandeld. Internetaanbieders over het algemeen – en zeker de grotere – zijn niet op de hoogte van de afzonderlijke informatieaanboden van hun abonnees en andere Internetgebruikers. Daarmee zal in de meeste gevallen het opzet ontbreken en de Internetaanbieder niet strafbaar zijn. Indien echter de Internetaanbieder een notificatie ontvangt van een derde (een bezorgde burger, een opsporingsambtenaar, het slachtoffer etc.) over de aanwezigheid van een strafbaar informatieaanbod op een van zijn servers, dan kan er wetenschap van een strafbaar feit bij de Internetaanbieder ontstaan. Dat is bijvoorbeeld het geval als de notificatie voldoende duidelijk maakt over welk informatieaanbod op zijn server het gaat, wat het strafrechtelijk relevante bezwaar is tegen de informatie en er voldoende duidelijkheid bestaat over de daadwerkelijke strafbaarheid van het informatieaanbod. Het is helder dat een Internetaanbieder in zo een geval op moet treden tegen het informatieaanbod om te voorkomen dat hij zelf in de strafrechtelijke gevarenzone belandt.

In beginsel biedt het traditionele strafrecht dan ook voldoende handvatten om:

1. de strafrechtelijke aansprakelijkheid van de Internetaanbieder zodanig te beperken dat een normaal zorgvuldig handelend Internetaanbieder niet aansprakelijk is, maar ook om
2. de Internetaanbieder te bewegen om aan NTD mee te werken.

In 2000 is de Europese Richtlijn inzake elektronische handel uitgevaardigd. Deze richtlijn bevat een regeling over de aansprakelijkheid van bepaalde dienstverleners in de informatie-maatschappij. Hoewel de richtlijn zelf de term Internetaanbieders niet hanteert, worden hier de bedoelde dienstverleners voor het gemak wel als Internetaanbieders aangeduid. De strekking van de regeling is niet om aansprakelijkheid van Internetaanbieders te vestigen, maar om hieraan – geharmoniseerd – grenzen te stellen.[7] In Nederland is de aansprakelijkheidsbeperking voor wat de strafrechtelijke aansprakelijkheid betreft geïmplementeerd door toevoeging van nieuw artikel aan het Wetboek van Strafrecht:

> **Art. 54a Sr**
>
> Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken.

Het belangrijkste effect van de invoering van art. 54a Sr voor Internetaanbieders is een vergroting van hun rechtszekerheid. De OvJ en r-c nemen – bij toepassing van art. 54a Sr – de Internetaanbieder het soms moeilijke oordeel over de strafbaarheid van een

[7] Zie M.H.M. Schellekens, Aansprakelijkheid van Internetaanbieders, Den Haag: SDU 2001, hfst. 10.

informatieaanbod uit handen. Komen r-c en OvJ tot de conclusie dat er sprake is van een strafbaar informatieaanbod, dan kan de OvJ de Internetaanbieder een bevel geven om de informatie van het net te halen. De Internetaanbieder moet dat bevel opvolgen, wil hij niet meer vervolgbaar zijn voor of in verband met het in het informatieaanbod gelegen delict. In hoofdstuk 3 zal bekeken worden of een OvJ inderdaad de bevoegdheid heeft om een bevel als bedoeld in art. 54a Sr te geven.

2.2 Technische aspecten van ontoegankelijkmaking

Zoals hiervoor al bleek is een ISP een bedrijf of organisatie die Internetdiensten levert en beheert voor afnemers. De afnemers kunnen toegang krijgen tot de geleverde diensten via de ISP, waarmee de ISP een zekere machtspositie heeft jegens de afnemer. De ISP is technisch gesproken bijvoorbeeld in staat de afnemer toegang tot de diensten te ontzeggen, en ook om een andere partij toegang tot diezelfde diensten te geven.

Het is deze feitelijke machtspositie van de ISP die de ISP tot een interessante partner maakt voor rechtshandhaving op het Internet. Door de toegang tot de geleverde diensten te blokkeren, kan een ISP ongewenst materiaal “offline halen”, bijvoorbeeld door al het webverkeer naar de website van een specifieke klant te blokkeren.

Niet alleen de machtspositie maakt de ISP tot een interessante partner, maar ook zijn relatief eenvoudige identificeerbaarheid. Voor een willekeurig stukje materiaal op het Internet is het in de regel bijzonder moeilijk om te achterhalen wie het online heeft gezet, mede omdat dat in het verleden is gebeurd. Daarentegen is het meestal redelijk eenvoudig om te achterhalen welke ISP of ISP’s het online zijn van dat materiaal faciliteren.

De combinatie van identificeerbaarheid en technische macht bij een ISP zorgt ervoor dat een informatieaanbod kan worden opgeheven zonder dat de inhoudsaanbieder hoeft te worden gevonden of mee hoeft te werken. Het is dan ook niet verwonderlijk dat partijen die bezwaar hebben tegen materiaal dat op het Internet aanwezig is vaak hun weg weten te vinden naar ISP’s.

Aan een ingrijpen door een ISP in het informatieaanbod van een ander kleven echter bezwaren. De inhoudsaanbieder zal doorgaans een belang hebben bij het voortduren van zijn informatieaanbod en dat belang wordt uiteraard geschaad indien de ISP zijn informatieaanbod ontoegankelijk maakt. Indien het desbetreffende informatieaanbod onrechtmatig of zelfs strafbaar is, dan is de schade aan het belang van de inhoudsaanbieder doorgaans juridisch goed te verantwoorden. Dat wordt anders indien het weggehaalde informatieaanbod niet onrechtmatig is. Dat informatie wordt weggehaald waartegen juridisch geen bezwaar bestaat is overigens geen theoretisch risico. Zo kan er onduidelijkheid bestaan over de juridische status van een informatieaanbod (een aanbod dat onrechtmatig leek, kan achteraf door de rechter rechtmatig bevonden worden), maar het kan ook zijn dat de technische maatregelen tot ontoegankelijkmaking van de ISP onvoldoende fijnkorrelig zijn. In het laatste geval wordt samen met het beoogde onrechtmatige materiaal ook ander materiaal waartegen geen bezwaar bestaat weggehaald. In dit verband spreken we hierna van bijvangst.

Bij het ontoegankelijk maken van internetpagina’s kunnen drie situaties onderscheiden worden:

- De webpagina staat op een server van de ISP
- De webpagina staat op de server van de klant en de ISP is slechts de pijp waarmee de server van de klant met het Internet is verbonden.
- De webpagina staat op de server van een derde (bijvoorbeeld in het buitenland).

a. De webpagina staat op een server van de ISP

Dit is een relatief eenvoudig geval. Het zal vaak gaan om de "kleinere" websites van particulieren. Dit zijn meestal statische webpagina's; dat zijn webpagina's waarvan de inhoud niet afhankelijk is van door de bezoeker van de pagina ingevoerde parameters, zoals zoekwoorden. De webpagina correspondeert met een of meer unieke bestanden en geeft bij bezoek altijd dezelfde inhoud weer. De bestanden die de inhoud van de pagina vormen staan in het algemeen op de server van de ISP. De ISP heeft daarmee directe toegang tot de gegevens van de websites, en kan ze relatief makkelijk ontoegankelijk maken. Het blijft natuurlijk zo dat dit enig zoekwerk kost, zeker om bijvangst te verhinderen. Maar de ISP zou gewoon botweg kunnen zeggen: een klant met illegaal materiaal sluit ik helemaal af.
Het wordt ingewikkelder indien de informatie die online wordt aangeboden dynamisch wordt gegenereerd. Dat betekent dat er een duidelijke scheiding is aangebracht tussen de computer die de webpagina aanbiedt en de computer waarop de inhoud van de webpagina wordt bewaard. Een eenvoudig voorbeeld is een online telefoongids van een bedrijf, waar de pagina's met de telefoonnummers niet als losse bestanden bestaan, maar de pagina pas wordt aangemaakt op het moment dat iemand een nummer opzoekt. De telefoonnummers worden op dat moment rechtstreeks uit de personeelsadministratie gehaald.

Essentieel voor dergelijk dynamisch aangeboden webpagina's is (1) dat de technische infrastructuur die nodig is om een webpagina aan te bieden uit verschillende stukken bestaat, en (2) dat er detaillistische kennis nodig is om de exacte informatiebron van een webpagina te lokaliseren.

Een dergelijke infrastructuur bestaat typisch uit een "webserver" (bezoekers vanaf het Internet leggen contact met deze webserver) en een "back-end" waarin de feitelijke informatie opgeslagen is. In het bovengenoemde voorbeeld is de personeelsadministratie de *back-end*.

Zo'n situatie doet zich bijvoorbeeld voor wanneer een klant een server huurt in een rack in een serverruimte van een ISP. Typisch staat de backend van de database daar dan in de buurt.

Het feit dat de technische infrastructuur uit meerdere delen bestaat, is een bron van allerlei mogelijke complicaties. Door het verwijderen van de webserver kan een gewraakte pagina onbereikbaar gemaakt worden, maar de gewraakte inhoud van de pagina wordt op deze manier niet uit de *back-end* gewist. Als de *back-end* verbonden is met meerdere webservers, zal na het verwijderen van één webserver de gewraakte inhoud nog steeds online toegankelijk zijn. De *back-end* en de webserver kunnen eigendom zijn van verschillende organisaties. Ook kunnen de webserver en de *back-end* door verschillende ISP(-ketens) beheerd worden. Ook kan de *back-end* op zichzelf weer een andere webserver zijn, waarmee een keten van dynamisch gegenereerde webpagina's ontstaat.

Het is vaak niet aan een webpagina af te zien of de inhoud dynamisch gegenereerd wordt. Het is in de regel niet aan een dynamische webpagina af te zien uit welke *back-end* deze zijn informatie haalt. Het gericht verwijderen van één webpagina door het aanpassen van de webserver kan slechts in beperkte gevallen. Daarbij is specialistische kennis over de technische structuur van de webpagina nodig. Het gericht verwijderen van één webpagina door het aanpassen van de *back-end* is doorgaans stukken eenvoudiger, maar vereist specialistische kennis over de technische structuur van de *back-end*.

Voor het gericht verwijderen van bepaalde inhoud is in de regel de medewerking van de beheerder van de *back-end* nodig. Deze beheerder kan meestal alleen door de beheerder van de webserver gevonden worden. Het is niet gegeven dat de beheerder van een webserver de *back-end* zonder meer zal willen, mogen of kunnen onthullen. In voorkomende gevallen zullen hiervoor strafvorderlijke bevoegdheden moeten worden ingezet.

b. De webpagina staat op de server van de klant en de ISP is slechts de pijp waarmee de server van de klant met het Internet is verbonden.

Grotere klanten van ISPs willen vaak het beheer van hun webpagina's volledig in eigen hand houden. Ze richten dan zelf een webserver in die via een ISP met het Internet is verbonden. In geval van dynamische gegenereerde webpagina's heeft een webserver bij de klant ook voordelen voor een ISP. ISPs stellen de mogelijkheden voor het maken van dynamische websites op hun eigen webservers niet graag beschikbaar. Daarvoor moeten de klanten namelijk executierechten hebben op de servers van de ISP, wat allerlei veiligheidsrisico's met zich meebrengt. Als het aankomt op het ontoegankelijk maken van webpagina's die op de server van een klant staan heeft de ISP weinig macht. Het enige wat hij kan zeggen is: als je dat-en-dat niet weg haalt sluit ik je pijp helemaal af (d.w.z. "poort 80" wordt gesloten, waarmee de volledige website van de klant onbereikbaar wordt). Het is duidelijk dat dit vergaande consequenties heeft voor de klant. Er moeten wel heel dringende redenen zijn tot een dergelijke afsluiting over te gaan. Het ligt in een dergelijk geval dan ook meer voor de hand dat de notificeerder dan wel de OvJ zich rechtstreeks richt tot de klant.

c. De webpagina staat op de server van een derde (bijvoorbeeld in het buitenland) en de ISP probeert te voorkomen dat zijn klanten de webpagina bezoeken.

In dit geval wordt het ongewenste materiaal niet verwijderd, maar wordt getracht om netwerkconnecties die het ongewenste materiaal transporteren af te sluiten, door middel van een soort firewall. Een Internetconnectie is een tijdelijke verbinding die tussen het bladerprogramma van de webgebruiker en de webserver van de gezochte webpagina wordt aangelegd om informatie uit te wisselen.

Er zijn verschillende technieken die zouden kunnen worden ingezet om ongewenst materiaal op netwerkniveau te blokkeren. De belangrijkste zijn de volgende.

- IP-blocks (traditionele firewall). Alle verkeer van en naar een bepaald IP-adres wordt tegengehouden. Technisch gezien is dit vrij eenvoudig uit te voeren. In heel veel gevallen zitten er achter één IP-adres echter meerdere webpagina's, waardoor de bijvangst doorgaans bijzonder groot zal zijn. Ook kan een webpagina (expres) gebruik maken van meerdere IP-adressen, waardoor de bijvangst nog groter wordt.
- URL-filtering (*transparent proxy*). Alle Internetverkeer dat te maken heeft met webpagina's wordt "geopend", en elke opgevraagde URL wordt vergeleken met een zwarte lijst van verboden webpagina's. Technisch gezien is dit een bijzonder dure oplossing, omdat vrijwel alle Internetverkeer moet worden gescand. Dit vergt veel extra apparatuur bij de ISP's, en is daardoor kostbaar. Wel is deze techniek erg selectief: er zal relatief weinig bijvangst zijn. De keerzijde is dat deze techniek grote privacy-implicaties kan hebben omdat er als het ware een tussenstation wordt geschapen waar de inhoud van het dataverkeer technisch redelijk makkelijk in te zien is.
- DNS-filtering. De meta-informatie over webpagina's, namelijk op welk IP-adres de bijbehorende webservers te vinden zijn, wordt aangepast. De technische complexiteit hiervan zit tussen die van de bovengenoemde technieken in. De bijvangst beperkt zich tot de webpagina waarop het ongewenste materiaal zich bevindt. Een belangrijk nadeel van deze methode is wel dat het de integriteit van het DNS-systeem aantast, waardoor de betrouwbaarheid van Internetverkeer op het spel komt te staan.

Door dit type technieken te gebruiken kan ervoor gezorgd worden dat argeloze surfers niet met ongewenst materiaal geconfronteerd zullen worden. Deze technieken zijn echter redelijk eenvoudig te omzeilen.

In de westerse wereld worden deze technieken dan ook niet ingezet vanwege het belang van de vrije meningsuiting (art. 7 Gw, art. 10 EVRM), behalve dan voor het blokkeren van kinderporno-webistes. Ook staat art. 15 van de Europese Richtlijn inzake elektronische handel een algemene filterplicht in de weg. Het inzetten van dit type technieken is wel

kenmerkend voor staten waarin minder belang wordt gehecht aan de vrijheid van meningsuiting. Het bekendste voorbeeld van toepassing van deze technieken is China, waar de overheid deze technieken gebruikt om haar onwelgevallige onderwerpen van het Internet te weren. De Chinese ISP's en dissidente surfers en bloggers voeren een continu gevecht inzake de omzeilingstechnieken.

Het filteren op het netwerkniveau is al met al geen haalbare kaart. Technisch gezien wordt óf de bijvangst óf de benodigde investeringen en de inbreuk op de privacy erg groot. Daarnaast zijn de technieken redelijk eenvoudig te omzeilen. Het is mede vanwege de beperkingen aan fijnmazigheid een vorm van censuur die juridisch bedenkelijk is.

2.2.3. Over subsidiariteit, effectiviteit en bijvangst

De vraag hoe ingrijpend en effectief het van Internet verwijderen van illegaal materiaal is, hangt van een aantal factoren af.

De hoeveelheid bijvangst. In het ideale geval verandert er bij het verwijderen van illegaal materiaal niets, behalve dan dat het ongewenste materiaal ontoegankelijk is gemaakt. Er is dan niets anders wat door de ingreep ontoegankelijk wordt gemaakt of anderszins schade ondervindt ("collateral damage").

De kennis en expertise om materiaal te verwijderen zonder dat daarbij bijvangst ontstaat is doorgaans alleen aanwezig bij de beheerder van de webpagina, en in het geval van een dynamische webpagina bij de beheerder van de *back-end*.

Als men om informatie te verwijderen zich niet richt op deze beheerder zelf, maar op de ISP van de beheerder, dan is het onontkoombaar dat er sprake zal zijn van bijvangst.
De hoeveelheid bijvangst hangt erg af van hoeveel moeite die getroost wordt om bijvangst te beperken. De mogelijkheden zijn niet alleen beperkt door geïnvesteerde moeite, maar ook door technische mogelijkheden. Als we een onderscheid maken naar de drie eerder beschreven situaties, dan zien we het volgende:

- De webpagina staat op een server van de ISP: Als het om een bijzonder eenvoudige webpagina gaat, is het mogelijk dat met enige inspanning er géén bijvangst zal zijn. Bij dynamisch gegenereerde webpagina's is dit op zijn best moeilijk, in de praktijk onmogelijk; de bijvangst zal dan minstens een heel domein zijn.
- De webpagina staat op de server van de klant en de ISP is slechts de pijp waarmee de server van de klant met het Internet is verbonden: de hoeveelheid bijvangst is de volledige website van de klant, mogelijk bestaand uit meerdere domeinen.
- De webpagina staat op de server van een derde (bijvoorbeeld in het buitenland): de bijvangst is minstens een heel domein, maar vaak vele malen groter.

Kortom, de bijvangst zal doorgaans minstens een heel *domein* zijn: een complete website met alles wat daaronder hangt. Voor het blokkeren van pagina's die buiten Nederland geherbergd worden kan alleen op netwerkniveau worden ingegrepen, waardoor de bijvangst snel vele malen groter wordt dan één enkele domeinnaam.

De effectiviteit. In het ideale geval is met het ontoegankelijk maken van het gewenste materiaal, het materiaal ook voorgoed van Internet verdwenen. De praktijk van de afgelopen jaren leert echter dat pogingen om materiaal offline te halen voor een tegenbeweging zorgen. Wanneer materiaal van het net is gehaald of dreigt te worden gehaald, zetten vele mensen over de hele wereld "mirror sites" op, kopieën van het materiaal in kwestie. Bekende voorbeelden hiervan zijn de Radikal-webpagina (waarop informatie te vinden was hoe men

het Duitse spoorwegennet zou kunnen saboteren), Scientology-documenten, en codes om dvd-beveiligingen te kraken.

In de regel kunnen partijen wier materiaal offline wordt gehaald op een bijzonder grote sympathie van burgerrechtenbewegingen en individuele sympathisanten rekenen, ook wanneer het materiaal zelf van discutabele aard is. Hoewel er zeer weinig voorstanders zullen zijn van sabotage van het Duitse spoorwegennet en velen het kraken van dvd-beveiligingen veroordelen, wordt het corresponderende materiaal vaak zonder aanzien des inhouds door sympathisanten en activisten voor vrijheid van meningsuiting vermenigvuldigd.

Het offline halen zelf genereert ook aandacht die het materiaal anders niet zou krijgen. Als de informatie in de bovenstaande voorbeelden niet offline zou zijn gehaald, zou deze informatie waarschijnlijk sneller in de vergetelheid zijn geraakt, terwijl zij nu actief in de aandacht wordt gehouden.

Kortom, het offline halen van informatie kan zich als een boemerang tegen de overheid keren. Wanneer materiaal offline wordt gehaald is de kans wezenlijk dat het op zoveel plekken opduikt dat het niet meer praktisch te bestrijden is. Bovendien krijgt het materiaal op deze wijze veel gratis publiciteit, waarmee het offline halen zijn eigen doel voorbij streeft. Dit effect zal vooral optreden bij bepaalde typen inhoud, zoals haatzaai-, discriminatie- en smaadpagina's alsmede pagina's met auteursrechtinbreuken, vanwege de aanwezigheid op het wereldwijde web van een actieve groep vrijemeningsuitings- en anti-DRM-activisten. Voor andere typen inhoud, zoals kinderporno en *phishing*-pagina's, zal dit effect minder optreden.

Het on line houden van een website heeft ook concrete voordelen voor de overheid die verloren gaan bij ontoegankelijkmaking. Zolang een webpagina in de lucht is kan zij door de autoriteiten gemonitord worden bijvoorbeeld door te kijken wie de webpagina bezoeken, of door kennis te nemen van de inhoud van de webpagina en de veranderingen die daarin worden aangebracht in de loop van de tijd. Ontoegankelijk maken houdt dan ook een verlies van monitoring mogelijkheden in. Bovendien bestaat het risico dat eventuele loksites van de eigen of andere inlichtingendiensten uit de lucht gehaald worden.

Subsidiariteit. Het principe van subsidiariteit brengt mee dat bijvangst bij het offline halen van materiaal zoveel mogelijk moet worden voorkomen. In de praktijk betekent dit maatwerk en mensenwerk, en dat kost tijd en geld. Er kan in de praktijk dus niet een zwarte lijst van webpagina's zijn, die met een spreekwoordelijke druk op de knop kan worden bijgehouden. Elke blokkade van informatie vergt een hoeveelheid handwerk. Er zullen in de regel dan ook dagen verstrijken tussen het signaleren van de aanwezigheid van ongewenst materiaal en het offline zijn van het ongewenste materiaal.

2.2.4. Conclusie

Bij het offline halen van ongewenst materiaal is er een belangrijk onderscheid: de (letterlijke en figuurlijke) aanspreekbaarheid van de server waar het materiaal wordt geherbergd. Als die bijvoorbeeld in het buitenland staat, kan het materiaal alleen maar geblokkeerd worden door het filteren op netwerkniveau. Daar kleven grote bezwaren aan: het is technisch ingrijpend, het is een vorm van actieve censuur, het levert veel bijvangst op, en het is juridisch moeilijk te verantwoorden.

Als het materiaal binnen Nederland wordt gehost, is er wel een mogelijkheid dit "bij de bron" ontoegankelijk te maken. Om de hoeveelheid bijvangst te beperken en voldoende effectiviteit te sorteren, moet het principe van subsidiariteit worden aangelegd. Dat betekent maatwerk en mensenwerk, en dat kost tijd en geld. Dit legt natuurlijke grenzen op aan de mate waarin dit middel kan worden ingezet. Het hangt van het soort materiaal af en de redenen van de ongewenstheid van dit materiaal, alsmede van de succeskans qua effectiviteit, of het weghalen voldoende belang heeft om de kosten, zowel de materiële als immateriële, te rechtvaardigen.

2.3. Conclusie

Uit de juridische en technische achtergronden blijkt dat het weghalen van strafbaar materiaal van het Internet door ISP's via een *notice-and-take-down*procedure juridische aanknopingspunten kent, met name bij art. 54a Sr in relatie tot de aansprakelijkheid van ISP's, maar dat er de nodige technische haken en ogen zitten vanuit het oogpunt van effectiviteit, subsidiariteit en proportionaliteit.

In dit onderzoek gaan we verder niet in op de vragen rond effectiviteit en subsidiariteit – die in de vervolgfase van dit onderzoek aan de orde zullen komen – maar beperken we ons tot de juridische aspecten van een NTD-procedure die samenhangen met art. 54a Sr.

3. De wettelijke grondslag voor een NTD-bevelsbevoegdheid

Het geven van een NTD-bevel zal vaak een grotere of kleinere inbreuk op de vrijheid van meningsuiting betekenen. Het is daarom van belang dat er een gedegen grondslag voor het NTD-bevel bestaat. In dit hoofdstuk wordt eerst een aantal mogelijke grondslagen geïnventariseerd. Vervolgens worden de reële kandidaten onder de geïnventariseerde grondslagen – art. 54a Sr en art. 125o Sv – aan een nadere analyse onderworpen.

3.1. Mogelijke grondslagen

Hiervoor is aangegeven dat een tussenpersoon niet vervolgbaar is voor het in een informatieaanbod gelegen strafbaar feit van een derde indien hij voldoet aan een bevel van de OvJ om de gegevens die deel uitmaken van het informatieaanbod ontoegankelijk te maken. Hier wordt de vraag beantwoord of een grondslag voor de bevelsbevoegdheid van de OvJ kan worden geïdentificeerd.

Om op deze vraag een antwoord te geven is in de eerste plaats nodig te bezien wat de aard is van een NTD-bevel. Het gaat dan met name om de vraag of het als een handeling in de sfeer van de opsporing of in de sfeer van administratieve handhaving gezien moet worden. Art. 132a Sv definieert wat onder opsporing moet worden verstaan:

> Onder opsporing wordt verstaan het onderzoek in verband met strafbare feiten onder gezag van de officier van justitie met als doel het nemen van strafvorderlijke beslissingen.

Kenmerkend voor opsporing is dus dat er een redelijk vermoeden bestaat dat een strafbaar feit is gepleegd[8] en dat het doel is het nemen van een strafvorderlijke beslissing. Een opsporingshandeling is dus ruimer dan het enkele onderzoek ter 'oplossing' van een misdrijf. Ook het inbeslagnemen van een Porsche van een verdachte van bedrieglijke bankbreuk (om die bij veroordeling verbeurd te laten verklaren) of het ontoegankelijk maken van op een computer aangetroffen kinderporno (ter onttrekking aan het verkeer) valt onder opsporing: er is sprake van een strafbaar feit en het doel is een strafvorderlijke beslissing (namelijk verbeurdverklaring of onttrekking aan het verkeer).

Evenzo moet een NTD-bevel worden gezien als een opsporingshandeling. De bevelsbevoegdheid zal alleen dan worden uitgeoefend waar sprake is van een (redelijk vermoeden van een) concreet strafbaar informatieaanbod, en de bevoegdheid heeft hetzelfde doel als het ontoegankelijk maken van aangetroffen onrechtmatige gegevens (art. 125o Sv), namelijk een einde te maken aan het strafbare feit.[9] Volgens ons is een NTD-bevel daarom een opsporingshandeling.

Een Officier van Justitie kan in dat licht niet zo maar tot ontoegankelijkmaking of een bevel tot ontoegankelijkmaking overgaan. Volgens de Commisie van Traa dient er bij het verrichten van gerichte opsporingshandelingen ten aanzien van bepaalde personen

> een specifieke bevoegdheid tot voor het toepassen van een opsporingsmethode te zijn, zeker indien er twijfel kan bestaan over de vraag of er sprake is van inbreuken op de rechten van burgers. De commissie overweegt daarbij dat opsporingsambtenaren niet al datgene mogen doen wat de gewone

[8] Misdrijven die in georganiseerd verband worden beraamd of gepleegd en aanwijzingen van terroristische misdrijven laten we hier verder buiten beschouwing.

[9] Het is ook mogelijk om een NTD-bevel als een bestuurlijke maatregel te construeren, vergelijkbaar met bijvoorbeeld bestuurlijke maatregelen in verband met terrorisme (zoals een gebiedsverbod of meldplicht). Er bestaat momenteel geen bestuurlijke wetgeving waarop een NTD-bevel zou kunnen worden gebaseerd, zodat in het bestuursrecht geen grondslag kan worden gevonden voor het bevel als genoemd in art. 54a Sr.

> burger vrijstaat. Opsporingsambtenaren handelen immers niet als gewone burgers. Als overheidsdienaren zijn zij gebonden aan specifieke regels, die bij of krachtens de wet voorzien zijn.[10]

Nu het toepassen van een bevel tot ontoegankelijk maken van Internet-informatie vaak de vrijheid van meningsuiting in het geding zal zijn, is er alle reden aan het uitgangspunt van de commissie-van Traa vast te houden.

Wat zijn kandidaten voor de grondslag voor de bevoegdheid tot ontoegankelijkmaking dan wel een bevel tot ontoegankelijkmaking? Art. 2 Politiewet impliceert een algemene bevoegdheid tot opsporingshandelingen met een geringe inbreuk op grondrechten (zoals niet-stelselmatige observatie of een vuilnissnuffel). Bij een bevel om gegevens van het Internet te halen gaat het echter om een aanzienlijke potentiële inbreuk op grondrechten, namelijk de vrijheid van meningsuiting.[11] Dat geldt niet alleen voor het weghalen van materiaal in het 'grijze gebied' (valt een uiting wel of niet onder haatzaaien, smaad of discriminatie? Is een foto van de kunstenaar met zijn zoontje kinderporno of een kunstuiting?), maar ook voor materiaal dat onmiskenbaar onrechtmatig is: het weghalen van een pagina die Joden discrimineert of de koningin beledigt perkt immers de vrije meningsuiting in.[12] Meestal zal er dus sprake zijn van een inbreuk op artikel 10 lid 1 EVRM (de vrije meningsuiting), die overigens gerechtvaardigd kan zijn op basis van artikel 10 lid 2 EVRM (want bij wet voorzien en noodzakelijk in een democratische samenleving). Artikel 2 Politiewet is onvoldoende expliciet om voor een NTD-bevel te gelden als 'bij wet voorzien', nu het gaat om een potentieel meer dan geringe inbreuk op grondrechten en er bovendien medewerking van een derde – de ISP – geëist wordt. Er zal dus een expliciete wettelijke bevoegdheid moeten worden gevonden.

Een eerste kandidaat is natuurlijk artikel 54a Sr zelf. Hoewel dit artikel voor een bevoegdheidstoekennend artikel wetssystematisch op een merkwaardige plaats staat (namelijk buiten het Wetboek van Strafvordering (Sv)), veronderstelt de formulering wel degelijk een bevoegdheidstoedeling aan de Officier van Justitie. Art. 54a Sr lijkt immers weinig zinvol als de OvJ geen bevoegdheid zou hebben een bevel 'om alle maatregelen te nemen die enz.' te geven – het zou dan een loze bepaling zijn. Er is één precedent dat een bepaling in het wetboek van strafrecht als grondslag dient voor een bevoegdheid: art. 139a t/m 139c Sr hebben van 1971 tot 2002 gediend als grondslag voor de bevoegdheid tot afluisteren door de BVD.[13]

Het lijkt echter niet direct de bedoeling geweest te zijn van de wetgever om deze ongebruikelijke constructie bij art. 54a Sr te hanteren. De Memorie van Toelichting bij wetsvoorstel 28 197 (waarbij art. 54a Sr is ingevoerd) wijst zelf in de richting van een tweede kandidaat voor een bevoegdheidsgrondslag.

> In de context van strafvorderlijke maatregelen zij gewezen op het aanhangige wetsvoorstel Computercriminaliteit II. In het daarin voorgestelde artikel 125o Wetboek van Strafvordering wordt de mogelijkheid geschapen voor de officier van justitie of de rechter-commissaris om te bepalen dat gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten (Kamerstukken II 1998/99, 26 671, nr. 2). **In het onderhavige wetsvoorstel wordt deze mogelijkheid benut als onderdeel van de**

[10] http://www.burojansen.nl/traa/e_10_8.htm.
[11] Met uitzondering van phishing-pagina's, waarbij de vrije meningsuiting minder in het geding is.
[12] De vrijheid van meningsuiting is in het geding ook als bepaald gedrag binnen de termen van een wettelijke strafbepaling valt: bij bijvoorbeeld smaad staat vast dat een veroordeling voor smaad een inperking van het recht op vrije meningsuiting inhoudt (art. 10 lid 1 EVRM), en wordt vervolgens getoetst of deze inperking gerechtvaardigd is gezien de eisen van art. 10 lid 2 EVRM, zie bijvoorbeeld EHRM 26 april 1995, Series A vol. 313, NJ 1996/497 (Prager en Oberschlick). Ook procedurele maatregelen, bijvoorbeeld indien een overheid publicatie van een krantenartikel verbiedt, perken de vrijheid van meningsuiting in en moeten worden getoetst aan art. 10 lid 2 EVRM, zie EHRM 26 april 1979 Series A vol. 30 (Sunday Times).
[13] Buuren, J. van, B.J. Koops & W. Wagenaar (2004), 'Inlichtingen- en veiligheidsdiensten en ICT', in: B.J. Koops (red.) (2004), *Strafrecht en ICT*, Den Haag: Sdu 2004, p. 195-196.

voorgestelde vervolgingsuitsluitingsgrond in artikel 54a Wetboek van Strafrecht.[14] [**vet** toegevoegd]

Artikel 125o Sv heeft inmiddels kracht van wet en het eerste lid van art. 125o Sv luidt als volgt.

> Indien bij een doorzoeking in een geautomatiseerd werk gegevens worden aangetroffen met betrekking tot welke of met behulp waarvan het strafbare feit is gepleegd, kan de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris bepalen dat die gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van het strafbare feit of ter voorkoming van nieuwe strafbare feiten.

In deze paragraaf analyseren wij deze twee bepalingen nader als mogelijke grondslag.

3.2. Art. 54a Sr als zelfstandige grondslag

In hoeverre biedt art. 54a Sr zelf een juridische grondslag voor een OvJ om een ontoegankelijkmakingsbevel te geven aan een ISP? Er is één belangrijk argument voor het aannemen van een juridische grondslag: art. 54a Sr geeft een voorwaarde aan waaronder een OvJ een bevel mag geven, namelijk een schriftelijke machtiging van de r-c. Dit is moeilijk anders te verklaren dan door aan te nemen dat art. 54a Sr een zelfstandige bevoegdheid regelt.

Er zijn echter vier argumenten tegen het inlezen van een bevoegdheid in art. 54a Sr. Ten eerste is er een *wetshistorisch* argument. De regering heeft bij de totstandkoming van art. 54a Sr, in wetsvoorstel 28 197, zelf aangegeven dat art. 125o Sv een bevoegdheid vestigt waarop toepassing van art. 54a Sr gebaseerd kan worden. De hierboven geciteerde passage uit de Memorie van Toelichting bij art. 54a is in de verdere totstandkomingsgeschiedenis van die wet niet weersproken (er wordt nergens gesteld dat art. 54a zelf de grondslag is), zodat deze als leidend moet worden beschouwd bij de wetshistorische interpretatie ervan.[15]

Merkwaardig is echter dat de wetgever later wel art. 54a Sr als grondslag heeft genoemd. In een lijst van vragen en antwoorden over terrorismebestrijding zegt de minister:

> Notice and takedown is bedoeld om op een snelle en efficiënte manier informatie van het internet te verwijderen. Als stok achter de deur is er in geval van strafrechtelijk onrechtmatig materiaal het bevel ex artikel 54a Sr. De officier van justitie kan op machtiging van de rechter-commissaris de provider bevelen de betreffende onrechtmatige informatie ontoegankelijk te maken.[16]

Het 'bevel ex artikel 54a' geeft aan dat de minister artikel 54a nu als bevoegdheidsscheppend beschouwt. De vraag is hoe dit standpunt zich verhoudt tot het standpunt ten tijde van de totstandkoming van artikel 54a Sr: gaat de nieuwere uitspraak voor de oudere? Sommigen zullen inderdaad de voorkeur geven aan de meest recente uitspraak in plaats van een oudere uitspraak. Wij neigen er echter naar om de wetsgeschiedenis van art. 54a Sr zelf te laten prevaleren boven een latere, losstaande uitspraak die in een geheel andere context is gedaan. Duidelijk is in elk geval wel dat de wetshistorische interpretatie geen eenduidig argument geeft om artikel 54a Sr als grondslag te beschouwen en op zijn minst de nodige twijfels oproept over de grondslag.

Ten tweede is er een *rechtssystematisch* argument. Strafvorderlijke bevoegdheden worden toegekend in het Wetboek van Strafvordering of in bijzondere wetten, niet in het

---

[14] *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 27.

[15] De passages over art. 54a Sr in *Kamerstukken II*, 2003-2004, 28 197, nr. 15, p. 3 en *Kamerstukken II*, 2002-2003, 28 197, nr. 5, p. 20 geven niet expliciet aan dat art. 54a Sr als de grondslag voor de bevelsbevoegdheid moet worden gezien. Als het de bedoeling van de wetgever was geweest om art. 54a Sr als grondslag aan te wijzen in deze passages dan had de wetgever dat expliciet moeten doen, en wel om de expliciete verwijzing naar art. 125o Sv in de MvT te ontkrachten. Ter ontkrachting daarvan zijn de genoemde passages te multi-interpretabel en te weinig expliciet.

[16] *Kamerstukken II* 2004/05, 29 754, nr. 6, p. 49 en 51.

Wetboek van Strafrecht. Het feit dat er een precedent in Sr is geweest (art. 139a-c Sr) versterkt dit argument: het is de enige uitzondering die de regel des te stelliger bevestigt.

Ten derde een *rechtsbeschermend* argument. Art. 54a Sr voorziet weliswaar in betrokkenheid van een rechter-commissaris als waarborg voor de belangen van vrijheid van meningsuiting en de belangen van de ISP, maar in andere opzichten schiet de bepaling ernstig tekort. Notificatie aan de inhoudsaanbieder is niet geregeld, er is geen beklag mogelijk (vgl. art. 552a Sv), noch is verzekerd dat de OvJ tot vervolging overgaat zodat rechterlijke toetsing achteraf plaatsvindt. Ook kan de OvJ niet in beroep gaan als de r-c geen machtiging geeft voor een NTD-bevel (vgl. art. 446 Sr, zie par. 4.6). Bovendien ontbreekt een regeling voor het beëindigen van de ontoegankelijkmaking zodra gebleken is dat deze niet langer nodig is. Deze waarborgen bestaan wel bij de ontoegankelijkmaking van art. 125o Sv (zie onder), en het zou ongerijmd zijn als de wetgever bij een NTD-situatie – waarin de vrijheid van meningsuiting vaak sneller in het geding zal zijn dan bij het ontoegankelijkmaken van gegevens op een inbeslaggenomen computer – minder waarborgen zou hebben geschapen dan bij een vergelijkbare, in zeker opzicht minder belastende, bevoegdheid.

Tenslotte kan een *tekstueel* argument aangevoerd worden. Art. 54a Sr geeft slechts aan dat de ISP niet vervolgbaar is als hij een bevel van de Officier van Justitie opvolgt. Er staat niet dat de OvJ bevoegd is om een zodanig bevel te geven; in het Wetboek van Strafvordering worden opsporingsbevoegdheden vrijwel steeds geformuleerd als 'de opsporingsambtenaar is bevoegd om...' of 'de officier van justitie kan...'. In art. 54a Sr ontbreekt een expliciet grondslagscheppend element als 'is bevoegd' of 'kan'. De tekst van art. 54a Sr laat daardoor in het midden of de officier op basis van dit artikel zelf bevoegd is om een bevel te geven. Gezien het strafvorderlijk legaliteitsbeginsel (art. 1 Sv) en het *Bestimmtheitsgebot* geeft een letterlijke interpretatie daarom geen aanknopingspunten om art. 54a als grondslag te beschouwen.

Het argument vóór kan volgens ons uiteindelijk niet opwegen tegen deze vier tegenargumenten. Het is ongerijmd om een bevoegdheidsvoorwaarde in art. 54a Sr te hebben zonder bevoegdheid – de wetgever zal niet bedoeld hebben een loze bepaling te scheppen. Maar noch de letterlijke, noch de wetshistorische, noch de systematische interpretatie van artikel 54a Sr biedt een duidelijk aanknopingspunt om hierin een bevoegdheidsgrondslag te lezen, eerder integendeel. Aangezien de vrije meningsuiting hier in het geding is – meer nog dan bij de ontoegankelijkmaking van art. 125o Sv waarbij de wetgever wel gekozen heeft voor een expliciete bevoegdheid in het Wetboek van Strafvordering – mag men gezien het legaliteitsbeginsel en het *Bestimmtheitsgebot* art. 54a Sr niet ruimhartig lezen als een impliciete grondslag voor een NTD-bevel. Het artikel biedt onzes inziens onvoldoende basis als bevoegdheidsgrondslag. Het ontbreken van een stelsel van waarborgen – het vierde argument – versterkt deze conclusie eens te meer.[17]

3.3. Art. 125o Sv als grondslag

Nu art. 54a Sr geen zelfstandige bevoegdheidstoedeling bevat, waarop kan de bevoegdheid van de OvJ dan worden gebaseerd? Zoals we hiervoor zagen suggereert de Memorie van Toelichting dat art. 125o Sv die grondslag biedt. Een dergelijke gedachtegang is op het eerste gezicht logisch, maar blijkt bij nadere beschouwing volgens de juridische dogmatiek problematisch te zijn.

[17] Een gevolg van deze conclusie zou kunnen zijn dat ook de strafuitsluiting van art. 54a Sr op losse schroeven staat: zonder een bevoegd bevel van de OvJ kan de ISP zich immers ook niet beroepen op het hebben voldaan aan de voorwaarden van art. 54a Sr. Theoretisch kan het OM de ISP dan ook vervolgen voor medeaansprakelijkheid van het informatieaanbod. In de praktijk zal dat geen probleem opleveren voor de ISP, aangezien art. 54a Sr richtlijnconform moet worden uitgelegd, wat onder andere inhoudt dat er niet meer voorwaarden (laat staan onmogelijke voorwaarden) mogen worden opgelegd aan de ISP om te profiteren van aansprakelijkheidsuitsluiting.

Als art. 54a Sr bouwt op art. 125o Sv, waarom geeft art. 54a Sr dan aan dat de OvJ door de r-c gemachtigd moet worden? Wie onder welke omstandigheden mag bepalen dat er ontoegankelijk wordt gemaakt is immers al geregeld in art. 125o Sv. Waarom zou art. 54a Sr niet gewoon aansluiten bij art. 125o Sv, als dat de bevoegdheid is waarop men bouwt voor het ontoegankelijk maken in het kader van art. 54a Sr? Een reden zou kunnen zijn dat de situatie van ontoegankelijkmaking door een tussenpersoon iets bijzonders is waarvoor andere, wellicht zwaardere, voorwaarden zouden moeten gelden. De vrijheid van meningsuiting is immers in het geding, terwijl dat bij 125o-bevelen niet altijd het geval hoeft te zijn. De Memorie van Toelichting biedt daarvoor geen specifieke aanknopingspunten, maar de ernst van de inbreuk op de vrijheid van meningsuiting bij een NTD-bevel lijkt ons op zich een valide reden om daarvoor een extra voorwaarde van rechterlijke toetsing vooraf te eisen. De voorwaarde in art. 54a Sr kan dan gezien worden als een modificatie van art. 125o Sv in het specifieke geval van een NTD-bevel. Het is echter wel een uitzonderlijke constructie om een dergelijke voorwaarde voor een opsporingshandeling te plaatsen in een bepaling van materieel strafrecht over aansprakelijkheidsuitsluiting, en het is op zijn minst curieus dat de wetgever bij invoering van art. 54a Sr de keuze voor deze uitzonderlijke constructie niet heeft toegelicht of onderbouwd.

Er zijn echter belangrijker problemen met art. 125o Sv als bevoegdheidsgrondslag voor een bevel als bedoeld in art. 54a Sr. Art. 125o Sv is ten eerste volgens de wettekst namelijk beperkt tot een situatie waarin een doorzoeking in een geautomatiseerd werk plaatsvindt. Daarvan is sprake bij een doorzoeking ter inbeslagneming (art. 96b, 96c, 97, 110 Sv) of een doorzoeking ter vastlegging van gegevens (art. 125i Sv). Indien een OvJ een notificatie ontvangt over een 'illegale webpagina', dan zal de OvJ normaliter geen doorzoeking gaan plegen om de notificatie te controleren: de gegevens staan immers op het Internet. Ook als de gegevens niet zonder meer publiek toegankelijk zijn, staan de OvJ lichtere bevoegdheden ten dienste om van de inhoud van de bewuste webpagina kennis te nemen, zoals art. 126nd Sv over verstrekking van gegevens. Het is niet gewenst dat de OvJ enkel om ontoegankelijkmaking aan een ISP te kunnen bevelen een doorzoeking zou moeten plegen, zeker niet als de gewraakte gegevens publiekelijk toegankelijk zijn.

De wetgever is echter dubbelzinnig geweest bij de wetsgeschiedenis van art. 125o Sv: de voorwaarde van een doorzoeking, die in de wettekst expliciet is vermeld, wordt in de Memorie van Toelichting afgezwakt:

> Beide maatregelen [ontoegankelijkmaking en vernietiging van gegevens] hebben slechts betrekking op gegevens die bij een onderzoek in een geautomatiseerd werk «worden aangetroffen». Dergelijk onderzoek moet op andere gronden berusten, zoals de mogelijkheid voor de RC om de «uitlevering» van computergegevens te bevelen (artikel 125i Sv) of de doorzoekings- of inbeslagnemingsbevoegdheden. (…) Ook is het mogelijk dat via Internet strafbare informatie wordt gevonden. Wanneer redelijkerwijs kan worden vermoed dat het gaat om gegevens die onder Nederlandse rechtsmacht vallen, kan ook dàn deze maatregel worden getroffen (…).[18]

Deze toelichting suggereert dat ontoegankelijkmaking kan worden bevolen ook als er geen sprake is van een doorzoeking. Dit heeft de wetgever kennelijk ook zo opgevat bij invoering van art. 54a Sr (zie het in par. 3.1.1 aangehaalde citaat). In een later stadium van de totstandkoming van art. 125o Sv heeft de wetgever echter juist weer expliciet gezegd:

> Het ontoegankelijk maken van gegevens is een maatregel die **onlosmakelijk verbonden is** met het doorzoeken van een geautomatiseerd werk.[19] [**vet** toegevoegd]

Nu de wetsgeschiedenis de 'afgezwakte' interpretatie van de MvT tegenspreekt, terwijl ook overigens het gros van de voorbeelden in de wetsgeschiedenis een doorzoeking betreft, moet worden geconcludeerd dat art. 125o Sv alleen kan worden toegepast bij een doorzoeking. Dat zal bij een NTD-situatie over het algemeen – uitzonderingen daargelaten – niet aan de orde zijn.

---

[18] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 51.
[19] *Kamerstukken I* 2005-2006, 26 671 en 30 036, D, p. 8.

Een tweede bezwaar is dat art.125o Sv spreekt over de OvJ die kan 'bepalen dat die gegevens ontoegankelijk worden gemaakt'. Het is een niet-triviale stap om aan te nemen dat dit mede de bevoegdheid omvat om een derde als een ISP te bevelen de gegevens ontoegankelijk te maken. In de context van art. 125o Sv is een bevel tot derden niet aan de orde. Het artikel gaat er immers van uit dat de OvJ, de r-c of onder hun gezag vallende personen de computer doorzoeken. Wordt iets aangetroffen dat vatbaar is voor ontoegankelijkmaking, dan kunnen en zullen deze personen dat in beginsel zelf doen. Ze hebben daar een derde (de beheerder van het doorzochte systeem) niet voor nodig. Niettemin kan dat volgens de wetgever soms wel worden gevraagd:

> In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is. Daarbij moeten uiteraard de eisen van proportionaliteit en subsidiariteit in acht worden genomen. Dit vereist in het bijzonder in netwerkomgevingen voorzichtigheid, opdat niet onnodig schade wordt toegebracht aan gegevens of systemen. Soms zal het daarom in de rede liggen om de medewerking van de netwerkbeheerder te vragen.[20]

Medewerking van een derde, zoals een ISP, is echter uitzondering, geen regel, zo blijkt ook uit dit citaat. Het is enkel aangewezen als politie of justitie zelf niet voldoende technische mogelijkheden of deskundigheid heeft om de ontoegankelijkmaking uit te voeren. Bij een NTD-bevel aan een ISP is dit echter omgekeerd: de medewerking door een derde wordt dan juist de regel, en art. 54a Sr geeft geen enkele indicatie dat de OvJ of een opsporingsambtenaar zelf iets aan ontoegankelijkmaking zou moeten of kunnen doen.

Het feit dat de beheerder in de regel juist niet geacht wordt mee te werken, wordt ook aangegeven door het tweede en derde lid van art. 125o Sv:

> 2. Onder ontoegankelijkmaking van gegevens wordt verstaan het treffen van maatregelen om te **voorkomen dat de beheerder** van het in het eerste lid bedoelde geautomatiseerde werk of derden verder van die gegevens kennisnemen of gebruikmaken, alsmede ter voorkoming van de verdere verspreiding van die gegevens. (…)
>
> 3. Zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen, bedoeld in het tweede lid, bepaalt de officier van justitie dan wel, tijdens het gerechtelijk vooronderzoek, de rechter-commissaris dat de gegevens **weer ter beschikking van de beheerder** van het geautomatiseerde werk worden gesteld. [**vet** toegevoegd]

De reguliere 125o-situatie is dus het onttrekken van de gewraakte gegevens aan de beschikkingsmacht van de beheerder.[21] Het derde lid is onbegrijpelijk in situaties waarin de beheerder zelf de gegevens ontoegankelijk maakt (bijvoorbeeld door versleuteling) – hij heeft dan immers steeds de beschikkingsmacht over de gegevens behouden. Ook hier blijkt dat art. 125o Sv niet bepaald is toegesneden op art. 54a Sr-situaties waarin de ISP zelf ontoegankelijk moet maken.

Bovendien geeft de Memorie van Toelichting hier aan dat medewerking van een derde kan worden *gevraagd*, maar dat betekent niet dat medewerking kan worden *bevolen*. Van een bevel is hier geen sprake, zo geeft de wetgever aan in de Nota naar aanleiding van het Verslag:

> Slechts indien sprake is van afgedwongen medewerking, biedt de wet een grondslag voor vergoeding. Een dergelijke medewerkingsplicht voor de systeembeheerder bij de ontoegankelijkmaking wordt door het wetsvoorstel niet in het leven geroepen.[22]

Dit is direct in strijd met de situatie van 54a Sr, waarin de ISP volgens de wetgever vervolgd kan worden voor het niet voldoen aan het bevel en waarin er dus wel een medewerkingsplicht is.[23]

---

[20] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 21.
[21] Zie ook *Kamerstukken II* 2004-2005, 26 671, nr. 10, p. 13.
[22] *Kamerstukken II* 2004-2005, 26 671, nr. 10, p. 16.
[23] 'Wanneer de tussenpersoon niet aan een bevel gevolg geeft, kan hij zich niet op de vervolgingsuitsluitingsgrond beroepen en kan hij strafrechtelijk worden vervolgd terzake van het niet voldoen

Een derde en laatste probleem is dat art. 125o Sv expliciet als voorlopige maatregel is geconstrueerd. De wetgever heeft veel moeite genomen om een sluitend systeem van waarborgen te scheppen: de ontoegankelijkmaking moet technisch omkeerbaar zijn, er is een notificatieplicht (art. 125m Sv) en een beklagmogelijkheid (art. 552a Sv), en – tenzij OvJ of r-c de maatregel zelf terugdraait – uiteindelijk zal een rechter zich moeten uitspreken over definitieve ontoegankelijkmaking (art. 354 Sv).

> De ontoegankelijkmaking is een voorlopige maatregel. In het nieuwe artikel 354 Sv wordt voorgeschreven dat de rechter bij een materiële einduitspraak over het feit (dat wil zeggen een veroordeling, een vrijspraak of een ontslag van rechtsvervolging) een definitieve beslissing neemt over de ontoegankelijk gemaakte gegevens, voor zover deze maatregel nog niet door de officier van justitie of de rechter-commissaris is opgeheven. (…) Niet voorzien is in de mogelijkheid voor de officier van justitie om in het kader van een transactie als voorwaarde te stellen dat de verdachte afstand doet van computergegevens die vatbaar zijn voor vernietiging op last van de rechter (…). De voorgestelde bevoegdheid dient aan de onafhankelijke rechter te worden voorbehouden, reeds omdat artikel 7 van de Grondwet eist dat elke inhoudelijke beperking van de vrijheid van meningsuiting die zich in het concrete geval effectueert, moet kunnen worden voorgelegd aan de onafhankelijke rechter (…).[24]

De situatie van art. 54a Sr is niet toegesneden op dit systeem van rechtswaarborgen. Waar het bij een 125o-maatregel namelijk de bedoeling is dat een rechter ter zitting een eindoordeel velt over de ontoegankelijkmaking, lijkt art. 54a juist te suggereren dat er géén rechterlijk eindoordeel komt: als de inhoud is weggehaald, wordt de tussenpersoon immers juist 'als zodanig niet vervolgd'. Dit laat onverlet dat een vervolging van de inhoudsaanbieder mogelijk is, maar dat zal lang niet altijd gebeuren (vgl. ook hoofdstuk 5 over jurisdictieproblemen).

Als art. 125o Sv echter als grondslag voor een 54a-bevel dient (bijvoorbeeld wanneer er sprake is van een doorzoeking), dan betekent dit automatisch dat alle 125o-waarborgen van kracht zijn. De betrokkenen, waaronder de inhoudsaanbieder, moeten worden genotificeerd (art. 125m Sv), en belanghebbenden (zowel de ISP als de inhoudsaanbieder) kunnen zich beklagen ex art. 552a Sv. De OvJ (of tijdens het gvo de r-c) moeten de gegevens weer toegankelijk laten maken 'zodra het belang van de strafvordering zich niet meer verzet tegen opheffing van de maatregelen' (art. 125o lid 3 Sv). Ook zal de rechter ter zitting zich over de ontoegankelijkmaking moeten uitspreken (art. 354 Sv). Hier is onduidelijk wat in een NTD-situatie 'het feit' is waarover de rechter zich uitspreekt: is dat het aanbieden van illegale inhoud door de inhoudsaanbieder – dus een beslissing bij de vervolging van de inhoudsaanbieder zelf – of is dat de strafrechtelijke aansprakelijkheid van de ISP voor medeplichtigheid aan het illegale inhoudsaanbod? Dat laatste kan niet, omdat de ISP juist niet vervolgd wordt als tussenpersoon indien hij het aanbod heeft weggehaald, terwijl als de ISP weigert en wel vervolgd wordt, er geen sprake is van ontoegankelijkmaking. Het moet dus een rechterlijke uitspraak over het oorspronkelijke inhoudsaanbod zijn bij vervolging van de inhoudsaanbieder. De aangehaalde passage uit de Memorie van Toelichting legt de nadruk op het belang van een einduitspraak, en dit lijkt daarom voor een NTD-bevel te impliceren (als 125o Sv daarvoor als grondslag dient) dat het OM verplicht is om vervolgens de inhoudsaanbieder te vervolgen. Het is sterk de vraag of de wetgever zich dit gerealiseerd heeft toen hij bij de totstandkoming van art. 54a Sr art. 125o Sv als grondslag noemde.

Concluderend kan gezegd worden dat art. 125o Sv volgens de wetgever weliswaar bij de totstandkoming van art. 54a Sr aangeduid is als grondslag voor een NTD-bevel bij de totstandkoming van art. 54a Sr, maar dat er veel haken en ogen aan zitten om dit als grondslag aan te nemen. De wetgever heeft bij de totstandkoming van art. 125o Sv (ingevoerd ná art. 54a Sr) geen aandacht besteed aan de specifieke omstandigheden van

---

aan een bevoegd gegeven ambtelijk bevel (artikel 184 Wetboek van Strafrecht).' *Kamerstukken II* 2001-2002, 28 197, nr. 3, p. 66.

[24] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 22.

een NTD-bevel, en heeft voorwaarden gesteld (zoals een doorzoeking) en toelichtingen gegeven (zoals bij uitzondering vragen om medewerking van derden) die al met al niet passen bij een NTD-situatie. Doorslaggevend is volgens ons dat de wetgever bij de totstandkoming van art. 125o Sv heeft aangegeven dat deze bevoegdheid geen medewerkingsplicht schept, zodat van een bevel aan derden om ontoegankelijk te maken geen sprake kan zijn. Het bevel van de OvJ zoals genoemd in art. 54a Sv kan daarom niet worden gegrond op de bevoegdheid van art. 125o Sv.

3.4. Conclusie

Het is zeer twijfelachtig of een NTD-bevel kan worden gegeven op grond van art. 54a Sr of art. 125o Sv. Bij beide artikelen bestaan enige aanknopingspunten, maar ook vele haken en ogen om deze als bevoegdheidsgrondslag te interpreteren. Nu de vrijheid van meningsuiting in het geding is en bovendien de medewerking van een derde wordt gevorderd, is een zorgvuldige procedure en voldoende expliciete en rechtszekere wettelijke basis noodzakelijk. Volgens ons moet daarom, gezien de gerede twijfel die bestaat over een wettelijke grondslag, worden geconcludeerd dat er geen voldoende wettelijke basis bestaat voor een NTD-bevel.

Daarom zal de wetgever alsnog een op NTD toegesneden bevelsbevoegdheid tot ontoegankelijkmaking moeten scheppen. Daarbij kan dankbaar geput worden uit art. 125o Sv, zoals het systeem van waarborgen, en het ligt ook in de rede om een NTD-bevelsbevoegdheid onder te brengen in of nabij art. 125o Sv. Daarbij zullen wel de problematische elementen van art. 125o Sv aangepast moeten worden aan de specifieke NTD-situatie. Tegelijk kan dan ook de voorwaarde van schriftelijke machtiging van de r-c uit art. 54a Sr overgeheveld worden naar de plaats waar een dergelijke voorwaarde thuishoort, in het Wetboek van Strafvordering.

In het vervolg van dit hoofdstuk gaan we in op diverse aspecten die aandacht behoeven bij een te scheppen bevoegdheid voor de OvJ voor een NTD-bevel. Dit beoogt aanknopingspunten te geven voor de meer omvattende NTD-regeling die in de vervolgfase van dit onderzoek zal worden onderzocht. In deze onderzoeksfase beperken we ons tot juridische aandachtspunten die samenhangen met art. 54a Sr.

4. Materiële en procedurele juridische vragen

4.1. Criteria voor de bevoegdheid

Welke criteria moeten worden aangelegd voor de toepassing van de te regelen bevoegdheid van de OvJ, mede in het licht van de vrijheid van meningsuiting?

Vanwege de grote potentiële inbreuk op de vrije meningsuiting, zal de door de OvJ uit te oefenen bevoegdheid aan rechterlijke controle onderworpen dienen te zijn: vooraf door de r-c (zoals al voorzien in art. 54a Sr) en achteraf via beklag ex art. 552a Sv of via de zittingsrechter. Aannemend dat wettelijk in beklag en betrokkenheid van de r-c is voorzien, onder welke voorwaarden zou een OvJ dan tot uitoefening van zijn bevelsbevoegdheid kunnen overgaan?

Het belangrijkste criterium waarop de r-c en OvJ zich richten is de strafbaarheid van het informatieaanbod. Gegeven de strafrechtelijke expertise van de r-c en de OvJ zijn zij in staat zich een kwalitatief goed oordeel te vormen over de strafbaarheid van een informatieaanbod. Waar ook in de ogen van OvJ en r-c twijfel mogelijk is over de strafbaarheid van een informatieaanbod, is terughoudendheid geïndiceerd, te meer voor informatieaanboden waarbij, zoals meestal het geval zal zijn, de vrijheid van meningsuiting gewicht in de schaal legt. Als er enige twijfel, hoe gering ook, bestaat over de strafbaarheid, maar het niettemin opportuun wordt geacht door de OvJ en gerechtvaardigd door de r-c om het materiaal ontoegankelijk te laten maken, dan is hetzij vervolging van de inhoudsaanbieder geïndiceerd om dusdoende een rechterlijk oordeel te verkrijgen over de strafbaarheid van het informatieaanbod, hetzij een andere vorm van rechterlijke eindtoetsing over de strafbaarheid van het materiaal (zoals bij het 125o-bevel plaatsvindt via 552a of 354 Sv). Een duidelijke uitspraak van de rechter ter zitting – bijvoorbeeld bij wijze van proefproces – zal ertoe bijdragen dat soortgelijke gevallen in de toekomst hetzij als strafbaar worden aangemerkt dan wel als strafrechtelijk onbezwaarlijk (vgl. ook par. 3.6).

In de privaatrechtelijke rechtspraak over de aansprakelijkheid van Internetaanbieders wordt het criterium van de onmiskenbare onrechtmatigheid aangelegd: een *hosting*-aanbieder is civielrechtelijk aansprakelijk indien hij – hoewel daartoe in staat – een informatieaanbod niet prompt weghaalt nadat hij een notificatie over de onrechtmatigheid heeft ontvangen en aan de juistheid van de notificatie (en de daarin neergelegde stelling van onrechtmatigheid) in redelijkheid geen twijfel kan bestaan.[25]

Voor de strafrechtelijke context lijkt dit criterium niet naadloos toepasbaar. Het strafrecht met zijn door het legaliteitsbeginsel ingegeven precieze omschrijvingen van delicten geeft de OvJ en r-c meer houvast om te bepalen wat strafbaar is dan het geval is in het privaatrecht, waar de open norm van art. 6:162 BW – strijd met de zorgvuldigheid die in het maatschappelijk verkeer betaamt – steeds om een nader invulling vraagt bij de bepaling van onrechtmatigheid. De OvJ beschikt bovendien over bevoegdheden waarmee nader onderzoek kan worden gedaan naar omstandigheden die van belang zijn voor een oordeel over de strafbaarheid van daad en (vermeende) dader. Daarnaast is het ook denkbaar dat bepaalde informatie niet onmiskenbaar onrechtmatig is (bijvoorbeeld in het grijze gebied van vrije meningsuiting en strafbaar aanzetten tot terroristisch geweld), maar wel potentieel grote risico's met zich meebrengt, bijvoorbeeld voor bepaalde personen die met name worden genoemd. In dergelijke gevallen kan het wenselijk zijn direct een ontoegankelijkmakingsbevel te geven en pas later een rechterlijke einduitspraak over de onrechtmatigheid te verkrijgen. Aangezien ontoegankelijkmaking echter, zeker in dit type gevallen, een grote inbreuk op de vrije meningsuiting kan maken, lijkt het strafrechtelijke

[25] Pres.Rb. Amsterdam 12 september 1996 (Scientology/XS4ALL).

standaardcriterium – de redelijke verdenking dat een strafbaar feit is gepleegd (art. 27 Sv) – een te lage drempel. Bij voorkeur zal een criterium moeten worden gehanteerd dat tussen 'redelijke verdenking' en 'onmiskenbaar onrechtmatig' in ligt. Wellicht kan hier aansluiting worden gezocht bij het in het strafrecht gehanteerde criterium van 'ernstige bezwaren' tegen de verdachte: er moeten ernstige bezwaren bestaan tegen het materiaal om een ontoegankelijkmakingsbevel te rechtvaardigen.

Een tweede eis die aan de OvJ gesteld kan worden is hiervoor al terloops aan de orde gesteld. Waar de OvJ vragen over strafbaarheid van daad en dader weg kan nemen door enig nader onderzoek te verrichten, dan kan dat ook vooraf van hem verlangd worden.

Voorts moet de bevoegdheidsuitoefening voldoen aan de eisen van subsidiariteit en proportionaliteit. De Memorie van Toelichting bij wetsvoorstel 28 197 (implementatie Richtlijn inzake elektronische handel) zegt het als volgt:

> De ontoegankelijkmaking van de gegevens moet redelijkerwijs kunnen worden gevergd. De verlangde maatregelen moeten derhalve in overeenstemming zijn met de eisen van subsidiariteit en proportionaliteit. Er mogen geen andere, minder verstrekkende mogelijkheden openstaan om een einde te maken aan de als onwenselijk ervaren situatie. En de verlangde maatregelen mogen niet verder strekken dan strikt noodzakelijk. De dienstverlener die van een ander afkomstige gegevens opslaat, is door de bank genomen in staat de gegevens ontoegankelijk te maken. De dienstverlener die de van een ander afkomstige gegevens doorgeeft, is doorgaans niet goed in staat daartegen adequaat op te treden. De in de artikelsgewijze toelichting bij artikel 196c van Boek 6 van het Burgerlijk Wetboek behandelde Radikall-zaak vormt daarvan een treffende illustratie (paragraaf 2). Toch zijn er al gevallen denkbaar waarin ook met een relatief eenvoudige ingreep door de tussenpersoon die louter van een ander afkomstige gegevens doorgeeft het gewenste resultaat kan worden bereikt.[26]

De subsidiariteitseis verlangt dat het minst bezwarende middel wordt gekozen om een doel te bereiken. De proportionaliteitseis verlangt dat het ingezette instrument een redelijk middel is tot het te bereiken doel. Aan de doelzijde betekent dit dat de aard en ernst van het strafbaar feit rechtvaardigen dat tot ontoegankelijkmaking wordt overgegaan. Aan de middelzijde wordt gekeken naar de eventuele inbreuk die op de vrijheid van meningsuiting wordt gemaakt, andere belangen van de inhoud- en Internetaanbieder (zoals financiële belangen bij het continueren van het informatieaanbod), naar de kosten van het ontoegankelijk maken en naar de te verwachten effectiviteit. De 'kosten' liggen enerzijds in de identificatie van de gegevens die deel uitmaken van het informatieaanbod en anderzijds in een eventuele bijvangst wanneer het ontoegankelijk maken onvoldoende gericht kan plaatsvinden. Voorts zal ook de inschatting van de effectiviteit van het ontoegankelijk maken niet zelden moeten leiden tot een besluit tot niet-ingrijpen: informatie die ontoegankelijk wordt gemaakt kan elders gemakkelijk weer online gebracht worden en aldus het effect van het ontoegankelijk maken grotendeels ongedaan maken (over dit 'boemerang'-effect, zie par. 2.2.3).

Hoe de doel-middel-afweging in de praktijk uitvalt, zal steeds beoordeeld moeten worden aan de hand van de concrete omstandigheden van het geval. Bij de te scheppen bevoegdheid zal wel duidelijk gemaakt moeten worden, bijvoorbeeld door het opnemen van een proportionaliteitsclausule als 'dringend noodzakelijk in het belang van de strafvordering', dat een strenge doel-middel-afweging moet plaatsvinden door OvJ en r-c.

Ten derde en laatste mag de Officier van Justitie geen aanvullende voorwaarden verbinden aan het bevel gegeven aan een tussenpersoon. Een tussenpersoon zoals een ISP zal in het systeem van de wet, mede vanwege de strafuitsluiting van art. 54a Sr, het bevel veelal niet als een last ervaren doch eerder als een gelegenheid om, zonder zelf een intellectuele verantwoordelijkheid te hoeven nemen, bevrijd te worden van de last van (dreigende) strafrechtelijke aansprakelijkheid. Dit kan echter geen aanleiding voor een Officier van

[26] *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 65-66.

Justitie zijn – zo daar überhaupt al behoefte aan zou bestaan – nadere voorwaarden te stellen, zoals het kenbaar maken van de identiteit van de inhoudsaanbieder. Dergelijke aanvullende voorwaarden laat de Richtlijn inzake elektronische handel (ter implementatie waarvan art. 54a Sr in het wetboek is ingevoegd) niet toe, dat wil zeggen niet als voorwaarde waarvan de vrijstelling van aansprakelijkheid afhankelijk gemaakt mag worden. De Memorie van Toelichting vermeldt in dit verband het volgende:

> In de artikelen 53 en 54 Wetboek van Strafrecht wordt aan de nietvervolgbaarheid van de uitgever respectievelijk de drukker de voorwaarde verbonden dat de dader bekend is of op de eerste aanmaning nadat tot het instellen van een gerechtelijk vooronderzoek is overgegaan, bekend wordt gemaakt. In de onderhavige bepaling is die voorwaarde niet opgenomen. De richtlijn staat daaraan in de weg. In de artikelen 12 tot en met 14 van de richtlijn wordt niet de mogelijkheid geboden aan de vrijwaring van aansprakelijkheid de voorwaarde te verbinden dat de dader bekend wordt gemaakt. Dat laat de in het wetsvoorstel Vorderen gegevens telecommunicatie voorgestelde bevoegdheid evenwel onverlet.[27]

In dat licht is het wenselijk om het ontoegankelijkmakingsbevel en het eventueel achterhalen van de inhoudsaanbieder los te koppelen. De OvJ kan altijd op basis van art. 126nc Sv (en soms ook 126na of 126nb Sv) van de ISP vorderen dat deze hem de identificerende gegevens van de inhoudsaanbieder verschaft. Er is dus geen reden om in de te scheppen bevelsbevoegdheid een verplichting tot bekendmaking van de identiteit van de inhoudsaanbieder op te nemen.

Samenvattend kan gesteld worden dat de OvJ zijn bevoegdheid slechts uitoefent ten aanzien van strafbare informatieaanboden. Waar over de strafbaarheid van daad of dader twijfels bestaan, kan van de OvJ enig onderzoek vooraf verlangd worden. Als criterium voor het uitoefenen van het ontoegankelijkmakingsbevel hoeft niet de 'onmiskenbare onrechtmatigheid' van het materiaal uit het civiele recht te worden gehanteerd, maar een zwaarder criterium dan de 'redelijke verdenking' van art. 27 Sv ten aanzien van de strafbaarheid van het materiaal, bijvoorbeeld 'ernstige bezwaren' tegen het materiaal, is wel vereist, vanwege het belang van de vrije meningsuiting. Aangezien velerlei bezwaren kunnen bestaan tegen het geven van een bevel, verdient voorts de proportionaliteits- en subsidiariteitstoetsing nadrukkelijk de aandacht van de r-c en OvJ. Aan het bevel mogen geen andere voorwaarden worden verbonden, zoals een verplichting tot bekendmaking van de identiteit van de inhoudsaanbieder. De bevoegdheidsuitoefening door de OvJ is overigens niet beperkt tot gevallen waarin de OvJ ook tot vervolging overgaat.

4.2. Onderscheid naar inhoud

In hoeverre dient in de criteria voor bevoegdheidsuitoefening gedifferentieerd te worden naar verschillende typen van inhoud?

Art. 54a Sr omvat in beginsel alle soorten strafbare inhoud:

> De vervolgingsuitsluitingsgrond betreft alle aan de doorgegeven of opgeslagen gegevens gelieerde delicten. Het gaat om gegevens met een strafbaar karakter. In het algemeen deel is er reeds op gewezen dat de uitwisseling van gegevens strafbaar kan zijn op grond van de aard van de gegevens, zoals bij uitings- en verspreidingsdelicten; de kwaliteit van de gegevens, zoals in het geval van valsheid in geschrifte en oplichting; en de status van de gegevens, zoals in het geval van auteursrechtschendingen en openbaarmaking van geheimen.[28]

Het is aan te nemen dat sommige vormen van illegale inhoud gemakkelijk te constateren zijn – zoals kinderpornografie en soms ook auteursrechtinbreuk – en dat andere vormen moeilijk te constateren zijn – zoals discriminatie, smaad en laster. Dat kan meebrengen dat de feitelijke drempel van met voldoende zekerheid vaststelbare strafbaarheid bij verschillende

[27] *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 66.
[28] *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 66.

inhoudstypen enigszins anders kan liggen. Ook zal bij sommige typen inhoud, zoals kinderpornografie en phishing-webpagina's, de vrijheid van meningsuiting minder in het geding zijn dan bij andere typen inhoud, zodat de proportionaliteitstoets hier veelal sneller in het voordeel van een ontoegankelijkmakingsbevel zal kunnen uitvallen. In beginsel kunnen zich echter bij alle vormen van illegale informatieaanboden gemakkelijke en moeilijk zaken voordoen.

Wat wel duidelijk verschilt, is de manier waarop de onrechtmatigheid vastgesteld kan worden. Bij kinderpornografie kan bijvoorbeeld deskundigheid vereist zijn met betrekking tot de vaststelling van de leeftijd van de afgebeelde kinderen, wanneer deze niet onmiskenbaar jonger zijn dan 18 jaar. De leeftijd kan afgeleid worden uit uiterlijk waarneembare fysieke kenmerken van de afgebeelde kinderen, maar ook uit vergelijking met al 'bekende' kinderpornografische afbeeldingen. De deskundigheid hiervoor is bij de politie aanwezig. Voor auteursrechtinbreuken is kennis vereist over wie rechthebbende is van op het Internet aangetroffen werken en over de licentiesituatie (aan wie zijn licenties verleend waarvoor?). Voor het aanspreken van deze kennis is de medewerking van rechthebbenden en in het bijzonder van collectieve rechtenorganisaties als Buma-Stemra vereist. Voor de beoordeling van moeilijker gevallen van smaad en laster is de medewerking van in het informatie- of mediarecht gespecialiseerde juristen vereist.

De te hanteren criteria hoeven dus – op abstract niveau – niet gedifferentieerd te worden naar type inhoud. Wat wel per type inhoud – of beter gezegd per type onrechtmatigheid – verschilt is de praktische deskundigheid. Als een NTD-systeem een structuur schept voor de toegang tot uiteenlopende deskundigheden dan zou daarin een belangrijke meerwaarde van een geïntegreerd NTD-systeem kunnen liggen.

4.3. Reikwijdte van uitsluiting van vervolgbaarheid

Wat is de omvang van de uitsluiting van vervolgbaarheid? Omvat dit mede het strafbare handelen tot aan het moment van het bevel?

Een bevel van de Officier van Justitie tot ontoegankelijkmaking heeft velerlei effecten en rechtsgevolgen:

- herstel van de rechtmatige toestand;
- niet-vervolgbaarheid van de ISP;
- kenbaarheid voor de verdachte van justitiële aandacht voor zijn informatieaanbod en daarmee het verlies van tactisch of strategisch voordeel van onbekendheid van de verdachte met het plaatsvinden van het opsporingsonderzoek.

Met name de kenbaarheid voor de verdachte kan een OvJ aanleiding geven het bevel uit te stellen. Mogelijk dat de OvJ de ISP zelfs inofficieel zal vragen de inhoud ook niet eigener beweging van het net te halen. Een dergelijke gang van zaken verhoogt voor de ISP het risico dat hij zich schuldig maakt aan medeplichtigheid aan het feit van de inhoudsaanbieder: de ISP is allicht op de hoogte van de aanwezigheid van strafbare inhoud en verhindert doorlopende beschikbaarheid daarvan niet hoewel hij daartoe in staat is. Het zou onredelijk zijn als de ISP het slachtoffer wordt van het feit dat de OvJ uiteenlopende belangen heeft af te wegen bij zijn beslissing om het bevel te geven, hetzij door het risico van strafbaarheid te lopen dan wel door de verhouding met de OvJ te belasten door de informatie – in de ogen van de OvJ – voortijdig weg te halen.[29] Dit pleit voor een niet-vervolgbaarheid die zich ook uitstrekt over de periode voorafgaand aan het bevel.

[29] Dat de ISP informatie ook zonder bevel ontoegankelijk mag maken is met zoveel woorden erkend in de Memorie van Toelichting bij de implementatiewet. Zie *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 66-67: 'Voorts laat de in de vervolgingsuitsluitingsgrond opgenomen voorwaarde dat een bevel om gegevens ontoegankelijk te maken moet worden opgevolgd onverlet, dat internet-providers uit eigen beweging tot het ontoegankelijk maken van gegevens over kunnen gaan, bijvoorbeeld naar aanleiding van een klacht van een gebruiker of signalering door een meldpunt. Over de wijze waarop internet-providers reageren op

Er is nog een tweede argument voor dit standpunt. De OvJ is namelijk niet verplicht een bevel te geven. De aanname dat bij uitblijven van het bevel de ISP in beginsel vervolgbaar zou zijn doet twijfel rijzen aan de juistheid van Nederlandse implementatie van de richtlijn. De richtlijn laat immers niet toe dat andere dan door haar genoemde voorwaarden aan vrijstelling van aansprakelijkheid verbonden worden. In het bijzonder kan niet een onzeker bevel van de OvJ als voorwaarde voor vrijstelling gesteld worden. Door art. 54a Sr richtlijn-conform te interpreteren – de ISP is ook zonder bevel niet vervolgbaar – wordt de ongewenste consequentie van onjuiste implementatie voorkomen. Dit standpunt kan verder nog onderbouwd worden door te wijzen op de Nota naar aanleiding van het Verslag waarin wordt opgemerkt:

> Dit veronderstelt dát een zodanig bevel is gegeven en niet is opgevolgd, wil het openbaar ministerie ontvankelijk zijn in zijn vervolging van een internet service provider als zodanig.

Het bevel is derhalve een nodige voorwaarde voor vervolgbaarheid, en in de periode voorafgaand aan een bevel is de ISP niet vervolgbaar. Een vraag is of dit standpunt doorgetrokken kan worden naar de situatie dat de OvJ geen bevel geeft omdat daartoe de bevoegdheid ontbreekt zoals we hiervoor hebben betoogd. Dat zou betekenen dat de mogelijkheden voor vervolging van een ISP erg beperkt worden: alleen een ISP die zich dusdanig met de omstreden inhoud afficheert dat hij niet meer ‘als zodanig’ optreedt zou dan nog vervolgbaar zijn. Indien men die implicatie te vergaand acht is ook een minder vergaande interpretatie mogelijk. Men zou kunnen aannemen dat de ISP ook vervolgbaar is als hij (anders dan via een bevel) op de hoogte geraakt van een strafbaar informatieaanbod op zijn systeem en de informatie niet prompt ontoegankelijk maakt. Dan is er wel een vrijstelling overeenkomstig de richtlijn. Maar door het ontbreken van de bevelsbevoegdheid moet de ISP dan wel de zekerheid over de (niet-)strafbaarheid van het informatie-aanbod ontberen die uit had kunnen gaan van een bevel of de expliciete beslissing om geen bevel te geven.

4.4. Vrijwaring van aansprakelijkheid

Vrijwaart het voldoen aan een bevel van de OvJ de ISP van elke aansprakelijkheid voor de illegale inhoud (bijvoorbeeld ook als achteraf blijkt dat het bevel onrechtmatig is gegeven of foutief wordt uitgevoerd)? Wat zijn de gevolgen van een en ander voor de civiele aansprakelijkheid van de ISP?

Indien een ISP informatie van de inhoudsaanbieder ontoegankelijk maakt kan deze dientengevolge schade leiden. De schade kan bijvoorbeeld bestaan uit omzetverlies indien op de webpagina goederen of diensten te koop worden aangeboden of uit derving van advertentieinkomsten, welke inkomsten uiteraard afhankelijk zijn van de beschikbaarheid van de desbetreffende advertenties en informatie waarbij de advertentie is geplaatst. De inhoudsaanbieder die zijn schade wil verhalen op de ISP zal zijn eis doorgaans baseren op wanprestatie door de ISP. De ISP zal zich echter erop beroepen dat hij niet de informatie op eigen initiatief ontoegankelijk heeft gemaakt doch dat hij ter uitvoering van een bevel van de Officier van Justitie heeft gehandeld. Hierna wordt bezien wat de juridische merites van een dergelijk verweer van de ISP zijn.

4.4.1. Aansprakelijkheid bij een rechtmatig gegeven bevel

In wezen beroept een ISP zich op overmacht, oftewel een niet-toerekenbare tekortkoming in de nakoming van een verbintenis. Onder welke omstandigheden is er sprake van overmacht? Art. 6:75 BW omschrijft het als volgt:

---

klachten van gebruikers en de wijze waarop invulling wordt gegeven aan de samenwerking met de meldpunten, worden binnen de branche afspraken gemaakt. Deze vorm van zelfregulering juich ik toe en wordt door de overheid ook bevorderd en gefaciliteerd.’

> Een tekortkoming kan de schuldenaar niet worden toegerekend, indien zij niet is te wijten aan zijn schuld, noch krachtens wet, rechtshandeling of in het verkeer geldende opvattingen voor zijn rekening komt.

Voor overmacht is vereist dat de schuldenaar (hier de ISP) in de onmogelijkheid verkeert alsnog zijn plicht na te komen en dat dat hem niet toegerekend kan worden. Brengt een bevel van een officier van justitie de ISP in een situatie van 'onmogelijkheid' om te presteren? Onder onmogelijkheden worden verboden bij wet of wettige overheidsmaatregel (een zogenaamd fait de prince) begrepen.[30] Dat een bevel van de Officier van Justitie als een fait de prince te zien is, is niet twijfelachtig: het bevel laat de ISP juridisch gezien geen keuze. Het opzettelijk negeren van het bevel van de Officier van Justitie is strafbaar op grond van art. 184 Sr.[31] Gegeven de onmogelijkheid tot presteren is de vervolgvraag of het aan de schuld van de schuldenaar (hier: de ISP) te wijten is dan wel anderszins voor zijn risico komt dat hij in een 'situatie van onmogelijkheid' is komen te verkeren. Bij wettelijke voorschriften en overheidsmaatregelen zal de verhindering te presteren doorgaans niet aan de schuldenaar toe te rekenen zijn als het overheidsverbod alle wijzen van nakoming verhindert.[32] Een bevel van de Officier van Justitie kent inderdaad geen ontsnappingsmogelijkheid, zodat een beroep op overmacht gerede kans heeft te slagen.

Slechts in uitzonderlijke gevallen wordt overmacht uitgesloten ondanks een overheidsmaatregel die alle mogelijkheden van nakoming uitsluit. In de privaatrechtelijke literatuur wordt bijvoorbeeld het geval genoemd waarin de overheidsmaatregel ten tijde van het aangaan van de overeenkomst voorzienbaar was. Dit lijkt echter van weinig belang te zijn voor niet-nakoming ten gevolge van een bevel tot ontoegankelijkmaking van een OvJ. Een ISP zal bij het aangaan van een dienstverleningsovereenkomst met een nieuwe abonnee in het algemeen niet kunnen voorzien dat een Officier van Justitie in het (dan nog toekomstige) informatieaanbod van deze nieuwe abonnee aanleiding ziet met een bevel te komen.

4.4.2. Aansprakelijkheid bij een onrechtmatig gegeven bevel

Betrof het voorgaande de situatie waarin de Officier van Justitie rechtmatig een bevel gaf, hier zullen we de positie van de ISP bezien in geval een Officier van Justitie onrechtmatig een bevel geeft. Dit is bijvoorbeeld het geval indien het informatieaanbod waarop het bevel tot ontoegankelijkmaking betrekking heeft niet strafbaar is of indien de r-c geen schriftelijke machtiging heeft gegeven.

Ook hier moeten weer de vragen naar de onmogelijkheid (of verhindering) en de toerekenbaarheid gesteld worden. Een onrechtmatig gegeven bevel verhindert de schuldenaar in beginsel niet te presteren. De schuldenaar hoeft zich aan een onrechtmatig gegeven bevel immers niet te storen. Dit geldt ook voor de ISP. Het opzettelijk negeren van een onbevoegd gegeven bevel is niet strafbaar op grond van art. 184 Sr.[33] Er zijn echter situaties waarin toch sprake kan zijn van overmacht. Indien bijvoorbeeld de r-c of de OvJ met toepassing van art. 125o Sv de desbetreffende gegevens zelf ontoegankelijk maakt zodanig dat de ISP niet meer over die gegevens beschikt dan is er uiteraard wel weer sprake van een onmogelijkheid tot presteren welke de ISP niet toegerekend kan worden. Ook indien het

---

[30] A.S. Hartkamp, Verbintenissenrecht, Deel 1, De verbintenis in het algemeen, Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, Zwolle: Tjeenk Willink 1988, p. 258. Zie ook A.C. van Empel, Overmacht, Serie: Studiepockets privaatrecht, Zwolle: Tjeenk Willink 1981, p. 26 e.v. en A.J. Goedmakers, Overmacht bij overeenkomst en onrechtmatige daad (dissertatie Rotterdam), 1998, p. 189 e.v.

[31] Zie *Kamerstukken II* 2001-2002, 28 197, nr. 3 , p. 66: 'Wanneer de tussenpersoon niet aan een bevel gevolg geeft, kan hij zich niet op de vervolgingsuitsluitingsgrond beroepen en kan hij strafrechtelijk worden vervolgd terzake van het niet voldoen aan een bevoegd gegeven ambtelijk bevel (artikel 184 Wetboek van Strafrecht).'

[32] A.S. Hartkamp, Verbintenissenrecht, Deel 1, De verbintenis in het algemeen, Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, Zwolle: Tjeenk Willink 1988, p. 273.

[33] Zie bijvoorbeeld HR 11 december 1990 NJ 1991, 423 m.nt. Th.W.v.V.

negeren van het onrechtmatig gegeven bevel de ISP blootstelt aan een 'unzumutbar' gevaar kan hij zich op overmacht beroepen.[34] Dit is bijvoorbeeld het geval indien de OvJ de ISP in hechtenis dreigt te nemen bij weigering de gegevens ontoegankelijk te maken.

De hamvraag bij de onrechtmatig gegeven bevelen is echter of het feit dat de ISP het bevel te goeder trouw als rechtmatig gegeven heeft beschouwd een grond voor overmacht oplevert. In het strafrecht kan het te goeder trouw opvolgen van een onbevoegdelijk gegeven bevel wel schulduitsluiting ex art. 43 lid 2 Sr opleveren, en wel wanneer de nakoming van het bevel binnen de kring van de ondergeschiktheid van de bevolene is gelegen. Het is moeilijk gebleken bevestigd te krijgen dat dit naar analogie ook in het privaatrecht geldt. Wij zouden daarom het volgende aan willen nemen. Indien het bevel van de OvJ kennelijk onrechtmatig is, dan komt de ISP die het bevel opvolgt geen beroep op overmacht toe. Indien echter de ISP in redelijkheid heeft kunnen dwalen omtrent de rechtmatigheid van het bevel, dan zou de ISP niet een beroep op overmacht onthouden mogen worden met het argument dat hij door onderzoek te verrichten de inadequate grondslag van het bevel had kunnen ontdekken. Wij achten de volgende argumenten daarvoor doorslaggevend.

- Het bevel tot ontoegankelijkmaking is gelegen binnen de kring van ondergeschiktheid van de ISP. Het betreft immers een soort bevel dat expliciet door de wet zal worden voorzien en dat de ISP – als het regeerakkoord daarvoor als maatstaf mag gelden – in de toekomst nog vaak zal krijgen.
- Het past niet bij het gezag dat van bevelen van de Officier van Justitie uitgaat dat zij 'standaard' op rechtmatigheid onderzocht zouden moeten worden.
- De ratio van art. 54a Sr is expliciet om de inhoudelijke beoordeling van een informatieaanbod uit handen te nemen van de ISP en in handen te leggen van de r-c en OvJ. Indien de ISP geen beroep op overmacht zou kunnen doen, zou hij met het oog op een eventuele schadeclaim van de inhoudsaanbieder alsnog de rechtmatigheid van het onderliggende informatieaanbod moeten onderzoeken om zo zicht te krijgen op de rechtmatigheid van het bevel van de OvJ. In het licht van de ratio van art. 54a Sr en de Richtlijn is een dergelijke 'onderzoeksplicht' onwenselijk, omdat zij de rechtszekerheid die art. 54a Sr beoogt te bieden voor een deel weer wegneemt.
- Als steunargument zou nog genoemd kunnen worden dat art. 6:75 BW voor datgene wat als overmacht heeft te gelden aansluiting zoekt bij de wet en de in het verkeer geldende opvattingen. Art. 43 lid 2 Sr zou als kenbron kunnen fungeren voor de in het verkeer geldende opvattingen.

Dit betekent wel dat er een verschil bestaat tussen de niet-strafbaarheid van het materiaal en andere vormen waardoor een NTD-bevel onrechtmatig is. Indien bijvoorbeeld in het bevel van de OvJ elke verwijzing naar een afgegeven schriftelijke machtiging van de r-c ontbreekt, zal men moeilijk kunnen beweren dat de ISP in redelijkheid dwaalt als hij blindelings het bevel uitvoert. Hij zal niet de details van de machtiging van de r-c moeten (of mogen) toetsen, maar een *prima facie*-toets op aanwezigheid van een rechterlijke machtiging zal wel voor de hand liggen, wil de ISP aansprakelijkheid jegens de inhoudsaanbieder voor het uitvoeren van een onrechtmatig gegeven bevel ontlopen. Mogelijk bestaat er in dit licht ook behoefte aan de ISP-kant om bezwaar te maken tegen een ontoegankelijkmakingsbevel als zij van oordeel zijn dat het bevel onmiskenbaar onjuist of ongerechtvaardigd is, vanwege de vrees aansprakelijk gesteld te worden door de inhoudsaanbieder.[35] De wetgever zal bij de vormgeving van een NTD-procedure de wenselijkheid van een dergelijke rechtsgang moeten bepalen.

---

[34] A.S. Hartkamp, Verbintenissenrecht, Deel 1, De verbintenis in het algemeen, Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, Zwolle: Tjeenk Willink 1988, p. 273.

[35] Vergelijk de behoefte bij sommige ISP's aan een beroepsmogelijkheid tegen een vermeend onjuist of onrechtmatig tapbevel, zie Koops, Bert-Jaap e.a. (2005), *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, Tilburg, november 2005, http://arno.uvt.nl/show.cgi?fid=46971, p. 40.

De niet-aansprakelijkheid van de ISP voor het opvolgen van een bevel heeft belangrijke consequenties. We verwijzen hier naar het feit dat het technisch en organisatorisch niet altijd haalbaar is alleen het strafbare materiaal te verwijderen, en er dus een wezenlijk risico is op 'bijvangst': rechtmatig materiaal dat en passant ook ontoegankelijk wordt gemaakt (zie par. 2.2.3). Ook voor die gegevens zal de ISP niet aansprakelijk zijn jegens de aanbieders van de rechtmatige inhoud. Zij kunnen echter substantiële schade lijden, bijvoorbeeld door advertentie-inkomsten gegenereerd door bezoekersaantallen te missen. Dit betekent niet alleen dat de OvJ zeer terughoudend zal moeten zijn met een ontoegankelijkmakingsbevel wanneer er gerede kans bestaat op bijvangst, maar ook dat er een vangnet zal moeten zijn voor gevallen waarin het bevel van de OvJ toch, voorzien of onvoorzien, leidt tot bijvangst (behoudens natuurlijk foutieve uitvoering van het bevel door de ISP, zie verderop). Wellicht is een schadefonds waarop benadeelden een beroep kunnen doen een mogelijkheid. Dit is een belangrijk aandachtspunt bij de opzet van een op te zetten NTD-procedure in de vervolgfase van dit onderzoek.

De ISP kan naast een beroep op overmacht – zoals in het burgerlijk wetboek omschreven - tot op zekere hoogte ook pogen de gevolgen van het ontoegankelijkmaken van gegevens zelf in de hand nemen door daarover bepalingen op te nemen in zijn algemene voorwaarden. Dit zouden enerzijds voorwaarden kunnen zijn die de catalogus aan feiten die overmacht opleveren uitbreiden ten opzichte van wat wettelijk geldt.[36] Anderzijds is het mogelijk aansprakelijkheid uit te sluiten of te beperken voor feiten die zonder exoneratie wanprestatie zouden hebben opgeleverd. In de praktijk is het effect vergelijkbaar. Het is echter twijfelachtig of een exoneratie c.q. uitbreiding van overmachtsfeiten zo ver kan reiken dat ook de aansprakelijkheid voortvloeiend uit het weghalen van een rechtmatig informatieaanbod uitgesloten kan worden. In de literatuur wordt aangegeven dat desbetreffende bedingen wel eens onredelijk bezwarend zouden kunnen blijken, dan wel in strijd zouden kunnen zijn met de redelijkheid en billijkheid.[37] Daar staat echter tegenover dat voorzover wij zien geen ISP specifiek in zijn algemene voorwaarden heeft opgenomen dat het 'dwalenderwijs' opvolgen van een niet onmiskenbaar onrechtmatig bevel van een Officier van Justitie strekkend tot ontoegankelijkmaking overmacht oplevert. Gegeven bovenstaande argumenten zouden wij niet willen aannemen dat een dergelijk beding onredelijk bezwarend of in strijd met de redelijkheid en billijkheid is.

We zagen hiervoor dat het uitvoeren van een onrechtmatig gegeven bevel niet steeds overmacht oplevert jegens de inhoudsaanbieder. Ook een exoneratie of contractuele uitbreiding van overmachtsfeiten is in de verhouding van ISP en inhoudsaanbieder met onzekerheden omgeven. Het instrument van de vrijwaring zou echter wel een oplossing kunnen bieden. Indien de ISP of de Officier van Justitie via een notificatie op de hoogte geraakt van een mogelijk strafbaar informatieaanbod, kan allicht de notificeerder of de Officier van Justitie de ISP vrijwaren voor eventuele aansprakelijkheden voortvloeiend uit de ontoegankelijkmaking. Daarbij dient wel gedifferentieerd te worden naar inhoudstype. Van een rechthebbende die een notificatie uitbrengt over inbreuk op zijn intellectueel eigendomsrecht is het redelijk een vrijwaring te verlangen. Van een goedwillende burger die een geval van kinderpornografie of haatzaaien meldt kan dat uiteraard niet verlangd worden. Dan ligt het eerder op de weg van de Officier van Justitie een vrijwaring te verlenen, indien wettelijke en contractuele regels over overmacht hier geen soelaas bieden.

[36] Enkele voorbeelden zijn te vinden bij L.A.R. Siemerink, De overeenkomst van Internet Service Providers met consumenten, Deventer: Kluwer 2007, p. 391-392.
[37] Zie L.A.R. Siemerink, De overeenkomst van Internet Service Providers met consumenten, Deventer: Kluwer 2007, p. 274-275.

Het is wel verstandig kaderafspraken over vrijwaring in een notice-and-take-down procedure op te nemen, met name om de procedure efficiënt te laten verlopen en ter vergroting van de rechtszekerheid voor de ISP. [38]

4.4.3. Aansprakelijkheid bij foutieve uitvoering door de ISP

Hoewel het bevel zelf rechtmatig kan zijn, kan onrechtmatigheid ontstaan door foutieve uitvoering door de ISP. Hiervan is bijvoorbeeld sprake indien de ISP andere gegevens ontoegankelijk maakt dan die waarop het bevel betrekking heeft. In beginsel is dit een omstandigheid die voor risico van de ISP komt. Een beroep op overmacht lijkt niet mogelijk. Slechts indien het bevel de ontoegankelijk te maken gegevens op een misleidende manier identificeert zou men dit misschien als een onrechtmatig gegeven bevel kunnen zien, maar dit lijkt meer een uitzonderingssituatie te zijn.

4.5. Vervolging van het gronddelict

Impliceert de inzet van de bevelsbevoegdheid de verplichting tot vervolging van het gronddelict?

Juist omdat de vrijheid van meningsuiting bij het ontoegankelijk maken van openbare informatie sterk op de voorgrond treedt, is het wenselijk dat de ontoegankelijkmaking achteraf getoetst kan worden door de rechter. Een verplichting tot vervolging van de inhoudsaanbieder voor het gronddelict is echter om een aantal reden niet gewenst. Bij buitenlandse inhoud is het lang niet altijd opportuun om tot vervolging over te gaan. Weliswaar kan onder omstandigheden Nederlandse rechtsmacht bestaan over in het buitenland geherbergde informatieaanboden die ook vanuit Nederland toegankelijk zijn (zie hoofdstuk 5), maar het is bijvoorbeeld niet altijd mogelijk het benodigde bewijsmateriaal te verzamelen of uitlevering van de verdachte te vragen, of het is uit respect voor de soevereiniteit van andere staten niet opportuun tot vervolging over te gaan.

Daarnaast kan het OM het ook bij Nederlands informatieaanbod opportuun achten om niet te vervolgen, bijvoorbeeld omdat het delict een relatief lage opsporingsprioriteit heeft (een ontoegankelijkmakingsbevel zal in de gevallen overigens alleen proportioneel zijn als de vrijheid van meningsuiting niet of nauwelijks in het geding is, zoals bij phishing-pagina's), of de middelen en expertise kunnen ontbreken om de inhoudsaanbieder te achterhalen. Verder kan het ook voorkomen dat een voorwaarde voor vervolging ontbreekt, zoals een klacht van het slachtoffer, of omdat de inhoudsaanbieder overleden is.

Kortom, een verplichting tot vervolging is niet wenselijk. Het is bovendien ook niet nodig, omdat toetsing achteraf hoeft niet per se plaats hoeft te vinden in een tegen de inhoudsaanbieder aanhangig gemaakte hoofdzaak. De toetsing kan ook geschieden in het kader van een beklagprocedure (zie par. 4.6).

4.6. Beroepsmogelijkheden

Welke beroepsmogelijkheden zijn er voor de OvJ en de ISP? Welke beroepsmogelijkheden zijn er voor de persoon die leverancier is van de inhoud?

Beroepsmogelijkheden voor de ISP en de inhoudsaanbieder zijn van groot belang. Enerzijds impliceert de betrokkenheid van de r-c voorafgaand aan ontoegankelijkmaking niet dat de r-c de ISP of inhoudsaanbieder hoort. Anderzijds is niet gegarandeerd dat de OvJ achteraf tot vervolging van de inhoudsaanbieder overgaat. Zelfs als hij wel vervolgt dan heeft de ISP

[38] *Kamerstukken II* 2003–2004, 28 197, nr. 15, p. 4: 'In de vijfde plaats zouden er afspraken kunnen worden gemaakt die er op neer komen dat degene die om ontoegankelijkmaking verzoekt, zo nodig, de internet service provider vrijwaart tegen een eventuele claim van de information provider vanwege wanprestatie.'

geen rol in dat proces. Beroepsmogelijkheden stellen de ISP en inhoudsaanbieder dus in staat door een rechter gehoord te worden over een ontoegankelijkmaking. In dit verband is art. 125m Sv van belang dat voorschrijft dat betrokkenen bij ontoegankelijkmaking (ex art. 125o Sv) daarvan – achteraf – op de hoogte worden gesteld.[39] Het schept daarmee een waarborg dat betrokkenen hun beroepsmogelijkheden ook daadwerkelijk kunnen uitoefenen.

Hiervoor is aangegeven dat noch art. 54a Sr, noch art. 125o Sv een adequate grondslag bieden voor het NTD-bevel. Tegelijk met het scheppen van een bevoegdheidsgrondslag, zullen dus ook zelfstandige beroepsmogelijkheden geschapen moeten worden. We geven hier enkele algemene overwegingen over beroepsmogelijkheden tegen de uitoefening van de te creëren bevoegdheid.

Voor anderen dan de OvJ is het beklagrecht van art. 552a lid 1 Sv van belang. Het luidt voor zover van belang als volgt:

> De belanghebbenden kunnen zich schriftelijk beklagen [...] over de vordering medewerking te verlenen aan het ontsleutelen van gegevens [...] over de ontoegankelijkmaking van gegevens, aangetroffen in een geautomatiseerd werk, bedoeld in artikel 125o, de opheffing van de desbetreffende maatregelen of het uitblijven van een last tot zodanige opheffing.

Het ligt voor de hand deze bepaling ook van toepassing te verklaring op het NTD-bevel. Belanghebbenden kunnen dan bezwaren die ze hebben tegen ontoegankelijkmaking, de opheffing van de ontoegankelijkheid, of het uitblijven van de beëindiging ervan voorleggen aan de raadkamer. Zowel de ISP als de inhoudsaanbieder zijn als belanghebbenden aan te merken. Wellicht dat ook de persoon die van de ontoegankelijk gemaakte gegevens kennis had willen nemen als belanghebbende aangemerkt kan worden. De OvJ wiens vordering tot ontoegankelijkmaking door de r-c is afgewezen is niet te zien als belanghebbende in de zin van deze bepaling. Hij kan echter van de beroepsmogelijkheid van art. 446 Sv gebruik maken, waarover later meer.

Zou het beklag van art. 552a Sv niet open staan, dan moet de ISP of de inhoudsaanbieder een kort geding bij de voorzieningenrechter aanspannen als hij zijn bezwaar tegen de ontoegankelijkmaking, de beëindiging ervan of het uitblijven van de beëindiging daarvan aan een rechter wil voorleggen. De voorzieningenrechter fungeert als een soort vangnetinstantie voor rechtsbescherming tegen strafvorderlijke beslissingen waartegen geen rechtsgang open staat op basis van het Wetboek van Strafvordering of specifieke wetten. Als vangnetinstantie lijkt het kort geding aardig te functioneren. Dit ondanks het feit dat het kort geding theoretisch slechte papieren heeft om als finale rechtsbescherming te dienen. Het kort geding is immers accessoir aan een bodemprocedure – die in de praktijk meestal achterwege gelaten wordt – en de uitspraak van de voorzieningenrechter is voorlopig. Dat kan bezwaarlijk worden indien de door de voorzieningenrechter te nemen beslissing enig onderzoek vergt. Voor het beoordelen van haatzaai-informatie kan bijvoorbeeld onderzoek naar de bron van de informatie vereist zijn, omdat de functie van de uitdrager – geestelijke, journalist – van invloed kan zijn op de (niet-)strafbaarheid van de uiting. Indien – zoals de intentie in het regeringsakkoord doet vermoeden – op grotere schaal gebruik gemaakt gaat worden van de bevoegdheid om gegevens ontoegankelijk te maken, dan is een kort geding zeker geen goede oplossing voor beklag. Bovendien is het kort geding naar zijn aard als algemeen vangnet weinig geschikt als rechtsbeschermingsinstrument voor specifieke doeleinden.[40] Aan een structurele behoefte aan specifieke rechtsbescherming moet structureel worden voldaan, en daarom verdient een specifieke strafvorderlijke rechtsgang de voorkeur.

---

[39] Onder bepaalde in art. 125m Sv genoemde omstandigheden kan mededeling achterwege blijven of uitgesteld worden.

[40] Vgl. Griend, E.S.G.N.A.I. van de (2002), *Hiaten in de strafrechtelijke rechtsbescherming. Een onderzoek naar aanleiding van het kort geding in strafzaken* (dissertatie Tilburg), Nijmegen: WLP 2002.

Als art. 54 a Sr of art 125o Sv als bevoegheidsgrondslag wordt gehanteerd, heeft de OvJ een machtiging van de r-c nodig respectievelijk is het de r-c die binnen een gvo bepaalt dat ontoegankelijk gemaakt wordt. Indien door wetswijziging in een bevoegdheidsgrondslag wordt voorzien, is aannemelijk dat ook dan de r-c voorafgaand betrokken is bij een bevel tot ontoegankelijkmaking. Een en ander roept de vraag op welke beroepsmogelijkheid de Officier van Justitie kan hanteren als hij bezwaar heeft tegen een beslissing van de r-c, bijvoorbeeld indien die beslist om niet tot ontoegankelijkmaking over te gaan. Hier is art. 446 Sv relevant. De eerste zin van het eerste lid van art. 446 Sv luidt:

> Voor zover niet bijzondere bepalingen het recht van hoger beroep van het openbaar ministerie regelen, kan dit van alle beschikkingen van de rechtbank of de rechter-commissaris waarbij een krachtens dit wetboek genomen vordering niet is toegewezen, binnen veertien dagen in hoger beroep komen bij het gerechtshof of de rechtbank.

Vereist is derhalve een krachtens het Wetboek van Strafvordering genomen vordering van de Officier van Justitie. De Hoge Raad interpreteert dit vereiste strikt, omdat art. 446 Sv wel aan het OM maar niet aan de verdachte een algemeen recht van hoger beroep toekent tegen beschikkingen.[41] Indien art. 54a Sr als bevoegdheidsgrondslag zou worden gehanteerd, dan zou de OvJ zonder beroepsmogelijkheden zitten. Dit is eens te meer een reden om de NTD-bevelsbevoegdheid als zelfstandige bevoegdheid in het Wetboek van Strafvordering op te nemen, zodat automatisch een beroep voor de OvJ open staat ex art. 446 Sv.

4.7. Rol van de inhoudsaanbieder

In hoeverre kan of moet de inhoudsleverancier betrokken worden in het besluitvormingstraject dat leidt tot het bevel van de OvJ en/of het uitvoeren ervan?

Indien er sprake is van in georganiseerd verband, of beroeps- of bedrijfsmatig of herhaald plegen van soortgelijke delicten of anderszins strafrechtelijk optreden geïndiceerd wordt geacht dan is er weinig reden het onderzoek te compromitteren door in voortijdig stadium de verdachte op de hoogte te brengen van een strafrechtelijk onderzoek dat op hem betrekking heeft. In die gevallen zal een NTD-bevel echter ook meestal niet worden overwogen, omdat hierdoor de verdachte of betrokkenen automatisch op de hoogte geraken van het strafvorderlijk onderzoek. Derhalve kunnen we aannemen dat het verwijderen van de inhoud belangrijker wordt geacht dan het geheimhouden van een strafvorderlijk optreden.

Het is dan allicht geïndiceerd eerst te beproeven of de inhoudsaanbieder bereid is de informatie vrijwillig van het net te halen.[42] De eis van subsidiariteit brengt zelfs mee dat deze weg eerst bewandeld wordt voordat tot het toepassen van dwangmiddelen wordt overgegaan. Bovendien kan van een contact met de inhoudsaanbieder een moraliserend effect uitgaan, zodat deze niet snel opnieuw tot plaatsing van een strafbaar informatieaanbod overgaat. Wanneer de inhoudsaanbieder echter weigert of niet reageert, alsmede in situaties waarin de inhoudsaanbieder niet eenvoudig te achterhalen valt, zal de OvJ het bevel aan de ISP kunnen richten zonder verdere eigen inspanning de inhoudsaanbieder erbij te betrekken.

Naast een verzoek aan de inhoudsaanbieder om vrijwillig het materiaal te verwijderen, kan de inhoudsaanbieder echter ook nog een andere rol krijgen in een NTD-procedure. Dit is vooral van belang in situaties waarin het materiaal niet onmiskenbaar onrechtmatig is, maar er wel behoefte bestaat bij het OM om het materiaal ontoegankelijk te maken. De rechterlijke

[41] HR 26 mei 1992 NJ 1992, 753 en HR 8 september 1992, NJ 1993, 266.
[42] Het meldpunt Discriminatie neemt in de meeste gevallen contact op met de plaatser van de illegale inhoud. In 85 tot 90% van de gevallen leidt dit tot verwijdering van de illegale inhoud door de plaatser zelf, aldus *Kamerstukken II* 2003–2004, 28 197, nr. 15, p. 4.

toets vooraf door de r-c is een belangrijke waarborg tegen het te snel ontoegankelijk maken van dubieus materiaal (zie par. 4.1), maar ook de inhoudsaanbieder zou hier een rol kunnen krijgen. We verwijzen naar het NTD-model zoals dat in de Verenigde Staten bij auteursrechtinbreuken wordt gehanteerd, vastgelegd in de Digital Millennium Copyright Act.[43] Hierbij haalt de ISP na notificatie het materiaal weg dat volgens de notificeerder inbreuk maakt op auteursrechten, onder gelijktijdige notificatie aan de inhoudsaanbieder van de ontoegankelijkmaking. Deze kan vervolgens aangeven dat het zijns inziens toch om rechtmatig materiaal gaat, waarna de ISP het materiaal weer beschikbaar stelt. Vervolgens is het aan de notificeerder om een juridische procedure aanhangig te maken als hij volhoudt dat het materiaal onrechtmatig is.

Dit model nu zou ook overwogen kunnen worden in de Nederlandse NTD-procedure, door de ISP direct na de uitvoering van het ontoegankelijkmakingsbevel de inhoudsaanbieder te notificeren. Indien deze binnen een bepaalde termijn, bijvoorbeeld een week, reageert met de stelling dat het zijns inziens wel degelijk om rechtmatig materiaal gaat (bijvoorbeeld omdat hij een licentie heeft van de auteursrechthebbende, omdat de pornografie 19-jarigen betreft, of omdat de uiting volgens hem binnen de vrijheid van meningsuiting valt), dan zou de ontoegankelijkmaking opgeheven kunnen worden totdat een definitief rechterlijk oordeel is verkregen over de onrechtmatigheid van het materiaal, via een vervolging van de inhoudsaanbieder of via een beklag door de OvJ tegen de weer-toegankelijkmaking (die in deze opzet geschapen zou moeten worden, bijvoorbeeld door toevoeging van een lid aan art. 446 Sv voor dit type NTD-situaties).

Een aldus vormgegeven NTD-procedure heeft belangrijke voordelen, omdat het een belangrijke aanvullende bescherming biedt voor de vrijheid van meningsuiting, met name in situaties waarin het gewraakte materiaal in een grijs gebied valt (wat bijvoorbeeld bij smaad-, discriminatie- en haatzaai-pagina's niet zelden het geval zal zijn). Wanneer de inhoudsaanbieder de gelegenheid heeft te protesteren tegen ontoegankelijkmaking, is een NTD-bevel bij materiaal dat niet onmiskenbaar onrechtmatig is eerder aanvaardbaar vanuit het oogpunt van subsidiariteit en proportionaliteit. Het zou daarmee een handvat kunnen bieden aan het OM bij de bestrijding van onwenselijk materiaal zonder verkillend effect op de vrijheid van meningsuiting. Zonder een dergelijke rol voor de inhoudsaanbieder, zal de OvJ in het grijze gebied van niet-onmiskenbaar onrechtmatig materiaal veel terughoudender moeten zijn om een NTD-bevel te geven. De keerzijde voor het OM is wel dat materiaal na protest van de inhoudsaanbieder weer standaard beschikbaar wordt gesteld, totdat een rechterlijke einduitspraak is verkregen. Naar onze inschatting is deze keerzijde overzienbaar, mede omdat de inhoudsaanbieder actief moet protesteren en zich daarmee bewust blootstelt aan het risico om vervolgens vervolgd te worden voor het inhoudsaanbod. De inhoudsaanbieder zal dat risico veelal alleen willen lopen als hij ervan overtuigd is dat het aanbod rechtmatig is. Het lijkt ons zinvol om deze mogelijkheid nader te onderzoeken bij de vormgeving van een NTD-procedure.

[43] Zie http://www.copyright.gov/legislation/dmca.pdf, p. 12, voor een samenvatting.

5. Jurisdictievragen

Aangenomen mag worden dat het alleen de bedoeling is een NTD-bevel te hanteren voor inhoud die in Nederland wordt aangeboden. Daarbij kan echter een buitenlandse ISP betrokken zijn, en niet zelden zal de inhoud in het buitenland zijn opgeslagen. De vraag is in hoeverre een NTD-bevel in dergelijke gevallen kan worden gegeven.

5.1. Buitenlandse ISP's

In hoeverre kan het bevel ingezet worden tegen buitenlandse ISP's, al dan niet met vestigingen in Nederland?

De Nederlandse strafwet is over het algemeen van toepassing op strafbare feiten die in Nederland worden gepleegd, en Nederlandse opsporingsautoriteiten hebben (enkele sporadische uitzonderingen daargelaten) alleen de bevoegdheid om in Nederland strafvorderlijke handelingen te verrichten. De soevereiniteit van nationale staten staat nauwelijks toe dat grensoverschrijdend wordt opgespoord.[44] Wat betekent dit voor een NTD-bevel wanneer strafbare inhoud in Nederland wordt aangeboden via een buitenlandse ISP?

Wanneer een buitenlandse ISP een vestiging in Nederland heeft, zal er veelal geen probleem optreden. Het bevel kan gericht worden aan de Nederlandse vestiging en blijft dus beperkt tot Nederlands grondgebied. Dat de ISP vervolgens al dan niet de hulp inroept van buitenlandse zuster- of moedervestigingen, doet op zich niet af aan het feit dat Nederland rechtsmacht kan uitoefenen op de ISP. De ISP is in dit geval vergelijkbaar met een Nederlandse ISP. Het zal echter wel afhangen van de situatie of de informatie ook door de Nederlandse vestiging verwijderd kan worden; als de informatie in het buitenland wordt geherbergd, kunnen zich wel problemen voordoen (zie volgende paragraaf).

Wanneer de buitenlandse ISP echter geen vestiging in Nederland heeft, is de situatie problematischer. Een rechtspersoon die diensten aanbiedt in Nederland – zoals het aanbieden van informatie op het Internet die in Nederland toegankelijk is – dient zich te houden aan de Nederlandse wet. Hij kan dus wel eventueel medeaansprakelijk worden gehouden voor strafbare inhoud die hij aanbiedt in Nederland, maar dat wil nog niet zeggen dat een NTD-bevel aan een buitenlandse ISP kan worden gegeven door de Nederlandse autoriteiten. Dat zou een opsporingsgerelateerde handeling betekenen die door het land waar de ISP gevestigd is, als inbreuk op de soevereiniteit kan worden opgevat.

Er zijn slechts enkele precedenten van mogelijkheden om opsporingshandelingen buiten het eigen grondgebied uit te oefenen, waarbij een verdragsrechtelijke of andere internationaalrechtelijke basis nodig is.[45] Binnen het ICT-recht betreffen dat de grensoverschrijdende netwerkzoeking, voorzover de gezochte gegevens publiekelijk toegankelijk zijn of de rechthebbende toestemming gegeven heeft (art. 32 Cybercrime-Verdrag; art. 125j Sv), en het – beperkt – grensoverschrijdend aftappen van telecommunicatie (art. 126ma/ta/zga Sv[46]). Beide zijn gebaseerd op een verdrag. Aangezien

[44] Dit geldt ook voor computernetwerken: ondanks het vermeende 'deterritorialiserende' effect van ICT, houden staten onverkort vast aan nationale soevereiniteit en rechtsmacht op hun eigen grondgebied. Zie Koops, Bert-Jaap & Susan W. Brenner (eds.) (2006), *Cybercrime and Jurisdiction: A Global Survey*, IT & Law Series Vol. 11, The Hague: T.M.C. Asser Press 2006.

[45] Vgl.: 'Overigens zijn grensoverschrijdende opsporingshandelingen wel toegelaten indien ze een basis vinden in het volkenrecht of het interregionale recht (vgl. art. 539a, derde lid, Sv). Daarbij moet allereerst worden gedacht aan een basis in een verdrag. In hoeverre de enkele toestemming van de autoriteiten van een vreemde staat, zonder verdragsrechtelijke grondslag, grensoverschrijdende handelingen van Nederlandse opsporingsambtenaren kan legitimeren, is onduidelijk.' *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 37.

[46] Gebaseerd op de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, 29 mei 2000, *Trb.* 2000, 96.

voor een NTD-bevel geen verdragsrechtelijke basis bestaat, valt niet aan te nemen dat de Nederlandse justitie bevoegd is een NTD-bevel te geven aan een in het buitenland gevestigde ISP.

De OvJ zal in dergelijke gevallen dus zijn toevlucht moeten nemen tot een rechtshulpverzoek aan de staat waar de ISP is gevestigd. Ook een dergelijk rechtshulpverzoek zal echter normaliter gestoeld moeten zijn op een internationale juridische basis – de buitenlandse staat zal immers slechts meewerken als zij ook een dergelijke bevelsbevoegdheid kent en daarvoor vergelijkbare voorwaarden hanteert. Het valt daarom aan te bevelen, als de Nederlandse overheid beoogt om ook een NTD-bevel aan in het buitenland gevestigde ISP's te kunnen geven, om in internationaal (bijvoorbeeld EU- of Raad van Europa-)verband te komen tot een gezamenlijke regeling van een NTD-procedure.

5.2. Buitenlandse informatie

In hoeverre is het bevel inzetbaar als de Nederlandse ISP slechts de in het buitenland geherbergde informatie doorgeeft (al dan niet via een proxy-server)?

Over situaties waarin de strafbare inhoud in het buitenland wordt geherbergd, heeft de wetgever zich uitgelaten in relatie tot het ontoegankelijkmakingsbevel van art. 125o Sv:

> Nederlandse opsporingsambtenaren mogen op computernetwerken slechts onderzoek doen voor zover de Nederlandse rechtsmacht reikt. Dit betekent dat zij geen onderzoek mogen doen wanneer de betrokken computers zich kennelijk buiten Nederland bevinden (…). Aangenomen mag worden dat dit slechts uitzondering lijdt voor zover de opsporingsambtenaar, zoals hierboven aangegeven, als ieder ander mag rondkijken op een openbaar netwerk. Het staat een opsporingsambtenaar dus vrij om met sites waarvan de databestanden zijn opgeslagen op buitenlandse computers, een verbinding te leggen teneinde die sites te bekijken. Wat de opsporingsambtenaar echter níet mag, is op die sites bevoegdheden uitoefenen waarbij inbreuk wordt gemaakt op de rechten van burgers. Voor de voorgestelde maatregel van ontoegankelijkmaking van gegevens betekent dit bijvoorbeeld dat hij **niet mag worden toegepast ten aanzien van gegevens** waarvan men redelijkerwijs kan vermoeden dat zij zijn opgeslagen **in een buitenlandse computer** en zich dus aan de Nederlandse rechtsmacht onttrekken.[47] [**vet** toegevoegd]

> Voor toepassing van de maatregel van ontoegankelijkmaking in computersystemen die zich buiten de Nederlandse rechtsmacht bevinden, zal derhalve een beroep moeten worden gedaan op internationale rechtshulp, ten behoeve waarvan het Cybercrime Verdrag tot stand is gebracht.[48]

Aannemend dat de wetgever bij een NTD-bevelsbevoegdheid niet afwijkt van dit standpunt bij de 125o-bevoegdheid – waarvoor internationaalrechtelijk ook nauwelijks ruimte lijkt –, zal een NTD-bevel dus niet kunnen worden gegeven voor de ontoegankelijkmaking van gegevens in het buitenland.

Dat betekent echter niet per se dat een NTD-bevel onmogelijk is. Justitie kan niet eisen, van Nederlandse noch van buitenlandse ISP's, dat zij buitenlands geherbergde gegevens als zodanig ontoegankelijk maken, maar wellicht is het wel mogelijk om Nederlandse ISP's te bevelen de gegevens *voor aanbod in Nederland* ontoegankelijk te maken. Er bestaat immers wel rechtsmacht over de gegevens voorzover deze in Nederland worden aangeboden. De ISP zou dan niet de gegevens op de server waarop zij staan mogen blokkeren, maar wellicht wel de doorgifte van de gegevens aan afnemers in Nederland. Dat is wat nu feitelijk gebeurt bij de publiek-private samenwerking tussen enkele Internetaanbieders en de politie voor blokkering van kinderporno: de gegevens op bepaalde, door de politie aangewezen, Internetpagina's blijven op zich ongemoeid; de bezoekers die de pagina opvragen krijgen

[47] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 36.
[48] *Kamerstukken II* 2004-2005, 26 671, nr. 10, p. 13. Merk echter op dat het Cybercrime-Verdrag geen regeling bevat van rechtshulp in relatie tot NTD. Het bevat wel een rechtshulpregeling tot bevriezen van gegevens (art. 29), maar dat is een tijdelijke maatregel met een geheel andere reikwijdte dan ontoegankelijkmaking.

echter niet deze pagina te zien, maar een ‘Stop!’-pagina met uitleg dat de desbetreffende pagina kinderporno bevat en wordt geblokkeerd.[49]

Er zijn geen principiële juridische bezwaren tegen het bevelen van een Nederlandse (of in Nederland gevestigde) ISP om buitenlandse pagina’s met strafbare inhoud te blokkeren voor gebruikers in Nederland. Of het technisch haalbaar is, is een ander verhaal, evenals de vraag hoe effectief dit is. Hoogstwaarschijnlijk is een NTD-bevel tot blokkering van doorgifte aan Nederlandse gebruikers minder effectief dan een NTD-bevel tot blokkering van de strafbare gegevens zelf, en transportaanbieders hebben over het algemeen minder mogelijkheden om gegevens te blokkeren dan *hosting*-aanbieders (zie ook par. 2.2).[50]

Deze aspecten zijn wel van belang voor de juridische aanvaardbaarheid van een NTD-bevel, aangezien de subsidiariteit en proportionaliteit in gedrang komen naarmate het bevel technisch moeilijker uitvoerbaar dan wel minder effectief is. Om dit te bepalen, is nader onderzoek naar de uitvoerbaarheid en effectiviteit gewenst.

[49] Zie bijvoorbeeld http://www.nu.nl/news/967126/52/UPC_gaat_kinderporno_blokkeren.html.

[50] Vgl. *Kamerstukken II* 2001–2002, 28 197, nr. 3, p. 65: ‘De dienstverlener die van een ander afkomstige gegevens opslaat, is door de bank genomen in staat de gegevens ontoegankelijk te maken. De dienstverlener die de van een ander afkomstige gegevens doorgeeft, is doorgaans niet goed in staat daartegen adequaat op te treden. De in de artikelsgewijze toelichting bij artikel 196c van Boek 6 van het Burgerlijk Wetboek behandelde Radikall-zaak [sic] vormt daarvan een treffende illustratie (…). Toch zijn er al gevallen denkbaar waarin ook met een relatief eenvoudige ingreep door de tussenpersoon die louter van een ander afkomstige gegevens doorgeeft het gewenste resultaat kan worden bereikt.’

6. Praktische vragen

6.1. Termijn

Op welke termijn moet redelijkerwijze voldaan zijn aan het bevel van de OvJ?

Gezien het feit dat de maatregel van ontoegankelijkmaking mede het karakter heeft tot herstel van een rechtmatige toestand te komen, dient de ISP prompt te handelen om ontoegankelijkheid te bewerkstelligen. Hoeveel tijd de ISP precies gegund moet worden om tot ontoegankelijkheid te komen hangt af van de gecompliceerdheid van de technische handelingen die daartoe verricht moeten worden. Zeker indien de ISP daartoe hulp zou moeten inroepen van andere netwerkbeheerders, is het van belang hem daartoe enige tijd te gunnen. De OvJ doet er uiteraard verstandig aan in het bevel een (redelijke) termijn op te nemen waarbinnen de ISP tot ontoegankelijkmaking over moet gaan. Indien de ISP binnen de aangegeven termijn niet aan het bevel kan voldoen, dan ligt het voor de hand daarover contact op te nemen met de OvJ en zijn best te doen het materiaal zo spoedig mogelijk, zij het na de gestelde termijn, ontoegankelijk te maken. Mocht de OvJ dit onredelijk lang vinden duren, dan kan hij (de ISP gehoord hebbend en de redenen voor de 'vertraging' in acht nemend) besluiten de ISP te vervolgen voor medeplichtigheid aan het beschikbaar stellen van strafbaar materiaal. De rechter kan dan vervolgens bepalen wat in casu een redelijke termijn was. Hopelijk zal een dergelijke procedure niet vaak gevolgd hoeven te worden en zal de praktijk, al dan niet ondersteund door enige jurisprudentie, leren wat een redelijke termijn is in welk type gevallen voor de ISP om uitvoering te geven aan het bevel.

6.2. Kosten

Wie draagt de kosten van de uitvoering van het bevel en, indien dit de ISP is, welke juridische verhaalsmogelijkheden heeft de ISP (op de inhoudsaanbieder of de overheid)?

De ISP die gevolg geeft aan een bevel van de OvJ wil allicht de kosten die hij daarvoor moet maken op de overheid verhalen. Het Wetboek van Strafvordering kent geen algemene regeling voor vergoeding van kosten, doch alleen een regeling voor enkele specifieke gevallen. De bepaling die voorziet in kostenvergoedingen aan anderen dan verdachten – art. 592 Sv – biedt momenteel geen basis voor een vergoeding aan de ISP voor kosten die gemoeid zijn met ontoegankelijkmaking.[51] Het valt te overwegen om de mogelijkheid van kostenvergoeding via art. 592 Sv open te stellen, zoals dit ook gebeurd is bij de Wet vorderen gegevens (voor art. 126nc en volgende Sv). Dit is een politieke afweging, die mede samenhangt met de visie op wat een normaal bedrijfsrisico is voor ISP's (zie ook onder).

Voorts is van belang de Wet Tarieven in Strafzaken, die algemener is geformuleerd, maar deze wordt in de praktijk vooral toegepast voor vergoeding van kosten gemaakt door psychologen, psychiaters en tolken. In de Memorie van Toelichting bij de Wet Computercriminaliteit II wordt echter de deur op een kier gezet voor een kostenvergoeding via de Wet tarieven in Strafzaken. Sprekend over art. 125o Sv wordt opgemerkt:

[51] Art. 592 lid 2 Sv noemt de bevoegdheden van art. 54a Sr en art. 125o Sv niet: 'De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 126m, 126n, 126nc tot en met 126ni, 126t, 126u, 126uc tot en met 126ui en 126zja tot en met 126zp kunnen de betrokkene uit 's Rijks kas worden vergoed. Hierbij kan een lager bedrag worden vergoed voor zover degene tot wie het bevel zich richt, niet de administratie heeft gevoerd en de daartoe behorende boeken, bescheiden en andere gegevensdragers heeft bewaard als voorgeschreven in artikel 10 van Boek 2 en artikel 15i van Boek 3 van het Burgerlijk Wetboek.'

> Daarbij moeten uiteraard de eisen van proportionaliteit en subsidiariteit in acht worden genomen. Dit vereist in het bijzonder in netwerkomgevingen voorzichtigheid, opdat niet onnodig schade wordt toegebracht aan gegevens of systemen. Soms zal het daarom in de rede liggen om de medewerking van de netwerkbeheerder te vragen. Deze kan daarvoor eventueel een vergoeding krijgen op grond van de Wet tarieven in strafzaken.[52]

Deze laatste opmerking is echter later ingetrokken:

> In de memorie van toelichting (nr. 3, blz. 21) was terzake van ontoegankelijkmaking het volgende gemeld: « (…) Deze kan daarvoor eventueel een vergoeding krijgen op grond van de Wet tarieven in strafzaken.». Deze laatste volzin is onjuist. Slechts indien sprake is van afgedwongen medewerking, biedt de wet een grondslag voor vergoeding. Een dergelijke medewerkingsplicht voor de systeembeheerder bij de ontoegankelijkmaking wordt door het wetsvoorstel niet in het leven geroepen. Er is dan ook geen aanspraak op een vergoeding, tenzij in een individueel geval een vergoeding wordt overeengekomen.[53]

De Wet Tarieven in Strafzaken biedt dus bij vrijwillige medewerking door de ISP geen soelaas. Nu bij een te creëren NTD-bevelsbevoegdheid wel een verplichting tot medewerking door de ISP wordt geschapen, zal de Wet Tarieven in Strafzaken echter wel van toepassing verklaard kunnen worden op een NTD-bevel. Het vergt nader onderzoek om te bepalen of vergoeding op basis van deze wet past bij het onderhavige type verplichte medewerking door ISP's, of dat een specifieke vergoeding ex art. 592 Sv meer in de rede ligt, of dat geen vergoeding aangewezen is omdat verwijderen van strafbaar materiaal op vordering van de OvJ valt onder het bedrijfsrisico van de ISP.

Bij gebreke aan een specifieke strafrechtelijke grondslag voor onkostenvergoeding, kan een ISP overigens mogelijk nog terugvallen op de algemene bestuursrechtelijke en civielrechtelijke regels over vergoedingen na rechtmatig overheidsoptreden. In dit verband is de uitspraak van de Hoge Raad in de zaak Staat/Lavrijsen relevant. In deze zaak werd bij een huiszoeking bij een ander dan de verdachte schade toegebracht door degenen die de huiszoeking verrichtten. Lavrijsen – bij wie de huiszoeking plaatsvond – vorderde schadevergoeding van de staat. De Hoge Raad overwoog:[54]

> het enkele feit dat een huiszoeking overeenkomstig de regels van strafvordering is geschied, staat niet in de weg aan het oordeel dat het daarbij toebrengen van zodanige schade onrechtmatig kan zijn. [...]
>
> Een van de verschijningsvormen van het gelijkheidsbeginsel is de regel dat de onevenredig nadelige, – dat wil zeggen: buiten het normale maatschappelijke risico of het normale bedrijfsrisico vallende, en op een beperkte groep burgers of instellingen drukkende – gevolgen van een overheidshandeling of overheidsbesluit niet ten laste van die beperkte groep behoren te komen, maar gelijkelijk over de gemeenschap dienen te worden verdeeld (vgl. HR 8 januari 1991, nr. 14 096, NJ 1992, 638, ABRvS, 6 mei 1997, AB 1997, 229, alsmede art. 3:4 lid 2 Awb). Uit deze regel vloeit voort dat het toebrengen van zodanige onevenredige schade bij een op zich zelf rechtmatige overheidshandeling als de onderhavige huiszoeking jegens de getroffene onrechtmatig is.

Het gelijkheidsbeginsel brengt dus mee dat uitsluitend onevenredig nadelige schade voor vergoeding in aanmerking komt. Voor wat betreft de ISP is de vraag of het uitvoeren van bevelen tot ontoegankelijkmaking behoort tot diens normale bedrijfsrisico. Dat lijkt wel het geval te zijn. Internetaanbieders kunnen – en willen allicht ook – niet volledig hun ogen sluiten voor de negatieve maatschappelijke implicaties die hun dienstverlening kan hebben. Dat ISP's een eigen verantwoordelijkheid hebben kan ook afgeleid worden uit de Richtlijn inzake elektronische handel.

> De richtlijn roept de lidstaten op om aan te moedigen dat op basis van vrijwillige overeenkomsten tussen alle betrokken partijen de uitwerking ter hand wordt genomen van snelle, betrouwbare mechanismen om onwettige informatie te verwijderen en ontoegankelijk te maken (preambule 40).

---

[52] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 21.
[53] *Kamerstukken II* 2004-2005, 26 671, nr. 10, p. 16.
[54] HR 30 maart 2001 AB 2001/412 (Staat/Lavrijsen).

Wellicht dat ook steun geput kan worden uit het Scientology-vonnis. In het vonnis deed de rechtbank haar oordeel dat van ISP's verlangd kon worden dat zij kennelijk onrechtmatige informatie prompt van het net moeten halen mede steunen op de overweging dat ISP's bedrijfsmatig handelen. Het bedrijfsmatig handelen impliceert kennelijk een zekere verantwoordelijkheid, waarbij optreden naar aanleiding van notificaties van een dergelijke bedrijfsmatig handelende ISP verlangd kan worden. De rechtbank heeft daarbij niet overwogen dat Scientology – de notificeerder – aan de ISP enige vergoeding verschuldigd zou zijn. We nemen aan dat het incidenteel ontoegankelijk maken van gegevens geen onevenredig nadeel oplevert voor de ISP en dat het valt binnen het normale bedrijfsrisico.

De vraag is echter wat te gelden heeft indien de overheid gericht en stelselmatig bepaalde informatie – zoals haatzaai-informatie – van het Internet wil weren met medewerking van de ISP's. Op zich is de kwantiteit van de notificaties niet zonder meer beslissend en zou men kunnen aannemen dat ook dit nog tot het normale bedrijfsrisico van de ISP behoort. Er zit echter wel een grens aan wat men van ISP's kan verwachten. Zij hebben reeds strafvorderingsgerelateerde plichten tot aftapbaarheid en medewerking bij aftappen en verstrekking van gebruikers- en verkeersgegevens (hoofdstuk 13 Telecommunicatiewet) alsmede in de toekomst opslag van verkeersgegevens (Richtlijn 2006/24/EG). Zeker omdat het niet vanzelfsprekend is de ISP aan te spreken op de aanwezigheid van strafbaar materiaal – daarvoor is toch in eerste instantie de inhoudsaanbieder verantwoordelijk – lijkt het niet op voorhand redelijk om ISP's zelf de kosten voor ontoegankelijkmaking te laten dragen.

Er is daarnaast nog een andersoortig argument om de overheid de kosten te laten dragen. De effectiviteit van een ontoegankelijkmakingsbevel zal vaak niet groot zijn, in elk geval bij bepaalde typen materiaal zoals discriminatie- of haatzaaipagina's of auteursrechtinbreukmakende pagina's, vanwege het mogelijke 'boemerang'-effect (zie par. 2.2). Dat behoort een zwaarwegend argument te zijn in de afweging door OvJ en r-c om een ontoegankelijkmakingsbevel te geven. Er is echter geen natuurlijke prikkel voor de overheid om hierin terughoudend te zijn – men zou kunnen redeneren dat elke pagina die weggehaald wordt er één is die helpt bij het 'schoonvegen' van het Internet. Wanneer de overheid nu mede de kosten draagt voor ontoegankelijkmaking, ontstaat een natuurlijke rem op het grootschalig laten verwijderen van materiaal zonder op de effectiviteit te letten. Een vergoeding door de overheid is een prikkel om het NTD-instrument zo doelmatig mogelijk in te zetten en dus te beperken tot die pagina's waar de ontoegankelijkmaking naar verwachting het meeste effect zal sorteren.

Concluderend kan gezegd worden dat het naar huidig recht ISP's geen recht hebben op vergoeding voor het uitvoeren van verzoeken tot ontoegankelijkmaking. Wanneer een NTD-bevelsbevoegdheid wordt geschapen, zal bepaald moeten worden of vergoeding op basis van de Wet Tarieven in Strafzaken aangewezen is, dan wel vergoeding door uitbreiding van art. 592 Sv. Het afwijzen van elke vorm van vergoeding lijkt ons onverstandig, gezien hun intermediërende rol tussen de strafbare inhoudsaanbieder en de overheid.

Afgezien van een vergoeding van de overheid kan een ISP uiteraard ook pogen een vergoeding te krijgen van de inhoudsaanbieder. Het verkrijgen van een vergoeding van de inhoudsaanbieder zal echter geen sinecure zijn. Er is namelijk een aantal hobbels te nemen. In de eerste plaats kan uiteraard alleen vergoeding verkregen worden indien het informatieaanbod dat ontoegankelijk is gemaakt ook daadwerkelijk onrechtmatig is. Indien de inhoudsaanbieder dat bestrijdt, dan is het aan de ISP om de onrechtmatigheid aan te tonen. Dat is geen gemakkelijke bewijsopdracht, tenzij de ISP de rechter ervan zou weten te overtuigen dat het bevel van de OvJ een voorshandse aanname rechtvaardigt dat het informatieaanbod strafbaar is. Dan zou de last naar de inhoudsaanbieder verschuiven, die dan dit oordeel onderuit zou moeten halen. Een tweede hobbel wordt gevormd door de Schutznormtheorie. Het feit dat een informatieaanbod onrechtmatig is tegenover sommigen, wil nog niet zeggen dat het informatieaanbod ook onrechtmatig is tegenover de ISP. Smaad

en laster zijn bijvoorbeeld onrechtmatig tegenover degene die op de korrel wordt genomen, maar niet tegenover de ISP. Voor een deel wordt dit probleem verholpen doordat ISP's in hun algemene voorwaarden een bepaling opnemen die de abonnee verplicht geen onrechtmatige informatieaanboden via de diensten van de ISP te verspreiden. De ISP hoeft zijn vordering tot vergoeding van de kosten dan niet te baseren op onrechtmatige daad maar kan op basis van zijn algemene voorwaarden optreden. De vraag blijft echter of al degenen van wie informatie ontoegankelijk wordt gemaakt ook gebonden zijn aan de algemene voorwaarden; de ISP is immers slechts één schakel in een grote keten van actoren op het Internet, waarbij er lang niet altijd een één-op-éénrelatie zal bestaan tussen inhoudsaanbieder en de ontoegankelijkmakende ISP. In de derde plaats kunnen er bedrijfseconomische overwegingen zijn voor de ISP om Internetgebruikers niet aansprakelijk te stellen. Dat kan immers ongunstige publiciteit opleveren.

Concluderend kunnen we vaststellen dat de ISP mogelijk de kosten van ontoegankelijkmaking kan verhalen op de inhoudsaanbieder, als een bepaling daartoe in de algemene voorwaarden is opgenomen. Nader onderzoek lijkt ons nodig om te bepalen of dat voldoende soelaas biedt. Er zijn daarnaast ook wetssystematische argumenten om een zelfstandige vergoeding door de overheid te scheppen, via de Wet Tarieven in Strafzaken of via art. 592 Sv, mede omdat de overheid hier een derde partij verplicht tot een handeling waarvoor deze derde niet de eerst aangewezene is om aan te spreken op verwijdering van het strafbare informatieaanbod.

7. Conclusies en aanbevelingen

7.1. Conclusies

Dit rapport is geschreven naar aanleiding van de in het regeerakkoord neergelegde behoefte juridische instrumenten te onderzoeken voor het ontoegankelijkmaken van haatzaai-informatie en andere vormen van strafbare inhoud door Internetaanbieders (ISP's). Uit de juridische en technische achtergronden blijkt dat het weghalen van strafbaar materiaal door ISP's via een *notice-and-take-down*procedure (NTD-procedure) juridische aanknopingspunten kent, met name bij art. 54a Sr in relatie tot de aansprakelijkheid van ISP's, maar dat er de nodige technische haken en ogen zitten vanuit het oogpunt van effectiviteit, subsidiariteit en proportionaliteit. In dit onderzoek zijn vragen rond effectiviteit en subsidiariteit van een NTD-procedure wel gesignaleerd maar verder achterwege gelaten voor de vervolgfase van dit onderzoek, en hebben wij ons verder beperkt tot de juridische aspecten van een NTD-procedure die samenhangen met art. 54a Sr.

De belangrijkste vraag die in dit onderzoek beantwoord is is de vraag naar de bevoegdheidsgrondslag voor een NTD-bevel. Vanuit de vaststelling dat een specifieke en voldoende expliciete wettelijke grondslag nodig is voor deze strafvorderlijke handeling, omdat de vrijheid van meningsuiting in het geding is, zijn twee kandidaatgrondslagen – art. 54a Sr en art. 125o Sv – onderzocht. Op basis van tekstuele, wetshistorische, wetssystematische en rechtsbechermingsargumenten is het zeer twijfelachtig of art. 54a Sr als grondslag kan dienen. Art. 125o Sv wordt in de wetsgeschiedenis wel genoemd als grondslag voor het bevel tot ontoegankelijkmaking bedoeld in art. 54a Sr, maar kent een aantal beperkingen die de bevoegdheid ongeschikt maken als basis voor een NTD-bevel. Zo is art. 125o Sv slechts bruikbaar bij een doorzoeking, gaat het in wezen uit van ontoegankelijkmaking door de OvJ of r-c zelf (medewerking van de beheerder van een systeem is uitzondering) en dient de ontoegankelijkheid weer opgeheven te worden zodra het belang van strafvordering zich daartegen niet meer verzet, en bovendien biedt art. 125o Sv geen basis tot een *bevel* aan een derde tot ontoegankelijkmaking. Alles overziend, moet volgens ons worden geconcludeerd, gezien de gerede twijfel die bestaat zowel bij art. 54a Sr als bij art. 125o Sv als wettelijke grondslag, worden geconcludeerd dat er geen voldoende

wettelijke basis bestaat voor een NTD-bevel. Een en ander impliceert dat aanpassing van de wet nodig is om in een adequate bevoegdheidsgrondslag te voorzien. In de hierna volgende paragraaf worden enkele aanbevelingen gedaan voor de vormgeving van een dergelijke wetswijziging.

Bij het gebruik van een NTD-bevel zijn ernstige bezwaren tegen het desbetreffende informatieaanbod – dat wil zeggen een hoge mate van waarschijnlijkheid van strafbaarheid, gelegen tussen 'redelijke verdenking' en 'onmiskenbaar onrechtmatig' in – , een machtiging van de r-c en proportionaliteit en subsidiariteit – de ontoegankelijkmaking moet dringend noodzakelijk zijn – de belangrijkste criteria voor de uitoefening van het bevel. Heeft een OvJ eenmaal een bevel gegeven dan is hij in het algemeen niet verplicht tot vervolging van de inhoudsaanbieder over te gaan. Zowel beleidsmatige redenen als juridische of praktische haalbaarheid van het verkrijgen van een veroordelend vonnis kunnen meebrengen dat niet vervolgd wordt.

Heeft het voorgaande vooral betrekking op de (uitoefening van de) bevoegdheid door de OvJ, er is tevens gekeken naar de positie van degene tot wie het bevel zich richt: de ISP. Hij is op grond van art. 54a Sr niet vervolgbaar indien hij een tot hem gericht bevel opvolgt. Het is echter aan te nemen dat de ISP ook niet aansprakelijk is voorafgaand aan de ontvangst van een bevel. Een ander oordeel zou twijfel zaaien over de correctheid van implementatie van de Richtlijn inzake elektronische handel in het strafrecht.

Het opvolgen van een bevel kan de ISP in conflict brengen met de inhoudsaanbieder, die schade kan lijden ten gevolge van de ontoegankelijkheid van zijn informatieaanbod en die allicht zijn schade kan proberen te verhalen op de ISP. De ISP lijkt zich doorgaans wel op overmacht te kunnen beroepen, omdat hij handelt op bevel van de OvJ. Waarschijnlijk is dat ook zo indien een bevel onrechtmatig is gegeven en de ISP in redelijkheid kon dwalen omtrent de rechtmatigheid van het bevel. De ISP zal in dit verband geen toets moeten of mogen uitvoeren op de strafbaarheid van het materiaal, maar heeft wel een zekere verantwoordelijkheid het bevel van de OvJ *prima facie* te beoordelen op formele vereisten, zoals een rechterlijke machtiging, wil hij niet-aansprakelijk zijn jegens de inhoudsaanbieder.

Gegeven het ingrijpende karakter van ontoegankelijkmaking van een informatieaanbod is het van belang dat de ISP of inhoudaanbieder in beroep kan gaan tegen ontoegankelijkmaking of tegen het uitblijven van verzochte opheffing. Hier valt aan te sluiten bij art. 125o Sv, door art. 552a Sv ook open te stellen voor de te scheppen NTD-bevelsbevoegdheid.

Indien de ontoegankelijk te maken informatie in het buitenland wordt geherbergd, kan in het algemeen niet rechtstreeks een NTD-bevel gegeven worden aan de desbetreffende ISP. In een dergelijk geval is het indienen van een rechtshulpverzoek bij de andere staat de geëigende weg. Of dat mogelijk is, is nog maar de vraag, want het is afhankelijk van de beschikbaarheid van een bevelsbevoegdheid aldaar. Wel kan eventueel aan Nederlandse of in Nederland gevestigde ISP's gevraagd worden de toegang vanuit Nederland tot het buitenlandse informatieaanbod te blokkeren. Zowel de effectiviteit van een blokkade als de kosten in de vorm van bijvangst – rechtmatige gegevens die mee ontoegankelijk worden gemaakt – zullen echter expliciet meegenomen moeten worden bij beslissingen om tot blokkering over te gaan.

De kosten van ontoegankelijkmaking kan de ISP soms verhalen op de inhoudsaanbieder, steunend op een daartoe strekkende bepaling in de algemene voorwaarden. Er zijn ook goede argumenten om een zelfstandige vergoedingsmogelijkheid door de overheid te scheppen, via de Wet Tarieven in Strafzaken of via art. 592 Sv.

7.2. Aanbevelingen

De hiervoor weergegeven conclusies impliceren dat de bestaande regeling van art. 54a Sr niet adequaat is voor een NTD-bevel door de OvJ. De wet behoeft daarom aanpassing. De volgende punten kunnen daarbij in aanmerking genomen worden.

- Regeling van een bevel tot ontoegankelijkmaking wordt geconcentreerd op één plaats en wel in het Wetboek van Strafvordering rond art. 125o Sv.
- Voor een NTD-bevel tot ontoegankelijkmaking aan een ISP wordt op deze plaats een zelfstandige bepaling ingevoegd, bijvoorbeeld een nieuw art. 125oa Sv. Deze bepaling voorziet expliciet in de mogelijkheid om derden een bevel tot ontoegankelijkmaking te geven. Bij de terminologie kan worden aangesloten bij de tekst van art. 54a Sr, bijvoorbeeld door een clausule als 'een tussenpersoon als bedoeld in art. 54a Sr'.
- Voor informatie die openbaar is en waarbij uit dien hoofde verwacht kan worden dat ontoegankelijkmaking een inbreuk maakt op de vrijheid van meningsuiting, geldt een zwaar regime dat in ieder geval voorziet in betrokkenheid vooraf van de r-c.
- Art. 54a Sr bouwt op die bevoegdheid voort zonder in de voorwaarden waaronder deze kan worden uitgeoefend te treden, door verwijzing naar de bevoegdheid in Sv. De voorwaarde van machtiging van de r-c wordt daarbij overgeheveld naar de nieuwe bepaling in Sv.
- Er wordt voorzien in een stelsel van rechtswaarborgen, waaronder beklag, beëindiging van ontoegankelijkmaking en toetsing door een rechter ter zitting, waarbij aangesloten kan worden bij de waarborgen van art. 125o, 354, 446, 552a en 552fa Sv. Ook vergoeding door de overheid van de kosten van ontoegankelijkmaking, op basis van de Wet Tarieven in Strafzaken of via art. 592 Sv, is aan te bevelen.
- Art. 54a Sr kent geen beperking tot bepaalde soorten delicten. Het is echter ondoenlijk voor het OM om voor ieder feit dat onder enige strafbepaling valt ontoegankelijkmaking te bevelen. Dat betekent dat een richtlijn ontwikkeld moet worden die aangeeft voor welke (typen) delicten een bevel van de OvJ gewenst is. Onder andere de volgende aanknopingspunten zouden daarbij gehanteerd kunnen worden: 1. de mate waarin duidelijkheid bestaat over de strafbaarheid van een informatieaanbod, 2. de mate waarin OvJ nadere handelingen moet verrichten voor het bepalen van de strafbaarheid van een informatieaanbod, 3. de ernst van het toegankelijk zijn van het materiaal op het Internet, 4. de te verwachten effectiviteit van het ontoegankelijkmaken in relatie tot het 'boemerang'-effect dat het materiaal elders in veelvoud weer opduikt.

Op basis van de juridische analyses die in dit rapport uitgevoerd zijn kunnen voorts de volgende aandachtspunten afgeleid worden voor het opzetten van een notice-and-take-downsysteem in bredere zin dan enkel een ontoegankelijkmakingsbevel door de OvJ. Wij bevelen aan deze aandachtspunten te betrekken in de vervolgstappen van dit onderzoek.

- Een kaderregeling voor vrijwaring van de ISP. Een inhoudsaanbieder wiens informatieaanbod ontoegankelijk is gemaakt door een ISP kan pogen de ISP aansprakelijk te stellen voor de schade die daaruit voor hem is voortgevloeid. De ISP die ter uitvoering van een bevel van de OvJ heeft gehandeld zal zich doorgaans op overmacht kunnen beroepen. Bij gebreke aan een bevel van een OvJ kan onder omstandigheden een vrijwaring van een notificeerder verlangd worden. Tevens kan in een regeling aangegeven worden van welke notificeerders een vrijwaring verlangd kan worden.
- Een regeling voor schadevergoeding voor rechtmatig materiaal dat, voortvloeiend uit een bevel van de OvJ, tezamen met het desbetreffende onrechtmatige materiaal ontoegankelijk wordt gemaakt.
- Het betrekken van de inhoudsaanbieder in de NTD-procedure, geïnspireerd door de DMCA-procedure uit de VS: de ISP notificeert bij ontoegankelijkmaking de inhoudsaanbieder, waarop deze binnen een bepaalde termijn kan protesteren met argumentatie dat het materiaal rechtmatig is. De ontoegankelijkmaking wordt dan opgeheven totdat een definitief rechterlijk oordeel is verkregen over de onrechtmatigheid van het materiaal.
- Voorts is ook transparantie een aandachtspunt. Het is van belang dat alle betrokkenen begrijpen hoe een NTD-systeem functioneert, zodat geen verkeerde verwachtingen

worden gewekt. Zo zou bijvoorbeeld voorzien moeten worden in algemene informatie waarin wordt uitgelegd dat niet alle feiten die een notificeerder aanbrengt worden vervolgd of aanleiding geven tot ontoegankelijkmaking. Tevens is van belang dat er transparantie bestaat met betrekking tot beklag- en beroepsmogelijkheden. Met name notificeerders en inhoudsaanbieders zullen niet steeds op de hoogte zijn van hun rechten of de voorwaarden waaronder deze uit te oefenen zijn.

- Tot slot valt aan te bevelen, vanwege het grensoverschrijdende karakter van het Internet, waardoor strafbaar materiaal dat in Nederland wordt aangeboden vaak in het buitenland geherbergd zal zijn, om in internationaal (bijvoorbeeld EU- of Raad van Europa-)verband te komen tot een gezamenlijke regeling van een NTD-procedure.

Literatuur

Buuren, J. van, B.J. Koops & W. Wagenaar (2004), 'Inlichtingen- en veiligheidsdiensten en ICT', in: B.J. Koops (red.) (2004), *Strafrecht en ICT*, Den Haag: Sdu 2004, p. 177-213.

Empel, A.C. van (1981) Overmacht, Serie: Studiepockets privaatrecht, Zwolle: Tjeenk Willink 1981.

Goedmakers, A.J. (1998), Overmacht bij overeenkomst en onrechtmatige daad (dissertatie Rotterdam), 1998.

Griend, E.S.G.N.A.I. van de (2002), Hiaten in de strafrechtelijke rechtsbescherming. Een onderzoek naar aanleiding van het kort geding in strafzaken (dissertatie Tilburg), Nijmegen: WLP 2002.

Hartkamp, A.S. (1988), Verbintenissenrecht, Deel 1, De verbintenis in het algemeen, Mr. C. Asser's handleiding tot de beoefening van het Nederlands burgerlijk recht, Zwolle: Tjeenk Willink 1988.

Koops, Bert-Jaap e.a. (2005), *Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet*, Tilburg, november 2005, http://arno.uvt.nl/show.cgi?fid=46971

Koops, Bert-Jaap & Susan W. Brenner (eds.) (2006), *Cybercrime and Jurisdiction: A Global Survey*, IT & Law Series Vol. 11, The Hague: T.M.C. Asser Press 2006.

Schellekens, M.H.M. (2001), Aansprakelijkheid van Internetaanbieders, Den Haag: SDU 2001.

Siemerink, L.A.R. (2007), De overeenkomst van Internet Service Providers met consumenten, Deventer: Kluwer 2007.

Over de onderzoeksgroepen en onderzoekers

TILT

Het Centrum voor Recht, Technologie en Samenleving (TILT) is een onderdeel van de rechtenfaculteit van de Universiteit van Tilburg. TILT heeft circa 25 onderzoekers en is een van de belangrijkste en meest ervaren Nederlandse onderzoek- en onderwijsinstituten op het gebied van regulering van technologie. Het specialisme van TILT bestrijkt een breed aantal onderwerpen rond ontwikkelingen in ICT, biotechnologie en andere technologieën. Deze ontwikkelingen worden bestudeerd in de context van de belangrijke domeinen in de kennismaatschappij, zoals e-overheid, e-handel, e-zorg, de regulering van informatie- en communicatietechnologie (ICT), bio- en nanotechnologie, privacy, identiteitsmanagement, elektronische handtekeningen, biometrie, computercriminaliteit, veiligheid, intellectuele-eigendomrechten, burgerschap en bestuur, mondialisering, Europeanisering en ethiek. Het onderzoek en onderwijs van TILT zijn gericht op de interactie tussen juridische, bestuurskundige en ethische expertise, tussen recht, regulering en bestuur, en tussen juridische, technische en maatschappelijke invalshoeken. De leiding van TILT is in handen van prof. Corien Prins.
TILT deed in het verleden diverse onderzoeken op het vlak van computercriminaliteit en Internet-opsporing, zoals het promotieonderzoek van Schellekens over aansprakelijkheid van internetproviders, de historische analyse 'Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy' van Koops, de ITeR-studie 'Strafbare feiten op de elektronische snelweg' van Schellekens en 'Aftapbaarheid van telecommunicatie. Een evaluatie van hoofdstuk 13 Telecommunicatiewet' van Koops en anderen. Verdere informatie is te vinden op onze Internetsite: http://www.uvt.nl/tilt.

Onderzoeksprogramma
Het onderzoek van TILT is gericht op een vijfjarig onderzoeksprogramma, 'Regulering in de informatiesamenleving: de wisselwerking tussen recht, technologie (in het bijzonder ICT) en maatschappelijke verhoudingen', dat loopt van 2004 tot en met 2008. Het programma omvat een herbezinning op rechtsvormen, reguleringsvraagstukken en handhavingsmechanismen in het licht van technologische ontwikkelingen. Daarbij wordt aandacht besteed aan diverse dilemma's rond de afweging van uiteenlopende maatschappelijke belangen (zoals veiligheid tegenover privacy, en vrijheid tegenover informatie-eigendom). De onderzoeksresultaten worden gebruikt, met de invalshoeken van recht, technologie en samenleving, om bouwstenen te ontwikkelen voor een normatief kader voor de regulering van technologie. De programmaleiders zijn prof. Bert-Jaap Koops, prof. Corien Prins en prof. Han Somsen.

Radboud Universiteit, Security of Systems (SoS) Group

De SoS groep (voorheen de LOOP group) houdt zich bezig met computer veiligheid. Veiligheid is een breed concept, dat loopt van wiskunde (in het bijzonder cryptografie) tot recht. De belangrijkste aandachtsgebieden van SoS zijn Java program security, smart cards en toegepaste cryptografie.
De SoS group ontvangt subsidies uit verscheidene nationale en internationale bronnen, zoals een Pionier subsidie van NWO voor onderzoek naar programma veiligheid en correctheid en een Europees IST project getiteld 'VerifiCard' dat over Java smart cards gaat. De groep werkt samen met diverse academische en industriële partners.

CyCriS

Het Center for CyberCrime Studies (CyCriS) is een academisch expertisecentrum i.o. over cybercriminaliteit. Het is gezamenlijk opgezet door de Radboud Universiteit (Nijmegen) en de Universiteit van Tilburg. Cycris beoogt technische, organisationele, en juridische expertise en onderzoeksactiviteiten op het gebied van cybercriminaliteit samen te brengen met het doel te komen tot up-to-date wetenschappelijke publicaties, evaluaties en advisering. CyCris beoogt daarbij expliciet technische en juridische kennis met elkaar in verband te brengen, zowel op academisch als op praktisch niveau. De onderliggende gedachte is om zo tot nieuwe inzichten te komen in de theorie en praktijk van cybercriminaliteit. Vanuit technisch perspectief (ICIS Nijmegen) geeft het multidisciplinaire onderzoek niet alleen inzicht in de technische mogelijkheden en onmogelijkheden om cybercriminaliteit te plegen, maar ook in de analyse en bestrijding ervan. Voor wat bestrijding van cybercriminaliteit betreft, is voorkoming, detectie en het behoud van digitaal bewijsmateriaal van belang. Vanuit juridisch en organisationeel perspectief (TILT Tilburg, Institute for Law Nijmegen) verschaft het onderzoek inzicht in de mogelijkheden en onmogelijkheden van regulering van technologie en regulering door middel van technologie, inzicht in de mate waarin cybercriminaliteit voorkomt, en de impact die het heeft op slachtoffers, burgers en de overheid. Voor wat rechtshandhaving betreft, helpt het onderzoek in het bepalen van prioriteiten, brengt het verschillendsoortige expertises bijeen en overbrugt het het verschil tussen theorie (het recht, het conceptuele) en praktijk. Kortom, het onderzoek biedt inzichten die gebruikt kunnen worden om wetgeving te verbeteren, die helpt cybercriminaliteit te voorkomen en te vervolgen en slachtoffers van cybercriminaliteit bij te staan. De belangrijkste vraag waarop het CyCris zich richt is: Welke combinatie van instrumenten (waaronder wetgeving, regulering, sociale normen, economische en technische maatregelen) kunnen – op basis van wetenschappelijke analyse – het best ingezet worden om cybercriminaliteit onder controle te houden, in termen van preventie, detectie en vervolging?

Onderzoekers

Prof.dr. Bert-Jaap Koops is hoogleraar regulering van technologie bij het Centrum voor recht, technologie en samenleving (TILT) van de Universiteit van Tilburg. Hij doet onderzoek naar regulering en technologie, in het bijzonder strafrechtelijke onderwerpen als opsporingsbevoegdheden en privacy, computercriminaliteit, cryptografie en DNA. Hij is ook geïnteresseerd in andere onderwerpen binnen technologieregulering, zoals veiligheid, identificatie, digitale grondrechten, regulering door techniek, de maakbare mens, en regulering van bio- en nanotechnologie. Vanaf 2004 leidt hij een onderzoeksprogramma over recht, techniek en schuivende machtsverhoudingen.

Koops studeerde wiskunde en algemene literatuurwetenschap in Groningen en werkte van 1994-1998 als AIO aan de UvT en de Technische Universiteit Eindhoven op het gebied van regulering van encryptie. Hij promoveerde in januari 1999 op het proefschrift *The Crypto Controversy*.

Koops is mederedacteur van vier boeken over ICT-regulering, *Emerging Electronic Highways* (1996), *ICT Law and Internationalisation* (2000), *Starting Points for ICT Regulation* (2006) en *Cybercrime and Jurisdiction: A Global Survey* (2006). Hij publiceerde diverse boeken en vele artikelen over recht en techniek. Zijn webpublicatie *Crypto Law Survey* wordt wereldwijd beschouwd als een standaardbron over cryptografie-regulering. In 2003 gaf hij gastcolleges aan de University of Dayton en George Washington University in de VS. Koops is sinds de oprichting (2005) lid van De Jonge Akademie, een onderdeel van de Koninklijke Nederlandse Akademie van Wetenschappen.

Dr. Maurice Schellekens (1966) heeft een vooropleiding in zowel recht (Universiteit van Maastricht) als in de technische informatica (Technische Universiteit Eindhoven). Hij is sinds 1995 verbonden aan het Tilburg Institute for Law, Technology, and Society

van de Faculteit der Rechtswetenschappen, Universteit van Tilburg. In 2001 verdedigde hij zijn proefschrift getiteld ‘Aansprakelijkheid van Internetaanbieders’ dat zowel de strafrechtelijke als de auteurechtelijke aansprakelijkheid van Internetaanbieders beslaat. Tevens deed hij hierin het voorstel voor het opzetten van een instantie die onafhankelijk inhoud op het Internet beoordeelt op strafbaarheid, in het kader van de vrijwaring van aansprakelijkheid van ISP’s. Sindsdien heeft hij verscheidene onderzoeken uitgevoerd dan wel mede-uitgevoerd over recht en informatisering. Hij heeft boeken (mede-)geschreven over de strafbare feiten op de elektronische snelweg, juridische implicaties van authenticatie-technieken, en regulering van informatietechniek. Eerdere boekpublicaties omvatten ‘Overheidsaansprakelijkheid voor informatieverstrekking’ (2002) en ‘ De universiteitsbibliotheek in het databankenrecht’ (2000). Hij heeft artikelpublicaties op zijn naam over o.a. een kritische evaluatie van de Wet Computercriminaliteit II in het nederlands Juristenblad, over juridische aspecten van de betrouwbaarheid van medische informatie op het Internet, over juridische aspecten van software agents en over On line Dispute Resolution. Maurice heeft zijn interessegebied uitgebreid tot recht en genomics. Het essay ‘Regulatory Aspects of Genomics, Genetics and Biotechnology: An Orientation on the Positions of Germany, the United Kingdom and the United States’ is daarvan het eerste resultaat.

Dr. W.G. Teepe (1977) studeerde wiskunde en technische cognitiewetenschap in Groningen. Hij promoveerde in 2007 op cryptografische oplossingen voor het vergelijken en koppelen confidentiële gegevens, waarmee hij in feite een technische oplossing presenteerde voor de discussie over levering van passagiersgegevens aan de VS. Sinds 2007 is hij verbonden aan de Security of Systems group van de Radboud Universiteit Nijmegen. Sinds 1998 is Teepe tevens freelance kennistechnoloog, en als zodanig voortrekker bij het online verstrekken van stemadviezen in Nederland en Vlaanderen voor een aantal grote publieke en private opdrachtgevers. Ook is Teepe trekker van de publieke discussie over de verantwoordelijkheden van de verstrekkers van persoonlijke stemadviezen.