Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien

J.J. Oerlemans[*]

1. Inleiding

De voortschrijdende ontwikkelingen op het terrein van informatie- en communicatietechnologie maken het noodzakelijk een aantal wetswijzigingen door te voeren ter bescherming van de persoonlijke levenssfeer van burgers en van vertrouwelijke informatie, aldus de Memorie van Toelichting op het conceptwetsvoorstel 'versterking bestrijding computercriminaliteit'. [1] Het conceptwetsvoorstel is van 28 juli tot en met 30 september ter consultatie aangeboden. Na eventuele wijzigingen wordt het wetsvoorstel naar de Tweede Kamer gestuurd.

De belangrijkste wijziging binnen het formele strafrecht is de creatie van een nieuwe bevoegdheid voor de officier van justitie tot het afgeven van een bevel tot Notice-and-Take-Down op grond van het voorgestelde art. 125p van het Wetboek van Strafvordering (Sv). Met deze maatregel beoogt de demissionaire Minster van Justitie strafbare informatie van het internet te halen. De bevoegdheid zou ingezet kunnen worden voor alle strafbare feiten. Teneinde het NTD-bevel af te dwingen wordt tevens een nieuw dwangmiddel binnen strafvordering geïntroduceerd met de mogelijkheid tot het opleggen van een dwangsom door de officier van justitie op grond van het voorgestelde art. 125q Sv.

Verder worden in het conceptwetsvoorstel drie gedragingen strafbaar gesteld te weten: het overnemen van gegevens uit een niet-openbaar werk in art. 139c lid 1 van het Wetboek van Strafrecht (Sr), heling van gegevens in art. 139e Sr en het met een technisch hulpmiddel heimelijk opnemen van een gesprek waarbij de dader zelf gesprekspartner is door wijziging van art. 139a lid 1 en 139b lid 1 Sr.

In dit artikel wordt ingegaan op de voorgestelde bevoegdheden tot het afgeven van een bevel tot Notice-and-Take-Down door de officier van justitie en het opleggen van een last onder dwangsom bij niet-nakoming van het NTD-bevel. Nagegaan wordt of de voorgestelde bevoegdheden daadwerkelijk een versterking van de bestrijding van computercriminaliteit tot gevolg hebben en waar de juridische knelpunten liggen.

2. Notice-and-Take-Down

De wijzigingen binnen het Wetboek van Strafvordering zien niet op een uitbreiding van (bijzondere) opsporingsbevoegdheden. Uit de inventarisatie van de knelpunten bij wet- en regelgeving bij de bestrijding van cybercrime was 'de belangrijkste conclusie' dat er een grote behoefte staat aan de uitleg over de wet- en regelgeving en over de toepassing van (bijzondere) opsporingsbevoegdheden op internet.[2] Uit diezelfde inventarisatie blijkt tevens dat het opsporingsveld behoefte heeft aan de mogelijkheid tot een 'online doorzoeking'. Uit onderzoek dat in opdracht van het Ministerie van Justitie is uitgevoerd bleek namelijk dat het extreem gecompliceerd is geworden criminele activiteiten op internet te traceren, omdat het betrekkelijk eenvoudig is te voorkomen dat sporen kunnen worden gevolgd. Dit zou het gevolg zijn software dat berichten versleutelt (zoals Skype) en sporen uitwist (zoals TOR).[3] Door middel van een 'online doorzoeking' kan op afstand (zonder dat een besloten plaats wordt binnen getreden) een geautomatiseerd werk worden binnengedrongen teneinde bewijsmateriaal te verzamelen. In het onderzoek wordt aanbevolen het grensoverschrijdend veiligstellen van gegevens door middel van een online doorzoeking in internationaal verband mogelijk te maken. In opdracht van de demissionaire minister zou worden onderzocht in hoeverre behoefte is aan een nationale regeling.[4]

Ten opzichte van deze punten worden in het wetsvoorstel geen maatregelen genomen. Blijkbaar worden de huidige opsporingsbevoegdheden voldoende geacht in de strijd tegen computercriminaliteit. Wel blijkt uit onderzoek dat de kennis en expertise op het gebied van computercriminaliteit bij politie en justitie op peil moet worden gebracht.[5] De voorgestelde wijzigingen in het Wetboek van Strafvordering zien vooral op het tegengaan van strafbare informatie op internet door middel van Notice-and-Take-Down.

In de huidige situatie kan iedereen, inclusief opsporingsambtenaren, .gebruik maken van de Notice-and-Take-Down gedragscode. Deze gedragscode is na publiek-private samenwerking tot stand gekomen.[6] Communicatieaanbieders zoals ISP's en hostingproviders kunnen de gedragsco-

---

* Mr. Jan-Jaap Oerlemans is als promovendus verbonden aan eLaw@Leiden, centrum voor recht in de informatiemaatschappij van de Universiteit Leiden. Daarnaast is hij onderzoeker en juridisch adviseur bij Fox-IT.

1. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 2.
2. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 2 en 3 met een verwijzing naar *Kamerstukken II* 2008/09, 28684, nr. 232.
3. *Kamerstukken II* 2008/09, 28684, nr. 232, p. 3.
4. Idem.
5. W.Ph. Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt, A. Lodder, 'Internetcriminaliteit: kinderpornografie in meervoudig perspectief', *Ars Aequi* 2008, (7/8), p. 538.
6. De gedragscode is beschikbaar op: http://www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf.

de in hun eigen Notice-and-Take-Down-regime verwerken.[7] Na een melding beoordeelt de communicatieaanbieder of het materiaal 'onmiskenbaar onrechtmatig' is en gaat vervolgens al dan niet over tot verwijdering. Bij pre-puberale kinderpornografie (zoals strafbaar gesteld in art. 240b Sr) is geen twijfel over de vraag of het materiaal strafbaar en onrechtmatig is. Deze vraag is echter lastiger te beantwoorden bij delicten zoals smaad (art. 261 Sr), het aanzetten tot haat, discriminatie of geweld tegen personen wegens hun ras, religie, geslacht, seksuele geaardheid of handicap (een vorm van haatzaaien strafbaar gesteld in art. 137d Sr) en het oproepen tot het plegen van misdrijven of geweld (opruiing, strafbaar gesteld in art. 131 Sr). Voor dit soort delicten zouden deskundigen moeten beoordelen of het materiaal strafbaar of onrechtmatig is en vaak is het antwoord op die vraag niet zwart-wit. Indien rechtmatig materiaal wordt verwijderd staat dat op gespannen voet met het recht op de vrijheid van meningsuiting zoals onder andere neergelegd in art. 10 EVRM en art. 7 Grondwet. Op dit moment bepalen communicatieaanbieders of materiaal van het internet moet worden verwijderd en afgevraagd kan worden of dit een wenselijke situatie is. In principe mag alleen 'onmiskenbaar onrechtmatige informatie' worden verwijderd. De kans bestaat echter dat uit angst voor procedures en uit onwetendheid over de strafbaarheid of onrechtmatigheid van het materiaal ook rechtmatig materiaal van het internet verwijderd wordt. Van den Hoven van Genderen waarschuwt dat de huidige regeling kan leiden tot zelfcensuur en aanleiding kan vormen voor aansprakelijkheidsprocedures als bepaalde informatie ten onrechte wordt verwijderd.[8]

De overheid wil communicatieaanbieders kunnen dwingen materiaal van het internet te doen verwijderen. Juist in die gevallen waarbij een communicatieaanbieder weigert het materiaal te verwijderen zou een bevel tot Notice-and-Take-Down onder de dreiging van strafrechtelijke vervolging of de oplegging van een dwangsom uitkomst moeten bieden.[9] Het is begrijpelijk dat Hirsch Ballin een NTD-bevel, tenminste in Nederland, wil kunnen afdwingen. Zogenaamde 'bulletproof hosting providers' bieden bijvoorbeeld internetdiensten aan waarbij zij de 'garantie' geven geen gegevens af te staan aan opsporingsdiensten of materiaal offline te halen. Niet verwonderlijk worden juist via dit soort diensten auteursrechtelijk beschermde werken, kinderpornografie, spam en malware beschikbaar gesteld. In de toekomst zou een NTD-bevel een extra middel tot handhaving kunnen vormen. De meeste bulletproof hostingproviders bevinden zich echter in het buitenland en diegene die zich in Nederland bevinden zullen zich niet gemakkelijk aan de wil van justitie overgeven. Al sinds 2004 bestaat de mogelijkheid een Notice-and-Take-Down bevel af te geven met een machtiging van de rechter-commissaris op grond van art. 54a Sr.[10] Tegelijkertijd wordt in het artikel aangegeven dat indien de aanbieder van de telecommunicatiedienst aan het bevel voldoet niet zal worden vervolgd.[11] Echter, aan het artikel kleven zoveel tekstuele, wethistorische, wetsystematische en rechtsbescherming bezwaren dat het bevel niet rechtmatig kan worden toegepast.[12] Dit is later ook gebleken. Rechters-commissarissen weigerden toestemming te geven voor een NTD-bevel op grond van art. 54a Sr. De zaken waarin de officier van justitie een NTD-bevel zonder machtiging afgaf werden niet-ontvankelijk verklaard.[13]

Art. 54a Sr wordt in het conceptwetsvoorstel gerepareerd. In het artikel zal komen te staan dat een aanbieder van een communicatiedienst niet wordt vervolgd indien de communicatieaanbieder geen wetenschap heeft van het strafbare feit dat via zijn dienst wordt gepleegd en zodra zij daarvan wel op de hoogte is onverwijld de gegevens ontoegankelijk maakt. Het begrip 'ontoegankelijkmaking' ziet overigens op het offline halen van de informatie met behoud van een kopie ten behoeve van strafvordering. Daarnaast kan een ontoegankelijkmaking ook bestaan uit het filteren of blokkeren van gegevens.[14] Verder is het begrip 'tussenpersoon die en telecommunicatiedienst verleent' veranderd in 'aanbieder van een communicatiedienst'. Onder een 'aanbieder van een communicatiedienst' vallen zowel aanbieders van openbare telecommunicatiediensten als aanbieders van besloten netwerken of diensten. Tevens vallen hieronder degenen die gegevens verwerken of opslaan ten behoeve van een communicatiedienst of diens gebruikers.[15]

De bevoegdheid tot het afgeven van een Notice-and-Take-Down bevel is nu geplaatst waar het thuishoort: in het Wetboek van Strafvordering. Met Schellekens, Koops en Teepe ben ik namelijk van mening dat een NTD-bevel een opsporingshandeling is.[16] Het NTD-bevel zal alleen worden ingezet waar sprake is van een (redelijk vermoeden van een) concreet strafbaar informatieaanbod en justitie een einde wil maken aan het strafbare feit. Het voorgestelde art. 125p Sv luidt als volgt:

> 1. De officier van justitie kan een aanbieder van een communicatiedienst of van degene die beschikkingsmacht heeft over een geautomatiseerd werk, vorderen om onverwijld alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit nodig

---

7. Zie bijvoorbeeld onderdeel 8 over Notice-and-Take-Down in de algemene voorwaarden van de sociale netwerksite Hyves: http://www.hyves.nl/useragreement/.
8. R. van den Hoven van Genderen, 'Notice and take down (NTD-) gedragscode, gewenste censuur?', *Computerrecht* 2008, 6, p. 323.
9. Zie de Memorie van Toelichting op het conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 4.
10. Wet van 13 mei 2004, *Stb*. 2004, 210.
11. Dit is een uitvloeisel van art. 15 van de Richtlijn inzake elektronische handel: Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* L 178.
12. M.H.M. Schellekens, B.J. Koops & W.G. Teepe, *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Universiteit van Tilburg 2007, p. 42.
13. Zie Rb. Assen 22 juli 2008, *LJN* BD8451 en Hof Leeuwarden 20 april 2009, *LJN* BI1645.
14. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 15 met een verwijzing naar *Kamerstukken II* 2001/02, 28197, nr. 3 (MvT), p. 65.
15. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 16.
16. M.H.M. Schellekens, B.J. Koops & W.G. Teepe, Wat niet weg is, is gezien. *Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Universiteit van Tilburg 2007, p. 16.

> is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. 2. De vordering is schriftelijk en vermeldt: a. het strafbare feit en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte; b. de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens nodig om een strafbaar feit te beëindigen of te voorkomen; c. de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens nodig om een strafbaar feit te beëindigen of te voorkomen; 3. Artikel 125o, tweede en derde lid, is van overeenkomstige toepassing.

De meest in het oog springende wijziging ten opzichte van art. 54a Sr is het wegvallen van het vereiste van een machtiging van de rechter-commissaris. Eerder is al aangegeven dat het strafbare karakter van haatzaaiende, smadelijke of opruiende teksten niet altijd duidelijk is en verwijdering daarvan op gespannen voet staat met het recht op de vrijheid van meningsuiting zoals vastgelegd in onder andere art. 10 EVRM en art. 7 Grondwet. In de toelichting op het conceptwetsvoorstel wordt erkend dat voor de beoordeling van uitingsdelicten een 'diepgaande juridische expertise vereist' is teneinde tot een afgewogen oordeel ten aanzien van de strafbaarheid van de gedraging te komen.[17] De bedoeling is dat de expertise wordt gewaarborgd door de aangewezen officieren een speciale opleiding te geven. Echter, de beslissing over het al dan niet verwijderen van de inhoud ligt in het voorgestelde artikel in handen van het Openbaar Ministerie en niet (meer) bij de onafhankelijke rechtsmacht. Daarmee verliest art. 125p Sv een belangrijke waarborg ten opzichte van art. 54a Sr. Een inbreuk op de vrijheid van meningsuiting kan op grond van art. 10 lid 2 EVRM gerechtvaardigd worden met een wettelijke bepaling en voor zover de inbreuk in een democratische rechtsstaat noodzakelijk is. Met de creatie van art. 125p Sv wordt in principe aan de eis van een wettelijke bepaling voldaan. Men kan zich afvragen of het wenselijk is zoveel macht bij het Openbaar Ministerie neer te leggen. Illustratief is de recente zaak rond internetjournalist Bert Brussen. De heer Brussen plaatste op zijn weblog de volgende retweet:[18] *'Rijkelijke beloning voor diegene die Wilders z'n keel doorsnijdt. Liefst van rechts naar links, maar van links naar rechts is ook ok!'*. Het Openbaar Ministerie liet de journalist vervolgens op het politiebureau komen met de mededeling dat het bericht moest worden verwijderd van zijn blog.[19] De heer Brussen weigerde en wordt nu verdacht van belediging en haatzaaiing. Indien het wetsvoorstel wordt aangenomen zou een officier van justitie in de toekomst een bevel tot verwijdering kunnen geven. Bij niet-nakoming van het bevel zou de heer Brussen vervolgd kunnen worden voor het niet-nakomen van een ambtelijk gegevens bevel of een dwangsom moeten betalen (over dit laatste meer in paragraaf 3). Wel kan een belanghebbende op grond van art. 552a Sv beklag instellen bij de raadkamer van de rechtbank. Aangezien de voorgestelde NTD-bevoegdheid voor *alle* delicten geldt, biedt art. 125p Sv mijns inziens onvoldoende waarborgen om rechtsgeldig te zijn.
Bovendien bestaat er onduidelijkheid over de vraag of het Openbaar Ministerie aangemerkt kan worden als 'administratieve autoriteit' in de zin van art. 12 lid 3 van Richtlijn inzake elektronische handel, waarin staat dat een rechtbank of administratieve autoriteit kan eisen informatie op internet ontoegankelijk te maken.[20] In de Duitse vertaling van de richtlijn wordt het begrip administratieve autoriteit vertaald met 'Verwaltungsbehörde' dat in het Nederlands vertaald kan worden met 'bestuurslichaam'. Het Openbaar Ministerie wordt gezien als een bestuurorgaan in zin van art. 1:1 lid 1 sub a van de Algemene wet bestuursrecht (Awb). Op basis hiervan heeft de demissionaire minister waarschijnlijk gedacht dat het Openbaar Ministerie kan worden aangemerkt als 'administratieve autoriteit' in de zin van art. 12 van de Richtlijn inzake elektronische handel. De rechtbank Assen overwoog echter in een zaak dat op grond van art. 12 van de richtlijn een inhoudelijke toets van *een rechtbank* bij een NTD-bevel was vereist.[21] Kortom, op dit punt bestaat nog discussie en dit had wellicht in de Memorie van Toelichting bij het conceptwetsvoorstel beter moeten worden onderbouwd.
Opvallend is de zinsnede in art. 125p Sv waarin staat dat het bevel tot ontoegankelijkmaking ook kan worden gegeven ter voorkoming van nog te plegen strafbare feiten. In de Memorie van Toelichting op het conceptwetsvoorstel wordt niet uitgesloten dat informatie moet worden verwijderd in verband met auteursrechtschendingen.[22] Aangezien de ontoegankelijkmaking ook kan inhouden dat informatie wordt gefilterd of geblokkeerd, zou theoretisch de mogelijkheid bestaan dat een officier van justitie communicatieaanbieders verplicht informatie te filteren en tegen te houden ter voorkoming van auteursrechtelijke inbreuken. In de Memorie van Toelichting wordt verder nog verwezen naar art. 26d Auteurswet 1912 en art. 15e van de Wet op de naburige rechten waarbij de rechter kan worden verzocht om een 'internetprovider' te bevelen om de inbreukmakende activiteiten van derden te staken. Vervolgens staat er dat het conceptwetsvoorstel daarbij aansluit *'door de bestaande strafrechtelijke bevoegdheid van de officier van justitie om te bevelen gegevens ontoegankelijk te maken, te versterken'*.[23] Hoewel het demissionaire kabinet heeft laten weten dat het primaat bij de handhaving van auteursrechten binnen het civiele recht ligt, stelt zij wel dat het kabinetsbeleid zich richt op de aanpak van het (grootschalig) illegale uploaden.[24] Wellicht wordt met de voorgestelde maatregel meer gestalte gegeven aan dit beleid.
Voor de opsporing is een nadeel van Notice-And-Take-Down dat met de verwijdering monitoring-mogelijkheden van de website verloren gaan. Het binnenkomende en uitgaande verkeer of wijzigingen op de betreffende website kunnen niet meer in de gaten gehouden worden en daar-

17. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 22.
18. Een tweet van iemand anders die opnieuw getwitterd wordt.
19. Zie http://www.nu.nl/internet/2306487/journalist-moet-retweet-verantwoorden-bij-politie.html.
20. Zie art. 12 Richtlijn inzake elektronische handel, Richtlijn inzake elektronische handel: Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG* L 178.
21. Rb. Assen 24 november 2009, *LJN* BK4226.
22. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 13.
23. Memorie van Toelichting concept wetsvoorstel versterking bestrijding computercriminaliteit, p. 23.
24. *Kamerstukken II* 2009/10, 29838, nr. 22, p. 13.

mee gaan mogelijkheden tot identificatie van de inhoudsaanbieder verloren.[25] Deze informatie kan cruciaal zijn voor de vervolging van de dader. Echter, een dergelijke actie kost veel tijd, capaciteit en expertise bij politie en justitie. Juist bij digitale opsporing is dat beperkt. Belangrijk is dat men zich realiseert dat met Notice-and-Take-Down alleen de gevolgen van het delict (tijdelijk) worden weggenomen. Daders kunnen binnen korte tijd op een alternatieve locatie de informatie weer beschikbaar stellen. Dit is ook de reden dat Notice-and-Take-Down bijvoorbeeld niet goed werkt bij de bestrijding van botnets. Botnets worden aangestuurd vanuit een centrale computer die een 'command-and-control server' wordt genoemd. Indien de command-and-control server zich bij een Nederlandse hostingprovider bevindt zou de server met een NTD-verzoek offline gehaald kunnen worden. Het gevaar bestaat echter dat de zodra de Nederlandse server wordt uitgeschakeld het commandocentrum zich direct verplaatst naar een minder bereikbare server in het buitenland met betere beveiligingsmaatregelen waardoor de opsporing en vervolging van verdachten lastiger wordt. Daarnaast is er volgens Schellekens, Koops en Teepe altijd sprake van bijvangst. Dit houdt in dat meer informatie ontoegankelijk wordt gemaakt dan slechts illegaal of onrechtmatig is. De bijvangst is afhankelijk van de technische mogelijkheden en moeite die de communicatieaanbieder doet om de bijvangst te beperken. Het zal echter doorgaans minstens een heel domein zijn, oftewel een complete website 'met alles wat daar onder hangt'.[26] Tenslotte moet er rekening mee worden gehouden dat bij delicten als smaad of haatzaaien het offline halen van het materiaal soms meer aandacht wordt gegenereerd dan aanvankelijk het geval was. De Tilburgse onderzoekers waarschuwen daarom voor een 'boemerangeffect' van het offline halen van het materiaal.[27]

3. Dwangsombevoegdheid officier van justitie

In het wetsvoorstel wordt in art. 125q Sv een nieuw dwangmiddel voor de officier van justitie gecreëerd, namelijk het opleggen van een last onder dwangsom (art. 5:31d Algemene wet bestuursrecht (Awb)) door de officier van justitie. De gedachtegang is dat deze van oorsprong bestuursrechterlijke herstelsanctie kan worden ingezet, omdat het Openbaar Ministerie een bestuursorgaan is (zoals bedoeld in art. 1:1a Awb) en de sanctie ziet op herstel van de rechtmatige toestand, namelijk de toestand voordat de strafbare informatie op de servers aanwezig was. Het Openbaar Ministerie kan al langer een 'bestuurlijke boete' opleggen (denk aan de boete bij het rijden door rood licht). Bij een dwangsom wordt de betrokkene echter verplicht een bedrag te betalen zolang niet wordt voldaan aan het bevel tot herstel van de rechtmatige situatie. Indien gedurende een langere tijd niet wordt voldaan aan het bevel kan het bedrag flink oplopen.
De last onder dwangsom fungeert als 'stok achter de deur' indien de betreffende ISP of hostingprovider de informatie niet ontoegankelijk wil maken.[28] Eigenlijk is het een 'dubbele stok achter de deur' aangezien de communicatieaanbieder tevens vervolging riskeert wegens het niet-nakomen van een ambtelijk gegeven bevel op grond van art. 184 Sr. Het is echter onduidelijk of het opleggen van een last onder dwangsom door een officier van justitie rechtmatig is. Art. 1:6 sub a Awb sluit bepaalde hoofdstukken van de wet uit - waaronder hoofdstuk 5 over handhaving waarin de last onder dwangsom zich bevindt - voor toepassing voor de opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van strafrechterlijke beslissingen. Op het eerste gezicht lijkt de oplegging van een last onder dwangsom voor de tenuitvoerlegging van een NTD-bevel binnen het bereik van art. 1:6 Awb te vallen. Bij de creatie van de Algemene wet bestuursrecht was de wetgever van mening dat het onwenselijk is dat *'de typisch in de sfeer van de strafvordering en de executie gelegen besluiten en handelingen van de betrokken bestuursorganen (de algemene en bijzondere opsporingsambtenaren, het openbaar ministerie en de Minister van Justitie) onder het bereik vallen. Gelet op de eigenstandige positie van het (materiële en formele) strafrecht en op het feit dat de strafrechtelijke regelgeving uitputtend is bedoeld, zou dat tot een ongewenste vermenging van rechtsferen leiden.'*[29] Uit het geciteerde stuk blijkt ontegenzeggelijk dat de last onder dwangsom niet door het OM kan worden toegepast, wegens de door de wetgever ongewenste samenloop van het straf- en bestuursrecht. De idee dat het strafrecht en het bestuursrecht twee gescheiden wereld zijn met elk hun eigen regelsysteem lijkt echter achterhaald en in het project Strafvordering 2001 is hiervan afstand genomen.[30] In het door de wetgever in de Memorie van Toelichting op het conceptwetsvoorstel aangehaalde WODC-onderzoek naar de herijking van het sanctiepakket in de Wet op de economische delicten wordt gesteld dat kwesties die in het strafrecht en bestuursrecht hetzelfde zijn gemeenschappelijk geregeld zouden kunnen worden.[31] De WODC-onderzoekers doen het voorstel dat bij niet-naleving van art. 8 onder c van de Wet op de Economische Delicten (WED) *de rechter* een last dwangsom zou kunnen opleggen.[32] Het artikel ziet immers op herstel van de rechtmatige situatie, net zoals de herstelsanctie van een last onder dwangsom daarop toeziet. Vervolgens stellen de onderzoekers dat *zou moeten wor-*

25. Zie ook M.H.M. Schellekens, B.J. Koops & W.G. Teepe, Wat niet weg is, is gezien. *Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Universiteit van Tilburg 2007, p. 14.
26. M.H.M. Schellekens, B.J. Koops & W.G. Teepe, Wat niet weg is, is gezien. *Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Universiteit van Tilburg 2007, p. 13.
27. Idem, p. 14.
28. Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 4.
29. *Kamerstukken II* 1988/89, 21 221, nr. 3 (MvT), p. 42.
30. E. Gritter, G. Knigge, N.J.M. Kwakman, De WED op de helling. *Een onderzoek naar de wenselijkheid de Wet op de economische delicten te herzien*, WODC, Meppel: Boom Juridische Uitgevers 2005, p. 151 onder verwijzing naar het project Strafvordering 2001, uitgevoerd door M.S. Groenhuijsen en G. Knigge (Rijksuniversiteit Groningen).
31. Memorie van Toelichting conceptwetsvoorstel, p. 24 onder verwijzing naar E. Gritter, G. Knigge, N.J.M. Kwakman, De WED op de helling. *Een onderzoek naar de wenselijkheid de Wet op de economische delicten te herzien*, WODC, Meppel: Boom Juridische Uitgevers 2005, p. 150: '*Tot die uitgangspunten behoort dat strafrecht en bestuursrecht beide publiekrecht zijn, en dat zij als zodanig veel gemeenschappelijk hebben. Op grond daarvan wordt gesteld dat er geen principieel bezwaar is om wat gemeenschappelijk is aan beide rechtsgebieden ook gemeenschappelijk te regelen*'.
32. Idem, p. 152.

*den onderzocht*of de maatregel niet alleen als rechtersmaatregel zou kunnen gelden, maar ook als 'voorlopige last onder dwangsom' zou kunnen worden opgelegd zoals in art. 83 van de Mededingingswet wordt gedaan. In dit artikel mag de raad van bestuur van de Nederlandse Mededingingsautoriteit (NMa) een last onder dwangsom opleggen. Mijns inziens is de NMa in elk geval onafhankelijker en beter te beschouwen als 'administratieve autoriteit' dan het Openbaar Ministerie in de zin van de Richtlijn inzake elektronische handel (zie paragraaf 2). De beperkte ruimte die de onderzoekers hebben gecreëerd een andere instantie dan de rechtbank een last onder dwangsom te doen opleggen voor de handhaving van economische delicten heeft de demissionaire Minister van Justitie met beide handen aangegrepen en stelde in een reactie op het rapport op 21 mei 2007 het volgende: *'oplegging van de last onder dwangsom zou bovendien niet alleen aan de strafrechter, maar ook – in het kader van de strafbeschikking – aan het Openbaar Ministerie kunnen worden toegestaan'*.[33] Blijkbaar voelde de wetgever zich door het rapport voldoende gesterkt de dwangsombevoegdheid aan de officier van justitie te verlenen bij niet-naleving van het NTD-bevel. Nogmaals, de onderzoekers van het WODC-rapport stellen dat de mogelijkheid tot het opleggen van een dwangsom door een niet-rechtelijke instantie nog moet worden onderzocht; het is geen vaststaand gegeven dat het Openbaar Ministerie deze bevoegdheid kan krijgen. Daarnaast is het Openbaar Ministerie een ander soort instantie dan de Mededingingsautoriteit waar in het onderzoek naar wordt verwezen en tenslotte zag het onderzoek op de herijking van de handhavingsinstrumenten van de Wet op de economische delicten en niet op het Wetboek van Strafvordering. Mijns inziens is nog onvoldoende duidelijk of deze regeling voldoende wettelijke basis heeft en moet hier meer onderzoek naar worden gedaan.

4. Tot slot

Het conceptwetsvoorstel ziet op de *versterking van de bestrijding* van computercriminaliteit. Wordt dit doel nu met het wetsvoorstel bereikt?

Het wetsvoorstel biedt vooral een versterking voor het Openbaar Ministerie ten opzichte van de verwijdering van strafbaar materiaal op internet. Ik zie echter niet in hoe het wetsvoorstel bijdraagt aan de bestrijding van andere vormen – meer high tech - van cybercrime, zoals denial-of-service aanvallen (art. 138b Sr) en de plaatsing van malware op computers (art. 350a Sr). De opsporing van cybercrime wordt gefrustreerd door technieken die sporen van criminelen verwijderen en een groot jurisdictieprobleem. Deze knelpunten in de opsporing worden met conceptwetsvoorstel helaas niet geadresseerd. Bovendien is veel aan te merken op de voorgestelde artikelen.

Het neerleggen van de bevoegdheid tot Notice-and-Take-Down bij de officier van justitie staat op gespannen voet met de vrijheid van meningsuiting. Juist voor delicten waarbij niet duidelijk is of de inhoud strafbaar is, is het NTD-bevel bedoeld. De waarborg van een machtiging van een rechter-commissaris is in deze gevallen mijns inziens wenselijk en dient als extra waarborg voor het recht op vrijheid van meningsuiting. Het is vooralsnog onduidelijk of een officier van justitie aangemerkt kan worden als een administratieve autoriteit zoals vereist in de Richtlijn inzake elektronische handel. Het is niet uitgesloten dat de NTD-bevoegdheid wordt gebruikt voor het tegengaan van auteursrechtschendingen op internet, al dan niet door middel van filtering en blokkering.

Men moet zich realiseren dat aan Notice-and-Take-Down ook nadelen zitten. Met Notice-and-Take-Down kunnen monitoring-mogelijkheden ten behoeve van een opsporingsonderzoek verloren gaan, rechtmatig materiaal kan 'meegenomen worden' bij het offline halen van het illegale materiaal en er kan een averechts effect optreden doordat de actie aandacht genereert en daardoor het materiaal meer aandacht krijgt dan het oorspronkelijk zou krijgen. De bevoegdheid moet dan ook zorgvuldig worden toegepast.

Het is niet zeker of de dwangsombevoegdheid van de officier van justitie ter naleving van het NTD-bevel rechtmatig is. In het aangehaalde WODC-onderzoek wordt voorgesteld bij niet-naleving van de Wet op de economische delicten de rechter de bevoegdheid te geven een last onder dwangsom op te leggen. Vervolgens stellen de onderzoekers dat onderzocht zou moeten worden of een andere instantie dan de rechter die maatregel op kan leggen, waarbij verwezen wordt naar de mogelijkheid tot het opleggen van een last onder dwangsom door de Nederlandse Mededingingsautoriteit. De resultaten van het onderzoek worden wel zeer ruim geïnterpreteerd wil men hier uit kunnen concluderen dat het Openbaar Ministerie zonder meer bevoegd is tot het opleggen van een last onder dwangsom. Mijns inziens moet hier meer onderzoek naar worden gedaan.

Nu de consultatieronde van het wetsvoorstel is afgesloten is het aan de demissionaire minister wat hij met de ingestuurde adviezen doet. Vervolgens bepalen de beide Kamers wat verder gebeurt met het wetsvoorstel.

33. *Kamerstukken II* 2006/07, 30 800VI, nr. 90, p. 7.