Conceptwetsvoorstel Computercriminaliteit III: onzorgvuldige wetgeving?

Oerlemans, J.J.

CONCEPTWETSVOORSTEL COMPUTERCRIMINALITEIT III: ONZORGVULDIGE WETGEVING?

Mr. J.J. (Jan-Jaap) Oerlemans is juridisch adviseur bij Fox-IT. Tevens is hij promovendus bij de afdeling eLaw@Leiden, centrum voor recht in de informatiemaatschappij, Universiteit Leiden. Jan-Jaap is bereikbaar op oerlemans@fox-it.com.

Ligt de grootste taak van bestrijding van computercriminaliteit door de wetgever bij de vervolging van mensen voor het stelen van naaktfoto's van BN'ers? Of misschien bij een nieuwe opsporingsbevoegdheid om grensoverschrijdend 'terughacken' mogelijk te maken? In dit artikel wordt een tipje van de sluier opgelicht over hoe de regering daar afgelopen jaar over dacht.

In de zomer van 2010 is namelijk een internetconsultatie van het conceptwetsvoorstel Computercriminaliteit III gehouden[1]. In het conceptwetsvoorstel wordt onder andere het bevel tot Notice-and-Take-Down door de officier van justitie als bevoegdheid gecreëerd en het helen van gegevens strafbaar gesteld. De formulering en toelichting op de artikelen laat echter nog te wensen over.

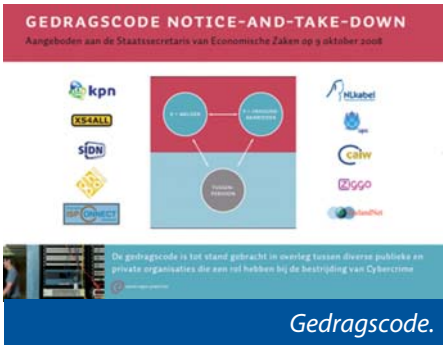
> Tóch denk ik dat de bevoegdheid tot het afgeven van een Notice-and-Take-Down-bevel er moet komen

In dit artikel wordt uitgebreid ingegaan op de belangrijkste punten uit het wetsvoorstel, namelijk het NTD-bevel, de bepaling voor heling van gegevens en het overnemen van gegevens uit een niet-openbaar werk. Uiteindelijk wordt antwoord gegeven op de vraag of het wetsvoorstel moet worden toegejuicht of nog aanpassing behoeft.

NTD-bevel officier van justitie

Notice-and-Take-Down houdt in dat de aanbieder van informatie in kennis wordt gesteld (de 'notice') van illegaal of onrechtmatig materiaal, en een verzoek wordt gedaan het materiaal te verwijderen (de 'take down'). Iedereen, inclusief opsporingsambtenaren, kunnen in de huidige situatie een beroep doen op de zogenaamde 'Notice-and-Take-Down-gedragscode'[2]. Onder deze gedragscode bepaalt uiteindelijk de beheerder van informatie, of de dienstaanbieder, of het verzoek 'onmiskenbaar onrechtmatige informatie' betreft en verwijderd moet worden. Onmiskenbaar onrechtmatige informatie is bijvoorbeeld prepuberale kinderpornografie. Twijfel kan bestaan over de onrechtmatigheid van informatie dat te maken heeft met delicten als smaad, haatzaaiing en het oproepen tot het plegen van misdrijven of geweld. Degene die de beschikkingsmacht heeft over de informatie bepaalt uiteindelijk of de informatie wordt verwijderd.

Op basis van artikel 54a van het Wetboek van Strafrecht (hierna: Sr) zou een officier van justitie, na machtiging van een rechter-commissaris, de bevoegdheid hebben een bevel tot Notice-and-Take-Down te geven. Let op! Het gaat hier om een *bevel* en niet om een verzoek waar vrijwillig aan kan worden voldaan. De formulering van het artikel is echter zó belabberd, dat het bevel niet rechtmatig is. Uit literatuur blijkt dat aan artikel 54a Sr zoveel tekstuele, wethistorische, wetsystematische en rechtsbescherming bezwaren kleven, dat het niet rechtmatig kan worden toegepast[3]. Dit is in de praktijk ook gebleken, want in twee zaken (bij de Rechtbank Assen op 22 juli 2008 en het gerechtshof Leeuwarden op 20 april 2009) weigerde een rechter-commissaris toestemming te geven voor een NTD-bevel op grond van artikel 54a Sr.



Gedragscode.

De huidige situatie, dat in de praktijk alleen een beroep op de NTD-gedragscode kan worden gedaan, wil de regering veranderen. In het conceptwetsvoorstel Computercriminaliteit III wordt in artikel 125p van het Wetboek van Strafvordering voorgesteld een gespecialiseerde officier van justitie de bevoegdheid te geven tot het afgeven van een bevel tot Notice-and-Take-Down. Het bevel om de gegevens ontoegankelijk te maken zou moeten gelden voor *elk* misdrijf en kan wor-

den afgedwongen met een last onder dwangsom (een boete die elke dag oploopt indien niet wordt voldaan aan het bevel). Het begrip 'ontoegankelijkmaking' ziet toe op het offline halen van informatie met behoud van een kopie ten behoeve van een eventueel strafproces. Belangrijk is dat volgens de Memorie van Toelichting de ontoegankelijkheidsmaking ook kan bestaan uit het *filteren of blokkeren* van

Computercriminaliteit bij Nieuwsuur.

gegevens bij een aanbieder van een communicatiedienst. Het bevel tot de ontoegankelijkheidsmaking van gegevens kan namelijk ook worden gegeven voor nieuwe strafbare feiten. Filteren is een methode om ontoegankelijkheidsmaking van nieuwe strafbare feiten te bewerkstelligen. De regering sluit niet uit dat de filterverplichting wordt gebruikt ter bestrijding van de schending van auteursrechten op internet[4]. Eerst zal echter nog de Tweede Kamer en Eerste Kamer moeten worden overtuigd van de noodzaak van zo'n vergaande maatregel. Aan de artikelen die te maken hebben met Notice-and-Take-Down is echter nog meer aan te merken.

Ten eerste vervalt in het voorgestelde artikel de machtiging van de rechtercommissaris. Dat betekent dat er geen onafhankelijke rechterlijke macht meer controleert of het NTD-bevel wel terecht is afgegeven. De machtiging van de rechter-commissaris heeft een belangrijke functie want het verwijderen van bepaalde informatie op internet staat in spanning met het recht op de vrijheid van meningsuiting, zoals onder andere neergelegd in artikel 7 Grondwet. In de Memorie van Toelichting op het conceptwetsvoorstel wordt aangegeven dat het NTD-bevel juist in die gevallen wordt toegepast waar de gedragscode niet toereikend is. Oftewel, in die gevallen waar twijfel bestaat of het om *onmiskenbaar* onrechtmatige informatie gaat. Zoals eerder is aangegeven gaat het hierbij in de praktijk vooral om delicten zoals smaad en haatzaaiing. De regering onderkent dat voor de beoordeling van uitingsdelicten een 'diepgaande juridische expertise' vereist is. Als oplossing wil zij een bepaalde groep officieren van justitie een opleiding geven om beter de afweging te kunnen maken of het materiaal van het internet verwijderd moet worden of niet. Ik ben niet overtuigd van deze waarborg en geloof dat het beter is het vereiste van de machtiging van een rechter bij de NTD-bevoegdheid terug te laten komen[5].

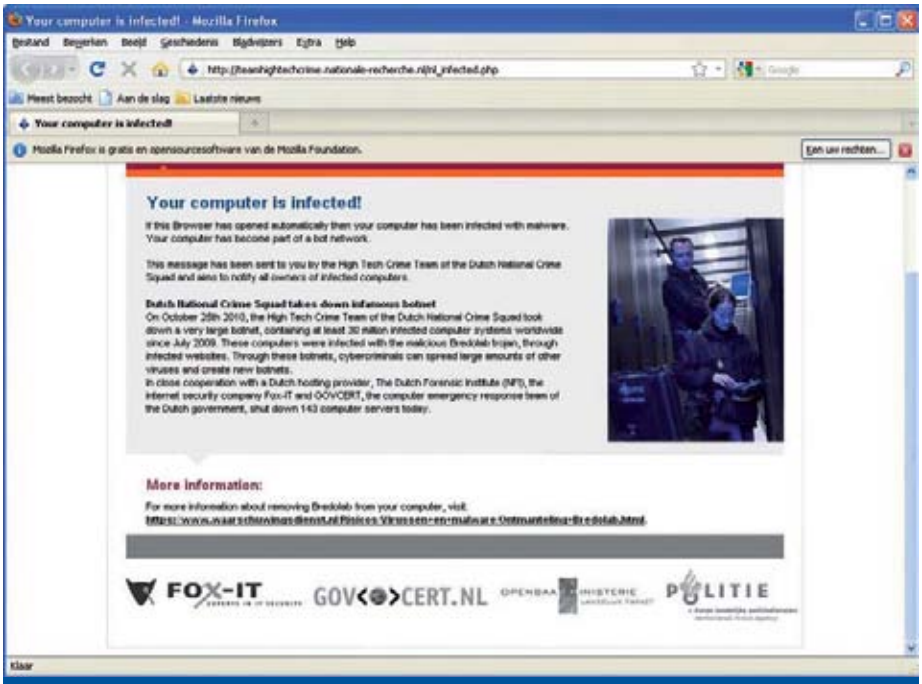
De argumentatie van de minister is flinterdun en behoeft meer toelichting

Ten tweede wordt nergens in het artikel of in de toelichting op het conceptwetsvoorstel gesproken van een melding aan de informatieaanbieder dat de informatie van de desbetreffende server ontoegankelijk wordt gemaakt. De internetaanbieder wordt ook niet verplicht een klant in kennis te stellen van de verwijdering van de informatie. Het 'slachtoffer' van de take down, moet er dus zelf achter komen of de informatie is verwijderd en moet dan zelf bedenken dat hij naar de raadkamer kan stappen om zijn recht van beklag (op grond van artikel 552a Sv) uit te oefenen[6]. De vraag is of dat in de praktijk wel gebeurt en een notificatieplicht is daarom wellicht wenselijk. Wel brengt het een extra administratieve werklast voor justitie met zich mee.

Ten derde is de dwangsombevoegdheid in het voorgestelde artikel 125q Sv curieus. Een last onder dwangsom is een handhavingsmaatregel uit het bestuursrecht. 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 boete te betalen zolang niet wordt voldaan aan het bevel tot herstel van de rechtmatige situatie. Het is echter maar de vraag of het opleggen van een last onder dwangsom door een officier van justitie rechtmatig is. De argumentatie van de toenmalige minister van Justitie voor de bevoegdheid is flinterdun en behoeft meer toelichting[7]. De vergaande maatregel is bovendien een vermenging van het bestuursrecht en strafrecht, iets waarover erg goed moet worden nagedacht[8].

Tóch denk ik dat de bevoegdheid tot het afgeven van een Notice-and-Take-Down-bevel er moet komen. Er zijn zeker situaties te bedenken waarin een afdwingbaar NTD-bevel wenselijk is. Bijvoorbeeld wanneer kinderpornografie wordt gehost, een botnet wordt aangestuurd of spam wordt verstuurd, bij een 'bulletproof hosting provider' in Nederland. Bij dit soort dienstaanbieders is het een onderdeel van hun business model niet mee werken met

politie en justitie. Het bevel tot Notice-and-Take-Down moet natuurlijk niet te snel worden afgegeven, omdat daarmee ook interessante monitoring-mogelijkheden verloren gaan waarmee wellicht het criminele netwerk achter de strafbare activiteiten kan worden achterhaald. Maar, bij een zorgvuldig afgewogen beslissing, na machtiging van de rechter-commissaris (eventueel mondeling gegeven wegens tijdsgebrek), kan ik mij een afdwingbaar NTD-bevel bij dit soort delicten goed voorstellen. Het voordeel van een bevoegdheid tot NTD in plaats van een beroep op de gedragscode is dat het bevel tot Notice-and-Take-Down kan worden afgedwongen en het OM niet afhankelijk is van de willekeur van de communicatieaanbieder.



Actief waarschuwen geïnfecteerde gebruikers.

Naast het NTD-bevel worden in de nieuwe Wet Computercriminaliteit wellicht een aantal belangrijke veranderingen doorgevoerd in het Wetboek van Strafrecht. Hier wordt in de volgende paragraaf op ingegaan.

Heling van gegevens

De Manon Thomas-zaak is een katalysator geweest voor de strafbaarstelling van het overnemen van gegevens uit een niet-openbaar werk en het beschikbaar stellen van die gegevens (heling van gegevens). In deze zaak werd een 'privéfilmpje' waarop de presentatrice naakt was te zien en naaktfoto's van de computer van Manon Thomas gestolen. Via YouTube en het chatprogramma MSN Messenger werd het beeldmateriaal verder verspreid. Door het Hof Leeuwarden werd schending van het portretrecht en auteursrecht van de presentatrice bewezen geacht en de verdachte veroordeeld tot werkstraf van 30 uur en een boete van €250,-. Daarnaast moest de verdachte €3000,- aan immateriële schadevergoeding betalen[9].

In deze zaak kon de dader niet strafrechtelijk worden vervolgd, omdat computervredebreuk niet kon worden bewezen. Het verder verspreiden van gegevens kon bovendien niet onder de normale helingbepaling worden geplaatst, omdat gegevens binnen het strafrecht in principe geen 'goed' zijn. Naar aanleiding van deze zaak zijn Kamervragen gesteld en heeft de regering besloten dat het wenselijk is het wederrechtelijk overnemen van gegevens uit een niet-openbaar werk strafbaar te stellen in artikel 139c Sr.

> Het toont aan waarom het Openbaar Ministerie de verantwoordelijkheid niet alleen zou moeten dragen

Als voorbeeld wordt de situatie genoemd dat een werknemer zonder toestemming bedrijfsinformatie kopieert met de bedoeling deze voor zichzelf of een ander te gebruiken. Het beschikbaar stellen van die gegevens, oftewel 'heling van gegevens', wordt in het conceptwetsvoorstel in artikel 139e Strafbaar gesteld.

> De bereidheid bij de regering is er om auteursrechtschending op internet beter te handhaven

Koops heeft uitvoerig commentaar geleverd op de artikelen. Hij merkt op dat wellicht nog expliciet een rechtvaardigingsgrond in de Memorie van Toelichting moet worden gezet, omdat klokkenluiders soms om hele goede redenen informatie 'stelen' en verder verspreiden. Ook stelt hij, mijns inziens terecht, dat het vreemd is dat heling niet van toepassing zou zijn als gegevens zijn verkregen door diefstal of afpersing van een laptop. Ten slotte geeft de auteur aan dat de clausule 'ten tijde van' in de helingbepaling ontbreekt. Als dit niet wordt gerepareerd in het artikel dan zou degene die de gegevens heeft verkregen ook strafbaar zijn als hij pas achteraf kennis krijgt van de strafrechtelijke afkomst van de gegevens[10].

Als laatste noemenswaardige artikel wordt in het conceptwetsvoorstel ook het heimelijk opnemen van communicatie strafbaar gesteld. Wellicht verrassend is echter de mogelijke *last-minute* wijziging van het mogelijk maken van hacken als opsporingsmethode.

Hacken als opsporingsmethode

Op 25 oktober 2010 heeft minister van Veiligheid en Justitie, Opstelten naar aanleiding van Kamervragen van PvdA-

kamerlid Recourt toegezegd voorstellen te doen om hacken als opsporingsbevoegdheid in de wet vast te leggen. De Kamervragen werden gesteld naar aanleiding van een uitzending van Nieuwsuur waarin officier van justitie Lodewijk van Zwieten pleitte voor het mogelijk maken van 'terughacken'[11]. Het vastleggen van hacken als opsporingsbevoegdheid in de wet is echter geen eenvoudige opgave.

Het zal waarschijnlijk niet gaan om één opsporingsbevoegdheid, maar meerdere. Hacken kan namelijk allerlei toepassingen hebben in een opsporingsonderzoek. Het kan gaan om het hacken van computers teneinde 'rond te kijken' of bestanden te kopiëren voor bewijsmateriaal. Verder kan overwogen worden dat het bij 'terughacken' gaat om het uitschakelen van een geautomatiseerd werk (bijvoorbeeld een computer of server) op afstand. Elk van deze toepassingen leveren echter verschillende inbreuken op de persoonlijke levenssfeer - en wellicht nog andere grondrechten - van de betrokkene. Naar mijn mening moeten voor toepassing van de opsporingsmethode daarom zware waarborgen gelden. Onduidelijk is welke waarborgen dat moeten zijn.

> De Manon Thomas-zaak is een belangrijke katalysator geweest om heling van gegevens strafbaar te stellen

Op deze en andere vragen moeten nog antwoorden komen. Bovendien is het maar de vraag in hoeverre 'grensoverschrijdend' hacken juridisch mogelijk is, aangezien opsporingsbevoegdheden in principe maar tot de Nederlandse grens mogen worden toegepast. Voor de toepassing van opsporingsbevoegdheden in het buitenland moet eerst een rechtshulpverzoek worden gedaan.
Indien hacken als opsporingsbevoegdheid in de Wet Computercriminaliteit III wordt vastgelegd levert dat in elk geval een andere dimensie aan het wetsvoorstel. Wellicht zal de discussie verschuiven van voornamelijk de NTD-bevoegdheid naar de vergaande opsporingsbevoegdheid tot hacken.

> De grensoverschrijdende toepassing van opsporingsbevoegdheden is juridisch gezien nog erg beperkt

Conclusie

Met het wetsvoorstel zal het voor het Openbaar Ministerie gemakkelijker worden illegaal materiaal van internet te halen. Door het als een opsporingsbevoegdheid aan te merken kan het NTD-bevel bovendien worden afgedwongen en dat is in sommige situaties zeer wenselijk. Wel is het artikel in haar huidige formulering naar mijn mening te vergaand, omdat het om 'elk misdrijf' kan gaan, geen toestemming van de rechter-commissaris meer is vereist en het een filterverplichting kan betreffen. De machtiging van de rechter-commissaris moet daarom wat mij betreft terugkomen in het artikel. Ten slotte is de dwangsombevoegdheid slecht beargumenteerd en het artikel over heling van gegevens slordig geformuleerd. Op deze punten is het conceptwetsvoorstel slordig te noemen. Toch leveren de voorgestelde maatregelen wellicht een bijdrage aan een effectievere vervolging van computer gerelateerde delicten.

Nu moet worden afgewacht in welke vorm het wetsvoorstel naar de Tweede Kamer wordt gestuurd. Zal de machtiging van de rechter-commissaris terugkomen en houdt Opstelten zich aan zijn toezegging hacken als opsporingsmethode mogelijk te maken?
Het zal spannend worden om te zien wat er van het wetsvoorstel overblijft na debat in zowel de Tweede Kamer als de Eerste Kamer.

Eindnoten

Het conceptwetsvoorstel, de Memorie van Toelichting en de reacties zijn te vinden op:

http://internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit. (Archived at www.webcitation.org/5yGLdr99m).

[2] De gedragscode is te downloaden via:

URL: www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf. Accessed: 2011-04-27. (Archived at www.webcitation.org/5yGKGDEXv).

[3] 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. Beschikbaar op: www.cycris.nl/uploads/NTD-54a_rapport_--_30_november_2007.PDF. (Archived at www.webcitation.org/5yGJb3ODX).

[4] Zie Memorie van Toelichting conceptwetsvoorstel versterking bestrijding computercriminaliteit, p. 13 en de brief van 11 april 2011 van staatssecretaris Teeven aan de Kamer over het beleid met betrekking tot auteursrechten. De regering is voornemens downloaden uit illegale bron te verbieden en als maatregel een filterverplichting mogelijk te maken.

[5] Ik ben niet de enige die hier zo over denkt. Op 15 september 2010 hebben twintig (!) hoogleraren en belangenorganisaties een 'brandbrief' gestuurd naar de toenmalige demissionaire Minister van Justitie. Een belangrijk punt is dat in de brief wordt gepleit voor de terugkeer van de machtiging van de rechter-commissaris bij het NTD-bevel wegens het spanningsveld met de vrijheid van meningsuiting. De brief is beschikbaar op: https://www.bof.nl/live/wp-content/uploads/brandbrief.pdf. (Archived at www.webcitation.org/5yGKU5a0R).

[6] Zie ook B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2463.

7 Zie uitgebreid: J.J. Oerlemans, 'Het conceptwetsvoorstel versterking bestrijding computercriminaliteit nader bezien', Tijdschrift voor Internetrecht 2010, nr. 5, p. 148-152. Beschikbaar op: http://weblog.leidenuniv.nl/media/blogs/106178/J.J._Oerlemans_-_Tijdschrift_voor_Internet_recht_-_conceptwetsvoorstel_nader_bezien.pdf. (Archived at www.webcitation.org/5yGKdhtq9).

[8] Zie ook B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2464.

[9] Hof Leeuwarden 4 mei 2010, LJN BM3169.

[10] B.J. Koops, 'Tijd voor Computercriminaliteit III', NJB 2010, afl. 38, p. 2465.

[11] Het fragment is beschikbaar via: http://nieuwsuur.nl/video/193776-de-strijd-tegen-cybercrime.html. (Archived at www.webcitation.org/5yGKpeW7H). De uitspraak werd gedaan naar aanleiding van het ontmantelen van botnets van computers die besmet waren met Bredolab-malware.