Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2008–2009

28 684 Naar een veiliger samenleving

Nr. 232 **BRIEF VAN DE MINISTER VAN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 26 juni 2009

Inleiding

Bij brief van 20 februari 2009[1] verzocht de vaste commissie van Justitie van uw Kamer. mij uw Kamer te informeren over de voortgang van de inventarisatie van de knelpunten in wet- en regelgeving bij de bestrijding van cybercrime. Met deze brief informeer ik u hierover en geef ik tevens invulling aan mijn toezegging tijdens het Algemeen Overleg over terrorismebestrijding van 2 april 2009, om uw Kamer te informeren over de samenhang van de Notice and Take Down(NTD)-code met het filteren en blokkeren van kinderporno op het internet en de motie van het lid Gerkens (SP) inzake de rechterlijke toets[2].

De inventarisatie

Vorig jaar zijn op mijn verzoek de politie (het versterkingsprogramma cybercrime Politie, de expertgroep forensische opsporing en het Korps landelijke politiediensten(KLPD)), het Openbaar Ministerie, de Nationaal Coördinator Terrorismebestrijding (NCTb), het Nederlands Forensisch Instituut (NFI), de bijzondere opsporingsdiensten, de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) en een wetenschapsbeoefenaar samen met medewerkers van mijn departement van start gegaan met de volgende drie trajecten:

- een verkenning naar de toereikendheid van juridische instrumenten aan de hand van een inventarisatie van knelpunten in wet- en regelgeving;
- een analyse van de wettelijke basis voor een NTD-bevel op grond van artikel 54a Wetboek van Strafrecht;
- een verkenning van de technische mogelijkheden voor opsporing op het internet en de aansluiting bij de technische omstandigheden van het heden en de toekomst.

[1] Tweede Kamer, vergaderjaar 2008–2009, kenmerk 2009Z03161/2009D07961.
[2] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nr. 17.

KST133403
0809tkkst28684–232
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2009

Een verkenning naar de toereikendheid van juridische instrumenten aan de hand van een inventarisatie van knelpunten wet- en regelgeving

De belangrijkste conclusie van deze verkenning is dat er grote behoefte bestaat, aan uitleg over weten regelgeving en over de toepassing van (bijzondere) opsporingsbevoegdheden op het internet.

Om hier in te voorzien wordt door de politie en het Openbaar Ministerie binnen het versterkingsprogramma aanpak cybercrime momenteel gewerkt aan de inrichting van een kennis- en expertisecentrum, dat online en via telefonische raadpleging kan worden benaderd voor alle soorten vragen. Dit wordt vergelijkbaar vormgegeven als de Helpdesk BOB die destijds ten behoeve van de uitvoering van de Wet bijzondere opsporingsbevoegdheden heeft gefunctioneerd. De Raad voor de rechtspraak heeft in samenspraak met het mijn ministerie bij het gerechtshof Den Haag voor de zittende magistratuur een kenniscentrum ingericht.

Op basis van de inventarisatie van het juridisch instrumentarium en de ervaringen van politie en OM uit recente cybercrime-onderzoeken is een aantal thema's benoemd. De komende periode zullen deze thema's nader worden uitgewerkt. Dit betreft bijvoorbeeld de bestrijding en ontmanteling van *botnets* of de vraag hoe om te gaan met opsporing in een wireless omgeving. Daarnaast zal de aandacht worden gericht op de toepassing van de strafvorderlijke bevoegdheden in relatie tot deze nieuwe, specifieke vormen van cybercrime. Twee van deze thema's, waarop de focus ligt, bespreek ik hier.

Het online doorzoeken

Een belangrijk voorbeeld van toepassing van de strafvordelijke bevoegdheden is het online doorzoeken. In het notaoverleg van 21 mei 2008[1] is de mogelijkheid van het online doorzoeken van een computer aan de orde gekomen. De VVD-fractie heeft gewezen op een uitspraak van het Duits federaal gerechtshof te Karlsruhe[2] dat opsporingsdiensten niet zonder dat kenbaar te maken de computer van verdachten mogen doorzoeken, bijvoorbeeld door het plaatsen van *trojans*. Meer precies: het hof vond de aan het hof voorgelegde regeling van het Land Noordrijn-Westfalen strijdig aan de Duitse grondwet omdat in de regeling toegang tot informatiesystemen onvoldoende was ingeperkt[3].
De VVD-fractie heeft haar voorkeur uitgesproken voor een wettelijke mogelijkheid tot het hacken door de politie van een computer om criminelen en terroristische activiteiten te onderzoeken, zonder dat de betrokkenen daarvan direct op de hoogte worden gesteld. Uw Kamer heeft daarnaast de motie Teeven (VVD) en Heerts (PvdA) aangenomen, die strekt tot het mogelijk maken van het virtueel doorzoeken op internet[4]. Bij de inventarisatie is gebleken is dat er binnen het opsporingsveld een behoefte bestaat aan de mogelijkheid van het op afstand doorzoeken van computers. Dit met het doel om gegevens te verzamelen dan wel veilig te kunnen stellen over de betrokkenheid van gebruikers bij ernstige strafbare feiten of ten behoeve van decryptie van versleutelde gegevens.

Zoals reeds gemeld in de brief over de Rechtshandhaving op internet[5] heeft het Cybercrimeverdrag nog niet geleid tot nadere regelgeving over de rechtsmacht bij online doorzoeking. Door een Nederlandse deskundige is inmiddels een eerste ontwerp opgesteld voor een discussienotitie over cybercrime en internetjurisdictie, ten behoeve van het project Cybercrime van de Raad van Europa. In dit document wordt geconcludeerd dat het extreem gecompliceerd is geworden om criminele activiteiten op internet te traceren omdat het betrekkelijk eenvoudig is om te voorkomen dat

[1] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 149.
[2] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1–267).
[3] Sinds enkele maanden is in Duitsland een wet van kracht die het Duitse Bondsrecherchedienst («Bundeskriminalamt») de bevoegdheid geeft om, ter bestrijding van het terrorisme, onder bepaalde voorwaarden heimelijk met behulp van technische middelen toegang te verschaffen tot informatiseringssystemen en daaruit gegevens te verkrijgen 20k BKAG (Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt)
[4] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 144.
[5] Tweede Kamer, vergaderjaar 2007–2008, 28 684, nr. 133.

sporen kunnen worden gevolgd. Daarvoor kan software worden gebruikt die berichten versleutelt (Skype) of sporen uitwist (TOR). Dit onderstreept de noodzaak van een snelle veiligstelling van gegevens. Aanbevolen wordt de gevallen waarin en de omstandigheden waaronder veiligstelling van gegevens plaatsvindt op unilaterale wijze nader te bepalen, zodat kan worden gekomen tot grensoverschrijdende veiligstelling van gegevens, waarbij het daadwerkelijke gebruik daarvan in een strafproces kan plaatsvinden op basis van de bestaande rechtshulpprocedures, zoals die onder meer in het Cybercrimeverdrag zijn vastgelegd. In dit licht wordt de behoefte aan een regeling, specifiek voor de Nederlandse situatie, nu nader onderzocht. Hierbij wordt ook de Duitse wetgeving betrokken, evenals de toepassing daarvan ten behoeve van de bestrijding van terrorisme.

Criminele activiteiten gerelateerd het internet

Een ander aspect betreft de strafbaarstelling van criminele activiteiten gerelateerd aan het internet. Dit betreft onder meer gedragingen waarbij computers van gebruikers worden gemanipuleerd en gedragingen waarbij gebruik wordt gemaakt van de technische mogelijkheden die door de informatietechnologie worden geboden om persoonlijke gegevens van de gebruikers te verkrijgen en te misbruiken. Hieronder wordt ingegaan op de strafbaarstelling van Phising/identity theft en heling van gegevens.

Phishing/identity theft

Phishing of identity theft betreft het onder valse voorwendselen afhandig maken van gevoelige gegevens, zoals creditcardnummers, gebruikersnamen, toegangscodes en wachtwoorden. Vervolgens kunnen die gegevens door de dader(s) te eigen bate gebruikt worden, zoals het verrichten van betalingen of het overboeken van geld. Op dit moment is phishing strafbaar als een vorm van oplichting (art. 326 Wetboek van Strafrecht). Vereist is dat een persoon – kort gezegd – door middel van misleiding wordt gebracht tot de afgifte van een goed of van gegevens met een geldswaarde in het handelsverkeer. De Hoge Raad heeft geoordeeld dat een pincode niet kan worden aangemerkt als een gegeven met geldswaarde in het handelsverkeer, omdat een pincode als zodanig geen geldswaarde heeft[1]. Dit zal ook gelden voor andere gegevens die relevant zijn in het kader van cybercrime, zoals gebruikersnamen of toegangscodes. Inmiddels heeft uw Kamer een wetsvoorstel aanvaard waarin wordt voorgesteld in artikel 326 Wetboek van Strafrecht de zinsnede «met geldswaarde in het handelsverkeer» te laten vervallen[2] Daarmee zal phishing of identity theft ook strafbaar zijn als het gaat om gegevens die op zichzelf geen geldswaarde hebben.

Heling van gegevens

Een bekend verschijnsel is het gebruik van gegevens van een computer die door middel van een misdrijf zijn verkregen. Daarbij kan het gaan om het hacken van computers of het door middel van verdichtsels afhandig maken van toegangscodes en wachtwoorden. De situatie dat na inbraak in een computer verkregen gegevens op verschillende websites worden vertoond, heeft in november 2007 aanleiding gegeven tot schriftelijke Kamervragen.[3] Heling van gegevens is thans niet strafbaar. Dit houdt verband met het feit dat computergegevens niet als «een goed» in de zin van de artikelen 310 en 416 Sr kunnen worden aangemerkt. Op grond van de wetsgeschiedenis en de jurisprudentie wordt als een wezenlijke eigenschap van «een goed» beschouwd dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft.[4] Bij diefstal van gegevens behoeft de

[1] HR 13 juni 1995, NJ 1995, 635.
[2] Tweede Kamer, vergaderjaar 2007–2008, 31 386.
[3] Tweede Kamer, Aanhangsel Handelingen, 2007–2008, nr. 888.
[4] HR 3 december 1996, NJ 1997, 574.

beschikkingsmacht van de rechthebbende echter niet beperkt te worden. Het is mogelijk gegevens te kopiëren zonder dat de rechthebbende de beschikkingsmacht verliest. Daar waar wel sprake is van het buiten de beschikkingsmacht van de rechthebbende brengen van gegevens is strafvervolging op grond van diefstal niet uitgesloten. Een voorbeeld hiervan betreft de diefstal van een virtueel amulet en een virtueel masker uit een online computerspel.[1]

In antwoord op de eerdergenoemde Kamervragen heb ik toegezegd het helen van computergegevens binnen het bredere kader van de bestrijding van cybercrime te zullen betrekken. Nader onderzoek heeft mij tot het inzicht gebracht dat een zelfstandige strafbaarstelling van *diefstal* van *gegevens dan wel het onrechtmatig voorhanden hebben van gegevens* wenselijk is. Bij een dergelijke strafbaarstelling zal niet meer vereist zijn dat de betreffende gegevens buiten de beschikkingsmacht van de rechthebbende worden gebracht. Immers, in de praktijk kunnen computergegevens eenvoudig gekopieerd worden. De beschikkingsmacht van de rechthebbende blijft dan onaangetast. Bij het ontwerpen van een dergelijke strafbaarstelling zal aandacht besteed worden aan de handhaafbaarheid in de praktijk en de inpassing in het bestaande wettelijk systeem, dat reeds afzonderlijke strafbaarstellingen kent voor computervredebreuk (art. 138a Sr), het wederrechtelijk aftappen van gegevens (art. 139d Sr), het vernielen van gegevens (art. 350a Sr) en het bekendmaken van bedrijfsgegevens (art. 273 Sr).
Voor de heling van gegevens geldt dat het voor de strafbaarheid vereist is dat de gegevens door middel van een misdrijf zijn verkregen. Ik ben voornemens tot een zelfstandige strafbaarstelling van de *heling* van gegevens te komen door gegevens onder de reikwijdte van artikel 416 van het Wetboek van Strafrecht te brengen. Het verwerven, voorhanden hebben of overdragen van computergegevens, terwijl de dader weet dat het door een misdrijf verkregen gegevens betreft, is dan zelfstandig strafbaar als een vorm van begunstiging. Ik zal in dit kader met een conceptwetsvoorstel komen, dat naar verwachting na het zomerreces in consultatie zal worden gegeven aan de adviesorganen.

De analyse van de wettelijke basis voor een bevel voor Notice and Take Down (NTD)

Een onderwerp dat daarnaast specifiek aandacht verdient, is de regeling van NTD, zoals dat nu is neergelegd in artikel 54a Wetboek van Strafrecht. In de praktijk is gebleken dat dit artikel niet vanzelfsprekend een eenvoudig en snel toepasbaar middel is om tot verwijdering van ongewenste of strafbare content te komen.[2] Voorts meldde ik u reeds in mijn brief Rechtshandhaving op internet het bestaan van een rapport van de Universiteit van Tilburg. De onderzoekers komen tot de conclusie dat er vragen bestaan over de wettelijke basis voor het NTD-bevel.

Artikel 54a Wetboek van Strafrecht bevat zowel een schulduitsluitingsgrond voor de aanbieder van een communicatiedienst die alleen als tussenpersoon fungeert als een bevelsbevoegdheid voor de officier van justitie om, na machtiging door de rechter-commissaris, onrechtmatige informatie van het internet te laten verwijderen. Deze combinatie van elementen blijkt, als gezegd, in de praktijk vragen op te roepen en een succesvolle toepassing van artikel 54a Wetboek van Strafrecht te bemoeilijken. Teneinde deze onduidelijkheid weg te nemen, zal artikel 54a Wetboek van Strafrecht worden herzien. Vanuit het oogpunt van wetsystematiek is het wenselijk om de bevelsbevoegdheid die nu in dat artikel besloten ligt, als een expliciete bevoegdheid op te nemen in het

[1] LJN: BG0939, Rechtbank Leeuwarden, 17/676123-07 VEV.
[2] LJN: BD8451, Rechtbank Assen, 19606216-07.

Wetboek van Strafvordering. Deze regeling voorziet dan in algemene zin in de mogelijkheid om onrechtmatige gegevens ontoegankelijk te laten maken.

Het uitgangspunt blijft echter dat de verwijdering zoveel mogelijk plaatsvindt op grond van de op vrijwilligheid gebaseerde NTD-gedragscode. Deze gedragscode is in het kader van de Nationale infrastructuur bestrijding cybercrime (NICC) ontwikkeld en ondertekend door vele relevante partijen. De NTD-gedragscode verandert niets aan het bestaande juridisch kader voor NTD, zoals neergelegd in artikel 54a Wetboek van Strafrecht.

De code bevat een procedure voor tussenpersonen (veelal internet service providers) voor het omgaan met meldingen van onrechtmatige en strafbare informatie (in dit verband wordt vooral de term *content* gebruikt) op internet.[1] De ISP verplicht zich informatie die onmiskenbaar in strijd met de wet is te verwijderen of ontoegankelijk te maken. De gang naar de rechter staat open indien strafbaarheid niet duidelijk is of het besluit van de ISP betwist wordt.

Dit vrijwillig verwijderen of ontoegankelijk maken, is ook standaard voor verzoeken van de politie als het gaat om het verwijderen van kinderpornografie op het internet die in Nederland gehost wordt. Er zal echter sprake blijven van gevallen, waarbij het verwijderen van content in opdracht van de politie en het Openbaar Ministerie niet zal plaatsvinden zonder een bevel.
In de situaties waar de NTD-code tekortschiet bij de verwijdering van onrechtmatige informatie, kan dan gebruik worden gemaakt van de hierboven beschreven mogelijkheid om op basis artikel 54a Wetboek van Strafrecht een bevel tot verwijdering van onrechtmatige gegevens te geven.

Ten behoeve van de voorbereiding van het wetsvoorstel, ter herziening van artikel 54a Wetboek van Strafrecht, zal de uitwerking hiervan eerst worden besproken met deskundigen uit de wetenschap en de praktijk. Nadat de uitkomsten hiervan zijn verwerkt, zal een conceptwetsvoorstel naar verwachting na het zomerreces in consultatie worden gegeven aan de adviesorganen.

In het Algemeen Overleg met uw Kamer over terrorismebestrijding van 2 april 2009 is door verschillende fracties een relatie gelegd tussen NTD en het filteren en blokkeren van kinderpornografie op internet. Hierbij gaat het om een manier van het op internet ontoegankelijk maken voor bezoekers van strafbare content op in het buitenland gehoste sites via blacklisting bij Nederlandse providers. Tijdens dat overleg werd ook gevraagd naar de uitvoering van de motie Gerkens[2]. Deze motie is in uw Kamer aanvaard voordat ik u het rapport van het WODC over het filteren en blokkeren van kinderporno op het internet had toegestuurd. Het systeem was destijds zodanig ingericht dat de politie (het KLPD) zorgdroeg voor een blacklist en deze lijst de providers ter beschikking stelde. De motie was bedoeld om nog twijfelende providers over te halen tot het afsluiten van een overeenkomst met het KLPD. Met mijn brief van 15 september 2008[3], waarmee ik u ook het WODC rapport toestuurde, heb ik deze motie afgedaan door uw Kamer mee te delen dat ik deze weg niet verder wil bewandelen en dat ik op een andere wijze zal voorzien in het filteren en blokkeren van kinderporno op het internet. Hierover bent u nader geïnformeerd in de voortgangsbrief over de aanpak kinderpornografie van 4 juni 2009[4]. Ik wil hier stellen dat het niet de bedoeling is om het middel van filteren en blokkeren in te zetten voor sites met kinderporno (of ander strafbaar content) die in Nederland worden gehost. Daar zal na signa-

[1] Tweede Kamer, vergaderjaar 2008–2009, 29 754, nr. 146.
[2] Tweede Kamer, vergaderjaar 2007–2008, 31 200 VI, nr. 17.
[3] Tweede kamer, vergaderjaar 2007–2008, 28 684, nr. 166.
[4] nog geen Kamernummer

lering tegen worden opgetreden: door middel van NTD en strafrechtelijk onderzoek.

Technische mogelijkheden opsporing op het internet en de aansluiting bij de technische omstandigheden van het heden en de toekomst

Sinds het vorige onderzoeksrapport naar de technische mogelijkheden voor opsporing op het internet uit 2006 is het gebruik van nieuwe of verbeterde technieken bij het plegen van cybercrime onmiskenbaar toegenomen. Uit vele publicaties, met name van instanties die zich bezig houden met de spam- en virusbestrijding, maar ook het Trendrapport 2008 van GOVCERT[1] blijkt dat de criminelen hun modi operandi aanpassen en perfectioneren. De opkomst van botnets en de vele vormen van phishing zijn daar voorbeelden van. Tegelijkertijd krijgen de opsporingsdiensten en het Openbaar Ministerie steeds meer ervaring met het opsporen op het internet. De oprichting van de Unit High Tech Crime bij het KLPD en het vergroten van de inspanningen bij andere politiekorpsen en opsporingsdiensten op grond van de versterkingsprogramma's cybercrime van de politie en het Openbaar Ministerie, zorgen voorts voor meer inzicht in cybercrime en de daarbij gebruikte methodieken. Ook de geïntensiveerde internationale samenwerking vergroot het inzicht en helpt kennis ten aanzien van de bestrijding van cybercrime te vergroten.

Een samen met een vertegenwoordiging van de veldorganisaties verrichte analyse van de technische mogelijkheden heeft tot de conclusie geleid dat de in 2006 in het NFI-rapport genoemde technische methoden en technieken (waaronder versleuteling, tunnels peer-to-peer netwerken, virtuele harde schijven, etc.) in de digitale wereld van het heden nog altijd aan de orde zijn en sterker nog, in gebruik nog steeds toenemen. De technieken worden geavanceerder en blijken breed beschikbaar.

Een andere conclusie die op basis van de gesprekken met de betrokkenen is getrokken, is dat het gebruik van digitale techniek door criminelen in een aantal gevallen geen onoverkomelijk probleem in het opsporingsproces (en voor de bewijsvoering) hoeft te vormen, zolang politie en justitie technische mogelijkheden zoals IP-taps kunnen inzetten en tijdens het onderzoek computer apparatuur van criminelen in beslag kunnen nemen en onderzoeken.

Zoals ik u vorig jaar aankondigde, werkt het NFI aan een actualisering van het door het NFI eerder verrichte onderzoek naar de (technische mogelijkheden van) opsporing op internet. Het onderzoek zal in 2010 gereed zijn. Gelet op het gevoelige karakter van het onderzoek zal ik de resultaten daarvan slechts in hoofdlijnen met uw Kamer delen.

De technische ontwikkeling van cybercrime verdient continue aandacht. Ik zal met het NFI en de belangrijkste opsporingsinstanties afspraken maken dat zij monitoren en daar waar nodig mij hierover informeren. Belangrijk hierbij acht ik ook de uitwisseling van ervaringen van het NFI en het KLPD met buitenlandse partners.

Ik zal uw Kamer in het kader van de jaarlijkse rapportage met betrekking tot het project Veiligheid begint bij Voorkomen, waar de bestrijding van cybercrime deel van uitmaakt, nader informeren over de voortgang van de in deze brief weergegeven acties.

De minister van Justitie,
E. M. H. Hirsch Ballin

[1] WWW.GOVCERT.nl: Trendrapport 2008 Inzicht in Cybercrime: trends & cijfers.