Kinderpornografie op internet

Dweilen met de kraan open

Afstudeerscriptie:
J.J. Oerlemans

Februari 2010

Titel:	Kinderpornografie op internet. Dweilen met de kraan open
Naam student:	J.J. Oerlemans
Datum:	Februari 2010
Begeleiders:	Prof. dr. B.J. Koops en mr. dr. B.W. Schermer
E-mail:	oerlemansjj@gmail.com

Inhoudsopgave

Hoofdstuk 1: Inleiding

1.1 Inleiding

De porno-industrie gedijt goed op het internet.[1] Erotische plaatjes en films kunnen door simpelweg te 'googelen' gemakkelijk worden gedownload en bekeken. Wist u echter dat er ook bekende 'kinderpornosterren' bestaan? In deze scriptie wordt inzicht gegeven in de ondergrondse wereld van kinderpornografie in cyberspace.

De productie van kinderpornografie brengt vaak misbruik van minderjarigen met zich mee en het is niet ongewoon dat het materiaal tientallen jaren op internet te vinden is. Dit is uiterst schadelijk voor het betrokken kind en de samenleving maakt zich dan ook grote zorgen over kinderporno. Als reactie hier op is de delictsomschrijving van kinderpornografie door de jaren heen uitgebreid en worden er steeds hogere straffen gesteld. Het bezitten, vervaardigen, verspreiden, invoeren, doorvoeren, uitvoeren, openlijk tentoonstellen van, betrokken zijn met en toegang verschaffen tot kinderpornografie is strafbaar gesteld in artikel 240b van het Wetboek van Strafrecht (hierna: Sr). Op een overtreding van dit artikel rust een gevangenisstraf op van maximaal acht jaar.

Deze scriptie gaat over kinderpornografisch materiaal dat op het internet voorhanden is. Er wordt niet ingegaan op fenomenen als 'grooming'[2], webcamseks, sekstoerisme en kinderprostitutie. Dit betreffen allemaal onderwerpen die zijdelings te maken hebben met kinderpornografie, maar de behandeling hiervan zou mijn scriptie te uitgebreid maken.

In deze scriptie wordt vaak gesproken over kinderpornogebruikers. Dit zijn mensen die kinderpornografisch materiaal bekijken en/of downloaden om in hun behoefte te voorzien. In de media worden deze mensen vaak geassocieerd met pedofielen. Een

[1] Volgens de website http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html waren er in 2006 4,2 miljoen pornowebsites op het internet. Dat was 12% van het totale aantal websites.
[2] Grooming is de seksuele toenadering van minderjarigen door een volwassen persoon via chatsites en webcams, waarbij deze persoon zich in eerste instantie voordoet als een leeftijdsgenoot. Zie Van der Hulst & Neve 2008, p. 99

pedofiel lijdt aan pedofilie en om dit ziektebeeld vast te stellen wordt in de psychologie de DSM-IV kwalificatie gebruikt. Volgens de DSM-IV kwalificatie heeft een pedofiel ten minste zes maanden terugkerende fantasieën, een seksuele drang of gedragingen die seksuele handelingen met een of meer kinderen in de prepubertijd (in het algemeen dertien jaar en jonger) met zich meebrengen. De fantasieën, seksuele drang of gedragingen veroorzaken een significant lijden of beperkingen in het sociaal of beroepsmatig functioneren of het functioneren op andere belangrijke terreinen. De pedofiel is ten minste zestien jaar oud en ten minste vijf jaar ouder dan het kind of de kinderen in de prepuberteit.[3] Dit is een geheel andere definitie dan een kinderpornogebruiker dat 'slechts' kinderporno gebruikt om aan zijn behoeftes te voldoen. Het sociaal of beroepsmatig functioneren wordt hierbij niet altijd verstoord en de gebruiker heeft geen minimumleeftijd. Een kinderpornogebruiker misbruikt niet altijd kinderen. De definitie van een kinderpornogebruiker is daardoor breder dan dat van een pedofiel. Kortom, kinderpornogebruikers en pedofielen kunnen niet over één kam geschoren worden.

Kinderpornografie op internet is te zien als een 'markt' die enerzijds onder invloed staat van producenten en distributeurs (de aanbodkant) en anderzijds de bezitters van kinderpornografie (de vraagkant). Opsporingsdiensten, banken, Internet Service Providers (hierna: ISP's) en private partijen spelen tevens een rol in deze markt.

Om te voorzien in de behoefte aan de zijde van de vraagkant, moet er kinderpornografisch materiaal beschikbaar zijn. Internet speelt hierbij een grote rol. Door de productie van kinderporno wordt nieuw materiaal aangeleverd en vaak direct online gezet. De plaatjes en filmpjes kunnen vervolgens razendsnel en in grote hoeveelheden via het internet verspreid en gedownload worden. Door ontwikkelingen in de informatie- en communicatietechniek (hierna: ICT) en met name dat van het internet blijft de markt van kinderpornografie op internet groeien.

[3] Frances 2000, p. 571-572.

Kinderpornografie op internet vormt aldus een probleem en de vraag is hoe dit probleem het beste kan worden opgelost. Men kan zich bij de bestrijding van kinderpornografie richten op de vraagkant of de aanbodkant van de markt.
Het bezit van kinderpornografie is relatief gemakkelijk te bewijzen met maar beperkt digitaal onderzoek. De opsporing en vervolging van de verspreiders en vervaardigers binnen de markt vergt echter veel meer capaciteit en wordt gefrustreerd door slim gebruik van anonimiserings- en versleutelingstechnieken. Tevens loopt men door de aard van het internet tegen een jurisdictieprobleem aan.

1.2 Probleemstelling

Gezegd kan worden dat de prioriteit in het officiële beleid van de Nederlandse overheid ligt bij de vervaardigers van kinderpornografie. In mijn scriptie wil ik onderzoeken of dit beleid ook daadwerkelijk in de praktijk wordt uitgevoerd en of dit wenselijk is. Nadat deze vraag is beantwoord ga ik na met welke middelen kinderpornografie het beste bestreden kan worden.

Concreet luidt de probleemstelling: *Moet de aanpak van kinderpornografie op internet in Nederland aangepast worden?*

Om deze vraag te beantwoorden zijn een aantal subvragen geformuleerd:

- Wat wordt onder kinderpornografie verstaan en wie zijn de daders?
- Hoe wordt kinderporno over het internet verspreid en hoe komt het op de computer terecht?
- Hoe is kinderpornografie strafbaar gesteld en op welke manier gaat de rechter daarmee om?
- Wat is het vervolgingsbeleid en de vervolgingspraktijk ten aanzien van kinderpornografie?
- Waarom moet kinderpornografie anders aangepakt worden?
- Wat zijn de voor- en nadelen van een nieuwe aanpak?
- Welke problemen komt men tegen met betrekking tot de opsporing en vervolging van kinderpornografie op internet?
- Hoe kan kinderpornografie op internet worden opgespoord en bestreden?

1.3 Opzet van het onderzoek

Hoofdstuk 2 begint met de omschrijving van de geschiedenis van de strafbaarstelling van kinderpornografie met daarbij een typologie van de bezitter, verspreider en producent van kinderporno. Vervolgens wordt in hoofdstuk 3 uitgelegd hoe kinderpornografie op internet verspreid en gedownload wordt. In hoofdstuk 4 wordt de jurisprudentie van artikel 240b Sr geanalyseerd en wordt nagegaan welke prioriteiten er in de vervolgingspraktijk liggen. Tevens zet ik uiteen waar naar mijn mening het accent in het opsporingsonderzoek zou moeten liggen. Hoofdstuk 5 gaat over de manier waarop de daders buiten het zicht van de opsporingsdiensten kunnen blijven en in hoofdstuk 6 wordt uiteengezet welke mogelijkheden er bestaan teneinde kinderpornografie op internet op te sporen. In hoofdstuk 7 wordt aangegeven met welke partijen samengewerkt kan worden voor de bestrijding van kinderpornografie. Tenslotte trek ik in hoofdstuk 8 mijn conclusies en geef ik antwoord op de vraag of de aanpak ter bestrijding van kinderporno op internet aanpassing behoeft en op welke manier dit het beste kan gebeuren.

Hoofdstuk 2: De strafbaarstelling van kinderpornografie in Nederland

2.1 De geschiedenis van de strafbaarstelling van kinderpornografie

In deze paragraaf wordt een beschrijving gegeven over de wetsgeschiedenis bij artikel 240b Sr. Daarbij worden ook maatschappelijke ontwikkelingen beschreven die hebben geleid tot de strafbaarstelling van kinderpornografie zoals dat tot op heden is vastgesteld.

2.1.1 De periode 1814-1960

Na de machtsovername van Napoleon in de negentiende eeuw wordt in Nederland de Franse Code Pénal (Wetboek van Strafrecht) ingevoerd. Ook na de troonbestijging van Willem I in 1814 bleef - bij gebrek aan beter - de Franse wetgeving gelden.[4]

Met de uitvinding van de fotografie in 1839 werd het pas mogelijk om de werkelijkheid zoals het is vast te leggen. Binnen korte tijd werd de fotografie gebruikt om kinderpornografie vast te leggen.[5] Dit gebeurde wel op zeer kleine schaal. Ten aanzien van de seksuele moraal heerste in die tijd de gedachte dat pornografie een privékwestie was en de overheid zich over dit onderwerp terughoudend diende op te stellen.

Na verloop van tijd ontstond toch de behoefte de zedelijkheidswetgeving minder terughoudend te reguleren. Tegelijk met de inwerkingtreding van het (Nederlandse) Wetboek van Strafrecht[6], werd het in voorraad hebben, de verspreiding en openlijke tentoonstelling van pornografie in artikel 240 Sr strafbaar gesteld. Het artikel luidde: *Hij die eenige voor de eerbaarheid aanstootelijke afbeeldingen of vliegend blaadje waarvan hij den inhoud kent, verspreidt, openlijk ten toon stelt,*

[4] Kool 1999, p. 36.
[5] Ferraro & Casey 2005, p. 20.
[6] De inwerkingtreding geschiedde op 1 september 1886, *Stb*. 1886, 6.

aanslaat of ter verspreiding in voorraad heeft, wordt gestraft met gevangenisstraf van ten hoogste drie maanden of geldboeten van ten hoogste driehonderd gulden. Het doel van dit artikel was het tegengaan van de opgedrongen confrontatie met pornografie. De wetgever trad niet op als controleur van het 'zedelijke leven' van individuen, maar trad uitsluitend op tot bescherming van de opvattingen en daarmee verband houdende kwetsbaarheden van personen tegenover de opdringerigheid van anderen.[7] Desondanks was de nieuwe strafwetgeving van 1886 ten opzichte van de latere wetsvoorstellen van liberaal karakter. De seksuele zelfbeschikking stond in deze tijd dan ook hoog in het vaandel.

Als gevolg van de industrialisatie komt de arbeidersklasse van de samenleving in armoedige levensomstandigheden te verkeren. Gevreesd werd dat het zedelijke verval in deze laag van de bevolking invloed had op het zedelijke peil van de samenleving als geheel. Politiek mondt dit uit in de zogeheten 'zedelijke kwestie'.[8] Het ging de wetgever van 1911 bij de strafbaarstelling van pornografie niet meer alleen om de bescherming van de persoonlijke vrijheid van het individu, maar tevens om het herstel van een bovenpersoonlijke 'zedelijke' orde.[9] In 1911 werd dan ook de zedelijkheidswetgeving aangescherpt.[10] Artikel 240 Sr werd zo aangevuld, dat ook geschriften, voorwerpen en de vervaardigers van het aanstotelijke materiaal onder de strafbepaling zouden vallen. Daarnaast werden artikel 240bis en 451bis aan het wetboek toegevoegd. Met betrekking tot kinderporno is zeer belangrijk dat in artikel 240bis het aanbieden of verstrekken van een aanstotelijk geschrift, afbeelding of voorwerp aan personen beneden de achttien jaar strafbaar werd gesteld. Artikel 451bis Sr stelde dat materiaal verboden was dat geschikt was "*om de zinnelijkheid van de jeugd te prikkelen"*. Daarmee werden objecten bedoeld "*die volwassenen niet behoeven te schaden, doch op het ontvankelijk kindergemoed ten hoogste verderfelijk moeten inwerken"*.

[7] Commissie de Melai 1980, p. 9.
[8] Kool 1999, p. 56.
[9] Commissie de Melai 1980, p. 9. Ook werden bijvoorbeeld homofilie en het gebruik van anticonceptiemiddelen in deze tijd verboden.
[10] Wet van 20 mei 1911, *Stb.* 1911, 130.

De periode van 1911 tot en met 1960 wordt door Kool het 'zedelijk interbellum' genoemd.[11] De fundamenten van de zedelijkheidspolitiek waren al in de jaren hiervoor gelegd. Deze tijd moet gezien worden als de tijd waarin dit gedachtegoed verder is uitgewerkt.

2.1.2 Kinderpornografie in jaren zestig en zeventig

In de jaren zestig werden anticonceptiemiddelen wijd verkrijgbaar en ontstond er een ongekende openheid naar seksuele vrijheid en expressie. Deze seksuele revolutie had een toename van de vraag naar pornografisch materiaal tot gevolg en het materiaal werd steeds makkelijker verkrijgbaar. Een periode brak aan waarin seksueel contact tussen volwassenen en kinderen niet zonder meer werd afgewezen.[12] Het feit dat de Deense regering de productie van porno alsmede kinderporno in 1969 legaliseerde, illustreert dit goed. Er werden in die tijd veel kinderpornotijdschriften geproduceerd. Om kinderporno te bemachtigen moest men naar seksshops of kon men het met de post bestellen.[13] Het grootste deel van het huidige kinderpornografisch materiaal dat op internet voorhanden is, komt van scans uit tijdschriften met kinderporno uit de jaren zestig en zeventig.[14]

In de jaren zestig ontstaat er een roep om een terughoudende opstelling van de overheid met betrekking tot kinderpornografie.[15] Aan het einde van de jaren zestig volgen dan ook de eerste wijzigingen in de zedelijkheidswetgeving: de verkoop van voorbehoedsmiddelen wordt niet langer strafbaar gesteld, overspel is niet langer strafbaar[16] en het verbod op homoseksuele contacten met minderjarigen komt te vervallen.[17] Op 1 mei 1970 werd de Adviescommissie herziening zedelijkheidswetgeving (hierna: commissie de Melai) ingesteld en in 1980 bracht zij haar eindrapport uit. In het rapport komt de tijdsgeest van de zestiger jaren goed naar voren. Centraal stelt de commissie dat de strafwetgever tot taak heeft de

[11] Kool 1999, p. 77.
[12] Aanwijzing kinderpornografie 2007, p. 8.
[13] Taylor & Quayle 2003, p. 9.
[14] Taylor & Quayle 2003, p. 45 en Groeneveld 2000, p. 80.
[15] Kool 1999, p. 86.
[16] Wet van 6 mei 1971, *Stb*. 1971, 291.
[17] Wet van 8 april 1971, *Stb*.1971, 212.

'integriteit van de menselijke persoon' te beschermen tegen inbreuk door derden.[18] De commissie vond dat de staat niet als 'zedenmeester' diende op te treden. De wilsvrijheid van de burger bij het aangaan, of afwijzen van seksuele relaties dient te worden gerespecteerd. De wetgever moet daarbij wel normen stellen ter bescherming van diegenen die wilsvrijheid ontberen. Primair ging het dus om de bescherming van jeugdigen. Het duurde tien jaar tot het eindrapport werd uitgebracht. In de tussentijd was men echter anders over het onderwerp gaan denken. Het eindrapport werd dan ook, met name door de toenmalige Minister van Justitie Van Agt, als controversieel ervaren en met weinig enthousiasme ontvangen.[19]

2.1.3 De jaren tachtig tot heden

Vanaf de jaren tachtig vond er een mentaliteitsverandering plaats. Dit had verschillende oorzaken. Vanuit de vrouwenbeweging werd bijvoorbeeld gewezen op de schadelijke effecten van pornografisch materiaal.[20] Ook vanuit de politie en justitie werd er op gewezen dat de productie van kinderpornografie vaak gepaard ging met seksueel misbruik van kinderen.[21]

Kinderporno kon in de jaren tachtig voor het eerst relatief gemakkelijk in een huiselijke omgeving vervaardigd worden door de ontwikkeling van de videocamera voor persoonlijk gebruik. Met video kon de gehele seksuele handeling vastgelegd worden. Het gevolg was dat kinderpornografisch materiaal gemakkelijk geproduceerd en gekopieerd kon worden. De distributie werd echter gelimiteerd doordat de kopieën van de films in kwaliteit verminderde. De introductie van de digitale camera in de jaren negentig maakte een einde aan dit 'probleem'. Kopieën waren vanaf toen van net zulke goede kwaliteit als het origineel en gemakkelijker te maken.

Halverwege de jaren tachtig is ook de tijd dat de media het bestaan van de 'pedofiel' ontdekte. Cijfers van het aantal pedofielen dat 'jacht' maakte op de

[18] Commissie de Melai 1980, p. 10.
[19] Kool 1999, p. 95 met een verwijzing naar W.N.A. Klever e.a., *Zedelijkheidswetgeving in de branding*, Nederlands Gesprek Centrum, Baarn, 1983.
[20] Kool 1999, p. 84. De invloed van de vrouwenbeweging op de strafbaarstelling van kinderpornografie is volgens Kool groot geweest.
[21] Savornin Lohman e.a. 1999, p. 8.

kinderen van burgers werden sterk overdreven, maar het gevolg was wel dat ook de gewone burger in aanraking kwam met het fenomeen 'pedofilie'.[22] Een zaak die veel aandacht kreeg was de zaak Thea Pumbroek. Zij overleed op 27 augustus 1984 op 6-jarige leeftijd aan een overdosis cocaïne. Het grootste deel van haar leven werd zij misbruikt voor de productie van kinderporno.[23] Wellicht mede als reactie op deze zaak werden in 1984 in diverse seksshops in Amsterdam invallen gedaan, waarbij de aanwezige kinderporno in beslag werd genomen.[24]
De Verenigde Staten oefenden tevens sterke politieke druk uit op Nederland. Nederland stond bekend als een van de grootste exporteurs van kinderporno en als een land dat geen adequate actie ondernam tegen kinderporno.[25] In januari 1985 bracht een Amerikaanse delegatie van de 'State Department' (Binnenlandse Zaken) een bezoek aan Nederland, Denemarken en Zweden om de landen een actiever beleid tegenover kinderpornografie te laten voeren. Blijkbaar heeft het bezoek zijn vruchten afgeworpen, want in 1985 werd een nieuw wetsvoorstel aangenomen.[26]
In een derde nota van wijziging, werd het nieuwe artikel 240b Sr opgenomen. Dit artikel luidde als volgt:
Met gevangenisstraf van ten hoogste drie maanden of geldboete van de derde categorie wordt gestraft degene die een afbeelding of een informatiedrager, bevattende een afbeelding van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van zestien jaar nog niet heeft bereikt, is betrokken, hetzij verspreidt of openlijk tentoonstelt, hetzij om verspreid of tentoongesteld te worden vervaardigt, invoert, doorvoert, uitvoert of in voorraad heeft.

Het nieuwe artikel had dezelfde reikwijdte als artikel 240 Sr, maar was specifieker ten aanzien van de vervaardiging, verspreiding en publieke tentoonstelling van kinderporno. Desondanks bleek artikel 240b Sr onvoldoende basis te geven voor de opsporing en vervolging van kinderporno. Het begrip 'seksuele gedraging' was onduidelijk en het begrip 'kennelijk de leeftijd van zestien jaar heeft bereikt' was ook onvoldoende omlijnd.

[22] O'Donnell & Miller 2007, p. 208.
[23] Taylor & Quayle 2003, p. 43.
[24] Van der Neut 2000, p. 112.
[25] Zie O'Donnell & Miller 2007, p. 18, Van der Neut 2000, p. 112 en Taylor & Quayle 2003, p. 44.
[26] Ondertekening geschiedde op 3 juli 1985, *Stb.* 1985, 385.

In 1994 werd een nieuw wetsvoorstel inzake kinderpornografie door de toenmalig Minister van Justitie, Hirsch Ballin, ingediend. Het achterliggende doel van het wetsvoorstel was het preventief en repressief bestrijden van seksueel misbruik van kinderen, dat gepaard ging met de vervaardiging van kinderpornografie.[27] Artikel 240b Sr werd flink aangescherpt.[28] Het strafmaximum werd van drie maanden verhoogd naar vier jaar en bij 'gewoonte' van de strafbare gedraging kon er een straf van zes jaar gevangenisstraf opgelegd worden. Er is van een gewoonte sprake als de verdachte gedurende een langere tijd afbeeldingen voorhanden heeft gehad waarop minderjarigen staan afgebeeld die betrokken zijn bij een seksuele gedraging.[29] De verzwaring van de strafmaat moest de ernst van de daarin strafbaar gestelde handeling tot uiting doen komen. Tevens werd door de strafverzwaring de mogelijkheid gecreëerd strafrechtelijk financieel onderzoek in te stellen.[30] Daarnaast werd het oogmerk tot verspreiding of openbaarmaking geschrapt. In het tweede lid werd, na amendering vanuit de Tweede Kamer, een wetenschappelijke onderzoeksexceptie ingevoerd.[31]

De ontwikkeling van het internet in de jaren negentig heeft misschien wel de grootste impact gehad op de beschikbaarheid van kinderpornografie. Snellere verbindingen, de exponentiële vergroting van de opslagcapaciteit en meer mogelijkheden tot anonimiteit, maken de verspreiding en het in bezit hebben van kinderporno gemakkelijker dan ooit. Voorheen hadden bezitters van kinderporno een collectie van bijvoorbeeld tientallen en soms honderden foto's, dit groeide al snel uit naar collecties van duizenden tot tienduizenden foto's met kinderpornografie.[32] Nu worden regelmatig collecties van miljoenen bestanden aangetroffen.[33] Recentelijk werd de harde schijf van een man door het Nederlands Forensisch Instituut (hierna: NFI) met een collectie kinderporno ontsleuteld. Naar

[27] Kool 1999, p. 126. Hij verwijst daarbij naar *Handelingen I*, 1994/95, nr. 250b, p. 1.
[28] Wet van 13 februari 1995, *Stb.* 1995, 575. De wet trad per 1 februari 1996 in werking.
[29] Lünnemann e.a. 2006, p. 80.
[30] Savornin Lohman e.a. 1999, p. 9.
[31] *Kamerstukken II* 1994/95, 23 682, nr. 14, (amendement Dittrich cs).
[32] Taylor & Quayle 2003, p. 161.
[33] Zie bijvoorbeeld Rb. Rotterdam 9 december 2009, *LJN* BK6022 en Rb. Rotterdam 10 juni 2009, *LJN* BI7331.

schatting betrof het een collectie van ten minste 7 miljoen bestanden.[34] Dit was groter dan de landelijke collectie aan kinderporno van de KLPD.[35]

2.1.3.1 Het Cybercrime Verdrag en Verdrag van Lanzarote

Speciaal ter bestrijding van computercriminaliteit werd het Cybercrimeverdrag door de Raad van Europa opgesteld.[36] Ter implementatie van dit verdrag vond er een belangrijke wetswijziging plaats in 2002.[37] Artikel 240b Sr werd hierdoor uitgebreid. Virtuele kinderporno is namelijk strafbaar gesteld door de toevoeging van het zinsdeel 'of schijnbaar betrokken', ondanks dat Nederland niet verplicht was deze toevoeging te implementeren (op grond van artikel 9 lid 4 Cybercrimeverdrag). Het doel van deze wijzigingen was om concreet seksueel misbruik tegen te gaan en de markt van kinderporno te ontmoedigen.[38] Belangrijk is dat er door het Cybercrimeverdrag ook andere rechtvaardigheidsgronden aan de wet zijn toegevoegd. Centraal staat nog steeds de schadelijkheid van kinderpornografie voor de jeugdige.[39] De nieuwe redenen om kinderporno strafbaar te stellen zijn: het voorkomen van verdere verspreiding en bezit van eenmaal gemaakt materiaal, het voorkomen dat afbeeldingen worden gebruikt om jeugdigen te verleiden tot seksuele handelingen en het voorkomen dat gedrag deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.[40]

De verhoging van de leeftijdsgrens van zestien naar achttien jaar komt voort uit de ratificatie van het ILO-verdrag betreffende het verbod en de onmiddellijke uitbanning van de ergste vorm van kinderarbeid.[41]

Het begrip 'in voorraad hebben' is in de jaren negentig veranderd in 'in bezit hebben'. Dit betrof een codificatie van een uitspraak van de Hoge Raad (hierna: HR)

---

[34] http://www.nu.nl/internet/2074405/nfi-opent-geheime-bestanden-pornoverzamelaar.html (laatst geraadpleegd: 3 september 2009).
[35] http://copsincyberspace.wordpress.com/2009/09/03/nfi-opent-geheime-bestanden-pornoverzamelaar/ (laatst geraadpleegd: 3 september 2009).
[36] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Trb. 2002, 18.
[37] Wet van 13 juli 2002, *Stb.* 2002, 388.
[38] Lünnemann e.a., 2006, p. 56. Zie Rb. 's-Hertogenbosch 4 februari 2008, *LJN* BC3225 m.b.t. virtuele kinderpornografie.
[39] *Kamerstukken II* 2001/02, 27 745, nr. 6, p. 11.
[40] Aanwijzing kinderpornografie 2007, p. 8.
[41] *Kamerstukken II* 2000/01, 27 745, nr. 3, p. 5.

in 1998.[42] Tevens kwam de wetenschappelijke onderzoeksexceptie van artikel 240b lid 2 Sr te vervallen. Men wilt hiermee een signaal afgeven dat het bezit van kinderporno strafwaardig en strafbaar is.[43] Door het afschaffen van de specifieke excepties is een verandering opgetreden in de bewijspositie van het Openbaar Ministerie (hierna: OM). Voorheen moest het OM aantonen dat onterecht gebruik werd gemaakt van de uitzondering in de wet. Nu moet de bezitter aannemelijk maken dat er goede redenen zijn voor de collectie van kinderpornografisch materiaal.[44]

In 2009 is de strafmaat opnieuw verhoogd, nu naar maximaal acht jaar gevangenisstraf.[45] De strafverhoging maakt het plaatsen van een afluisterapparaat in een woning zonder toestemming van de bewoner op grond van artikel 126l Sv mogelijk.[46]

Tenslotte is per 1 januari 2010 het verschaffen van toegang tot kinderporno strafbaar gesteld. Artikel 240b Sr is namelijk uitgebreid met de gedraging: *met gebruikmaking van een communicatiedienst toegang verschaffen tot kinderpornografie*.[47] De verbreding van de strafbaarstelling is een uitvloeisel van het Verdrag van Lanzarote.[48] Met deze uitbreiding is ook het 'realtime' naar kinderporno kijken zonder sporen achter te laten op de harde schijf strafbaar op grond van artikel 240b Sr.[49] Vereist is daarbij wel dat er een actieve handeling moet zijn gevoerd dat gericht is op het verkrijgen van toegang.[50]

2.2 Enkele bestanddelen van artikel 240b Sr uitgelicht

Artikel 240b Sr luidt momenteel:

[42] HR 21 april 1998, *NJ* 1998, 782.
[43] Lünnemann e.a. 2006, p. 42.
[44] Lünnemann e.a. 2006, p. 81.
[45] Wet van 12 juni 2009, *Stb*. 2009, 245.
[46] *Kamerstukken II*, 2007/08, 31 386, nr. 3, p. 9 (MvT). Zie hierover paragraaf 6.2.2.7.
[47] Zie *Kamerstukken II* 2008/09, 31 810, nrs. 1-6.
[48] Het toegang verschaffen tot kinderpornografie is strafbaar gesteld in artikel 20 lid 1 onderdeel f van het Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, *Trb*. 2008, 58 (Verdrag van Lanzarote).
[49] Zie hierover wordt in paragraaf 4.1.
[50] *Kamerstukken II* 2008/09, nr. 3, p. 4 (MvT).

1. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding - of een gegevensdrager, bevattende een afbeelding - van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezit heeft of zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft.
2. Met gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of een gewoonte maakt.

De begrippen 'seksuele gedraging' en 'kennelijke leeftijd' worden hieronder toegelicht.

2.2.1 'Seksuele gedraging'

Het is niet altijd duidelijk of een afbeelding een seksuele gedraging weergeeft. Het begrip seksuele gedraging wordt in elk geval ruim opgevat. De seksuele gedraging hoeft niet zo ver te gaan dat er werkelijk sprake is van seksueel misbruik.

De manier waarop en de toestand waarin het geslachtsdeel van een minderjarige is weergegeven, kan potentieel een seksuele gedraging opleveren.[51] Een blootfoto van een minderjarige in een natuurlijke houding wordt niet als seksuele gedraging gekwalificeerd. De nadruk ligt op de schadelijkheid voor de jeugdige. Dit is af te leiden van de uit de afbeelding naar voren komende ambiance of van de publicatie van de afbeelding.[52]

2.2.2 'Kennelijke leeftijd'

Het woord 'kennelijk' duidt erop dat de leeftijd van het slachtoffer niet bewezen hoeft te worden, maar moet worden geschat aan de hand van de afbeelding. Onder de twaalf jaar is het duidelijk dat de betrokkenen niet ouder zijn dan achttien jaar, aangezien ze de pubertijd nog niet hebben bereikt en er bijvoorbeeld nog geen

[51] HR 16 januari 2007, *LJN* AZ0221.
[52] HR 26 september 2000, *NJ* 2001, 61.

haargroei bij de genitaliën of borstontwikkeling te zien is. Twijfel kan zich voordoen bij gevallen waar de betrokken individuen zich in de postpuberale fase bevinden (15-18 jaar). Aangezien de leeftijd niet bewezen hoeft te worden, kan het geval zich voordoen dat er een vervolging en veroordeling plaatsvindt bij pornografisch materiaal dat individuen bevat die ouder dan achttien jaar zijn, maar zich voordoen als jonger dan achttien jaar en niet van ouder te onderscheiden zijn. Dit criterium is opgenomen om bewijsproblemen te voorkomen.[53]

2.3 Typologie van kinderpornogebruikers

Het is lastig een daderprofiel te geven van kinderpornogebruikers. Zowel de leeftijd als beroepen van de kinderpornogebruikers lopen zeer uiteen en lijken niet te conformeren aan een bepaald stereotype.[54] In het rapport van het WODC "*High-tech crime, soorten criminaliteit en hun daders"* worden er vier categorieën onderscheiden: vervaardigers en handelaren, verzamelaars, reizigers (daders die een fysieke ontmoeting willen bewerkstelligen om de kinderen seksueel te misbruiken), en 'groomers' of 'chatters' (die ongepaste seksueel getinte communicatie voeren met kinderen).[55] In deze scriptie worden hiervan drie groepen behandeld: de vervaardigers, verspreiders ('handelaren') en bezitters ('verzamelaars') van kinderpornografie.

Over verzamelaars en verspreiders wordt in het rapport gezegd dat het meestal een blanke man betreft en variabel in leeftijd (tussen de 13 en 65 jaar). De verzamelaar heeft een sterkte behoefte aan macht en controle, maakt overmatig (compulsief en obsessief) gebruik van het internet en heeft een enorme verzamelingdrang. Door de veelheid aan afbeeldingen gebruikt men veel computergeheugen en beschikt men over extra gegevensdragers. De verzamelaar verkrijgt het meeste materiaal gratis via internet of door te ruilen met anderen. Op dat moment is de verzamelaar door

[53] Lünnemann e.a. 2006, p. 41.
[54] O'Donnell & Miller 2007, p. 84.
[55] Van der Hulst & Neve 2008, p. 94 en 95.

uitwisseling van afbeeldingen met anderen ook verspreider geworden van kinderporno.[56]

De vervaardiger van kinderporno is volgens het rapport meestal een man van een leeftijd tussen de 26 en 53 jaar met technische kennis en vaardigheden. Hij is manipulatief, bezoekt publieke ruimte en verleent onderdak aan weggelopen kinderen. Hij heeft relatief vaak een strafblad (voor zedendelicten en/of kindermishandeling).[57]
Er wordt veel onderzoek gedaan om een link te vinden tussen het gebruik van kinderpornografie en seksuele handelingen met minderjarigen in de praktijk. De resultaten van deze onderzoeken lopen sterk uiteen.[58] Het is dan ook moeilijk aan te geven hoe vaak kinderpornogebruikers kinderen misbruiken.
Er is minder discussie over de link tussen kinderpornografie en het misbruik van kinderen die in de afbeeldingen of films betrokken zijn. Als er op een afbeelding een kind wordt geportretteerd dat misbruikt wordt, dan is het duidelijk dat er sprake is van kindermisbruik. Als een foto eenmaal op internet is geplaatst, is het bijna onmogelijk om het er weer vanaf te halen aangezien het wordt gedownload, gekopieerd en weer verspreid wordt over het internet.[59] Het gevolg hiervan is dat als de slachtoffers ouder worden het materiaal nog steeds op internet staat en toegankelijk is. Slachtoffers van kinderpornografie hebben geen andere keus dan hiermee te leven. Er is onvoldoende empirisch onderzoek gedaan naar de kenmerken van kinderen die het slachtoffer zijn van kinderpornografie.[60]

Tussenconclusie

Dit hoofdstuk heeft duidelijk gemaakt dat de samenleving zich zorgen maakt over kinderpornografie. De verontrusting komt tot uiting in de delictsomschrijving voor kinderpornografie. De definitie van kinderpornografie is in razendsnel tempo

[56] Van der Hulst & Neve 2008, p. 97 en 98. Profiel is samengesteld mede op basis van onderzoek van J.F. McLaughin, *Cyber child sex offender typology*, 2000, http://www.ci.keene.nh.us/police/typology.html (laatst geraadpleegd op 25 september 2009).
[57] Van der Hulst & Neve 2008, p. 97. Profiel is samengesteld mede op basis van onderzoek van J.F. McLaughin, *Cyber child sex offender typology*, 2000, http://www.ci.keene.nh.us/police/typology.html (laatst geraadpleegd op 25 september 2009).
[58] Taylor & Quayle 2003, p. 13.
[59] Taylor & Quayle 2003, p. 24.
[60] Holmes & Holmes 2009, p. 144.

uitgebreid. De straf die staat op het bezitten en verspreiden van kinderporno is verhoogd van maximaal drie maanden naar maximaal acht jaar. Virtuele kinderpornografie is tevens strafbaar gesteld, zodat er in die filmpjes of afbeeldingen geen echte kinderen betrokken zijn. De belangrijkste rechtvaardiging dat wordt gegeven voor de strafbaarstelling van kinderporno is de schadelijkheid voor het kind. Het voorkomen van verdere verspreiding en bezit van eenmaal gemaakt materiaal, het voorkomen dat afbeeldingen worden gebruikt om jeugdigen te verleiden tot seksuele handelingen en het voorkomen dat gedrag deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert zijn later als rechtvaardigingsgronden toegevoegd.

Van een dader van artikel 240b Sr kan geen klip en klaar daderprofiel gegeven worden. Wel is duidelijk dat kinderpornogebruikers vaak tegelijkertijd bezitters en verspreiders zijn van kinderpornografie. De link tussen kinderpornogebruikers en seksueel misbruik van kinderen blijft onduidelijk.

In het volgende hoofdstuk wordt uiteen gezet hoe kinderporno via het internet verspreid en binnen gehaald wordt.

Hoofdstuk 3: Kinderpornografie op internet

In het vorige hoofdstuk is al verteld dat het internet een enorme invloed heeft op de beschikbaarheid van kinderpornografie. Het is een misvatting dat het internet vooral gebruikt wordt als 'ruilmarkt' om seksvideo's met kinderen te verkopen of te ruilen.[61] Kinderporno is digitaal beschikbaar en kan razendsnel verspreid en binnengehaald worden via het internet. Berichten over digitaal materiaal met kinderpornografie die werden uitgewisseld via *Bulletin Board Systems* in Groot-Brittanië gaan al terug naar het jaar 1985.[62] Pas in 1995 raakte het bestaan van 'perverse porno' op internet pas écht bekend aan de wereld met de publicatie van het artikel "*On a screen near you: Cyberporn*" van Time Magazine.[63] Het artikel was gebaseerd op een onderzoek van Marty Rimm.[64] Later bleek echter dat dit onderzoek slecht was uitgevoerd en dat de cijfers waren overdreven.[65] Het artikel heeft in elk geval de wereld wakker geschud over het bestaan van porno op internet.

3.1 Kinderpornografie en internet

Het internet is slechts een verzameling van kabels die met elkaar communiceren en is in essentie een netwerk van netwerken. Het internet werkt, zoals elk communicatiesysteem, met een adresseringsmechanisme. Het TCP/IP protocol is het 'adresseringssysteem' voor het internet.[66] Het Internetprotocol bestaat uit vier combinaties van cijfers die variëren van 0 tot 225. IP-adressen bestaan uit twee delen, een netwerknummer en een 'host-nummer' (computernummer). Het netwerknummer is uniek en identificeert een computernetwerk dat vastzit aan het internet en het host-nummer is een uniek nummer dat de computer op het netwerk identificeert. Dit is vergelijkbaar met een telefoonnummer dat bestaat uit een 'zone-nummer' en een 'locaal nummer'.[67]

---

[61] Jenkins 2001, p. 84.
[62] Akdeniz 2008, p. 5. In paragraaf 3.1.8 wordt uitgelegd wat 'Bulletin Board Systems' zijn.
[63] P. Elmer-Dewitt, 'On a screen near you: cyberporn', *Time magazine*, 1995, no. 1, Volume 146, p. 34-41.
[64] M. Rimm, 'Marketing pornography on the information superhighway', *Georgetown Law Journal*, 83, 1995, p. 1839-1934.
[65] Jenkins 2001, p. 50.
[66] Casey 2004, p. 442.
[67] Ferraro & Casey 2005, p. 22.

Het 'Domain Name System' (DNS) is gecreëerd om namen aan IP-adressen te geven. Door dit systeem wordt een internetgebruiker bij het intypen van het adres (een domeinnaam) in de adresbalk naar de juiste website geleid. Alhoewel kinderpornografie ook op eenvoudig benaderbare websites is te vinden, is het aanbod gaandeweg verschoven naar de minder gemakkelijk door politie en justitie te controleren delen van het internet.[68]

Op internet bestaan in hoofdlijnen twee verschillende circuits ten aanzien van het verspreiden van kinderporno: commerciële aanbieders met betalende klanten en 'verzamelaars' die onderling materiaal uitwisselen.[69] Het aanbod voor kinderporno op internet wordt grotendeels ontwikkeld in de non-commerciële '*cottage industry'*. Hiermee wordt bedoeld dat het kinderpornografische materiaal niet wordt gemaakt in een commerciële sfeer, maar in een huishoudelijke context.[70] De laatste vijf jaar heeft er echter een explosie aan commerciële productie met betrekking tot internetkinderpornografie plaatsgevonden.[71] De drijfveer van commerciële aanbieders is simpelweg financieel gewin. Het lijkt er op dat met kinderporno veel geld te verdienen valt.[72] Grootschalige commerciële verspreiding komt in Nederland waarschijnlijk niet voor.[73] De productiecentra voor commerciële kinderpornografie zijn vooral in de voormalige Oostbloklanden te vinden.[74]
Verzamelaars hebben een sterke behoefte om collecties van kinderporno aan te leggen en te bewaren. Het lijkt wel of het aanleggen van een indrukwekkende collectie kinderporno een doel op zich is geworden. Het is niet ongewoon voor kinderpornogebruikers om keurig gecategoriseerde collecties van honderdduizenden afbeeldingen aan te leggen.[75] Kinderpornogebruikers voelen de drang om complete series met kinderporno te pakken te krijgen en om dat te bereiken worden de plaatjes of filmpjes vaak geruild in de besloten netwerken.[76] Zo kan iedereen steeds

[68] Stol e.a. 2008, p. 1.
[69] Stol e.a. 2008, *Ars Aequi*, p. 537.
[70] Zie Jenkins 2001, p. 8, Taylor & Quayle 2003, p. 162 en Akdeniz 2008, p. 7.
[71] Akdeniz 2008, p. 6.
[72] Lünnemann e.a. 2006, p. 108 en 109.
[73] Stol, van Treeck & van der Velde 1999, p. 87. Zie ook onderzoek van Lünnemann e.a. 2006, p. 123: "*Grote producenten die puur uit zijn op winstbejag komen niet voor in de onderzochte dossiers."*
[74] Verbeterprogramma 2009, p. 11.
[75] Taylor & Quayle 2003, p. 94.
[76] Groenveld 2000, p. 79.

meer materiaal bemachtigen. Volgens Jenkins is dat dé manier waarop kinderpornografie verspreid en binnengehaald wordt. Hij verwoordt het als volgt: "*Ultimately, the subculture is driven by quest for new material, the urge to complete collections.*"[77] Ook in andere literatuur wordt gewezen op de verzameldrift van kinderpornogebruikers.[78] Zelf ben ik het met Jenkins eens dat de handel in kinderpornografie op internet wordt stand gehouden door de verzameldrift van kinderpornogebruikers.

Sommige netwerken hanteren een 'groeimodel' waarbij nieuwe leden eerst zelf 'vers materiaal' moeten aanleveren, voordat ze toegang krijgen tot een databank. Dit kan mensen uitlokken tot het maken van nieuwe pornografische foto's.[79] In het W0nderland-netwerk waren honderden mensen actief en om toegang te krijgen tot de exclusieve club moesten nieuwelingen naar verluidt 10.000 nieuwe afbeeldingen aanleveren.[80] Min of meer structurele netwerken van mensen die kinderporno uitwisselen en verspreiden bestonden ook al voor internet. Het materiaal werd toen vaak per post verzonden. Het verspreiden is door het internet sterk vereenvoudigd. Stol verwoord het als volgt: *"door internet ontstaat een ander soort organisatie van kinderpornoactiviteiten: diffuser, minder afhankelijk van de harde kern van pedofielen."*[81]

Het is onduidelijk hoeveel mensen kinderporno op internet verzamelen en daarom is het onmogelijk aan te geven hoe groot de markt van kinderporno op internet precies is.[82] Wel is duidelijk dat het een zeer groot aantal mensen betreft. De Landslide-zaak uit 2002 illustreerde dat goed. Het bedrijf Landslide Productions Inc. beheerde een website via welke abonnementen voor toegang naar kinderpornowebsites werden verkocht. Tijdens het onderzoek naar dit bedrijf bleek dat er alleen al 35.000 mensen in de Verenigde Staten geabonneerd waren.[83] In het

[77] Jenkins 2001, p. 105.
[78] Zie O'Donnell & Miller 2007, p. 83 referent naar een onderzoek van P. Walsh van het Granada Instituut in Dublin van mei 2004, Taylor & Quayle 2003, p. 16, Van der Hulst & Neve 2008, p. 96 en Lünnemann e.a. 2006, p. 123.
[79] Stol, van Treeck en van der Ven 1999, p. 93 verwijzend naar de beschrijving van de uitwisselingsmarkt door internetjournaliste Marie-José Klaver.
[80] Jenkins 2001, p. 99.
[81] Stol, van Treeck en van der Velde 1999, p. 89.
[82] Zie ook Taylor & Quayle 2003, p. 5.
[83] Taylor & Quayle, p. 5.

Verenigd Koninkrijk werd er naar ongeveer 6500 Britse abonnees een onderzoek ingesteld.[84]
Bedenk dat het hier maar om één bedrijf ging dat abonnementen naar betaalde kinderpornowebsites, ook wel *paysites* genoemd, aanbood en er nog vele anderen moeten zijn.

In de volgende paragrafen wordt onderzocht over welke delen van het internet kinderporno verspreid kan worden. Daarvoor deel ik het internet op in de volgende diensten: websites, e-mail, chat netwerken, peer-to-peer netwerken, FTP-diensten, virtuele harde schijven, nieuwsgroepen en bulletin boards. Elk van deze diensten worden in deze paragraaf afzonderlijk behandeld.

3.1.1 Websites

Het World Wide Web is mogelijk gemaakt door het 'hypertext markup language' (HTML). Websites bestaan uit HMTL-*tags* of instructies die aan de browser software vertellen hoe de webpagina weergegeven moet worden. Voorbeelden van webbrowsers zijn Internet Explorer, Mozilla Firefox en Opera. Webpagina's maken het gemakkelijker voor mensen om gebruik te maken van de diensten dat het internet biedt.
Een website kan gevonden worden via zijn 'Uniform Resource Locator' (URL). Op sommige websites staan afbeeldingen en filmpjes met kinderporno. Sommige websites zijn gratis, maar vaak wordt kinderporno tegen betaling aangeboden. De kinderporno kan via websites gedownload of direct bekeken worden (bij video wordt dit 'streaming video' genoemd*)*. Soms worden er nog informatiedragers met kinderporno via een soort 'webshop' verkocht. Een voorbeeld daarvan was de *Blue Orchid*-website die tussen maart en oktober 2000 online was. De website verkocht collecties en videobanden en cd-roms van volwassenen die acht- tot en met vijftienjarige kinderen misbruikten. De films werden voor een bedrag tussen de 300 en 500 dollar verkocht en trok klanten uit 15 verschillende landen. Uiteindelijk werd de beheerder van webpagina opgepakt en in zijn huis troffen ze het gehele klantenbestand van de website aan.[85] Deze zaak illustreert goed dat er veel geld

[84] Akdeniz 2008, p. 26 en 27.
[85] O'Donnell & Miller 2007, p. 36 en 37.

kan worden verdiend met kinderporno. Tegenwoordig wordt kinderpornografie sneller digitaal beschikbaar gesteld dan via de verkoop van fysiek materiaal. De meeste meldingen bij het Meldpunt Kinderporno gaan over kinderporno via websites, op afstand gevolgd door kinderporno via peer-to-peer netwerken, chatboxen en nieuwsgroepen.[86] Echter, uit deze gegevens kunnen we geen conclusies trekken omdat de *dark number* onbekend is en we niet beschikken over slachtofferenquêtes. We kunnen alleen concluderen dat vooral kinderporno via spam[87] en websites tot meldingen leidt.[88]

3.1.2 E-mail

Electronic mail stelt mensen in staat om snel en gemakkelijk digitaal berichten aan elkaar te versturen. Het bestaat al sinds 1971 en is uitgevonden door de Amerikaan Ray Tomlinson.[89] In de jaren negentig brak het pas echt door.

E-mail maakt meestal gebruik van het 'Simple Mail Transport Protocol' (SMTP). De meeste e-mail programma's maken het mogelijk om een bestand bij te voegen. De grootte van dit bestand wordt alleen door het programma en de snelheid van de internetverbinding beperkt.

Kinderporno wordt soms via e-mail verspreid, soms in de vorm van spam, echter niet in grote hoeveelheden. Meestal zijn het bepaalde foto's die de verstuurder met een andere verzamelaar of distributeur wil delen.[90]

3.1.3 Chatprogramma's

Chatten is het in *realtime* praten tussen twee of meer gebruikers. Dit gesprek vindt plaats in een zogenaamde *chatbox* dat in het Nederlands ook wel 'babbelbox' wordt genoemd.

3.1.3.1 IRC

Een van de grootste chatnetwerken ter wereld is 'Internet Relay Chat' (IRC). Het is in 1988 ontwikkeld door Jarkko Oikarinen.[91] Iedereen kan toegang verschaffen tot dit systeem en het is niet altijd nodig te betalen of zelfs te registreren. IRC bestaat

[86] Jaarverslag 2008, Meldpunt Kinderporno.
[87] Spam is ongevraagde commerciële communicatie.
[88] Stol e.a. 2008, *Ars Aequi*, p. 546.
[89] Dasselaar 2008, p. 40.
[90] Ferraro & Casey 2005, p. 23.
[91] Dasselaar 2008, p. 42.

uit afzonderlijke netwerken, zoals het QuakeNet, Undernet, DALnet, EFnet en IRCnet en geen van deze organisaties controleert de andere. Elk van deze 'subnets' is eigenlijk een server[92], of een combinatie van verschillende servers, die door verschillende groeperingen in stand gehouden wordt. Ze maken allen onderdeel uit van IRC, maar fysiek zijn ze afzonderlijk.[93]

In het programma kunnen *channels*, oftewel kanalen gecreëerd worden. Wereldwijd zijn op elk moment duizenden kanalen actief. De kanalen zijn op thema georganiseerd en er kan met meerdere gebruikers tegelijkertijd gepraat worden. Live gesprekken kunnen plaatsvinden via tekst, audio en video op internet. Kinderpornogebruikers kunnen in bepaalde kanalen bijvoorbeeld afspreken om materialen uit te wisselen en IRC is zelfs gebruikt om live beelden uit te zenden van kinderen die seksueel misbruikt worden.[94] Op deze chatkanalen waren leden actief van de W0nderland club. De W0nderland Club werd ontdekt naar aanleiding van onderzoek naar de veel kleinere Orchid Club.

3.1.3.1.1 DCC

IRC heeft een 'direct client connection' (DCC) mogelijkheid die het mogelijk maakt dat twee mensen met elkaar een privégesprek hebben en bestanden kunnen uitwisselen zonder dat anderen in de chatbox het kunnen zien. DCC zorgt ervoor dat het IRC-netwerk wordt 'overgeslagen', waardoor er bijna of geen spoor achter gelaten wordt op de servers van IRC.[95]
Een andere mogelijkheid van IRC heet '*fserve*' (afkorting voor fileserver), dat ervoor zorgt dat mensen bestanden op hun PC's (anoniem) beschikbaar kunnen stellen aan andere IRC-gebruikers.

3.1.3.2 Messengers

Chatprogramma's zoals *Windows Live Messenger* (van Microsoft) en *AOL* (het populaire chatprogramma van de Amerikaanse ISP America Online) zijn tevens zeer populair, maar zullen minder door kinderpornogebruikers gebruikt worden. Met

[92] Een server is een computer of programma dat diensten verleent aan andere computers.
[93] Casey 2004, p. 486.
[94] Jenkins 2001, p. 78.
[95] Casey 2004, p. 487.

behulp van versleutelingprogramma's kan het verkeer echter versleuteld worden en zo kan wel vertrouwelijk gecommuniceerd worden. De vermeende leden van de Hofstadgroep maakten gebruik van een versleutelingsprogramma.[96] Er kunnen ook bestanden verstuurd worden via de chatprogramma's, dat uiteraard de verspreiding van kinderpornografie in de zin van artikel 240b Sr oplevert.

3.1.3.3 ICQ

ICQ - dat staat voor 'I seek you' - is een ander groot, gratis chatnetwerk dat iedereen op internet kan gebruiken, maar het onderscheid zich van IRC, omdat er een registratieproces is. Nadat een formulier (al dan niet naar waarheid) is ingevuld met details zoals naam, e-mailadres en persoonlijke interesses krijgt iedereen een 'user identification number' (UIN) voor het ICQ-netwerk.[97]
In plaats van in chatkanalen te ontmoeten, moeten ICQ gebruikers elkaar opzoeken en allebei akkoord gaan om een gesprek aan te gaan. Dit limiteert het contact op ICQ netwerken, maar zorgt ook voor meer privégesprekken dan op andere chat netwerken. Echter, ICQ stuurt al haar boodschappen door een centraal systeem, zodat het berichtenverkeer in de gaten kan worden gehouden.

3.1.4 Peer-to-Peer (P2P) netwerken

De komst van *Napster* in 1999 introduceerde het peer-to-peer bestandsuitwisselingsprincipe aan het grote publiek.[98] Bij peer-to-peer programma's stelt een internetgebruiker (een *peer*) een deel van zijn eigen computer open (hij deelt een map, standaard is dit 'mijn gedeelde map') om zo muziek- en videobestanden met andere internetgebruikers uit te wisselen. Een computer werkt dan zowel als *client* en als *server*. Bestanden kunnen dus gedownload worden van andere gebruikers, terwijl andere gebruikers bestanden van de computer van de eigenaar downloaden. Bij sommige programma's kan echter ingesteld worden dat er niets gedeeld mag worden. De snelheid van downloaden wordt bij peer-to-peer programma's gelimiteerd door de uploadsnelheid van de gebruikers die het bestand delen. Napster werd aangeklaagd door de muziekindustrie en dat betekende het einde van deze dienst.

[96] Dasselaar 2008, p. 43
[97] Casey 2004, p. 487.
[98] Biddle 2002, p. 5.

Uit de ipoque-studie[99] van 2008 en 2009 blijkt dat 53% van het internetverkeer in Duitsland werd veroorzaakt door peer-to-peer programma's. Verder blijkt uit het onderzoek dat in Duitsland *BitTorrent* het populairste programma is. In Nederland zullen deze cijfers niet heel anders zijn. De cijfers illustreren de populariteit van de netwerken.

Kazaa en *Gnutella* zijn twee andere zeer populaire P2P programma's. In tegenstelling tot Napster is Gnutella een decentraal peer-to-peer programma (het maakt dus geen gebruik van een centrale server of dienst). Dit maakt het zowel robuuster op zowel technisch als juridisch vlak. Om van deze programma's gebruik te maken, moet een gebruikersnaam aangemaakt worden, maar dat kan natuurlijk ook een schuilnaam (nickname) zijn.
Alleen het IP-adres identificeert dan nog de gebruiker. De zwakheden van het systeem zijn het probleem van *free riding* (bestanden downloaden zonder dat ze gedeeld worden) en het is lastiger het systeem anoniem te maken in vergelijking met andere peer-to-peer diensten. Peer-to-peer programma's zijn zeer populair bij het uitwisselen van muziek en films. Ook kinderporno blijkt gemakkelijk gevonden en gedownload te kunnen worden van peer-to-peer netwerken.[100] Van peer-to–peer netwerken is bekend dat zij op substantiële wijze bijdragen aan de verspreiding van kinderporno en sommige wetenschappers verwachten dat haar rol in de markt van kinderporno in de toekomst zal groeien.[101]

3.1.4.1 (Bit)Torrent

BitTorrent is een andere vorm van een peer-to-peer bestandsuitwisseling. Hierbij is wel een centrale server werkzaam die de vraag en aanbod naar bestanden met elkaar verbindt. Het netwerk bij BitTorrent's is eigenlijk een netwerk dat wordt gebruikt voor een specifiek BitTorrent-bestand. Voor het gebruik van BitTorrent moet een BitTorrent-client geïnstalleerd worden. Bestanden worden in kleine deeltjes opgedeeld en vervolgens over het internet verspreid en gedownload. Het is vooralsnog onduidelijk of het gebruik van Bittorent op grond van de Auteurswet

[99] http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009 (laatst geraadpleegd op 6 oktober 2009).
[100] Akdeniz 2008, P. 7.
[101] Stol e.a. 2008, *Ars Aequi*, p. 536 en Leukfeldt, Domenie & Stol 2009, p. 26.

1912 is toegestaan, aangezien het uploaden niet uitgezet kan worden. Zeer recent zijn de sites The Pirate Bay en Mininova veroordeeld.[102] Zij lieten de locaties zien waar de bestanden met BitTorrent's stonden en dat werd door de rechter als onrechtmatig geacht. Het is nog onduidelijk wat voor invloed deze uitspraken hebben op deze vorm van bestandsuitwisseling. Het zou kunnen dat de gebruikers van peer-to-peer programma's overstappen naar nieuwsgroepen of besloten peer-to-peer netwerken (zie hoofdstuk 5.4). Het is onduidelijk hoeveel kinderporno er via BitTorrent-programma's verspreid en binnengehaald wordt.

3.1.5 FTP

Het 'File Transfer Protocol' (FTP) is exclusief bedoeld om bestanden van één computer naar een andere computer te transporteren. Een FTP-server is een aan een netwerk (meestal internet) gekoppelde computer die een verzameling bestanden ter beschikking stelt aan mensen die toegang hebben tot deze server.[103] Een bekend FTP-programma is *FileZilla*.[104] Het verschil met peer-to-peer programma's is dat computers niet tegelijk een client en server zijn. Er is maar één server en andere computers (clients) kunnen bestanden bij de server ophalen of aanleveren.

Niet alle FTP-servers zijn aangemeld bij het Domain Name System (DNS). De servers kunnen dan alleen bezocht worden door mensen die het IP-nummer van de server kennen en in staat zijn om daarmee een verbinding te maken. Ook kan een wachtwoord zijn vereist alvorens toegang te krijgen tot de server, zodat het nog veiliger wordt gemaakt om bestanden uit te wisselen. Kinderpornohandelaars kunnen door het gebruik van FTP op ieder moment honderdduizenden foto's downloaden of ruilen.[105]

3.1.6 Virtuele harde schijven

Virtuele harde schijven zijn ook een mogelijkheid om kinderpornografie te verspreiden. Een virtuele harde schijf is ruimte voor dataopslag dat op internet wordt aangeboden. De opslagruimte van een e-mailaccount, bijvoorbeeld *Gmail,*

[102] Pirate Bay: Rb. Amsterdam 30 juli 2009, *LJN* BJ4466 en Rb. Amsterdam 22 oktober 2009, *LJN* BK1067. Mininova: Rb. Utrecht 26 augustus 2008, *LJN* BJ6008.
[103] Eshof e.a. 2002, p. 38.
[104] http://filezilla-project.org/
[105] Ferraro & Casey 2005, p. 37.

kan ook dienen als harde schijf. De plaatjes en/of video's kunnen worden geüpload naar de virtuele harde schijf en op een ander moment weer worden gedownload. Er zijn op dit moment geen aanwijzingen dat dergelijke accounts door kinderpornoverzamelaars worden gebruikt. Dit kan echter komen doordat hiernaar geen structureel zaakonderzoek wordt gedaan.[106] Het is aldus nog onduidelijk in hoeverre deze verspreidings- en downloadtechniek gebruikt wordt door kinderpornogebruikers. Mijn verwachting is dat het algemene gebruik van virtuele harde schijven zal toenemen en het ook als distributiewijze voor kinderporno gebruikt zal worden.

3.1.7 Nieuwsgroepen

Nieuwsgroepen zijn de online versie van publieke prikborden (denk aan bijvoorbeeld supermarkten). Door iedereen kunnen er behalve tekst ook afbeeldingen, geluid, video en software in bijna alle extensies worden geüpload. De inhoud op de nieuwsgroepen kan vervolgens gedownload worden. Met nieuwsgroepen kan net zo snel gedownload worden als dat de bandbreedte van de internetverbinding en de server van de downloader toelaat. Deze eigenschappen maken dat nieuwsgroepen de grootste bron van gratis porno op internet.[107] Het gebruik van nieuwsgroepen is een van de oudste manieren om kinderporno te verspreiden en te downloaden.[108] De meeste nieuwsgroepen maken deel uit van een gratis, wereldwijd systeem dat het 'User's Network' (hierna: Usenet) genoemd wordt. In 1979 is Usenet begonnen.[109] Usenet bestaat uit nieuwsservers die overal ter wereld staan en communiceren via het 'Network News Transport Protocol' (NNTP). Elke server 'abonneert' zich bij een aantal nieuwsgroepen en slaat een kopie op van elke Usenet nieuwsgroep waartoe het zich heeft ingeschreven. Er is geen centrale server die Usenet coördineert; het is een samenwerkend netwerk.[110]
Nieuwsgroepen worden opgedeeld in verschillende categorieën, namelijk: "comp." (*computer)*, "*Humanities.*", "misc." (*miscellaneous), "news.",* "rec." (*recreational)*, "sci." (*science fiction*), "soc." (*social*), en "alt." (*alternative)*.

[106] Stol e.a. 2008, p. 10, onder verwijzing naar Oosterink en Van Eijk 2006, *Opsporing Kinderpornografie op internet, Een statusoverzicht,* 's-Gravenhage: Ministerie van Justitie.
[107] Ferraro & Casey, 2005, p. 31.
[108] Britz 2009, p. 40.
[109] Casey 2004, p. 489.
[110] Casey 2004, p. 508.

Binnen de *alternative* groep zijn weer subgroepen te vinden die zich specifiek richten op kinderpornografie. In dit soort nieuwsgroepen worden vaak tips gegeven over websites waarop kinderporno te vinden is. Mensen surfen dan snel naar de website en bekijken of downloaden daar de kinderporno. Een paar uur later worden de foto's vaak alweer verwijderd en houdt de site op te bestaan.[111]

ISP's kunnen een zekere mate van censuur toepassen. De meeste nieuwsgroepen worden constant gecontroleerd op woorden (met een zoekrobot) die aanwijzingen geven dat er naar kinderporno verwezen wordt. Deze berichten worden vervolgens verwijderd. Toch gebeurt het dat sommige nieuwsgroepen met kinderporno door de ene provider wel worden geblokkeerd en de andere niet.
De laatste jaren is het aanbod van kinderpornografisch materiaal op nieuwsgroepen dankzij de inspanningen van ISP's drastisch omlaag gegaan. Stol heeft onderzoek gedaan naar kinderporno op nieuwsgroepen en daar bleek uit dat in 2002 op 3,5 procent van de nieuwsgroepen naar websites werd verwezen waar kinderporno zou staan. In 2004 trof hij geen verwijzingen meer aan naar websites met kinderporno.[112]

Een discussieforum lijkt op een nieuwsgroep door het feit dat men boodschappen achter kan laten en de discussie over een vastgesteld onderwerp gaat. Het grote verschil is waar de data zich bevindt. Bij nieuwsgroepen bevindt het materiaal zich op servers over de gehele wereld die worden gerund door verschillende mensen, terwijl de meeste discussieforums onderhouden worden op één server door een eigenaar of een beheerder van het forum.

3.1.8 Bulletin Boards

In 1978 gaat het eerste Bulletin Board System (hierna: BBS) 'de lucht' in. Het systeem is uitgevonden door Ward Christensen en Randy Seuss.[113] Een BSS is eigenlijk een digitaal prikbord en daarmee vergelijkbaar met discussieforums en

[111] Jenkins 2001, p. 68.
[112] Stol 2004, p. 90. In de volgende nieuwsgroepen werd er gezocht naar kinderporno: in 2002: alt.fan.jerky.boys, alt.sex.realdol, alt.teens.sexuality, alt.sex.young en in 2004 dezelfde plus alt.sex.boys, alt.sex.girls en alt.sex.first-time.
[113] Dasselaar 2008, p. 24.

nieuwsgroepen. Op dit prikbord kunnen bestanden en berichten worden uitgewisseld. Op sommige BBS wordt verwezen naar de locaties waar kinderpornografie te vinden is.
Het aantal mensen dat gebruik maakte van BBS's liep terug met de opkomst van het internet voor de massa. Het grote verschil met nieuwsgroepen is dat de BBS's gehost worden door de eigenaar of beheerder en niet via de ISP beschikbaar wordt gesteld. Vanwege het feit dat er geen ISP of derde in het spel is, zijn BBS systemen opnieuw een populaire manier geworden om kinderpornografie en ander materiaal te verspreiden.[114]

3.2 Een typologie van kinderpornografisch materiaal

Kinderpornografie is in allerlei soorten op internet aanwezig. Met betrekking tot de aard van het materiaal van naaktfoto's tot seksfilms en met betrekking tot de ernst van *softcore* tot *hardcore* materiaal. De meest populaire foto's zijn, volgens Jenkins, foto's van seksuele handelingen met kinderen uit Noord-Amerika en Europa.[115]
Een groot deel van het op internet aangetroffen materiaal is afkomstig uit de jaren 1960 tot 1975. Van deze opnamen, meestal aangeduid met namen als 'Lolita', 'Lolita-color', enzovoort, zijn gedigitaliseerde video's en afbeeldingen op het internet te vinden. Er was in 2000 al een voorzichtige tendens te bespeuren van steeds nieuwere afbeeldingen op het internet. De verhouding van 80-20% verschoof naar zo'n 70-30%.[116] Dat is een zeer zorgelijke tendens, omdat telkens als er nieuw materiaal wordt vervaardigd dit leidt tot misbruik van kinderen. Evenzo zorgelijk is dat het in beslag genomen kinderpornografisch materiaal de laatste jaren steeds grover en gewelddadiger lijkt te worden.[117]

Op basis van kleding- en achtergrondkenmerken is vastgesteld dat veel opnamen met als slachtoffer jonge jongens uit Oost-Europese landen komen en de opnamen met als slachtoffer jonge meisjes met name uit de Verenigde Staten, West-Europa en Aziatische landen.[118] De commerciële productie is vooral afkomstig uit Oost-

[114] Ferraro & Casey 2005, p. 33.
[115] Jenkins 2001, p. 85.
[116] Groeneveld 2000, p. 80.
[117] Verbeterprogramma kinderporno 2009, p. 10 en Groenveld 2000, p. 80.
[118] Groeneveld 2000, p. 80 en 81.

Europa en Azië.[119] De slachtoffers zijn vaak kwetsbare kinderen. Illustratief is een passage uit het vonnis van de rechtbank Roermond[120] over een (commerciële) Russische website met kinderporno: "*Daar waar de KLPD afbeeldingen kon terugbrengen naar opgehelderde zaken, betroffen dit vaak kinderen die in de familiesfeer ernstig misbruikt waren of kansarme kinderen die met dit doel door professionele bendes van de straat geplukt werden."*

Hoewel er vaak blootfoto's van kinderen (softcore materiaal) in netwerken op internet uitgewisseld worden, zonder dat er sprake is van kinderpornografie in de zin van de wet, is er ook meer weerzinwekkend materiaal in omloop.[121] Door de jonge leeftijd van de kinderen vindt er in de meeste van deze foto's en video's geen penetratie plaats, maar is er op de foto's en video's vaak orale seks of masturbatie te zien. Soms is er op het beeldmateriaal wél vaginale en anale penetratie te zien en worden er zelfs vibrators gebruikt.[122] Dit soort materiaal wordt als hardcore materiaal beschouwd. De bij kinderpornogebruikers bekende 'Hel-lo-series' laat bijvoorbeeld penetratie zien.[123] Deze serie is erg populair en illustreert goed hoe extreem het materiaal dat te vinden is op internet kan zijn. 'Hel-lo' staat voor 'Helena-lolita'. 'Helena' is een waarschijnlijk Brits meisje van ongeveer zeven à acht jaar waarvan eind jaren tachtig een fotoserie is gemaakt. Van het meisje is een fotoserie gemaakt waarin zij allerlei seksuele poses aanneemt, maar verricht zij daarnaast ook seksuele handelingen met het jongetje Gavin van ongeveer dezelfde leeftijd. Er zijn ook foto's waarin beiden kinderen seks hebben met een volwassen man; waarschijnlijk de vader van Helena. De serie schijnt een soort 'starterserie' te zijn geworden voor nieuwe kinderpornogebruikers.[124] De serie is onderdeel van een veel grotere collectie met titels als 'hel-anal', 'hel-cum' en 'hel-louise', waarvan de namen voor zich spreken. Hardcore-materiaal zoals de Hel-lo-series zijn in grote aantallen verkrijgbaar. Andere voorbeelden van series met 'kinderpornosterren' zijn

[119] Lünnemann e.a. 2006, p. 109.
[120] Rb. Roermond, 7 juli 2006, *LJN*: AX9921.
[121] Stol, van Treeck en van der Velde 1999, p. 68.
[122] Groenveld 2000, p. 80: "Afbeeldingen van verkrachtingen van baby's vormen geen uitzondering meer."
[123] Jenkins 2001, p. 83.
[124] Jenkins 2001, p. 2.

Vicky, Laika, Hayley en 'Louisiana'.[125] Zoals al eerder is aangegeven worden de series door veel kinderpornogebruikers verzameld.

Tussenconclusie

In dit hoofdstuk is geconstateerd dat het internet een belangrijke rol speelt bij het bekijken, downloaden en verspreiden van kinderpornografie. Het kinderpornografische materiaal bestaat vandaag de dag uit bits en bytes in plaats van foto's in een magazine of een videoband. Dit heeft tot gevolg dat het materiaal met grote snelheid over het internet kan worden verspreid. Het materiaal wordt vervolgens vaak gedownload en gecategoriseerd op een gegevensdrager.
Door commerciële vervaardigers en verspreiders van kinderporno wordt het materiaal beschikbaar gesteld. De markt wordt uiteindelijk in stand gehouden door de verzameldrang van de verzamelaars van kinderpornografie. Het grootste deel van het totale aanbod bestaat uit kinderpornografie dat in de huishoudelijke sfeer is gemaakt. Nieuw materiaal is daarbij het meest begeerlijk. De verzameldrang van kinderpornogebruikers leidt ertoe dat hele collecties van 'kinderpornosterren' worden aangelegd. Het materiaal varieert van 'gewone' naaktfoto's van minderjarigen tot hardcore kinderporno.

Feit is dat als er kinderporno op internet gekeken of gedownload wordt, dit meestal een spoor achterlaat op de harde schijf. Dat kan leiden tot het bezit van kinderpornografie wat strafbaar is gesteld in artikel 240b Sr. In het volgende hoofdstuk wordt hier verder op in gegaan en wordt tevens de vervolgingspraktijk van 240b Sr geanalyseerd.

[125] Jenkins 2001, p. 21.

Hoofdstuk 4: Kinderporno op de computer

Zowel bij het downloaden als het bekijken van kinderporno op internet blijven er normaal gesproken sporen achter op de harde schijf van een computer. Deze sporen geven het nodige bewijs om te spreken van het bezit van kinderporno. Als de harde schijf van een kinderpornogebruiker eenmaal in beslag is genomen, kan er uitgebreid onderzoek worden gedaan naar de documenten op de harde schijf. De harde schijf speelt dan ook een sleutelrol in kinderpornozaken. In het boek *Cyber alert*[126] wordt de rol van de harde schijf mooi verwoord: "*The hard drive of a computer is like an all-seeing, all-knowing witness, silently recording all that the computer (and by extension the computer user) is doing, and keeping its secrets intact until the moment when someone chooses to interrogate it.*"[127]

In dit hoofdstuk wordt uitgelegd hoe, al dan niet onopgemerkt, kinderporno op de harde schijf van een computer terecht kan komen. Vervolgens wordt ingegaan onder welke omstandigheden dat bezit in de zin van artikel 240b Sr oplevert. Daarna wordt aangegeven hoe de verspreiding en vervaardiging van kinderpornografie strafbaar is gesteld en of de focus van de vervolging bij de vraagkant of de aanbodkant van de markt van kinderporno ligt. Tenslotte wordt de opsporings- en vervolgingspraktijk van artikel 240b Sr verklaard.

4.1 Kinderporno op de harde schijf

Kinderporno op internet is in twee vormen beschikbaar: als '*realtime*' en 'downloadbaar' materiaal. Realtime is de term dat gebruikt wordt voor een activiteit dat in de werkelijke tijd in plaats van bijvoorbeeld in gecomprimeerde of vertraagde tijd plaatsvindt. Bij kinderporno op internet betekent dit dat het materiaal direct bekeken kan worden, zonder dat het wordt opgeslagen op de harde schijf. Een video kan bijvoorbeeld in de vorm van een '*stream*' worden aangeboden. Dit kan een soort live-uitzending zijn waar je halverwege in kan vallen of een uitzending dat vanaf het begin bekeken kan worden. Downloadbaar materiaal verschilt van

[126] P. Warren en M. Streeter, *Cyber Alert, how the world is under attack from a new form of crime*, London, 2005.
[127] Warren & Streeter 2005, p. 79.

realtime materiaal, omdat het vanaf het internet op een harde schijf computer (of een andere gegevensdrager) opgeslagen kan worden en later nog eens bekeken kan worden.

4.1.1 Bezit

Bij het in bezit hebben van een kinderpornografische afbeelding moet er sprake zijn van opzet. Dit staat niet expliciet in artikel 240b Sr, maar de opzet wordt in het artikel ingelezen.[128] Opzet bestaat uit twee elementen: willen en weten. De nadruk ligt daarbij in de meeste gevallen op het vaststellen van het cognitieve element: 'zich bewust zijn'.[129]

Door Stevens en Koops is een uitgebreide analyse gemaakt van de jurisprudentie over kinderporno op de harde schijf.[130] Zij onderscheiden drie elementen voor de strafrechtelijke aansprakelijkheid van digitale kinderporno: *kennen*, *kunnen* en *willen*. Bij *kennen* gaat het om het bewustheidcriterium dat ook in de vorm van voorwaardelijk opzet voorkomt (d.w.z. het welbewust het risico nemen om kinderpornografisch materiaal in bezit te krijgen). Bij *kunnen* gaat het om de beschikkingsmacht over de kinderpornografische afbeeldingen en bij *willen* dat de kinderpornogebruiker de bedoeling had om de afbeeldingen te bewaren en daarmee in zijn bezit te hebben.
Zij hebben het volgende, naar mijn mening juiste, criterium geformuleerd: *"Degene op wiens harde schijf kinderporno is aangetroffen, is strafbaar wegens het opzettelijk in bezit hebben van deze kinderporno, indien hij zich bewust is van de aanwezigheid van de bestanden, hierover beschikkingsmacht heeft, en de bedoeling heeft ze in bezit te hebben."* In dit criterium komen de drie elementen naar voren die Advocaat-Generaal Knigge al eerder had genoemd, namelijk: vastlegging, opzet en een zekere beschikkingsmacht.[131]

[128] Zie HR 28 feburari 2006, *LJN* AU9104.
[129] De Hullu 2009, p. 213.
[130] L. Stevens & E.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', *DD*, 2009, 51, p. 669-696.
[131] HR 28 februari 2006, *LJN* AU9104, r.o. 15 (concl. A-G Knigge).

Een afbeelding of filmpje kan in een bepaald formaat opgeslagen worden op de harde schijf van een computer. Veel kinderpornogebruikers doen dit, omdat zij het materiaal dan later nog eens kunnen bekijken of om aan hun verzameldrift te voldoen (zie hoofdstuk 3.1). Deze bestanden kunnen gemakkelijk op een computer gevonden worden en forensische software kan zelfs de kleinste sporen van kinderporno terugvinden. Sporen van kinderporno zijn namelijk ook op andere plekken te vinden dan in de zichtbare mappen op de harde schijf.

4.1.2 Onbewust in bezit hebben

Als er via een webbrowser naar plaatjes en video wordt gekeken dan worden er '*caches*' gebruikt om het surfen te versnellen. Een cache is een automatische opslag op de computer die met het internet verbonden is en download automatisch informatie dat nuttig is voor toekomstige bezoeken op websites van het internet.[132] Afbeeldingen worden bijvoorbeeld in de map 'tijdelijke internet bestanden' in het cache opgeslagen, zodat het de volgende keer niet meer gedownload hoeft te worden. Zoektermen in bijvoorbeeld Google of andere webpagina's worden ook opgeslagen en daarnaast worden er automatisch '*cookies*' op de computer opgeslagen. Cookies zijn kleine databestanden waar onder andere in kan staan wanneer een bepaalde website voor het laatst is bezocht. Het te voorschijn halen van pagina's gaat op die manier sneller. Als de bestanden vervolgens afgespeeld worden in een mediaspeler, wordt daarvan in een register van een computer een spoor achtergelaten. Ook in andere registers en logbestanden kunnen sporen van kinderporno gevonden worden.
Kinderporno kan tevens onbedoeld op de computer terecht komen, doordat het onbedoeld is gedownload samen met een grote hoeveelheid legale porno. Dat materiaal wordt bijvangst genoemd.

Worden de bestanden van de harde schijf verwijderd dan betekent dit nog niet dat de bestanden niet meer op de harde schijf staan. Als bestanden in de prullenbak geplaatst worden en vervolgens verwijderd worden, dan wordt slechts de benaming

[132] Gillespie 2008, p. 3.

van het bestand verwijderd. Casey[133] vergelijkt dit systeem met de boeken in de kasten van een bibliotheek. Als het kaartensysteem kapot gemaakt wordt staan de boeken er nog wel, het is alleen niet meer duidelijk waar ze staan. De bestanden worden dan 'unallocated files' en kunnen, met specialistische forensische software, te voorschijn worden gehaald.

Kinderporno kan ook gevonden worden in de '*slack space'* van computers. Dit is het deel van een cluster in een harde schijf dat niet opgevuld wordt. Als een bestand minder ruimte inneemt dan een cluster, kunnen andere bestanden de overige ruimte in de cluster niet opvullen. Kort gezegd, als een cluster data bevat, is de gehele cluster gereserveerd. Casey[134] maakt daarbij opnieuw een handige vergelijking met een situatie dat in veel restaurants voorkomt. Als drie mensen aan een tafeltje zitten waar eigenlijk vier mensen aan kunnen zitten, dan blijft de overige stoel leeg totdat de mensen klaar zijn met eten. Het idee is dat een vierde vreemde tafelgast de maaltijd zal verstoren. Vergelijkbaar is het als een computer in de overige ruimte van de cluster informatie probeert te duwen. De nieuwe data kan dan in conflict raken met de oude. Die extra sectoren in een cluster noemen we slack space. Soms kunnen daar ook sporen van kinderporno in gevonden worden.

Tenslotte kunnen er in de wisselbestanden (in het Engels 's*wap files'* genoemd) van een harde schijf sporen van kinderporno worden gevonden. Als Windows meerdere programma's tegelijk verwerkt, plaatst het besturingssysteem een deel van de inactieve programma's op de harde schijf. De computergebruiker krijgt het idee dat meerdere programma's tegelijk op de computer lopen, maar dat is in werkelijkheid niet zo. De bestanden worden namelijk tussen de harde schijf en het werkgeheugen snel aan elkaar uitgewisseld. Het besturingssysteem probeert alleen die geheugenblokken in het werkgeheugen te houden die het meest worden gebruikt. De gegevens die in de wisselbestanden staan kunnen sporen van kinderporno bevatten. Deze sporen zullen echter niet altijd tevoorschijn gehaald kunnen worden.

[133] Casey 2004, p. 203.
[134] Casey 2004, p. 205.

Tijdelijke wisselbestanden gaan namelijk verloren als het besturingssysteem wordt afgesloten.[135]
Uit het bovenstaande blijkt wel dat de gemiddelde computergebruiker niet altijd bewust is van de kinderporno op zijn harde schijf. De vraag is hoe dit zich verhoudt met de eis dat iemand *opzettelijk* kinderporno in bezit heeft.

4.1.3 De 'actieve bemoeienis met kinderporno'

De gemiddelde internetgebruiker hoeft niet op de hoogte te zijn van tijdelijke internetbestanden, unallocated files, slack space en wisselbestanden.[136] Als daar sporen van kinderporno op worden gevonden, dan constitueert dit niet per definitie het bezit van kinderpornografie. Het is wel als een aanwijzing te beschouwen, dat iemand zich bezig heeft gehouden met kinderporno. Bij de eerder genoemde situatie van bijvangst wordt het bezit van kinderporno vaak wel aangenomen.[137] Slechts als het maar om enkele plaatjes met kinderporno gaat en er geen enkele aanwijzing is dat de verdachte actief heeft gezocht naar kinderporno, is er geen sprake van bezit wegens het ontbreken van het element: opzet.[138]

Het hangt sterk af van de omstandigheden van het geval of er sprake is van bezit of niet. Stevens en Koops hebben in hun artikel een aantal factoren uit de jurisprudentie gedistilleerd waarmee rechters rekening dienen te houden bij de strafbaarstelling van het bezit van kinderporno. Veel van deze factoren worden overigens ook aangegeven in de Aanwijzing kinderpornografie[139] en het rapport van Lünnemann e.a.[140] De factoren zijn onder andere: de computerkennis van de verdachte, het aanwezig zijn van speciale programmatuur voor het wissen en tevoorschijn halen van bestanden, het aantal kinderporno bestanden op de harde schijf en de tijdsduur tussen het downloaden en bekijken van de bestanden. Thoonen stipt in haar artikel[141] over het bezit van digitale kinderpornografie hier

[135] Stephenson 2000, p. 101.
[136] Zie Hof 's-Hertogenbosch 30 oktober 2006, *LJN* AZ1412.
[137] Zie bijvoorbeeld Rb. Utrecht 27 maart 2006, *LJN* AV7354, Rb. 's-Hertogenbosch 29 oktober 2008, *LJN* BG3640 en Rb. Groningen 5 augustus 2004, *LJN* AQ6334.
[138] Aldus Stevens & Koops 2009, p. 684.
[139] Aanwijzing kinderpornografie (artikel 240b WvSr), *Stcrt*. 2007, 162.
[140] Lünnemann e.a. 2006, p. 65-70.
[141] E.C.M. Thoonen, 'Bezit van digitale kinderpornografie', *NJB* 2009, 84, p. 2117 – 2122.

een interessant punt aan. Als het tijdsbestek kort is en de gegevens snel verwijderd worden dan is er volgens de jurisprudentie geen sprake van bezit.[142] De vraag blijft hoe lang dit tijdsbestek precies mag zijn. Daar is vooralsnog vanuit de rechtspraak geen duidelijk antwoord op gegeven. De factor 'tijdsduur tussen het downloaden en bekijken van bestanden' blijft daarom vaag.

Het komt er op neer dat opzet moet blijken uit de 'actieve bemoeienis met kinderporno' van de computergebruiker.[143] Indien er bewust op zoek is gegaan naar kinderpornografie, dan wordt het bezit daarvan doorgaans aangenomen.[144] Is er incidenteel 'per ongeluk' geklikt op een link en kwam men op een kinderpornowebsite terecht, dan wordt opzet door de computergebruiker niet aangenomen. Voor deze groep geldt volgens Stevens en Koops 'niet strafbaar, tenzij'. Zodra de verdachte meer bemoeienis met kinderporno lijkt te hebben dan incidenteel, slaat de standaard al snel om naar 'strafbaar, tenzij'.[145]

Een groot probleem op dit moment is dat een deel van de kinderpornogebruikers alleen kinderporno op internet kijken en daarna meteen alle sporen op de harde schijf wissen. Volgens de jurisprudentie is er hier geen sprake van 'bezit' en kan men niet vervolgd worden voor artikel 240b Sr.[146] De Nederlandse deelname aan het Verdrag van Lanzarote heeft hier verandering in gebracht.

4.1.4 Toegang verschaffen tot kinderporno

In paragraaf 2.1.3.1 is al aangeven dat het toegang verschaffen tot kinderporno sinds kort strafbaar is gesteld. Met deze uitbreiding is ook het realtime naar kinderporno kijken zonder sporen achter te laten op de harde schijf strafbaar op grond van artikel 240b Sr. Vereist is daarbij wel dat er een *actieve handeling* moet zijn gevoerd dat *gericht* is op het verkrijgen van toegang.[147] Er kan geconcludeerd

[142] Bijvoorbeeld Rb. Breda 22 februari 2006, *LJN:* AV2996, Hof Arnhem 4 april 2005, *NBSTRAF* 2005, 279 en Rb. Middelburg 12 februari 2003, *LJN:* AF4981.
[143] Stevens & Koops 2009, p. 695.
[144] Zie bijvoorbeeld HR 11 september 2007 *LJN:* BA6316, Rb. Groningen 28 januari 2008, *LJN:* BC3529 en HR 30 september 2008 *LJN:* BD4872.
[145] Stevens & Koops 2009, p. 691.
[146] Zie onder andere Gerechtshof Leeuwarden 22 maart 2005, *LJN*: AT6636 en Rb. Alkmaar 28 november 2006, *LJN*: AZ3173 met een verwijzing naar *Kamerstukken II* 2001/02, 27 745, nr. 15, p. 2.
[147] *Kamerstukken II* 2008/09, nr. 3, p. 4 (MvT).

worden dat ook hier het criterium van de 'actieve bemoeienis met kinderporno' gebezigd wordt.[148] De actieve handeling uit zich bijvoorbeeld in de betaling voor een website waar kinderporno op te vinden is, maar ook door te klikken op een link waarvan de naam een indicatie geeft dat het om kinderporno gaat.[149] Als er niets op de harde schijf staat en er wel log- en/of betalingsgegevens beschikbaar zijn die wijzen op het bezit of verspreiden van kinderporno, dan kan iemand toch voor het toegang verschaffen tot kinderporno veroordeeld worden. De uitbreiding van artikel 240b Sr is bedoeld als een vangnet voor die gevallen die niet onder de strafbaarstelling van bezit kunnen worden gebracht.[150] Stevens en Koops twijfelen aan deze vangnetfunctie.[151] Volgens hen kan een kinderpornogebruiker, die geen spoor op de harde schijf achterlaat, ook gemakkelijk zijn zoeksporen uitwissen. Hier ben ik het mee eens. Door slim gebruik van anonimiseringstechnieken, cryptografie of alleen met 'vertrouwelingen' bestanden uit te wisselen zullen weinig sporen achter gelaten worden die wijzen op een actieve bemoeienis met kinderporno. Hier ga ik in hoofdstuk 5 verder op in. Wel zal de uitbreiding het gemakkelijker maken om mensen te kunnen veroordelen voor artikel 240b Sr.

4.2 De verspreiding en productie van kinderporno

Het verspreiden van kinderpornografisch materiaal is tevens strafbaar gesteld in artikel 240b Sr. Het bestanddeel verspreiden wordt in de rechtspraak ruim geïnterpreteerd.[152] Worden er cd-roms of andere gegevensdragers met kinderpornografisch materiaal uitgewisseld, dan is dat evident een verspreiding van kinderpornografie.[153] Er is tevens sprake van het verspreiden van kinderpornografie indien bestanden worden geüpload naar nieuwsgroepen.[154] Minder duidelijk is het verspreiden via peer-to-peer netwerken. Vaak staat de optie om bestanden te delen in 'My shared folder' ('Mijn gedeelde map') automatisch aan. De vraag is of er dan opzet op het verspreiden van kinderpornografie is.

---

[148] Stevens & Koops 2009, p. 694.
[149] *Kamerstukken II* 2008/09, nr. 3, p. 4 (MvT).
[150] *Kamerstukken II* 2008/09, nr. 3, p. 3-4 (MvT).
[151] Stevens & Koops 2009, p. 696.
[152] Koops e.a. 2007, p. 63.
[153] Zie bijvoorbeeld Rb. Utrecht 1 december 2005, *LJN* AU7307.
[154] Zie bijvoorbeeld Rb. 's-Gravenhage 3 oktober 2005, *LJN* AU3675.

4.2.1 De aanmerkelijke kans aanvaarden op het verspreiden van kinderporno

Kinderpornografisch materiaal kan toegankelijk worden gemaakt aan anderen terwijl niet beoogd wordt anderen te laten meedelen in het gebruik. Er kan dan beargumenteerd worden dat er geen sprake is van verspreiding. In een uitspraak van het hof 's-Hertogenbosch[155] stelde de verdachte dat hij niet had beoogd het materiaal te verspreiden door de bestanden aan te bieden in de 'gedeelde map' van zijn peer-to-peer programma Kazaa Lite. Het Hof besliste dat uit het feit dat de verdachte bij het installeren van het computerprogramma de optie gedeelde mappen heeft gekozen, zonder van de mogelijkheid gebruik te maken deze optie uit te zetten, kan worden afgeleid dat de verdachte voorwaardelijk opzet heeft gehad op de verspreiding van kinderpornografie.

De rechtbank 's-Gravenhage oordeelde anders en vond het enkele feit dat de mogelijkheid bestond dat kinderpornografische bestanden in de gedeelde map opgeslagen waren, niet voldoende om aan het voltooide delict van verspreiden van kinderporno te voldoen.[156] Volgens de rechtbank was daarbij vereist dat anderen ook daadwerkelijk gebruik hebben gemaakt van de mogelijkheid (waarvan de verdachte bewust was) om uit de gedeelde map van de verdachte afbeeldingen te downloaden. Indien er geen bestanden geüpload zijn wordt er niet voldaan aan het element 'verspreiden', ook al behoefde de verdachte geen enkele actie meer te ondernemen om het downloaden door derden mogelijk te maken.

Koops en de Roos zijn van mening dat de rechtbank 's-Gravenhage het hier bij het rechte eind heeft.[157] In een zaak van rechtbank 's-Hertogenbosch, van 11 februari 2008[158] wordt ook aangenomen dat het enkele gebruik van een file-sharing programma onvoldoende leidt tot (een aanmerkelijke kans op) verspreiding van kinderporno.[159] Ik sluit mij aan bij de mening van Koops en de Roos dat het enkele feit dat de mogelijkheid bestaat dat bestanden via een gedeelde map gedownload kunnen worden nog geen verspreiding oplevert. Er moeten minstens aanwijzingen

[155] Hof 's-Hertogenbosch 5 oktober 2005, *LJN* AU4032. Zie ook bijvoorbeeld Rb. Zutphen 28 april 2006, *LJN* AW5462.
[156] Rb. 's-Gravenhage 17 november 2006, *LJN* AZ5109.
[157] Koops & de Roos 2007, p. 64.
[158] Rb. 's-Hertogenbosch 11 februari 2008, *LJN* BD4501.
[159] In de zaak wordt gesproken van het file-sharing programma "Emiel". Meer waarschijnlijk bedoelt de rechtbank hier het peer-to-peer programma eMule.

of sporen gevonden worden dat de bestanden daadwerkelijk door anderen zijn gedownload.

Vervolging waarbij sprake is van het vervaardigen van kinderpornografisch materiaal kan niet alleen op grond van artikel 240b Sr vervolgd worden, maar óók op grond van artikel 245, 247 en 248ter Sr. Uit mijn jurisprudentieonderzoek blijkt dat dit vaak gebeurt.[160] Het is moeilijk in te schatten of er eerst kinderporno ontdekt wordt en dan de slachtoffers geïdentificeerd worden, of dat de kinderporno naar aanleiding van aangifte van de slachtoffers wordt ontdekt.

4.3 Prioritering in de vervolging van artikel 240b Sr

De Aanwijzing kinderpornografie geeft een richtlijn aan het OM voor het vervolgen van artikel 240b Sr. In de Aanwijzing wordt hoge prioriteit gegeven aan (pre)puberale kinderporno, kinderporno waar geweld in het spel is of sprake is van een 'evidente afhankelijkheidsrelatie' en tenslotte aan de grootschalige verspreiding en commerciële productie van postpuberale kinderporno.[161] In de opsporing is slechts beperkte capaciteit en die capaciteit moet zo goed mogelijk benut worden. Hoe verwerpelijker de aard van het materiaal, hoe hoger de prioriteit dat er binnen de opsporing aan wordt gegeven. Dit lijkt mij een wenselijke prioritering. Daarnaast wordt er tevens een hoge prioriteit gegeven aan verspreiders en vervaardigers van kinderporno. In de Richtlijn kinderpornografie van het College van procureurs-generaal gebeurt hetzelfde.[162] Over de verklaring van het onderscheid in prioritering tussen bezitters, verspreiders en vervaardigers wordt het volgende gezegd: "*In dit kader dient enkel het bezit hebben van pornografisch materiaal minder zwaar te worden aangerekend dan de (grootschalige) verspreiding of de productie van kinderpornografisch materiaal of (de zwaarste categorie binnen dit criterium) het op professionele manier verspreiden van of produceren van materiaal. Alhoewel ook het bezit van kinderporno al bijdraagt aan de instandhouding van een 'markt' voor kinderpornografisch materiaal, leveren laatstgenoemde activiteiten de relatief*

[160] Zie de bijlage voor het jurisprudentieoverzicht.
[161] Aanwijzing kinderpornografie 2007, p. 1.
[162] Richtlijn kinderpornografie, College van procureurs-generaal, *Stcrt*. 2007, 79. Het is een richtlijn voor de te eisen strafeis door de officieren van justitie bij de vervolging van kinderpornografie. Deze richtlijn vormt een aanvulling op de Aanwijzing kinderpornografie 2007 en is per 1 mei 2007 in werking getreden.

grootste bijdragen aan de instandhouding van een 'markt' voor kinderpornografisch materiaal, de seksuele exploitatie van kinderen en de voortduring van het slachtofferschap van misbruikte kinderen."[163] De Minister van Justitie heeft aangegeven zich ook te willen richten op de producenten van kinderpornografie.[164] Kortom, de prioritering van de overheid in de vervolgingen van artikel 240b Sr is tweeledig. Ten eerste wordt meer prioriteit gegeven aan extremer en nieuwer materiaal en ten tweede is het volgens de overheid wenselijker verspreiders en vervaardigers van kinderporno te vervolgen dan de eindgebruiker.
Het gegeven dat het wenselijker is om verspreiders en distributeurs te vervolgen in plaats van bezitters is niet nieuw. Een van de conclusies van het onderzoek van de Savornin Lohman en anderen in 1999 was al dat het wenselijk was om strafrechtelijk op te treden tegen de commerciële en professionele distributie en de grootschalige ruilhandel in kinderporno.[165]

In het vorige hoofdstuk is aangegeven dat de kinderpornomarkt op internet door twee groepen in stand wordt gehouden, namelijk commerciële verspreiders en door kinderpornogebruikers in besloten netwerken. Verschillende deskundigen wijzen er op dat in dit soort besloten kinderpornonetwerken extreme kinderpornografie uitgewisseld wordt en dat in deze netwerken de 'echte' pedofielen te vinden zijn.[166] Dit zijn de daders en het materiaal waarvoor in de Aanwijzing en Richtlijn een hoge prioritering wordt gegeven. Dat maakt het noodzakelijk om dit soort kinderpornonetwerken aan te pakken.
Het meest begeerlijke materiaal is nieuw materiaal. Nieuw materiaal moet geproduceerd worden en vaak worden in dat proces kinderen misbruikt en daarmee psychische en fysieke schade aangedaan. In het vorige hoofdstuk is al aangegeven dat nieuw materiaal wordt vervaardigd voor commerciële productie en geldt als ruilmiddel binnen online netwerken van kinderpornogebruikers. Daarom is het

[163] Richtlijn kinderpornografie 2007, p. 5.
[164] Brief over de voortgang aanpak kinderpornografie 2009, p. 1: *"Deze constatering noopt tot de hierna beschreven verlegging van de focus in opsporing van "bezit" naar "productie"."*
[165] Savornin Lohman e.a. 1999, p. 14.
[166] Jenkins 2001, p. 71 en ICT-specialist Roland Vergeer van Fox-IT in een interview van het televisieprogramma *Een Vandaag* (beschikbaar via: http://www.eenvandaag.nl/criminaliteit/32233/de_jacht_op_kinderporno (laatst bekeken op 16-01-2010)).

belangrijk dat het OM en de politie zich op deze groepen richten.[167] Door het oppakken van deze mensen stopt het misbruik en kunnen slachtoffers uiteindelijk hulpverlening worden geboden.

Niet alle bezitters van kinderporno zullen ook kinderpornografie uitwisselen of vervaardigen (en daarmee kinderen misbruiken). Soms wordt de kinderporno 'slechts' gedownload. Gezien het centrale doel van artikel 240b Sr, het voorkomen van kindermisbruik, zou het niet logisch zijn het opsporingsonderzoek te veel op deze groep te concentreren. Natuurlijk is het wel zo dat álle eindgebruikers bij elkaar de markt van kinderpornografie in stand houden, maar het vervolgen van één individuele bezitter levert een weinig effectieve slag aan de markt van kinderpornografie. De indirecte invloed van het vervolgen van bezitters is op de markt van kinderporno in elk geval héél marginaal.

We kunnen ter verduidelijking een vergelijking maken met de aanpak van de markt van online muziekhandel en de drugsmarkt. We zien bij de bestrijding van de illegale muziekmarkt dat er niet op de downloaders wordt geconcentreerd, maar op de websites of programma's die de uitwisseling van muziek faciliteren.[168] Dit doen ze met het idee het downloaden van muziek onmogelijk te maken en te ontmoedigen. Ook in de drugsmarkt ligt geen nadruk op het oppakken en vervolgen van drugsverslaafden, omdat een focus op hen ineffectief zou zijn.[169]

Kortom, ik ben van mening dat het wenselijker is verspreiders en vervaardigers op te pakken dan eindgebruikers. Dat er grote prioriteit ligt bij nieuw en extreem materiaal vind ik ook zeer terecht, omdat het bij dit materiaal evident is dat kinderen misbruikt worden. Met de aanpak hiervan is de kans het grootst kinderen uit hun slachtofferschap te ontzetten. Dit wil niet zeggen dat naar mijn mening verzamelaars genegeerd moeten worden. Door bij deze groep te 'doorrechercheren' kan men namelijk bij de netwerken van verspreiders of vervaardigers uitkomen.[170] Bovendien is het goed af en toe bezitters te vervolgen om zo een signaal aan de

[167] Zie ook Stol e.a. 2008, p. 115, geïnterviewde zedenrechercheurs vertellen: "*Het is effectiever om de bron te zoeken en weg te nemen, dan om je te richten op de eventuele downloaders van kinderpornografisch materiaal.*".
[168] Zie bijvoorbeeld de Pirate Bay-zaak. Rb. Amsterdam 30 juli 2009, *LJN* BJ4466. Pirate Bay werd ook in het buitenland 'uit de lucht' gehaald.
[169] Zie ook Jenkins 2001, p. 215.
[170] Zie ook Lünnemann 2006, p. 109.

maatschappij af te geven dat ook het bezit van kinderpornografie onwenselijk en strafbaar is. Wellicht gaat er een zekere generale preventie van uit.

4.4 Analyse van de vervolgingspraktijk

In deze paragraaf wordt een analyse gemaakt van de jurisprudentie van de zaken die over artikel 240b Sr gingen. Teneinde uit te zoeken welke 'marktpartij' het meest vervolgd wordt heb ik jurisprudentie onderzocht via de website rechtspraak.nl op het sleutelwoord "240b".[171] Van de zoekresultaten heb ik een overzicht gemaakt dat is bijgevoegd in de bijlage van deze scriptie. In totaal zijn 274 uitspraken in kaart gebracht en onderaan heb ik een overzicht gemaakt van het aantal uitspraken waarbij sprake was van de strafbaarheid op alléén bezit, bezit en verspreiding, bezit en vervaardiging en bezit en ontuchtelijke handelingen. Het overzicht geeft inzicht in de vraag of er vooral eindgebruikers, verspreiders of vervaardigers vervolgd worden. Na een bespreking van het overzicht zal ik een verklaring geven voor de onderzoeksresultaten.

4.4.1 Resultaten onderzoek

Op basis van mijn onderzoek kan geconstateerd worden dat het aantal zaken die op grond van artikel 240b Sr in Nederland afgehandeld worden sinds 2006 een stuk hoger liggen dan het aantal zaken in de jaren daarvoor.
Uit het overzicht blijkt verder dat in zowel 2008 als 2009 de meeste vervolgingen alléén bezit van kinderpornografie betroffen. In deze zaken ging het puur om eindgebruikers van kinderpornografie en dat was ook het enige dat in deze zaken tenlaste werd gelegd en bewezen is.
Opvallend is dat een in groot aantal zaken waar er voor artikel 240b Sr is vervolgd tevens voor het plegen van ontuchtelijke handelingen is vervolgd. Hierbij is het echter niet duidelijk of er op de computer van een pedofiel die in eerste instantie vervolgd werd van kindermisbruik kinderporno is gevonden of dat iemand in eerste instantie verdacht werd van het in bezit hebben van kinderpornografie en de opsporingsambtenaren vervolgens ontdekten dat de verdachte ook ontuchtelijke handelingen pleegde.

[171] De jurisprudentie loopt van 2000 tot en met 12 december 2009 en is opgezocht via de website http://www.rechtspraak.nl.

Het resultaat van mijn jurisprudentieonderzoek - dat de focus in de praktijk wordt gelegd op de bezitters van kinderpornografie - wordt bevestigd in andere stukken. Lünnemann en anderen zeggen hierover in hun rapport: *"Alle respondenten wijzen erop dat meestal eindgebruikers worden vervolgd en dit blijkt eveneens uit het dossieronderzoek."*[172] Dit blijkt ook uit het rapport van het Verbeterprogramma[173], de Korpsmonitor[174] en andere bronnen, zoals de website van het Ministerie van Justitie.[175] Sterker nog, volgens Lünnemann en anderen had het Openbaar Ministerie haar focus in de jaren tussen 1999 en 2006 verschoven van verspreiders en vervaardigers naar eindgebruikers (bezitters) van kinderporno.[176]

De reden dat de focus vooral op de eindgebruikers van kinderpornografie ligt komt naar mijn mening door de opsporingspraktijk in Nederland en capaciteitsredenen in combinatie met de politieke druk om zoveel mogelijk zaken af te handelen.

4.4.2 Opsporingspraktijk

Politiemensen beschikken over een aanzienlijke autonomie om hun werkzaamheden te kunnen beheersen. Door hun ruime werkaanbod is een selectie noodzakelijk: welke onderzoeken 'gedraaid' kunnen worden en welke blijven (voorlopig) 'op de plank liggen'? De selectie, maar ook de aanpak van een bepaald probleem, hangt grotendeels af van de manier waarop de situatie door de politie wordt geïnterpreteerd en beoordeeld. De sturing van de politie door het OM gaat vaak anders dan op grond van alleen voorschriften, bevoegdheden en procedures kan worden verwacht.[177] De politie heeft over het algemeen een belangrijke rol in de keuze van te starten onderzoeken en de manier waarop de onderzoeken worden uitgevoerd. Dit is ook noodzakelijk om het grote aantal zaken aan te kunnen. Echter,

---

[172] Lünnemann e.a. 2006, p. 108.
[173] Verbeterprogramma kinderporno 2009, p. 14.
[174] Korpsmonitor 2009, p. 20.
[175] http://www.justitie.nl/onderwerpen/criminaliteit/cybercrime/kinderporno/aanpak-door-politie/index.aspx *"Momenteel ligt de focus bij de opsporing van kinderporno vooral bij de eindgebruikers (de downloaders of bezitters) van kinderporno."* (Laatst geraadpleegd op 15 oktober 2009).
[176] Lünnemann e.a. 2006, p. 123 refereert naar het onderzoek van de Savornin Lohman e.a. 1999: *"De conclusie van het vorige evaluatieonderzoek dat bij meer dan de helft van de verdachten sprake was van commerciële en professionele productie, distributie en grootschalige ruilhandel, kunnen we op basis van dit onderzoek zeker niet meer trekken."*
[177] Krommendijk, Terpstra & van Kempen 2009, p. 138 onder verwijzing naar M.S. de Vries, *Improving police performance*, Enschede : IPIT 2001.

aan de informatieverstrekking aan het OM gaat een proces van selectie en interpretatie van gegevens door de politie vooraf. Het OM kan hierdoor slechts beperkt invloed uitoefenen op de selectie van zaken en de wijze waarop zaken worden aangepakt.[178] Uit de praktijk kunnen we afleiden dat vaker de technisch minder onderlegde kinderpornogebruikers vervolgd worden en dat de kinderpornogebruikers die handig gebruik maken van de techniek grotendeels buiten het beeld van de opsporingsdiensten blijven. Kinderpornogebruikers maken steeds vaker slim gebruik van nieuwe technische mogelijkheden en daarom is er een tendens zichtbaar dat de kinderpornohandel verschuift naar locaties op internet waar de informatie moeilijker te observeren is.[179] Stol zegt hierover: *"'Gewone' wetsovertreders weten zich minder goed te verbergen dan internetspecialisten en dat speelt de opsporing in de kaart."*[180] Het gevolg is dat de opsporing en vervolging op dit moment zich vooral richt op de mensen die geen gebruik maken van de technische mogelijkheden die beschikbaar zijn. Het onderzoek van Lünnemann en anderen toont aan dat het grootste deel van de mensen die vervolgd worden voor kinderpornografie geen ICT-specialisten zijn.[181] Zij zegt dat de meeste verdachten 'de kleine jongens' zijn.[182] Een zedenrechercheur noemt deze groep mensen 'sukkels'.[183] De bevindingen van Lünnemann en anderen zijn blijkbaar nog steeds actueel, want ook de Korpsmonitor spreekt van een focus op de 'eenvoudige' downloader.[184] Indien er vaker zaken met 'simpele gebruikers' worden aangedragen worden er logischerwijs ook meer bezitters dan verspreiders en vervaardigers vervolgd.

Tevens werd er vooral reactief opgespoord. In 2006 bleek uit meer dan de helft van de door Lünnemann en anderen geanalyseerde dossiers dat de opsporingsonderzoeken waren gestart naar aanleiding van meldingen van burgers.

---

[178] Krommendijk, Terpstra & van kempen 2009, p. 138.
[179] Stol 2004, p. 88.
[180] Stol 2004, p. 78
[181] Stol 2004, p. 78
[182] Lünnemann e.a. 2006, p. 108.
[183] 'Een eeuwige strijd, Kinderporno neemt snel toe', *Blauw* – Recherche, 3 februari 2007, nummer 3, p. 20: *Het zijn dan ook vooral de 'sukkels' die Marcel Nek naar eigen zeggen tegenkomt in zijn werk.* (…) *'De echte slimmerds zijn heel moeilijk te achterhalen.'"*
[184] Korpsmonitor 2009, p. 20: *"Door capaciteitsgebrek is de focus van de politie noodgedwongen gericht op de aanpak van de "eenvoudige" downloader (vaststellen van bezit) en minder gericht op het traceren van slachtoffers en misbruikers."*

Het ging bijvoorbeeld om computerreparateurs die kinderporno op een harde schijf aantroffen.[185] Tevens waren meldingen van het Meldpunt Kinderporno op internet soms startpunt van een zaak. Soms werd zelfs in een geheel andere zaak, bijvoorbeeld drugssmokkel of een moordzaak, kinderporno op een computer aangetroffen, waarna het opsporingsonderzoek aanving. Slechts in een kwart van de zaken komt de verdachte in beeld na gericht onderzoek van de politie zelf.[186] Het betrof bijvoorbeeld een opsporingsonderzoek van de politie betreffende infiltratie van rechercheur in een besloten netwerk van kinderpornogebruikers op een besloten BBS. Indien er niet verder wordt 'doorgerechercheerd' naar de bron van de kinderpornografie, kan men alleen het bezit van kinderpornografie vaststellen. De reden dat er weinig zaken door de politie zelf worden aangevangen is volgens veel wetenschappers de geringe kennis bij de politie over de bestrijding van cybercrime.[187] De overheid spant zich gelukkig in om haar achterstand op het gebied van computercriminaliteit in te halen. Onderdeel daarvan is het Programma Aanpak Cybercrime van de politie en Intensiveringprogramma Cybercrime van het OM. Tevens houdt het Nationaal Forensisch Instituut (hierna: NFI) zich bezig met ontwikkelingen in de opsporing in verband met datacommunicatie en cryptografie.

Vanwege specialistische kennis dat opsporing op internet vergt en het bovenlokale karakter van het internet worden grotere zaken, zoals bijvoorbeeld acties tegen kinderpornonetwerken, al snel op landelijk niveau aangepakt.[188] Voor deze landelijke aanpak is het KLPD-team Bestrijding Kinderpornografie gecreëerd. Gelukkig neemt Nederland ook regelmatig deel aan internationale acties tegen kinderpornografie.[189] Naar mijn mening moeten dit soort internationale onderzoeken naar verspreiders en vervaardigers van kinderpornografie geïntensiveerd worden. Daarvoor is een andere opsporingspraktijk noodzakelijk, waarbij het KLPD-team

[185] Lünnemann e.a. 2006, p. 121.
[186] Lünnemann e.a. 2006, p. 122.
[187] Zie bijvoorbeeld Stol e.a. 2008, *Ars Aequi*, p. 538.
[188] Stol e.a. 2008, *Ars Aequi*, p. 538.
[189] Zie bijvoorbeeld Volkskrant 10 december 2009, 'Europol pakt 115 pedoseksuelen op': *"De Europese politiedienst Europol heeft tijdens een groot onderzoek naar de online verspreiding van kinderporno 115 pedoseksuelen opgepakt. 'Operatie Tyfoon' duurde twee jaar en bestond uit huiszoekingen in negentien Europese landen, waaronder Nederland, België en Luxemburg"*
http://www.volkskrant.nl/buitenland/article1326175.ece/Europol_pakt_115_pedoseksuelen_op (laatst bekeken op 24 januari 2010).

Bestrijding Kinderpornografie een grotere rol zou moeten spelen. In de loop der jaren is kinderpornografie uitgegroeid tot een ernstig misdrijf met een internationale dimensie, waarbij soms de georganiseerde misdaad in het spel is. Vanwege de vaak (technisch) complexe zaken en internationale dimensie van het probleem zou naar mijn mening kinderpornografie ondergebracht moeten worden bij het takenpakket van het Landelijk Parket van het Openbaar Ministerie. Er kunnen dan meer landelijke opsporingsonderzoeken naar commerciële verspreiders en besloten kinderpornonetwerken gestart worden.

4.4.3 Capaciteit

Op de politie en het OM ligt een grote (politieke) druk om zoveel mogelijk zaken af te handelen. Het vervolgen van bezitters vergt veel minder capaciteit dan het vervolgen van verspreiders en vervaardigers van kinderpornografie. In het Verbeterprogramma van de politie wordt aangegeven dat de kosten van het opsporingsonderzoek bij verzamelaars maar beperkt zijn. De harde schijf moet slechts in beslag worden genomen en er moeten voldoende sporen op worden gevonden om te bewijzen dat er sprake was van 'een actieve bemoeienis met kinderporno' (zie paragraaf 4.1). Bewijzen dat er sprake is van de verspreiding en vervaardiging van kinderporno is veel kostbaarder (zowel in tijd als geld), want het vereist enige mate van doorrechercheren en digitaal onderzoek is daarbij noodzakelijk.[190] Het is dus veel gemakkelijker bezitters te vervolgen dan verspreiders en vervaardigers van kinderpornografie. Het is met de huidige capaciteit niet mogelijk zowel veel zaken te draaien als een focusverschuiving van bezitters naar verspreiders en vervaardigers te bewerkstelligen. Het is niet zozeer een bewuste keuze van de politie en het OM dat de nadruk ligt op bezitter. Bovendien moet er nog een flinke werkvoorraad afgehandeld worden. In 2007 waren er 270 "plankzaken" en september 2009 is de werkvoorraad gestegen tot 879 zaken.[191] Hiervan waren ongeveer de helft rechtsverzoeken uit het buitenland. De Minister van Justitie heeft in september 2009 besloten tijdelijk de recherchecapaciteit uit te breiden op bovenregionaal niveau, specifiek voor de

[190] Verbeterprogramma kinderporno 2009, p. 16: *"Let wel: de vereiste capaciteit is afhankelijk van de gekozen focus. Wordt de nadruk verlegt van downloaders naar slachtoffers, misbruikers, betrokken dienstverleners, producenten en commerciële verspreiders dan kost dat meer tijd."*
[191] *Kamerstukken II* 2009/10, 32 123 VI, nr. 79, p. 4.

aanpak van kinderpornografie. Hierbij heeft de hoogste prioriteit het terugdringen van de werkvoorraad en niet het verleggen van de focus van de bezitter naar de verspreider en vervaardiger van kinderporno.[192] Gezien de ontwikkelingen op ICT-gebied ligt het niet in de lijn der verwachting dat het probleem van kinderpornografie op internet minder zal worden. Een *tijdelijke* capaciteitsuitbreiding is daarom niet logisch. Om naast het terugdringen van de werkvoorraad ook een focusverschuiving te bewerkstelligen moet de capaciteit op bovenregionaal niveau verder permanent uitgebreid worden.

In paragraaf 4.3 is uitgebreid uiteengezet waarom de focus bij de bestrijding van kinderpornografie moet liggen bij de verspreider en vervaardiger. Het vervolgen van zoveel mogelijk (amateuristische) verzamelaars levert geen effectieve slag op de markt van kinderpornografie. Indien kinderporno niet bij de bron wordt aangepakt lossen we het probleem niet op en blijft de hoeveelheid kinderpornografie op internet groeien. De huidige praktijk met de nadruk op het vervolgen van 'simpele' bezitters kan daarom getypeerd worden als 'dweilen met de kraan open'. Een andere werkwijze vergt meer kennis over cybercrime bij de politie en het OM en meer capaciteit teneinde verspreiders en vervaardigers op te sporen en te vervolgen. Tevens zullen er zaken geseponeerd moeten worden die volgens de Aanwijzing en Richtlijn kinderpornografie minder prioriteit krijgen. Dit is een noodzakelijk kwaad om kinderpornografie beter te bestrijden. Het onderbrengen van kinderpornografie bij het Landelijk Parket en nog meer internationale zaken oppakken is nog een stap verder in de goede richting.

Tussenconclusie

Het criterium dat gebezigd wordt bij de strafbaarheid van kinderporno is de 'actieve bemoeienis van de gebruiker met kinderpornografie'. Realtime kinderporno kijken wordt door de implementatie van het Verdrag van Lanzarote in artikel 240b Sr strafbaar gesteld met de toevoeging van 'het toegang verschaffen tot kinderpornografie'. Of de beoogde vangnetfunctie van deze wetswijziging behaald wordt is echter de vraag.

[192] *Kamerstukken II* 2009/10, 32 123 VI, nr. 79, p. 3.

Met betrekking tot de verspreiding van kinderporno is het nog niet duidelijk of het enkele bestaan van bestanden met kinderpornografie in een gedeelde map op de harde schijf het voltooide delict ‘verspreiding van kinderpornografie’ oplevert.
Niet verwonderlijk is dat er bij de productie van kinderpornografie vaak wordt vervolgd op grond van artikelen die misbruik van kinderen strafbaar stellen.

Op dit moment ligt de nadruk bij vervolgingen op grond van artikel 240b Sr bij de bezitters van kinderpornografie. Bovendien worden er veel technisch minder onderlegde verzamelaars vervolgd. Dat is niet in lijn met de Aanwijzing en Richtlijn kinderpornografie en het is onwenselijk, omdat het weinig effect heeft op de markt van kinderpornografie. De huidige praktijk kan daarom bestempeld worden als ‘dweilen met de kraan open’ en is aan aanpassing toe. Om de focusverlegging van de bezitter naar de verspreider en vervaardiger van kinderpornografie te bewerkstelligen is echter wel een versterking van capaciteit en meer kennis van cybercrime bij de politie en het OM noodzakelijk. Het onderbrengen van kinderpornografie bij het Landelijk Parket en het oppakken van meer internationale zaken zou wenselijk zijn.

In het volgende hoofdstuk wordt ingegaan op problemen met betrekking tot de opsporing van kinderpornografie op internet.

Hoofdstuk 5: Problemen met betrekking tot de opsporing van kinderpornografie op internet

"On the internet, nobody knows you're a dog." – Peter Steiner

De laatste jaren zijn kinderpornogebruikers meer ondergronds gegaan en wordt er meer gebruik gemaakt van technieken om buiten het beeld van opsporingsdiensten te blijven. Dit werd stevig duidelijk gemaakt aan mensen in Nederland door een artikel uit de Nieuwe Revu[193] en een uitzending van Nova[194]. Naar aanleiding van het artikel uit de Nieuwe Revu heeft het NFI in 2006 een groot onderzoek gedaan naar kinderpornografie op internet.[195] Helaas is het rapport niet voor de wetenschap toegankelijk, aangezien de Minister van Justitie besloten heeft het rapport alleen aan de Kamer vrij te geven uit angst dat kinderpornogebruikers die nog geen gebruik maken van de technieken na het lezen van het rapport dit wel zouden doen.[196]
Sommige verzamelaars nemen deel aan besloten netwerken en schermen zich af door gebruik technieken om opsporingsinstanties buiten de deur te houden. Dat meldingen van kinderporno bij het Meldpunt Kinderporno vooral over commerciële websites gaan is dan ook een signaal dat het aardig lukt om buiten het beeld van opsporingsinstanties te blijven.[197]

Het is belangrijk uit te leggen hoe kinderporno buiten het beeld van opsporingsinstanties verspreid kan worden. Het laat namelijk zien dat er een soort ondergrondse handel in kinderporno op internet kan floreren dat lastig is op te sporen en te bestrijden. Zonder dit inzicht in de ondergrondse handel van

[193] H. Lensing, 'Ziek & Slim, pedo's ontraceerbaar op het internet', *Nieuwe Revu* 52, 2004, p. 33-34 en J. van Kleef, 'Kinderporno, kinderspel', *Nieuwe Revu*, 52, 2004, p. 28-32.
[194] *De hopeloze strijd tegen* kinderporno, 15 december 2004, Rudy Bouma, Marcel Hammink, Silvia Pilger, http://www.novatv.nl/page/detail/uitzendingen/3105# (laatst gezien op 20 oktober 2009).
[195] Oosterink en Van Eijk 2006, *Opsporing Kinderpornografie op internet, Een statusoverzicht*, 's-Gravenhage: Ministerie van Justitie.
[196] Brief aan de Tweede Kamer over het NFI onderzoek Opsporing Kinderpornografie op internet, 21 maart 2006, kenmerk: DDS 5399943/506, p. 2.
[197] Stol e.a. 2008, *Ars Aequi*, p. 537.

kinderporno kan er geen goed antwoord worden gegeven op de hoofdvraag hoe kinderpornografie het beste kan worden aangepakt.

Gesteld kan worden dat er drie factoren bijdragen aan het ongrijpbaar maken van de daders van artikel 240b Sr. Dit zijn: anonimiteit, encryptie en het grensoverschrijdende karakter van het internet.[198] Deze drie factoren worden in dit hoofdstuk uitvoerig behandeld.

5.1 Anonimiteit

Op internet worden allerlei anonimiseringstechnieken gebruikt. Aan het gebruik van deze technieken ligt niet altijd een criminele motivatie ten grondslag. Voor de beroepsuitoefening van journalisten kan het bijvoorbeeld gewenst zijn om anoniem te blijven. Sommige mensen gebruiken de techniek om hun privacy te beschermen en niet altijd omdat ze iets te verbergen te hebben.

Er zijn in principe twee dingen die een computer binnen een netwerk identificeren: het MAC-adres[199] en het IP-adres. Beiden kunnen veranderd worden. Zodra een netwerkpakketje over een *gateway* van een netwerk wordt verzonden, verandert het MAC-adres van de computer in het MAC-adres van de gateway. Het IP-adres blijft dan alleen nog als herkenningspunt van een computer in een bepaald netwerk. Het IP-adres speelt om deze reden de belangrijkste rol bij anonimiseringstechnieken en daarom wordt verder toegelicht hoe het IP-adres afgeschermd of veranderd kan worden.

5.1.1 Afschermen van het IP-adres

Een belangrijke manier om een IP-adres te verbergen is om alle paginaverzoeken door een proxy te sturen. Een proxy is een server via welke al het verkeer van een gebruiker over internet wordt gestuurd. Proxies worden door ISP's ingezet om pagina's die gebruikers opvragen, sneller te kunnen tonen. Als een gebruiker een webpagina opvraagt, wordt eerst op de proxy gekeken of de pagina daar misschien al aanwezig is omdat een andere gebruiker hem recentelijk heeft opgevraagd.[200]

[198] Zie ook Franken 2004, p. 406.
[199] MAC staat voor Media Access Layer.
[200] Eshof e.a. 2002, p. 27.

Computergebruikers kunnen tevens gebruik maken van proxies, waarbij al het internetverkeer langs een bepaalde server loopt. Webservers waarbij toegang wordt verschaft door middel van een proxy registreren het IP-adres van de proxy en niet dat van iemands computer. Hierdoor kan de internetgebruiker niet meer aan de hand van zijn IP-adres geïdentificeerd worden. Commerciële webproxies zoals *Anonymizer* zijn vrij verkrijgbaar.[201]
Openbare bibliotheken en internetcafés zijn ook populaire methodes om anoniem op internet te surfen.[202] Het is natuurlijk alleen anoniem indien de gebruikers van de computers in een internetcafé niet op de één of andere manier geregistreerd worden. Met betrekking tot kinderporno is het mijns inziens onvoorstelbaar dat dit materiaal bekeken wordt in een openbare bibliotheek of internetcafé. De verspreiding van kinderporno kan eventueel plaatsvinden als de bestanden een onschuldige naam hebben.

Via een onbeveiligd Wifi-netwerk kan kinderporno ook anoniem verspreid en bekeken worden.[203] Het IP-adres van het netwerk waar gebruik van wordt gemaakt, wordt dan geregistreerd.

Tenslotte is het mogelijk dat een gebruiker zijn IP-adres afschermt door 'IP-spoofing' toe te passen. Bij IP-spoofing wordt het IP-adres vervalst. Om dit mogelijk te maken is er veel ICT-kennis van de computergebruiker voor nodig. Het gevolg van
IP-spoofing is dat een vals IP-adres wordt achtergelaten dat ongeveer hetzelfde resultaat oplevert als bij het gebruik van proxyservers.[204]

5.1.2 Nicknames

De echte naam van mensen wordt op internet vaak verborgen gehouden. Het is namelijk op internet gebruikelijk dat men een 'nickname' aanneemt. Een nickname is een pseudoniem waaronder men op internet met anderen communiceert. De

[201] http://www.anonymizer.com/
[202] Casey 2004, p. 495.
[203] Zie bijvoorbeeld http://www.nu.nl/internet/1047915/amerikaan-gepakt-met-kinderporno-door-lek-wifi.html (laatst geraadpleegd op 20 oktober 2009).
[204] Eshof e.a. 2002, p. 28.

echte naam van iemand is niet bekend en dat bevordert de anonimiteit van mensen op internet.

5.1.3 Anoniem chatten

Nicknames op chatnetwerken vergroten de anonimiteit, maar proxies kunnen ook ingezet worden in IRC of ICQ (met bijvoorbeeld Wingate of een SOCKS-proxy) dat de anonimiteit van de gebruikers vergroot.[205] Veel IRC netwerken laten geen connecties toe van computers die een proxyserver gebruiken, maar met programma's als *mIRC* is dat wel mogelijk. Dit programma is zeer populair en is alleen al in 2008 150 miljoen keer gedownload.[206]

5.1.4 Freemail en remailers

E-mail lijkt veel op normale post. Er zijn computers op internet die als een postkantoor fungeren en die worden 'Message Transfer Agents' (MTA) genoemd. Wanneer een e-mail wordt verzonden dan gaat het eerst langs een locale MTA. Net zoals postzegels op een envelop geplakt worden, voegt de MTA de tijd en de naam van de MTA samen met wat technische informatie op de bovenkant van het e-mailbericht. Dit equivalent van de postzegel noemt men een '*received header'*. Het bericht wordt dan naar andere MTA's doorgestuurd totdat het zijn bestemming bereikt. Elke MTA die het bericht ontvangt, plaatst een received header bovenaan het bericht. Dit betekent dat de laatste computer die het bericht doorstuurt, bovenaan de 'header' zit en de eerste computer zit helemaal onderaan. De herkomst van de e-mail kan dus worden teruggevonden (dit wordt ook wel '*tracking*' genoemd) door de recieved headers van een e-mail af te lezen.[207]
E-mail kan anoniem verzonden worden door middel van een proxyserver. De 'received headers' krijgen dan het IP-adres van de proxy mee en niet van de computer van de gebruiker. Hierdoor is het lastiger te achterhalen waar de e-mail vandaan komt.

[205] SOCKS is een afkorting voor SOCKetS.
[206] http://www.mirc.com/news.html (laatst geraadpleegd op 20 oktober 2009).
[207] Casey 2004, p. 503.

Op internet zijn vele 'freemail' ('free e-mail') providers aanwezig. De bekendste zijn Hotmail en Gmail, maar er zijn nog vele anderen.[208] Een gebruiker registreert bij de provider een willekeurig e-mailadres en daarvoor moeten gegevens worden ingevuld. Het is echter gemakkelijk onjuiste gegevens in te vullen. Het is daarom niet met zekerheid te zeggen dat met de gegevens van de gebruiker van de e-mailservice de ware identiteit achterhaald kan worden. Als het IP-adres van de gebruiker bij registratie wordt vastgelegd kan dit uitkomst bieden.
Een *anonymous remailer* is een (vaak gratis) e-mailservice, dat gebruikt wordt als 'tussenstation' tussen de verzender en de geadresseerde. In plaats van e-mail rechtstreeks naar de geadresseerde te sturen, stuurt de gebruiker zijn e-mail naar de remailer.[209] De identificeerbare informatie wordt dan in de header verwijderd voordat het bericht opnieuw verzonden wordt. De meest effectieve anonieme remailers (zoals *Mixmaster* en *Cyberphunk*) zijn complex en bij gebruik van deze programma's is het zeer moeilijk te achterhalen van wie het bericht afkomstig is.[210] Perfecte anonieme remailers maken het voor de verzender niet mogelijk om een antwoord te ontvangen op de berichten, zodat het niet mogelijk is om de berichten terug te verbinden met het individu die de berichten heeft gestuurd. Daarom zijn 100% anonieme services alleen handig voor mensen die geen tweezijdig verkeer willen gebruiken. Door de aard van hun dienst is de informatie die over de gebruikers door remailers wordt opgeslagen minimaal en zal een vordering tot verstrekking van gegevens weinig resultaat bieden.[211] Bovendien vinden veel providers van anonieme proxyservers of remailers zich in het buitenland. Om inzage te krijgen in de gegevens zal de vordering gepaard moeten gaan met een verzoek tot rechtshulp.[212]

5.1.5 Betalingsmiddelen op internet

Om te betalen voor producten of diensten op internet wordt tegenwoordig in plaats van een creditcard steeds vaker 'digitaal geld' gebruikt. Bij deze betalingsdiensten

[208] Zie ook Eshof e.a. 2002, p. 23.
[209] Eshof e.a. 2002, p. 25.
[210] Casey 2004, p. 499.
[211] Zie paragraaf 6.2.5.1 over het vorderen van gegevens.
[212] Eshof e.a. 2002, p. 29.

(als WebMoney[213]) kan gebruik worden gemaakt van een prepaidkaart waarmee betaald kan worden of een directe transactie op een beveiligde manier worden gedaan. Paypal[214] is een andere bekende online betaaldienst. In Nederland is de betalingsdienst iDeal erg populair. Aangezien het hoofdkantoor (of servers) van deze diensten zich niet altijd in Nederland bevinden wordt door het gebruik van deze betaalmiddelen de opsporing van de transacties bemoeilijkt, aangezien er voor de vordering van betalingsgegevens altijd een rechtshulpverzoek moet worden gedaan (zie paragraaf 3 en hoofdstuk 6.2.2.5.1).

5.2 Cryptografie en steganografie

Kinderpornogebruikers maken in toenemende mate gebruik van cryptografie en steganografie om hun bestanden beter te beschermen.[215] Cryptografie kan ook gebruikt worden voor legitieme doeleinden zoals de beveiliging van telecommunicatie, persoonsgegevens, elektronische betaalsystemen, intellectuele eigendomsrechten, gevoelige overheids- en bedrijfsinformatie en mensenrechten.[216]

Cryptografie (ook wel 'encryptie' genoemd) betreft het zodanig versleutelen van een boodschap dat zij onleesbaar wordt. Slechts degenen die de sleutel kennen, die benodigd is voor het ontsleutelen van de boodschap, kunnen deze weer lezen.[217] Bij versleuteling wordt leesbaar digitaal materiaal ('plaintext') omgevormd in onleesbaar materiaal ('ciphertext') door middel van een wiskundig algoritme. Plaatjes of video's met een kinderpornografische inhoud kunnen met deze techniek onherkenbaar worden gemaakt en over het internet worden verstuurd. Eén van de meest bekende (gratis) versleutelprogramma's is *Pretty Good Privacy* (PGP), waarvan op grote schaal gebruik wordt gemaakt.[218] Leden van de 'Orchid club' maakten bijvoorbeeld gebruik van cryptografie en wisselden snel van IRC servers. Op deze manier probeerden zij wetshandhavers te slim af te zijn. Deze methodes hinderden het onderzoek naar de Orchid Club aanzienlijk. In één geval werd de computer van een verdachte van het Verenigd Koninkrijk naar de Verenigde Staten

[213] http://www.wmtransfer.com/ (laatst geraadpleegd op 26 januari 2010).
[214] http://www.paypal.nl/ (laatst bekeken op 26 januari 2010).
[215] Ferraro & Casey 2005, p. 574.
[216] Koops 2002, p. 9.
[217] Eshof e.a. 2002, p. 65.
[218] Casey 2004, p. 208.

verzonden om de bestanden op de harde schijf te ontcijferen. Dit bleek echter onmogelijk.[219]

Net zoals cryptografie, wordt er bij steganografie informatie beveiligd door de manipulatie van gegevens. Steganografie verschilt van cryptografie omdat het geen toegang weigert tot bepaalde bestanden door 'ciphertext', maar de data wordt 'verstopt'.[220]
Steganografie gaat standaard als volgt in werking. Een willekeurige boodschap wordt gekozen, het zogeheten *cover object*. Met behulp van de *stego-key* wordt de geheime boodschap in de onschuldige boodschap verborgen, wat een zogenaamd *stego-object* creëert. In een perfect systeem is dit stego-object onscheidbaar van een onschuldig object. Na ontvangst van het stego-object gebruikt de ontvangende partij de stego-key die hij heeft verkregen, om de geheime boodschap te ontsluiten. Kennis van het originele, onschuldige object is daarbij meestal niet nodig.[221]

Kinderpornografie op internet kan door ISP's er uit worden gefilterd (zie paragraaf 7.1.1) en daarom kan het voor de verzender van deze bestanden waardevol zijn om zijn bestanden te camoufleren als onschuldig materiaal, zodat het niet voor diepere bestudering geselecteerd wordt. Het is onduidelijk in hoeverre deze techniek door kinderpornogebruikers ingezet wordt.

5.3 Tor-servers

Tor is een systeem dat de privacy van internetgebruikers verhoogt door het internetverkeer via het TCP/IP-protocol te anonimiseren. Tor creëert een anonieme laag door de pakketjes een route te laten nemen door een netwerk van Tor-servers of routers met het gebruik van gelaagde cryptografie dat 'onion-routing' wordt genoemd. Het systeem is ontwikkeld om die mensen toegang te geven tot een vrij en ongecensureerd internet daar waar dat niet gegarandeerd is.[222]

[219] Casey 2004, p. 498.
[220] Britz 2009, p. 337.
[221] Eshof e.a. 2002, p. 75.
[222] McCoy e.a. 2007, p. 3.

Standaard wordt het internetverkeer over drie routers geleid. Het verkeer komt binnen bij de 'entrance Tor-router', gaat dan naar de middelste router, de 'mix Tor-router' genoemd, en gaat als laatste door de 'exit Tor-router'. Alleen de entrance Tor-router weet waar het originele verzoek vandaan komt en alleen de exit Tor-router weet de inhoud en eindbestemming van het verzoek.[223] Het inkomende en uitgaande verkeer kan niet met elkaar in relatie worden gebracht, waardoor men er niet achter kan komen welke ingaande internetstromen corresponderen met de geobserveerde uitgaande stroom van het netwerk.[224] Tor kan ook geïnstalleerd worden als 'plug-in' bij een webbrowser zodat er anoniem gesurft kan worden op internet.

De belangrijkste reden dat maar weinig mensen Tor gebruiker is dat mensen het systeem traag vinden. Dit komt doordat alle pakketjes door de drie Tor-routers moeten gaan. Sommige routers raken verstopt omdat hun beperkte bandbreedte al het verkeer van verschillende internetcircuits tegelijk moet afhandelen.[225]
Op grond van het bovenstaande ligt het voor de hand dat op Tornetwerken kinderporno uitgewisseld wordt. Hier zijn geen cijfers over bekend.

5.4 Darknets

Het begrip 'darknet' dook voor het eerst op in 2002 naar aanleiding van een artikel van werknemers van Microsoft.[226] Een darknet lijkt op een peer-to-peer netwerk, maar wordt ook wel een *'friend-to-friend network'* (F2F) genoemd. De reden daarvoor is dat het alleen gebruikt wordt tussen mensen die elkaar vertrouwen. Het darknet is een collectie van netwerken en technologieën die gebruikt worden om bestanden uit te wisselen.[227] Het is te vergelijken met een Instant Messenger waarbij niet alleen kan worden gepraat, maar ook de mogelijkheid bestaat met hoge snelheid bestanden uit te wisselen met vrienden.

[223] McCoy e.a. 2007, p. 3.
[224] Murdoch & Danezis 2005, p. 1.
[225] McCoy e.a. 2007, p. 5.
[226] P. Biddle, P. England, M. Peinado, B. Willman, 'The Darknet and the Future of Content Distribution', Microsoft, 2002.
[227] Biddle ea. 2002, p. 1.

Het zwaktebod van darknets is, dat maar een gering aantal 'vrienden' tegelijk online zijn om de bestanden mee te delen. Dat maakt het systeem langzamer en minder aantrekkelijk dan 'normale' peer-to-peer programma's.

5.4.1 Turtle hopping

Een project van de Vrije Universiteit heeft een oplossing voor het probleem dat slechts zeer gering aantal mensen tegelijk online is. Door middel van '*turtle hopping*' kan men in feite ook verbinden met vrienden van vrienden en ook bestanden met hen (op een versleutelde manier) uitwisselen.[228] Het bereik van het friend-to-friend netwerk wordt door deze techniek enorm vergroot en maakt darknets aantrekkelijker voor gebruik. Het uitwisselen van grote bestanden blijft, ondanks het gebruik van Turtle, minder snel dan bij peer-to-peer programma's als Kazaa en Gnutella.[229]

5.4.2 Freenet

Freenet is bedacht door Ian Clarke.[230] Zijn doelstelling was het ontwikkelen van een systeem waarmee anoniem informatie uitgewisseld kon worden. Freenet is gratis software welke mensen in staat stelt anoniem bestanden te delen en sites te bezoeken die alleen via Freenet beschikbaar zijn (die worden 'freesites' genoemd). Elke computer waar Freenet op wordt geïnstalleerd, wordt onderdeel van het netwerk waar bestanden opgeslagen en gedownload kunnen worden. Het Freenet programma gebruikt namelijk een deel van de capaciteit van de computer en dit deel wordt versleuteld. De gebruiker van Freenet kan het versleutelde deel niet zelf bekijken en weet ook niet wat voor materiaal op dat deel van de schijf staat. Freenet is gedecentraliseerd om het minder kwetsbaar voor aanvallen te maken en in de darknet-modus worden gebruikers alleen verbonden met hun vrienden, wat het lastig maakt ze op te sporen. De bestanden worden bovendien veelvuldig verschoven van de ene computer naar de andere. Dit maakt het moeilijk om na te gaan waar de informatie werkelijk vandaan komt. [231] Deze eigenschappen maakt het dat Freenet heel aantrekkelijk is voor kinderpornogebruikers en men denkt dan

[228] Popescu, Crispo & Tanenbaum 2004, p. 2.
[229] Popescu, Crispo & Tanenbaum 2004, p. 4.
[230] Eshof e.a. 2002, p. 41.
[231] Casey 2004, p. 502.

ook dat Freenet gebruikt wordt voor het verspreiden van kinderpornografisch materiaal.[232]

5.5 Brightnet

Een 'brightnet' is het tegenovergestelde van een darknet. In een darknet controleert de gebruiker met wie data gedeeld wordt en is het bekend wat er gedeeld wordt. In een brightnet maakt het niet uit met wie de data gedeeld wordt, maar de data zelf is geheim.[233] Met een programma als *OFFSystem* wordt de gedeelde data door elkaar gehusseld en versleuteld in blokken die gedownload kunnen worden van elk 128 kilobyte groot. Als alle data verkregen is, wordt een URL naar een website gecreëerd waarmee de data weer in elkaar gezet kan worden tot de originele vorm. Een individueel blok is niets anders dan 'digitaal lawaai'. Het is niet duidelijk wat voor content in de blokken data staat en daarom kan volgens de makers van het programma niemand aanspraak maken op bijvoorbeeld de auteursrechten van de data.[234] Het is onduidelijk in hoeverre kinderpornogebruikers gebruik maken van brightnets.

Het is belangrijk te onderstrepen dat niet alle mensen die van dit soort technieken gebruik maken kinderpornogebruikers zijn. De bescherming van de eigen privacy en het recht op de vrijheid van meningsuiting kunnen belangrijke (en legitieme) redenen zijn van deze technieken gebruik te maken. Zo is het bekend dat journalisten soms gebruik maken van proxies of Tor-servers. Met deze technieken kunnen websites anoniem bezocht worden en kan men veilig met bronnen communiceren. Het kan ook voor opsporingsambtenaren nuttig zijn van bepaalde technieken (zoals Tor) gebruik te maken zodat zij niet 'herkend' worden aan de hand van hun IP-adres door kwaadwillenden.

5.6 De internationale dimensie van kinderpornografie op internet

Kinderpornografie is een grensoverschrijdend probleem. Dit werpt vragen op met betrekking tot de strafbaarheid van kinderpornografie in het buitenland en of de opsporingsbevoegdheden uit het Wetboek van Strafvordering ook in het buitenland

[232] Alisdair 2008, p. 6.
[233] M. Seeger, *The current state of anonymous file-sharing*, Hochschule der Medien Stuttgart, 2008, p. 31.
[234] http://en.wikipedia.org/wiki/Brightnet

ingezet mogen worden. In deze paragraaf wordt antwoord op die vragen gegeven en wordt nagegaan of internationale samenwerking een bijdrage aan de oplossing van het probleem kan geven.

5.6.1 Jurisdictieproblemen

Het begrip jurisdictie duidt op de door de soevereiniteit van andere staten beperkte rechtsmacht van de Nederlandse rechter.[235] De Nederlandse rechter mag in principe alleen rechtspreken over delicten die in Nederland zijn gepleegd. Nederland heeft op grond van artikel 2 tot en met 8 Sr rechtsmacht over kinderpornografisch materiaal dat via Nederlandse ISP's wordt verspreid of gedownload. Staat de server in het buitenland, dan heeft Nederland geen jurisdictie. Een uitzondering op dit beginsel vormt de Nederlander die zich in het buitenland schuldig maakt aan artikel 240b Sr. Op grond van artikel 5 lid 3 Sr kan hij of zij in Nederland toch vervolgd worden. De vreemdeling die ná het plegen van het feit een vaste woon- of verblijfplaats in Nederland verkrijgt, valt tevens onder de werking van dit artikel. Voor artikel 5 geldt niet het vereiste van dubbele strafbaarheid.[236] Dit vereiste houdt in dat het feit niet alleen in Nederland een misdrijf moet opleveren, maar ook door de wet van het land waar het misdrijf begaan is er een straf op is gesteld. In de meeste landen is kinderpornografie wel strafbaar gesteld, aangezien er wereldwijd wel enige consensus is dat kinderpornografie schadelijk is voor het betrokken kind. Het begrip kinderpornografie is door onder andere het Cybercrime Verdrag en Verdrag van Lanzarote grotendeels geharmoniseerd. Wel zijn er nog altijd landen die nog niet zijn aangesloten bij deze verdragen. Zelfs al is een land aangesloten bij het Cybercrimeverdrag en het Verdrag van Lanzarote, dan nog kunnen er kleine verschillen in definities bestaan. In Noorwegen zijn bijvoorbeeld alle kinderpornografische uitingen (dus ook tekeningen) strafbaar, terwijl het Nederlandse artikel 240b Sr spreekt over beeldmateriaal.[237] Daarnaast zijn er landen waarbij de bestrijding van kinderpornografie nauwelijks prioriteit heeft. Op deze landen moet politieke druk uitgeoefend worden zodat zij zich meer inzetten voor de aanpak van kinderpornografie op internet.

[235] Cleiren & Nijboer 2007, p. 1575.
[236] Aanwijzing kinderpornografie 2007, paragraaf 3.1.
[237] Stol e.a. 2008, *Ars Aequi*, p. 535.

In Nederland heeft de samenhang tussen de artikel 1 en 539a Sv tot gevolg dat het Nederlandse Wetboek van Strafvordering ook bij opsporing in het buitenland van toepassing is.[238] Jurisdictie vormt bij de opsporing van kinderpornografie een probleem, omdat een groot deel van het kinderpornografische materiaal zich op servers in het buitenland bevindt. De Nederlandse politie en justitie mogen haar strafvorderlijke bevoegdheden alleen inzetten bij misdrijven op Nederlands grondgebied. Dit geldt ook voor opsporingshandelingen in de virtuele wereld.[239] Indien er toch grensoverschrijdend opsporingsonderzoek wordt gedaan dan is het verkregen bewijs in beginsel onrechtmatig.[240] Door middel van een rechtshulpverzoek aan een ander land mogen opsporingsbevoegdheden soms toch worden ingezet. Vaak wordt een rechtshulpverzoek alleen ingewilligd als de strafvorderlijke bevoegdheid ook in dat land en in die situatie mag worden ingezet.

Rechtshulp wordt verleend op basis van bilaterale of multilaterale verdragen die na internationaal overleg tot stand zijn gekomen. Het EU-rechtshulpverdrag[241] is bijvoorbeeld een belangrijk rechtshulpverdrag dat Nederland ondertekend heeft. Het vervelende van rechtshulpverzoeken is dat het altijd vertraging met zich mee brengt. Men kan immers niet meteen de opsporingsbevoegdheid inzetten, maar moet de toestemming of de hulp van de rechtshulpinstantie eerst afwachten. Bij bestrijding van kinderpornografie op internet is dat nog eens extra lastig aangezien de gegevens zeer vluchtig zijn. Het materiaal staat soms maar enkele uren op een server op internet en ook andere cruciale gegevens voor het bewijsmateriaal, zoals loggegevens[242] en gegevens over het betalingsverkeer, zijn vaak maar korte tijd beschikbaar. Om deze gegevens veilig te stellen voor de bewijsgaring moet snel worden gehandeld. In het Cybercrimeverdrag wordt het belang daarvan onder ogen gezien en in artikel 35 is daarom de verplichting aan de verdragsstaten opgelegd het 24/7-contactpunt te creëren. Het contactpunt moet een permanente

[238] Melai & Groenhuijsen 2003, p. 25.
[239] Kaspersen 2007, p. 167.
[240] HR 12 december 2000, *LJN* AA8965.
[241] EU-overeenkomst betreffende wederzijdse rechtshulp in strafzaken van 29 mei 2000, Trb. 2000, 96 en het Protocol bij deze Overeenkomst, Trb. 2001, 187.
[242] Dit zijn gegevens die bijvoorbeeld op een server worden bijgehouden van het verkeer dat een locatie op internet bezoekt. IP-adressen van bezoekers die op een bepaalde tijd een website hebben bezocht of van een dienst gebruik hebben gemaakt worden bijvoorbeeld soms een bepaalde periode bewaard.

bereikbaarheid van de verdragsstaat verzekeren voor de voorbereiding of ontvangst van rechtshulpverzoeken van andere verdragsstaten.[243] Kinderpornografie is in artikel 9 van het Cybercrimeverdrag strafbaar gesteld en voor rechtshulp bij dit delict mag het contactpunt worden gebruikt.
Om zeker te zijn van de beschikbaarheid van gegevens na het inwilligen van een verzoek tot verstrekking van gegevens kan een bevriezingsbevel worden afgegeven. De verdragsstaten zijn verplicht tot het creëren van a) een bevoegdheid voor opsporingsdiensten ter bevriezing van verkeersgegevens[244] en b) een bepaling die de bevoegdheid tot het realtime vergaren van verkeersgegevens regelt.[245] Dit betekent dat in een vordering aangegeven kan worden dat bepaalde gegevens van een bepaald tijdstip en datum bewaard moeten worden, zodat deze later gevorderd kunnen worden door een opsporingsinstantie.
Verder roept het Cybercrimeverdrag in artikel 25 lid 1 partijen op om elkaar "*to the widest extent possible*" rechtshulp te verlenen. Bij de totstandkoming van het Cybercrimeverdrag is veel overleg geweest over een verdragsrechtelijke bevoegdheid tot grensoverschrijdend onderzoek. Dat heeft echter niet geleid tot overeenstemming.[246] Wel zijn er twee situaties in het Verdrag opgenomen waarbij dit mogelijk is.[247] Ten eerste als het betrekking heeft op informatie dat openbaar beschikbaar is op internet en ten tweede de situatie die betrekking heeft op computergegevens die met toestemming van de bevoegde autoriteit worden verstrekt. Deze bevoegdheid kan men afleiden uit de wet, een overeenkomst of aan zijn relatie tot de gegevens. Op grond van de Nederlandse wet is voor het verzamelen van informatie uit openbare bronnen geen opsporingsbevoegdheid vereist (zie hoofdstuk 6.1.1). In dat opzicht voegt het Verdrag niet zoveel toe. Wel neemt de bepaling in elk geval alle discussie op internationaal vlak over dit onderwerp bij de verdragstaten weg.
Door deze bepalingen in het Cybercrimeverdrag kan er snel adequaat worden gereageerd op een rechtshulpverzoek. Het is echter geen garantie dat dit ook altijd in de praktijk gebeurt. Het is afhankelijk van de prioriteitsstelling van de aanpak

[243] Kaspersen 2007, p. 178.
[244] Artikel 19 lid 3 Cybercrimeverdrag.
[245] Artikel 20 lid 1 Cybercrimeverdrag.
[246] Kaspersen 2004, p. 70.
[247] Artikel 32 Cybercrimeverdrag.

kinderpornografie in het desbetreffende land hoe snel en adequaat er op een rechtshulpverzoek wordt gereageerd.

5.6.3 Internationale samenwerking

Rechtshulpverzoeken en de bijkomende vertraging kunnen met internationale samenwerking verminderd of voorkomen worden. Het opzetten van een 'joint investigation team' (gezamenlijk opsporingsteam) vormt hier een mooi voorbeeld van. Op grond van onder andere artikel 13 van het Europese Rechtshulpverdrag[248] kan het multilaterale samenwerkingsverband opgezet worden. In het gezamenlijke opsporingsteam mogen ambtenaren van Europol, Eurojust en derde landen (zoals de Verenigde Staten) deelnemen. Een van de grote voordelen van een gezamenlijk opsporingsteam is dat het de grenzen van lidstaten van de deelnemende lidstaten mag overtreden, afhankelijk van de noodzakelijkheden van de operaties. [249] Op grond van artikel 13 lid 3 sub b van het Europese Rechtshulpverdrag bepaalt dat de rechtsmacht van het land geldt waar het team zijn werkzaamheden uitoefenent. Binnen het team is een vrije uitwisseling van informatie mogelijk. De benodigde informatie kunnen de leden van het team verzoeken en verkrijgen van hun eigen autoriteiten.[250] In grote kinderpornozaken met een internationaal karakter kan een dergelijk team zeer nuttig zijn.

Een belangrijke rol bij Europese samenwerking op het gebied van opsporing vervullen de instellingen Eurojust en Europol.

Eurojust is in het leven geroepen om de coördinatie tussen lidstaten op opsporingsverzoeken en vervolgingen te verbeteren en te stimuleren. Vooral ten aanzien van het verlenen van rechtshulp en uitleveringen.[251] Zij kan tevens een voorstel doen aan de betrokken lidstaten om een 'joint investigation team' op te

[248] Overeenkomst, door de Raad vastgesteld overeenkomstig artikel 34 van het Verdrag betreffende de Europese Unie, betreffende de wederzijdse rechtshulp in strafzaken tussen de lidstaten van de Europese Unie, met verklaringen; Brussel, 29 mei 2000, Tcrt. 2000, nr. 96.
[249] Klip 2009, p. 400.
[250] Idem, p. 400.
[251] Idem, p. 401.

zetten.[252] Computercriminaliteit, kinderpornografie daaronder inbegrepen, valt onder het terrein waar Eurojust zich mee bezig houdt.[253]
Europol kan hulp verschaffen door haar kennis en expertise beschikbaar te stellen en sommige misdrijven te analyseren. Zij mag echter slechts een ondersteunende rol bieden en niet zelf dwingende maatregelen nemen of een opsporingsonderzoek opstarten.[254]
Naar mijn mening kunnen beide instellingen een bijdrage leveren aan de bestrijding van kinderpornografie op internet. Het past binnen de beoogde focusverschuiving van de bezitter naar de verspreiders en vervaardigers van kinderpornografie, waarbij voor de opsporing internationale samenwerking en rechtshulp noodzakelijk is.

Volgens het Verbeterprogramma van de politie zijn er allerlei internationale projecten, met als gezamenlijk doel het in kaart brengen en tegenhouden van criminele organisaties welke zich bezighouden met de commerciële productie en de verspreiding van kinderpornografie.[255] Nederland is tevens vertegenwoordigd in het project CIRCAMP (Cospol Internet Related Child Abusive Material Project). Op basis van afspraken tussen de aangesloten landen wordt kinderpornografisch materiaal dat op een van de lokale servers wordt aangetroffen, op verzoek van het KLPD verwijderd.[256] Er zijn ook landen waarmee geen rechtshulpverdrag of ander samenwerkingsverband op dit gebied bestaat. Internet service providers kunnen materiaal uit deze landen dan op vrijwillige basis blokkeren.[257]

Tenslotte is het Meldpunt Kinderporno op Internet onderdeel van een internationaal netwerk: de 'Association of Internet Hotline Providers in Europe' (INHOPE).[258] De

[252] Artikel 7 Besluit de Raad van 28 februari 2002 betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken (2002/187/JBZ).
[253] Artikel 4 Besluit de Raad van 28 februari 2002 betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken (2002/187/JBZ).
[254] Klip 2009, p. 399.
[255] Verbeterprogramma kinderporno 2009, p. 12.
[256] Stol e.a. 2008, p. 120.
[257] Stol e.a. 2008, p. 121.
[258] Lünnemann e.a. 2006, p. 25.

doelstelling van INHOPE is het faciliteren en coördineren van het werk van de meldpunten. Paragraaf 7.3 gaat dieper in op het Meldpunt Kinderporno op Internet.

Tussenconclusie

In dit hoofdstuk is vastgesteld dat kinderpornogebruikers en –verspreiders gebruik kunnen maken van verschillende anonimiseringstechnieken en de technieken van cryptografie en steganografie teneinde de opsporing van kinderporno te frustreren. Het lijkt erop dat het met deze technieken deels lukt om buiten het beeld van opsporingsdiensten te blijven. Daarnaast wordt de opsporing op internet gefrustreerd doordat internet niet gebonden is aan grenzen. Door dit jurisdictieprobleem moet er gewacht worden op rechtshulpverzoeken van Nederland aan het buitenland en dan kan het bewijsmateriaal verloren gaan. Dit probleem wordt gelukkig voor een deel ondervangen met het 24/7-contactpunt en de mogelijkheid een bevriezingsbevel af te geven teneinde de gegevens veilig te stellen. Met een gezamenlijk opsporingsteam speelt het probleem van de vertraging bij rechtshulp in veel mindere mate. Instellingen als Europol en Eurojust kunnen opsporingsdiensten bijstaan bij opsporingsonderzoeken.
Geconcludeerd kan worden dat internationale samenwerking positief bijdraagt aan het aanpakken van kinderporno op internet. De samenwerking kan in de toekomst verder geïntensiveerd worden.

In het volgende hoofdstuk wordt nagegaan welke opsporingsmogelijkheden er bestaan, rekeninghoudend met wat in dit hoofdstuk is gezegd, teneinde kinderpornografie op internet op te sporen.

Hoofdstuk 6: Het opsporen van kinderpornografie op internet

"Welcome to DALNet! Where the men are men, the woman are men, and the teenage girls are undercover FBI Agents!"[259]

Het gebruik van technieken ten behoeve van anonimiteit, cryptografie, steganografie en slim gebruik van jurisdictieverschillen door kinderpornogebruikers heeft tot gevolg dat er een verschuiving gaande is bij kinderporno op internet. Van min of meer openbare delen op het internet, naar kinderpornografie op moeilijker te bereiken delen op internet. Daardoor wordt de algemene blootstelling aan kinderpornografisch materiaal wellicht verminderd, maar dit impliceert ook dat bijzondere opsporingsmethoden nodig zijn om een effectieve aanpak mogelijk te maken.[260]

In hoofdstuk 4 is vastgesteld dat een corrigerende benadering niet altijd effectief is. De overheid ziet ook meer heil in proactieve opsporing en 'monitoring'.[261] Bij proactieve opsporing wacht men niet meer de aangifte af, maar gaan de opsporingsautoriteiten zelf actief op onderzoek uit. Het gaat daarbij niet alleen om de opsporing van reeds gepleegde misdrijven, maar tevens om het in beeld brengen van criminele organisaties.[262] Onder monitoring wordt in dit verband verstaan: het op structurele en systematische wijze volgen van uitingen en gedragingen op het internet waarmee inzicht verkregen wordt ten behoeve van beleidsvorming en beleidsevaluatie, zonder gebruik te maken van bijzondere opsporingsbevoegdheden.[263]

In dit hoofdstuk wordt onderzocht in hoeverre opsporing, monitoring en de inzet van bijzondere opsporingsbevoegdheden op internet toegepast kunnen worden bij de bestrijding van kinderpornografie op internet.

[259] Welkomstbericht op IRC-chatnetwerk DALNet, Dasselaar 2008, p. 186.
[260] *Kamerstukken II* 2007/08, 28 684, nr. 133, p. 19.
[261] *Kamerstukken II*, 2007/08, 28 684, nr. 133, p. 12.
[262] Sietsma 2006, p. 38.
[263] Zie ook *Kamerstukken II* 2007/08, 28 684, nr. 133, p. 12.

Illustratief voor de nieuwe aanpak van de overheid tegen kinderporno is de 'proeftuin kinderporno' waarbij geëxperimenteerd wordt met onderzoeks- en opsporingsbevoegdheden. Kinderpornografie wordt voor het eerst op landelijk niveau vanuit de KLPD aangepakt. Zo kan op één punt de aanwezige kennis en technologie bij de politie worden samengebracht en nieuwe inzichten worden uitgeprobeerd.[264]
In eerste instantie worden opsporingsonderzoeken aangewezen waarbij alles nauwlettend wordt gedocumenteerd voor nadere analyse, zodat eventuele verbeteringen daaruit kunnen voortvloeien. In deze voorbeeldzaken wordt ook expliciet gekeken naar de inzet van preventieve maatregelen gericht op het opwerpen van barrières tegen seksueel misbruik en de verspreiding van kinderporno.
In tweede instantie zullen teams toegewezen worden waarin geëxperimenteerd wordt met nieuwe onderzoeksmethodieken, nieuwe procedures en werkwijzen.[265] Dit heeft bijvoorbeeld geleid tot de ontwikkeling van een 'digitale wasstraat' waarmee grote kinderpornobestanden geautomatiseerd onderzocht en gecategoriseerd kunnen worden. In de proeftuin wordt ervaring opgedaan met innovatieve digitale en tactische opsporings- en preventieve middelen.[266]

De inzet van opsporingsbevoegdheden creëert een spanningveld met het recht op de persoonlijke levenssfeer dat is neergelegd in artikel 10 Gw en artikel 8 van het Europees Verdrag van de Rechten van de Mens (hierna: EVRM). Inbreuken op de persoonlijke levenssfeer kunnen echter gerechtvaardigd worden. De inbreuk moet op een wettelijke grondslag berusten en de inbreuk moet noodzakelijk zijn om het bij overheidswege gestelde doel te bereiken (het noodzakelijkheidsbeginsel). Bovendien moet er altijd een afweging gemaakt worden tussen de inbreuk op de persoonlijke levenssfeer en het beoogde doel (proportionaliteitsbeginsel). Daarnaast dient dat doel niet met andere middelen te bereiken te zijn (subsidiariteitsbeginsel). Kinderpornografie wordt in de maatschappij als zeer verwerpelijk gezien dat een inbreuk op de privacy van de kinderpornogebruiker vaak gerechtvaardigd kan

[264] *Kamerstukken II*, 2007/08, 31 200 VI, nr. 146, p 6.
[265] *Kamerstukken II*, 2007/08, 31 200 VI, nr. 146, p. 7.
[266] Brief over de voortgang aanpak kinderpornografie 2009, p. 3.

worden. Daarbij geldt uiteraard wel dat de opsporingsbevoegdheid in de wet moet zijn vastgelegd.
Uitgebreide analyses over het recht op privacy en de inzet van (proactieve) opsporingsbevoegdheden door middel van ICT zijn in het verleden al gedaan.[267] In deze scriptie wordt hier verder niet op in gegaan.

6.1 Opsporing in de controlefase

Bij opsporing wordt een onderscheid gemaakt tussen de controlefase en de opsporingsfase. In de controlefase mogen opsporingsambtenaren handelen op grond van artikel 2 van de Politiewet 1993 (Polw 1993) en in de opsporingsfase wordt de officier van justitie betrokken en mogen opsporingsbevoegdheden worden ingezet.

6.1.1 Opsporingshandelingen op grond van artikel 2 Politiewet 1993

In de controlefase handelt de opsporingsambtenaar op grond van artikel 2 Polw 1993. De politietaak in dit artikel komt neer op de handhaving van de rechtsorde. Voor het handhaven van de rechtsorde beschikt de politie over onderzoeksbevoegdheden jegens burgers, ook als nog geen sprake is van een strafbaar feit.[268] Na de controlefase vangt de opsporingsfase aan indien er een redelijk vermoeden bestaat dat er een strafbaar feit is gepleegd.[269] Voordat de officier van justitie bij het opsporingsonderzoek wordt betrokken, verrichten opsporingsambtenaren zoveel mogelijk onderzoek op grond van artikel 2 Politiewet 1993.

Opsporingsambtenaren mogen in principe vrijelijk rondstruinen op het internet en noteren wat zij daar tegenkomen.[270] Voor zover het openbare communicatie op een openbaar netwerk betreft, mogen opsporingsambtenaren, net als iedere burger, kennis nemen van deze informatie.[271] Wordt er door het intypen van bepaalde sleutelwoorden in de zoekmachine Google[272] kinderporno gevonden dan vormt

[267] Zie bijvoorbeeld Schermer 2007, en Sietsma 2006.
[268] HR 19 december 1995, *NJ* 1996, 249.
[269] Corstens 2008, p. 272.
[270] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 38 (MvT).
[271] Siemerink 2000, p. 3.
[272] Zoals ‘kinderporno’, ‘pre-teen porn’, ‘child erotica’, etc.

artikel 2 Polw 1993 de grondslag voor deze handeling. Men kan denken aan het inzetten van *intelligent agents,* die het internet afscannen naar kinderporno. Schermer wijst erop dat al op heden *software agents* ingezet worden op internet: *"all sorts of spiders, crawlers, and softbots are used to extract useful information from the internet."*[273] Zolang het hier om het zoeken in openbare delen van het internet gaat zou de inzet van dergelijke hulpmiddelen wellicht nog geplaatst kunnen worden onder artikel 2 Politiewet 1993. Dat geldt ook voor het doorzoeken van berichten uit nieuwsgroepen die Google in een openbare database heeft opgeslagen. Deze database gaat terug naar 1981 en bevat meer dan 800 miljoen berichten.[274]

Indien geconstateerd wordt dat het materiaal kinderpornografisch van aard is, kan op grond van artikel 2 Polw 1993 tot op zekere hoogte worden nagegaan uit welke bron het illegale materiaal afkomstig is. Via de Whois-database[275] kan men door simpelweg een domeinnaam in te typen onder andere gegevens van de websitehouder achterhaald worden. Tevens wordt aangegeven of de website actief is of niet. Dit is relevant voor het opsporingsonderzoek. Een opsporingsambtenaar kan de gegevens uit een Whois-database, net als ieder ander, opvragen. Per 1 januari 2010 is het aantal gegevens dat van .nl-domeinnamen opgevraagd kan worden drastisch verminderd. Waar men bij een zoekactie eerst nog adresgegevens en telefoonnummers kon verkrijgen zijn nu slechts namen en e-mailgegevens te verkrijgen. Telefoonnummers en adresgegevens kunnen overigens wel met de inzet van een opsporingsbevoegdheid verkregen worden (zie paragraaf 6.2.2.5.1), maar dan zitten we al in de opsporingsfase. Toch levert de Whois-database nog best veel informatie. Stel je wilt van de website van de Universiteit Leiden de gegevens weten, dan levert een zoekactie[276] de volgende gegevens op:

Domeinnaam:	leidenuniv.nl
Status:	actief
Houder:	Universiteit Leiden
Administratieve contactpersoon:	postmaster@leidenuniv.nl

[273] Schermer, 2007, p. 58.
[274] http://www.google.com/googlegroups/archive_announce_20.html (laatst geraadpleegd op 15 oktober 2009).
[275] http://www.whois.net/ (laatst geraadpleegd op 20 oktober 2009).
[276] Via de whois-database van http://www.sidn.nl (laatst geraadpleegd op 30 januari 2010).

Registrar:	Universiteit Leiden Niels Bohrweg 1 2333CA LEIDEN Netherlands
Technische contactpersonen:	a.d.pasqual@igroep.leidenuniv.nl postmaster@leidenuniv.nl postmaster@leidenuniv.nl w.p.fleischer@i-groep.leidenuniv.nl
Domeinnaamservers:	ns1.surfnet.nl 192:87:106:101 ns1.surfnet.nl 192.87.106.101 sherlock.leidenuniv.nl 132.229.8.6 watson.leidenuniv.nl 132.229.22.2
Datum registratie:	01-01-1980
Administratie door NL Domain Registry	

Soms wordt er een IP-adres weergegeven, maar vaak ook niet. In het bovenstaande voorbeeld is dat wel het geval. Stel wij kiezen uit de beschikbare IP-adressen het IP-adres van 'sherlock.leidenuniv.nl' (132.229.8.6). Door vervolgens te surfen naar http://www.ripe.net en het IP-adres in te typen en op 'enter' te drukken verschijnt de volgende informatie:

```
inetnum:        132.229.0.0 - 132.229.255.255
netname:        RUL-NL
descr:          Leiden University
descr:          P.O. box 9500
descr:          2300 RA  Leiden
country:        NL
admin-c:        RP711-RIPE
tech-c:         RP711-RIPE
mnt-by:         SN-LIR-MNT
mnt-irt:        irt-SURFcert
status:         ASSIGNED PI
source:         RIPE # Filtered

irt:            IRT-SURFcert
address:        SURFnet bv
address:        attn. SURFcert
address:        P.O.Box 19035
address:        NL-3501 DA
address:        Utrecht
address:        Netherlands
phone:          +31 302 305 305
fax-no:         +31 302 305 329
abuse-mailbox:  cert@SURFnet.nl
signature:      PGPKEY-EA137DFC
encryption:     PGPKEY-EA137DFC
admin-c:        TI123-RIPE
tech-c:         TI123-RIPE
auth:           PGPKEY-EA137DFC
auth:           PGPKEY-834125A1
auth:           PGPKEY-3D10C493
remarks:        emergency phone number +31 622 923 564
```

```
remarks:        timezone GMT+1 (GMT+2 with DST)
remarks:        https://www.trusted-introducer.org/teams/surfcert.html
remarks:        This is a TI accredited CSIRT/CERT
irt-nfy:        cert@SURFnet.nl
mnt-by:         TRUSTED-INTRODUCER-MNT
source:         RIPE # Filtered
person:         Ryko Prins
address:        Leiden Universiteit
address:        Netherlands
phone:          +31 71 5276 912
fax-no:         +31 71 5276 510
mnt-by:         SN-LIR-MNT
nic-hdl:        RP711-RIPE
source:         RIPE # Filtered
% Information related to '132.229.0.0/16AS1103'
route:          132.229.0.0/16
descr:          RUL-NL
origin:         AS1103
mnt-by:         AS1103-MNT
source:         RIPE # Filtered
```

De onafhankelijke organisatie RIPE verleent deze dienst aan ISP's in Europa, het Midden-Oosten en Azië die bij de organisatie zijn aangesloten.[277] Er zijn ook nog andere organisaties zoals RIPE.[278] De bovenstaande (openbare) informatie kan van belang zijn in een opsporingsonderzoek. De bovengenoemde handelingen vallen onder artikel 2 Politiewet 1993. Het bekijken van een website met kinderporno is voor een opsporingsambtenaar echter ook niet zonder risico. De website zelf kan namelijk ook IP-adresen vastleggen. Indien bekend wordt aan de hand van het IP-adres dat een opsporingsambtenaar de website heeft bekeken kan dat aanleiding geven de website op te heffen of naar een andere locatie te verplaatsen.

Veelal leveren de hierboven beschreven handelingen echter niets op. Zoals in hoofdstuk 5 uiteen is gezet, maken veel kinderpornogebruikers gebruik van technieken om het de opsporingsdiensten lastiger te maken. Niet alle ISP's zijn bij RIPE aangesloten en soms levert een zoekactie niets op. Ook kunnen de geregistreerde gegevens naar een dood spoor leiden. Wel kan met behulp van de gegevens vaak verder worden gerechercheerd.

[277] http://www.ripe.net/info/ncc/index.html (laatst geraadpleegd op 20 oktober 2009).
[278] AfriNIC, APNIC, ARIN en LACNIC.

6.1.2 Verkennend onderzoek

Artikel 126gg Sv biedt een mogelijkheid om verkennend onderzoek te verrichten naar kinderpornografie op internet. Op bevel van de officier van justitie kan een verkennend onderzoek worden ingesteld met als doel de voorbereiding van de opsporing naar misdrijven, die een ernstige inbreuk op de rechtsorde opleveren en beraamd worden binnen een verzameling personen. Hierbij is nog geen sprake opsporing.[279]

Over het algemeen wordt aangenomen dat bij kinderpornografie sprake is van een 'ernstige inbreuk van de rechtsorde'. De samenleving beschouwt kinderporno namelijk als uiterst verwerpelijk en er staat een hoge gevangenisstraf op van maximaal acht jaar. Echter, als het gaat om plaatjes van een zestienjarige of ouder - die vrijwillig seksuele handelingen verricht - kan er naar mijn mening niet meer gesproken kunnen worden van een ernstige inbreuk op de rechtsorde. Het antwoord op de vraag of er sprake is van een ernstige inbreuk op de rechtsorde en verkennend onderzoek mag worden verricht is naar mijn mening dus afhankelijk van het geval.

Een voorstel tot verkennend onderzoek moeten worden voorgelegd aan de hoofdofficier van het Landelijk Parket en aan het College van procureurs-generaal. Het hoge niveau dat beslist over de toepassing van verkennend onderzoek suggereert dat verkennend onderzoek niet te snel moet worden aangenomen.[280] De bevoegdheid tot verkennend onderzoek is in de praktijk al een keer toegepast bij het SKIM-project (Surveillance Kinderporno Internet Methoden) waarbij het project 'Digitaal Rechercheren' van de KLPD werd uitgevoerd. Hierbij werd actief gesurveilleerd op internet om kinderpornografie te bestrijden en werden er methoden en technieken ontwikkeld om de bestrijding te bevorderen.[281]

6.1.2.1 Datamining

In het kader van verkennend onderzoek wordt door Sietsma betoogd dat de techniek van datamining (datadelven) kan worden toegepast bij de bestrijding van

[279] *Kamerstukken II* 2004/05, 30 164, nr. 3, p. 17 (MvT).
[280] Zie ook Buruma 2001, p. 136.
[281] Koops e.a. 2007, p. 117.

kinderporno.[282] Hij wijst er op dat indien er aanwijzingen zijn dat personen zich aan artikel 240b Sr strafbaar maken door bepaalde websites te bezoeken, er gericht dataminingonderzoek gedaan kan worden. Bij datamining worden gegevensbestanden verzameld en bij elkaar gebracht. Vervolgens vindt een analyse plaats hetgeen neerkomt op een vergelijking tussen bestanden, maar dit kan soms ook complexere vormen aannemen. Met datamining kunnen verbanden tussen leden of een op voorhand onbepaalde groep van personen ontdekt worden. Ook verbanden tussen gebeurtenissen die op bepaalde trends wijzen kunnen met datamining worden ontdekt.[283] Op grond van artikel 126gg lid 2 Sv is het mogelijk om gegevens te verwerken, die in openbare registers zijn verzameld welke bij wet zijn ingesteld. Hoewel deze gegevens voor een ander doel zijn vastgelegd, mogen zij worden verwerkt indien dit noodzakelijk is voor de uitvoering van het onderzoek.[284] Zo zouden de gegevens uit een politieregister wellicht vergeleken mogen worden met openbare informatie op internet. Interessant is in dit kader het onderzoek van T. Cocx, waarbij gegevens uit een politieregister vergeleken worden met gegevens uit openbare profielen van de sociale netwerksite Hyves.[285] Uit zijn onderzoek bleek dat bekende pedofielen die actief zijn op het internet meer minderjarigere vrienden hadden dan niet-pedofielen.[286] De vraag is echter of dit gegeven voldoende aanleiding kan geven tot een opsporingsonderzoek naar de mensen met bovengemiddeld veel minderjarige vrienden. Mensen die met kinderen werken (docenten, zwemleraren, etc.) zullen misschien ook wel meer minderjarige online vrienden hebben dan anderen. Dit rechtvaardigt naar mijn mening dan ook zeker niet het instellen van een opsporingsonderzoek.

Datamining heeft grotendeels dezelfde functie als verkennend onderzoek, namelijk het bijeenbrengen van gegevens om daaruit concrete kennis te destilleren die eventueel aanleiding vormt voor een opsporingsonderzoek. Wanneer een verkennend onderzoek een concrete verdenking oplevert, eindigt het verkennend

[282] Sietsma 2006, p. 344.
[283] Buruma, 2001, p. 137.
[284] *Kamerstukken II* 1998/99, 26 410, nr. 3, p. 10-11 (MvT).
[285] T. Cocx, *Algorithmic Tools for Data-Oriented Law Enforcement*, (diss. Leiden), Universiteit Leiden 2009.
[286] Cocx 2009, p. 128 en 129. In de leeftijdsgroep 56-65 jaar hadden de mensen gemiddeld 18% aan minderjarige vrienden, vergeleken met 10% minderjarige vrienden van de mensen uit de gewone groep.

onderzoek en neemt het opsporingsonderzoek aanvang.[287] Het is vooralsnog niet duidelijk hoe datamining kan bijdragen aan de bestrijding van kinderporno op internet.

6.2 Opsporingsfase

In artikel 132a van het Wetboek van Strafvordering is het begrip opsporing gedefinieerd: *"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."* Met opsporing zijn de personen belast als genoemd in artikel 141 Sv, zoals de officier van justitie en ambtenaren van de politie (artikel 3 lid 1 onder a en c Polw 1993). De officier van justitie is de leider van het opsporingsonderzoek en voor de inzet van de meeste opsporingsbevoegdheden is zijn toestemming vereist. Politieambtenaren mogen lichte opsporingsbevoegdheden zelf uitvoeren. Voor de meest ingrijpende bevoegdheden is toestemming van de rechter-commissaris vereist. In paragraaf 5.6.1 is aangegeven dat voor het inzetten van een opsporingsbevoegdheid een rechtshulpverzoek noodzakelijk is.

Kinderpornografisch materiaal op een gegevensdrager is eigenlijk niets meer dan 'gegevens' op een 'geautomatiseerd werk'. Koops en Buruma identificeren hier onder verwijzing naar het werk van Wiemans het probleem dat het Wetboek van Strafvordering geen definities bevat van 'gegevens' of 'geautomatiseerd werk', zodat hier een theoretische lacune bestaat.[288] Echter, in de praktijk lijkt er geen probleem te zijn en worden de begrippen gehanteerd in de betekenis zoals het Wetboek van Strafrecht die geeft.[289]

Voorop bij de strafvordering staat het legaliteitsbeginsel, vastgelegd in artikel 1 Sv. Hieruit volgt dat opsporingsbevoegdheden duidelijk in de wet moeten zijn vastgelegd. Opsporingsbevoegdheden grijpen in op de persoonlijke levenssfeer van

[287] Sietsma 2006, p. 344.
[288] Koops & Buruma 2007, p. 78, met een verwijzing naar F.P.E. Wiemans, 2004a, *Onderzoek van gegevens in geautomatiseerde werken* (diss. Tilburg), Nijmegen: Wolf Legal Publishers 2004, p. 238-240.
[289] Koops & Buruma 2007, p. 79. Een 'gegeven' is gedefinieerd in artikel 80quinquies en een 'geautomatiseerd werk' is gedefinieerd in artikel 80sexies Sr.

burgers en behoeven daarom deze wettelijke grondslag.[290] Als het onderzoek een beperkte inbreuk op de persoonlijke levenssfeer levert, dan biedt artikel 2 Polw 1993 een toereikende grondslag.[291]

6.2.1 Vroegsporing

Binnen het begrip opsporing kan een onderscheid worden gemaakt tussen 'gewone' opsporing en opsporing naar 'georganiseerde verbanden', dat ook wel vroegsporing wordt genoemd.[292] Bij dat laatste is sprake van onderzoek naar strafbare feiten, waarbij sprake moet zijn van een redelijk vermoeden dat ernstige feiten in georganiseerd verband zijn of zullen worden gepleegd. Bij vroegsporing mogen een beperkt aantal bevoegdheden worden ingezet ondanks dat er nog geen sprake is van opsporing. Wat onder misdrijven in georganiseerd verband wordt verstaan is geconcretiseerd in artikel 126o Sv. Dit artikel stelt dat er een redelijk vermoeden uit feiten en omstandigheden dient te bestaan dat misdrijven omschreven in artikel 67 lid 1 Sv worden beraamd of begaan, die gezien hun aard of samenhang met andere misdrijven die in georganiseerd verband worden beraamd of gepleegd, een ernstige inbreuk opleveren op de rechtsorde. De mogelijkheid om onderzoek te doen naar een vermoeden dat ernstige misdrijven in georganiseerd verband worden beraamd of gepleegd, past bij de ontwikkeling naar een meer pro-actieve opsporing.[293]
De strafbare handelingen met betrekking tot kinderpornografie zijn omschreven in artikel 240b Sr en leveren een gevangenisstraf van maximaal 4 jaar op. Op grond van lid 2 geldt een maximum gevangenisstraf van 8 jaar als het om een gewoonte gaat. Op grond van artikel 67 lid 1 sub a Sv in samenhang met artikel 240b Sr valt kinderpornografie onder de noemer: misdrijf. Bij een 'georganiseerd verband' gaat het om 'een meer of minder vast verband van (wisselende) personen'.[294] Als een georganiseerde groep kinderporno vervaardigt, wordt er voldaan aan het criterium 'in georganiseerd verband'. Eerder is aangegeven dat er een groei is in de commerciële exploitatie van kinderporno door de georganiseerde misdaad. De bevoegdheden bij vroegsporing kunnen op van deze groep personen worden

[290] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 9 (MvT).
[291] HR 19 december 1995, *NJ* 1996, 249, overweging, 6.4.5.
[292] Corstens 2008, p. 258.
[293] Krommendijk, Terpstra en van Kempen 2009, p. 140.
[294] Cleiren & Nijboer 2007, p. 459.

toegepast. Tevens is in deze scriptie aangegeven dat er kinderpornonetwerken (op internet) bestaan, waarbij kinderporno uitgewisseld wordt. Deze groep valt naar mijn mening ook onder een georganiseerd verband. Bij kinderpornografie dat in een openbaar
peer-to-peer netwerk uitgewisseld wordt is geen sprake van een georganiseerd verband, maar in een besloten peer-to-peer netwerk (een darknet, zie paragraaf 5.4) kan hier wel sprake van zijn. De reden hiervoor is dat in dit soort netwerken alleen binnen een groep vertrouwelingen kinderpornografie wordt uitgewisseld. Meningen kunnen hierover verschillen.

In de praktijk wordt de mogelijkheid tot vroegsporing niet op grote schaal toegepast. De reden daarvoor is dat veel onderzoeksvoorstellen worden opgebouwd rondom een verdenking. Er is dan startinformatie met concrete aanwijzingen over gepleegde misdrijven en verdachten. Het primaire doel van het opsporingsonderzoek blijft beperkt tot het ophelderen van een concreet misdrijf.[295]
Vroegsporing biedt echter aanzienlijke voordelen. Men kan van een criminele organisatie verbanden onderzoeken en de omvang, structuur, leden en criminele activiteiten in beeld brengen, zonder dat een concrete verdenking ten aanzien van een van de leden van het veronderstelde verband hoeft te bestaan.[296] De wetgever heeft beoogd met vroegsporing de mogelijkheden voor het doen van onderzoek naar georganiseerde criminaliteit uit te breiden. De veronderstelling is dat deze vormen van criminaliteit voor politie en justitie verborgen blijven en dat is precies wat er bij kinderpornografie op internet gebeurt. Vroegsporing biedt de mogelijkheid een groep van vervaardigers van kinderpornografie in kaart te brengen en uiteindelijk die verdachten te vervolgen die het meest van belang zijn.[297] Dat kunnen bijvoorbeeld diegenen zijn die daadwerkelijk de kinderen misbruiken, diegenen die het materiaal online beschikbaar stellen of de organisatie in stand houden. Dit levert daadwerkelijk een effectieve aanslag op de organisatiestructuur en kinderen worden hiermee uiteindelijk beschermd tegen uitbuiting door criminele organisaties. Kortom, vroegsporing biedt tal van mogelijkheden op het gebied van

[295] Krommendijk, Terpstra en van Kempen 2009, p. 132.
[296] Idem, p. 134.
[297] Idem, p. 140.

kinderpornografie op internet en de inzet ervan moet vaker overwogen worden. Hierna zal ik elke keer dat ik een opsporingsbevoegdheid wordt genoemd, ook het equivalent van de bevoegdheid bij opsporing in een georganiseerd verband worden genoemd.

6.2.2 Bijzondere opsporingsbevoegdheden

Bijzondere opsporingsbevoegdheden kunnen ook in een digitale omgeving worden toegepast.[298] Waar in de Memorie van Toelichting van de Wet op de Bijzondere Opsporingsbevoegdheden (hierna: Wet BOB) nog werd gesteld dat digitale recherche een nieuw fenomeen is[299], kan nu worden gesteld dat digitaal rechercheren meer een gemeengoed is geworden. Door de aard van het internet is digitaal rechercheren teneinde het illegale materiaal op te sporen, onontbeerlijk geworden. Met de inzet van bijzondere opsporingsbevoegdheden kunnen kinderpornogebruikers geïdentificeerd worden en kan er voldoende bewijsmateriaal worden verzameld. De bevoegdheden mogen ingezet worden met het doel de opheldering van en afdoening van strafbare feiten te bewerkstelligen. Het verbeteren van de informatiepositie mag slechts een tussengelegen doel zijn.[300] Dit geldt niet voor de toepassing van bijzondere opsporingsbevoegdheden bij vroegsporing (zie vorige paragraaf). In de volgende subparagrafen worden de relevante bijzondere opsporingsbevoegdheden behandeld.

6.2.2.1 Stelselmatige observatie

'Stelselmatig' is een sleutelbegrip binnen de Wet BOB.[301] Het begrip betekent dat er een min of meer volledig beeld van bepaalde aspecten van iemands leven worden verkregen.[302] Stelselmatige observatie vindt haar grondslag in artikel 126g en 126o Sv en hier gaat het om het heimelijk of niet-heimelijk volgen van een persoon of object, al dan niet met een technisch hulpmiddel. Het gebruik van technische hulpmiddelen is op grond van artikel 126g lid 3 en 126o lid 3 Sv toegestaan, voor zover daarmee geen vertrouwelijke informatie wordt opgenomen. Met betrekking

[298] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 36 (MvT).
[299] *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 72.
[300] *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 3 (Mvt).
[301] Y. Buruma, 'Een sleutelbegrip binnen de Wet Bijzondere Opsporingsbevoegdheden', *NJCM-Bulletin*, 2002, p. 649-658.
[302] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 26 (MvT).

tot stelselmatige observatie op internet kan men denken aan het gebruik van *cookies* en *applets*, voor zover deze gebruikt worden om te volgen welke websites iemand heeft bezocht. Daarbij kan een min of meer volledig beeld van iemands persoonlijke leven tot stand komen. Buruma acht het gebruik hiervan als een 'observatie' in wettelijke zin.[303]

In principe mag een opsporingsambtenaar op basis van artikel 2 Polw 1993 rondkijken op een peer-to-peer netwerk teneinde vast te stellen of er onrechtmatige informatie op staat. Wordt er een speciaal zoekprogramma ingezet zodat dit automatisch in werking gaat, dan beschouwd Schermer dit als stelselmatige observatie. Dit omdat de gedeelde mappen op de harde schijven van de gebruikers systematisch worden afgezocht en daarmee een inbreuk op de persoonlijke levenssfeer wordt geleverd.[304] Echter, de bestanden in 'Mijn gedeelde map' worden opzettelijk gedeeld zodat deze uitgewisseld kunnen worden. Er worden niet zomaar persoonlijke bestanden in de map geplaatst, maar slechts de bestanden die uitgewisseld moeten worden. Mijn inziens wordt daarom geen of slechts een geringe inbreuk geleverd op de persoonlijke levenssfeer en is de inzet van zoekprogramma's in peer-to-peer netwerken te scharen onder artikel 2 Polw 1993.

6.2.2.2 Stelselmatig inwinnen van gegevens

Op grond van artikel 126j en 126qa Sv mag een opsporingsambtenaar, op bevel van de officier van justitie en in het belang van het onderzoek, stelselmatig informatie inwinnen over de verdachte zonder dat hij kenbaar optreedt als opsporingsambtenaar. Stelselmatige informatie-inwinning is die vorm van informatie-inwinning die een inbreuk maakt op het recht op privacy van burgers. Het bevel mag op grond van lid 2 voor een periode van ten hoogste drie maanden worden gegeven. Dit bevel mag met nogmaals drie maanden worden verlengd. Het belang van de verlening moet wel opnieuw volledig worden getoetst door een officier van justitie. Voor het inzetten van deze bevoegdheid is een wettelijke grondslag vereist, aangezien het een misleidingelement met zich mee draagt en er

[303] Buruma 2001, p. 47.
[304] Schermer 2003, p.78

sprake is van een stelselmatig karakter.[305] Bovendien maakt het een inbreuk op de persoonlijke levenssfeer van de verdachte of betrokkene, omdat het in de (virtuele) persoonlijke omgeving van de verdachte kan plaatsvinden. Indien er geen sprake is van het stelselmatig inwinnen van informatie kan teruggevallen worden op artikel 2 Polw 1993 en artikel 141 en 142 Sv als het opsporingsonderzoek al is aangevangen.

Met betrekking tot kinderporno kan hier bijvoorbeeld sprake van zijn wanneer een opsporingsambtenaar aan een nieuwsgroep deelneemt[306] of op een ICQ-kanaal met de verdachte chat.[307] De opsporingsambtenaar interfereert met zijn actie in het leven van de verdachte. Als een verdachte bijvoorbeeld een profiel heeft op sociale netwerksites als LinkedIn, Facebook en Hyves dat alleen voor 'vrienden' zichtbaar is, zou een opsporingsambtenaar naar mijn mening op grond van artikel 126j en 126qa Sv zich ook als 'vriend' kunnen toevoegen bij de verdachte teneinde de gegevens die op zijn profiel staan te bekijken en te verzamelen.

De scheidslijn tussen infiltratie en het stelselmatig inwinnen bestaat in het feit dat bij het stelselmatig inwinnen van informatie niet wordt deelgenomen of meegewerkt aan een groep personen waarbinnen een misdrijf wordt gepleegd. De opsporingsambtenaar is dan ook niet gerechtigd op basis van deze bevoegdheid kinderpornoplaatjes of filmpjes van de verdachte af te nemen, laat staan met de verdachte uit te wisselen.

6.2.2.3 Politiële pseudokoop en dienstverlening

Onder politiële pseudokoop- en dienstverlening op internet moet worden verstaan: de situatie dat een opsporingsambtenaar voorwendt goederen of diensten te willen afnemen van een aanbieder op internet, strekkende tot aankoop en aflevering van goederen met de bedoeling in te grijpen op het moment dat de verdachte tot aflevering overgaat.[308] Op grond van artikel 126i of 126q Sv kan een bevel tot pseudokoop door een officier van justitie worden afgegeven. De inzet van de bevoegdheid moet in het belang van het onderzoek zijn.

---

[305] U. van de Pol, '(Op)sporen op internet, privacybescherming onder druk', *Privacy en Informatie*, 2000, p. 154.
[306] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 34 (MvT).
[307] Schermer 2003, p. 65.
[308] HR 30 september 2003, *NJ* 2004, 84.

Onder de pseudokoop valt ook de zogenaamde voorkoop. De opsporingsambtenaar neemt goederen af met de bedoeling vast te stellen of de goederen een ongeoorloofd karakter hebben, dan wel of met de goederen een strafbaar feit is gepleegd.[309] Aangezien afbeeldingen of films van kinderpornografie niet als een goed kunnen worden gezien, maar als een gegeven worden beschouwd, kan van pseudokoop geen sprake zijn.[310] Sub b biedt daarvoor een uitkomst, omdat ook gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk, van de verdachte afgenomen kunnen worden. Een opsporingsambtenaar kan bijvoorbeeld tijdens een chatgesprek tot afname van kinderpornografisch materiaal over gaan. Levert de verdachte het materiaal, dan is deze schuldig aan de verspreiding van kinderpornografie. Er kan echter niet zoals bij een pseudokoop in de fysieke wereld meteen overgegaan worden tot arrestatie van de verdachte, wat de pseudokoop op internet problematischer maakt.
Sub c van artikel 126h of 126q gaat in op het afnemen van een dienst. Van een dienst kan sprake zijn indien er bijvoorbeeld betaald moet worden voor de toegang tot een website. Een opsporingsambtenaar zou bijvoorbeeld met een speciale creditcard van de politie toegang kunnen verschaffen tot de pornowebsite teneinde vast te stellen of er strafbare inhoud aanwezig is. De bevoegdheid tot pseudokoop- of dienstverlening heeft een eenmalig karakter en men dringt niet door tot de organisatie.

De uitzondering waarop deze bevoegdheid toegepast mag worden staat in lid 2: *"de opsporingsambtenaar mag bij de tenuitvoerlegging van het bevel de verdachte niet brengen tot andere strafbare feiten dan waarop diens opzet reeds tevoren was gericht"*. Dit heeft betrekking op het zogenoemde Talloncriterium.[311] De overdracht of dienstverlening had dus ook al plaats moeten vinden als de opsporingsambtenaar niet ertussen was gekomen.[312] Bij het bovenstaande voorbeeld van een paysite waarbij aanwijzingen zijn dat daar kinderporno wordt aangeboden mag de

[309] Cleiren & Nijboer 2007, p. 406.
[310] *Kamerstukken II*, 1998/99, 26 671, nr. 3, p. 37 (MvT).
[311] HR 4 december 1979, *NJ* 1980, 356.
[312] *Kamerstukken II* 1996/97, 25 403, nr. 3, p. 32 (MvT).

bevoegdheid mijns inziens toegepast worden. De houder had namelijk toch al de intentie kinderpornografie beschikbaar te stellen.

6.2.2.4 Politiële infiltratie

Politiële infiltratie houdt in dat een opsporingsambtenaar deelneemt of medewerking verleent aan een groep of georganiseerd verband door een andere identiteit aan te nemen. Deze bevoegdheid kan op grond van artikel 126h en 126p Sv door de officier van justitie gegeven worden bij misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Het College van procureurs-generaal beslist echter over de inzet van deze bevoegdheid na advies van de Centrale Toetsingscommissie (CTC). Voor infiltratie is het nodig dat het onderzoek het inzetten van de bevoegdheid dringend vordert. Hieruit vloeien de eisen van proportionaliteit en subsidiariteit voort.

Bij kinderporno op internet vindt de toepassing van dit artikel waarschijnlijk plaats binnen kinderpornonetwerken.[313] Een opsporingsambtenaar kan bijvoorbeeld deelnemen aan een besloten peer-to-peer netwerk (darknet) of een ander besloten netwerk waarin kinderpornografie wordt uitgewisseld. Bij een normaal peer-to-peer netwerk, zoals Kazaa, merkt Schermer naar mijn mening terecht op dat hier een onvoldoende organisatiegraad bestaat om te spreken van een ‘groep personen’ zoals is vereist in artikel 126h en 126p Sv.[314] De W0nderland-club is een voorbeeld van een kinderpornonetwerk waar het, mijns inziens, toegestaan is om te infiltreren. In de W0nderlandclub waren naar verluidt ‘snuff pictures’ het enige materiaal dat op het netwerk niet toegestaan was.[315] Snuff pictures zijn afbeeldingen waarop mensen vermoord worden. Hier wordt zonder meer voldaan aan de eis van een ‘ernstige inbreuk op de rechtsorde’. Aan de proportionaliteitseis wordt aldus voldaan. Met betrekking tot de subsidiariteitseis moet het niet mogelijk zijn met de inzet van minder zware bevoegdheden hetzelfde resultaat te bereiken. De pseudokoop-bevoegdheid kan eerst ingezet worden teneinde inzicht te krijgen hoe ernstig het materiaal is dat wordt uitgewisseld alvorens tot infiltratie over te gaan.

[313] Buruma 2001, p. 63.
[314] Schermer 2003, p. 64. Zie ook paragraaf 6.2.1 over vroegsporing.
[315] Jenkins 2001, p. 83.

Voor zover voorzien kan de officier van justitie in het bevel opnemen welke strafbare feiten (niet) mogen worden gepleegd. Bij kinderporno is de enige strafbare handeling het verspreiden van kinderporno. Het is daarom bij het infiltreren in een kinderpornonetwerk duidelijker welk strafbaar feit de undercover agent zal plegen dan als men in een fysieke criminele organisatie infiltreert.

Bij infiltratie is tevens het Talloncriterium van toepassing. Indien een infiltrant kinderporno moet aanleveren om lid te worden van een besloten netwerk, dan komt men in de sfeer van een *storefront*.[316] Een storefront is een vorm van infiltratie dat gebruikt wordt door aan een criminele organisatie faciliteiten, bijvoorbeeld transportmiddelen of mogelijkheden om kinderporno uit te wisselen, teneinde inzicht te krijgen in de criminele organisatie of om bewijsmateriaal te verzamelen. Bij kinderpornografie lijkt het mij hier belangrijk dat de opsporingsambtenaar niet het initiatief neemt tot het uitwisselen van de afbeeldingen of filmpjes en in verband met de proportionaliteit zo min mogelijk 'extreme' inhoud aanbiedt aan de andere gebruikers in het netwerk. Siemerink stelt voor om de logbestanden van computers te gebruiken om te controleren of het Talloncriterium niet is overtreden.[317] Van den Hoven van Genderen merkt op dat het aanleveren van 'oud' materiaal niet voldoende is om toegang te krijgen tot een besloten netwerk. Hij betoogt in essentie dat het aanleveren van 'nieuw' materiaal de proportionaliteitstoets niet doorstaat en uiteindelijk niet leidt tot het aanpakken van de producenten van kinderpornografie waar het eigenlijk om moet gaan.[318] Hierbij negeert Van den Hoven van Genderen het feit dat in veel literatuur gesteld wordt dat niet alleen vervaardigers bijdragen aan kindermisbruik door nieuw materiaal op de markt te brengen. Ook in de huishoudelijke sfeer worden kinderen misbruikt en binnen besloten netwerken wordt dit materiaal als (ruil)middel gebruikt. Niet alle pedofielen hebben de behoefte met het materiaal geld te verdienen. Bovendien moeten commerciële vervaardigers op de een of manier naar buiten treden waardoor zij meer kans hebben ontdekt te worden door opsporingsdiensten. De mogelijkheid van

[316] Zie ook Siemerink 2000, p. 42.
[317] Siemerink 2000, p. 100.
[318] R. van den Hoven van Genderen, 'Inzet kinderpornofilmpjes door politie in strijd tegen kinderporno, aanvaardbaar?', 2009. (http://jurel.nl/2009/06/10/inzet-kinderpornofilmpjes-door-politie-in-strijd-tegen-kinderporno-aanvaardbaar/)

infiltratie biedt naar mijn mening een schat van informatie over de organisatiestructuur en het soort materiaal dat in zo'n netwerk wordt uitgewisseld. Op het moment dat men nieuw materiaal of zeer extreem materiaal signaleert kan men ingrijpen. De bevoegdheid past mijn inziens goed bij opsporing naar georganiseerde verbanden waarin kinderpornografie wordt uitgewisseld.

6.2.2.5 Vorderen van gegevens

Nog niet zo lang geleden konden opsporingsambtenaren bedrijven en burgers verzoeken gegevens te verstrekken voor opsporingsonderzoek. De gegevensverstrekkers konden dan zelf een afweging maken of zij de gegevens gingen verstrekken of niet. Hierbij konden zij zelf een afweging maken tussen het opsporingsbelang, het privacybelang van de betrokkene en hun eigen belang.[319] Na de implementatie van de Wet bevoegdheden vorderen gegevens in 2005[320] werd dit systeem van vrijwilligheid vervangen door dwingende wetsregels. Het is voor de bewijsgaring en identificatie van de verdachte vaak noodzakelijk gegevens op te kunnen vragen. Door de wetswijziging kan een rechtsgeldig verzoek niet meer worden geweigerd.

Met de invoering van de Wet bewaarplicht telecommunicatiegegevens[321] zijn aanbieders van telecommunicatiediensten, dat wil zeggen alle Nederlandse ISP's en de meeste hostingsproviders, per 1 september 2009 verplicht de verkeersgevens met betrekking tot het internetverkeer voor 6 maanden te bewaren. De wet is een implementatie van de Dataretentierichtlijn[322]. De gegevens moeten bewaard worden teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit.[323] Er is veel discussie over de bewaarplicht.[324] Het grootste punt van kritiek is dat opsporingsdiensten al voldoende middelen ter beschikking hebben om hun werk te doen en het een onevenredige inbreuk op de privacy van burgers zou opleveren. Andere wetenschappers zien het als *"de onderkenning van de normatieve werking van*

[319] Mac Gillavry 2001, p. 1412.
[320] Wet van 16 juli 2005, *Stb.* 2005, 390.
[321] Wet van 25 augustus 2009, *Stb*. 2009, 360.
[322] Richtlijn 2006/25/EG, PB EG L 105, 13 april 2006, p. 0054-0063.
[323] Artikel 1 Dataretentierichtlijn en *Kamerstukken I*, 2006/07, 31 145, nr. 3, p. 1 (MvT).
[324] Zie bijvoorbeeld 'Vrijwillig op weg naar de politiestaat', *NRC Handelsblad*, 2 april 2008, ondertekend door 14 Nederlandse hoogleraren.

nieuwe technologie."[325] Hoe men er ook over denkt, feit is dat de bewaarplicht garandeert dat waardevolle gegevens voor de opsporing bewaard blijven. Op grond van artikel 126n en 126u Sv is de officier van justitie bevoegd verkeersgegevens over een gebruiker op te vragen. Bij verkeersgegevens gaat het om de uiterlijke kenmerken van de communicatie. Bij internet zijn dat bijvoorbeeld de IP-adressen die over het internetverkeer van de gebruiker zijn vastgelegd. Tevens vallen hieronder de soorten diensten waarvan de gebruiker gebruik heeft gemaakt. Uit een lijst met IP-adressen kan misschien het IP-adres van de verdachte of dat van een website met kinderpornografie gedestilleerd worden.

Vorderingen van gegevens kunnen niet worden gericht aan de verdachte, vanwege het nemo-teneturbeginsel (de verdachte hoeft niet mee te werken aan zijn eigen veroordeling). Ook zijn de verschoningsrechten op grond van artikel 96a lid 3 Sv steeds van toepassing. Gegevens kunnen slechts opgevraagd worden bij Nederlandse instellingen. Vanzelfsprekend kunnen alleen die gegevens opgevraagd worden die bij een bedrijf of burger beschikbaar zijn. Indien de vordering op een buitenlandse instelling betrekking heeft moet het verzoek gepaard gaan met een rechtshulpverzoek en wordt de vordering getoetst aan de nationale wetgeving van het desbetreffende land. Dit heeft tot gevolg dat het niet altijd mogelijk is de gewenste gegevens te vorderen.

6.2.2.5.1 Identificerende gegevens

ISP's en hostingproviders kunnen beschouwd worden als aanbieders van een communicatiedienst in de zin van artikel 126la Sv. Bij verdenking van kinderpornografie kan een opsporingsambtenaar op grond van artikel 126na en 126ua Sv de naam, adres, postcode, woonplaats, nummer en soort dienst van een gebruiker opvragen. Onder een nummer wordt tevens het e-mailadres, accountnaam en het IP-adres van de gebruiker van de dienst verstaan.[326] Deze informatie is cruciaal voor het vaststellen van de identiteit van de verdachte. Op grond van artikel 126nc en 126uc Sv kan een opsporingsambtenaar bij *een ieder* die

[325] P. Kleve & R.V. de Mulder, 'Niets verkeerd met het bewaren van telefoongegevens', *NRC Handelsblad*, 7 april 2008.
[326] Cleiren & Nijboer 2008, p. 495.

daarvoor in aanmerking komt identificerende gegevens opgevraagd worden. Dit artikel is relevant bij het opvragen van gegevens bij banken of een online betalingsdienst zoals iDeal. Tevens kunnen er gegevens van een webmailprovider of proxyserver-dienstverlener opgevraagd worden. Op basis van dit artikel kunnen de administratieve kenmerken van een persoon opgevraagd worden, zoals het rekeningnummer en een klantnummer van de verdachte. Als bij de registratie op internet het IP-adres vastgelegd wordt kan dit tevens opgevraagd worden.

6.2.2.5.2 Overige gegevens

Op grond van artikel 126nd en 126ud Sv kunnen overige gegevens bij een ieder opgevraagd worden. De officier van justitie is bevoegd deze vordering in te stellen. De term 'overige gegevens' is zo breed als doet vermoeden. Het gaat bijvoorbeeld om gegevens over diensten die verleend zijn, zoals de duur, de data, de plaats en de aard van de dienstverlening en rekening- en betalingsgegevens.[327] Op basis van deze bevoegdheid kunnen bijvoorbeeld de logbestanden bij een dienst (zoals een proxyserver of online betalingsdienst) worden opgevraagd. Uit de gegevens kan misschien het IP-adres van een verdachte gehaald worden. Gegevens van creditcardmaatschappijen kunnen, met een rechtshulpverzoek, tevens worden opgevraagd. In een zaak van de rechtbank Zutphen[328] kwam de vraag aan bod of creditcardgegevens die door Amerikaanse autoriteiten waren verstrekt en waarmee werd betaald voor de toegang tot kinderporno op een website wel een redelijk vermoeden van schuld van een strafbaar feit opleverde. De rechtbank constateerde dat de creditcard op naam was gesteld en niet bedoeld was voor gebruik door een willekeurige derde en daarom in redelijkheid gesteld kon worden dat er sprake was van verdenking van een strafbaar feit, gepleegd door diegene op wiens naam de creditcard was gesteld. Het OM was hierdoor gerechtigd de creditcardgegevens op te vragen en vervolgens, na machtiging van de rechter-commissaris, een doorzoeking in het huis van de verdachte te plegen. Het probleem is wel dat door grootschalige creditcardfraude we er niet altijd meer van op aan kunnen dat de creditcardgegevens ook daadwerkelijk aan een gebruiker toebehoren.

[327] Cleiren & Nijboer 2008, p. 504.
[328] Rb. Zutphen 28 april 2006, *LJN* AW5462.

6.2.2.5.3 Toekomstige gegevens

Gegevens die pas na de vordering van artikel 126nd en 126ud Sv gegenereerd worden kunnen met artikel 126ne en 126ue Sv worden opgevraagd. Het betreffen dan toekomstige gegevens aangezien zij pas na het tijdstip van de vordering worden verwerkt.

6.2.2.5.4 Opgeslagen gegevens

Opgeslagen gegevens bij een communicatieaanbieder kunnen op grond van artikel 126ng lid 2 Sv, op bevel van de officier van justitie, na machtiging van de rechter-commissaris (lid 4), gevorderd worden indien het belang van het onderzoek dat dringend vordert. Hier gaat het bijvoorbeeld om de inhoud van een mailbox van een ISP.[329] Ook de inhoud van een webmailbox kan worden opgevraagd, maar aangezien veel webmailbedrijven zich in het buitenland bevinden is daar vaak een rechtshulpverzoek bij nodig. Het verzoek wordt vervolgens aan het nationale recht van de verstrekker getoetst. In een opsporingsonderzoek kan de inhoud van een mailbox belangrijke aanwijzingen geven. Als er berichten met kinderpornografisch materiaal verzonden zijn kan dat soms teruggevonden worden bij de verzonden berichten.

6.2.2.6 Internettap

De wereld van kinderpornogebruikers speelt zich vooral achter de computer en in cyberspace af. Het is van belang dat de gegevens die door de computer worden gegenereerd ook ‘afgeluisterd’ kunnen worden. Communicatieaanbieders zoals ISP’s en de meeste hostingproviders moeten verplicht aftapbaar zijn. Het internetverkeer van een verdachte kan daarom met een zogenaamde ‘IP-tap’ afgetapt worden.[330] Met een IP-tap wordt het gegevensverkeer van een bepaald IP-adres afgevangen. Zowel inkomende als de uitgaande gegevensstromen van de verdachte kunnen worden getapt op grond van artikel 126m of 126t Sv. Het bevel kan alleen worden gegeven door de officier van justitie, na machtiging van de rechter-commissaris, als het onderzoek het dringend vordert en het misdrijf een ernstige inbreuk op de rechtsorde oplevert.

[329] Cleiren & Nijboer 2008, p. 512.
[330] Schermer 2003, p. 56.

Het is niet duidelijk hoe vaak een IP-tap in de praktijk wordt ingezet. Wel is duidelijk dat er door opsporingsdiensten gebruik van wordt gemaakt. Uit een zaak van het Hof 's-Hertogenbosch[331] blijkt dat met een IP-tap meegekeken kan worden met het websurfen: *"Vanaf het getapte IP-adres van verdachte is te zien dat gekeken wordt in Ebay accountgegevens van slachtoffers van bovengenoemde virussen."* Bovendien blijkt uit deze zaak dat met het e-mailverkeer kan worden meegelezen: *"Uit een IP-tap van het IP-adres in gebruik bij verdachte is te zien dat verdachte een mailbericht ontvangen heeft waarin de zending van de schoenen bevestigd wordt."* Uit een zaak van de rechtbank Breda[332] blijkt dat ook chatgesprekken kunnen worden meegelezen: *"Een aanzienlijk deel van deze chat is echter ook via de (Nederlandse) tap van het internetverkeer waargenomen doordat [verdachte] deze gegevens heeft 'geplakt' in een chat met [verdachte 2] op 2 augustus tussen 18.00 en 19.00 uur."* Deze zaken maken duidelijk dat een internettap kan functioneren en waardevol bewijs kan opleveren.

Er zijn echter een paar praktische uitvoeringsproblemen bij een IP-tap te constateren. Zo is het niet altijd gemakkelijk voor opsporingsdiensten uit de enorme gegevensstroom, die door computers worden gegenereerd, de relevante gegevens te destilleren. De laatste jaren is het dataverkeer explosief gegroeid. Voor privaatgebruik zijn de snelheiden van 56 Kbps (Kilobyte per seconde) van de telefoonlijn veranderd naar een standaard DSL lijn dat meestal 0,5 of 1 Mbps (Megabyte[333] per seconde) ondersteunt. Dit heeft het volume van het dataverkeer enorm doen toenemen.[334] De verwachting is dat deze ontwikkeling in de toekomst toeneemt. Bovendien worden vaker verschillende diensten tegelijk gebruikt, zoals het verzenden van bestanden via FTP terwijl er ook gechat wordt via een Instant Messenger. Deze hybride diensten zijn moeilijker te verwerken.[335]

Een ontwikkeling dat het aftappen van internetverkeer lastiger maakt is '*seamless routing'*. Door seamless routing gaat het signaal van de ene dienst naadloos over op

[331] Gerechtshof 's-Hertogenbosch 12 september 2009, *LJN* BF0770.
[332] Rb. Breda, 30 januari 2007, *LJN* AZ7281.
[333] Één Megabyte is 1024 Kilobyte.
[334] Koops & Bekkers 2007, p. 53
[335] Idem, p. 64.

de andere. Zo kan men voor een internetverbinding gebruik maken van verschillende netwerken, zoals een UMTS-netwerk, WiFi-netwerken of Hotspots.[336] Hierbij wisselt het IP-adres en is het lastig, zo niet onmogelijk, de communicatie af te vangen.

Indien de communicatie versleuteld is, kan op grond van artikel 126m of 126t lid 6 de officier van justitie het bevel geven tot vordering van de wijze van versleuteling van de communicatie. Niet altijd heeft de dienstaanbieder kennis van de wijze van versleuteling, waardoor dit soms onmogelijk is. Tevens kunnen er programma's op de computer werken die peer-to-peer telefonie mogelijk maken zoals Skype en Instant Messenger programma's.[337] Dit zijn geen aanbieders van telecommunicatiediensten en zij zijn niet verplicht aftapbaar. Hier biedt de bevoegdheid van direct afluisteren soms uitkomst.

6.2.2.7 Direct afluisteren

Bij de behandeling van de opsporingsbevoegdheid tot het direct afluisteren beperk ik mij tot het direct afluisteren van de communicatie die van een computer uitgaat. De bijzondere opsporingsbevoegdheid van direct afluisteren leent zich vooral als alternatief voor de bevoegdheid tot aftappen en opnemen van communicatie, omdat daar in toenemende mate gebruik wordt gemaakt van de versleuteling van gegevens.[338] Direct afluisteren mag alleen ingezet worden als het gaat om een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, de zaak de inzet van de bevoegdheid dringend vordert en de rechter-commissaris na verzoek van de officier van justitie het bevel heeft afgegeven. Op grond van artikel 126l en 126s Sv moet er sprake zijn van een misdrijf waarop een gevangenisstraf van 8 jaar of meer staat. Dit is bij kinderpornografie het geval indien van een gedraging in de zin van artikel 240b Sr een gewoonte wordt gemaakt.

Vertrouwelijke communicatie kan afgeluisterd worden door het plaatsen van een *bug* op een toetsenbord. Dat is een apparaatje met een microfoon waarmee

[336] Idem, p. 61.
[337] Koops & Bekkers 2007, p. 60.
[338] Zie *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 35 (MvT) en Eshof e.a. 2002, p. 26.

communicatie afgevangen kan worden, maar ook toetsaanslagen geregistreerd kunnen worden. Zo kan ook worden nagegaan wat er op de computer ingetypt en gecommuniceerd wordt. Het gebruik van een bug voor het afvangen van wachtwoorden en encryptiesleutels wordt door de wetgever beperkt: *"Indien vooraf redelijkerwijs bekend kan zijn dat door de plaatsing van een technisch hulpmiddel geen communicatie, maar alleen andere uitingen worden opgenomen, mag het technisch hulpmiddel niet worden geplaatst. Het is dus niet toegestaan een bug te plaatsen op een toetsenbord van een PC die niet op een netwerk is aangesloten."*[339] Aansluiting van een computer op een netwerk is dus een extra vereiste bij het plaatsen van bug op het toetsenbord. De bevoegdheid wordt als ingrijpender beschouwd dan aftappen.[340] Om het apparaat te plaatsen moet namelijk vaak een huis worden binnengetreden.

Het plaatsen van een softwarematige bug op een computer dat de toetsaanslagen registreert, een *keylogger* genoemd, is niet toegestaan. Om dat mogelijk te maken moet namelijk een geautomatiseerd werk worden binnen gedrongen. Dit is echter computervredebreuk (ook wel *hacken* genoemd) en dat is vooralsnog geen opsporingsbevoegdheid van de politie en het OM. Er wordt gesuggereerd dat hacken onder de bevoegdheid van 126k of 126r Sv (het heimelijk betreden van een besloten plaats) kan worden geschaard.[341] Een harde schijf moet dan als besloten plaats aangemerkt worden, maar dat is wel een heel grote oprekking van het begrip.[342] Bovendien vindt hacken als opsporingsbevoegdheid geen enkele ondersteuning in de wetsgeschiedenis en is deze bevoegdheid wél gecreëerd voor de veiligheidsdiensten op grond van artikel 24 van de Wet op de inlichtingen- en veiligheidsdiensten.[343] Als de wetgever had gewild dat ook justitie computervredebreuk kon plegen, dan had hij dat expliciet moeten aangeven in het Wetboek van Strafrecht, net zoals dat bij de andere opsporingsmethodes van de Wet BOB is gebeurd.[344] Een 'online doorzoeking', waarbij van buitenaf een computer doorzocht mag worden is ook niet toegestaan omdat een wettelijke grondslag voor

[339] *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 35 (MvT).
[340] *Kamerstukken II*, 1996/97, 25 403, nr. 3, p. 6 (MvT).
[341] Boek 2000.
[342] Schermer 2003, p. 53.
[343] Buruma 2001, p. 50.
[344] Koops & Buruma 2007, p. 118.

hacken ontbreekt. In Duitsland is bij de bestrijding van terrorisme en onder bepaalde voorwaarden hacken wel toegestaan. De VVD-fractie heeft haar voorkeur al uitgesproken om de online doorzoeking ook in Nederland toe te staan met daarbij een uitbreiding voor de opsporing van misdrijven (waaronder kinderpornografie).[345]

6.2.2.8 Inbeslagname en doorzoeking ter inbeslagname van gegevens

Als kinderpornografie op internet wordt bekeken laat het sporen achter op de harde schijf (zie hoofdstuk 4). Het is daarom belangrijk dat het materiaal op gegevensdragers veiliggesteld kunnen worden. Daarnaast geven gegevens aanwijzingen voor opsporingdiensten of dragen zij bij aan het bewijsmateriaal.

De bevoegdheid tot de doorzoeking van een plaats ter vastlegging van gegevens is vastgelegd in artikel 126i en 126ui Sv. Gegevens zijn geen voorwerpen en kunnen daarom niet krachtens de bepalingen van de inbeslagneming van voorwerpen zelfstandig in beslag worden genomen. Tot doorzoeking zou pas overgegaan mogen worden als andere bevoegdheden, waaronder het vorderen van gegevens, niet effectief zijn.[346] Aan de vordering tot verstrekking van gegevens wordt niet altijd voldaan en dan kan met behulp van deze bevoegdheid de gegevens toch verzameld worden. Het gaat in zo een situatie bijvoorbeeld om betalingsgegevens die bij een bank zijn opgeslagen in een geautomatiseerd werk of gegevens die zich op een server van een hostingprovider bevinden. Na toestemming van de rechter-commissaris kan, ambtshalve of op verzoek van de officier van justitie, elke plaats doorzocht worden teneinde de gegevens vast te leggen.[347] Als tijdens de doorzoeking wordt opgemerkt dat de computer in verbinding staat met andere computers, dan mag de officier van justitie een netwerkzoeking verrichten, maar alleen voor zover de reguliere gebruikers van het doorzochte pand rechtmatig toegang hebben tot het geautomatiseerde werk elders (artikel 126j en 126uj Sv).

Alle gegevensdragers die de waarheid aan het licht kunnen brengen mogen op grond van artikel 94 Sv in beslag worden genomen. De gegevensdragers van een

[345] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 2.
[346] *Kamerstukken II* 2003-04, 29 441, nr. 6, p. 16.
[347] Art. 110 Sv.

verdachte waar zich misschien kinderpornografisch materiaal op bevindt kunnen, op grond van artikel 94a jo 103 Sv na machtiging van de rechter-commissaris op vordering van de officier van justitie, in beslag worden genomen. Vervolgens kunnen de gegevensdragers onderzocht worden op sporen van kinderpornografie. In hoofdstuk 4 is uitgebreid ingegaan waar deze sporen zich op een computer kunnen bevinden.

6.2.2.9 Ontsleutelingsbevel

In het vorige hoofdstuk is aangetoond dat kinderpornogebruikers regelmatig gebruik maken van versleuteltechnieken. Zo kunnen ook de gegevensdragers zelf of individuele bestanden met kinderporno worden versleuteld. Op grond van artikel 125k Sv kan iemand waarvan wordt verwacht dat hij of zij kennis draagt van de beveiliging van een bestand een bevel krijgen de toegang te verschaffen. Deze bevoegdheid kan uiteraard niet aan de verdachte worden gegeven, omdat dit in strijd zou zijn met het nemo-teneturbeginsel (zie ook artikel 126m lid 7 Sv). Personen die zich kunnen beroepen op hun verschoningsrecht, zoals genoemd in artikel 218 Sv, hoeven tevens geen medewerking te verlenen aan het ontsleutelbevel. Wel kan geprobeerd worden de code te kraken, maar dat is met de meer moderne versleuteltechnieken een onmogelijke opgave.

Tussenconclusie

In dit hoofdstuk is vastgesteld dat in de controlefase en opsporingsfase allerlei mogelijkheden zijn om kinderpornografie op te sporen. Proactieve opsporing op grond van artikel 3 Polw 1993 is tot zekere hoogte mogelijk, maar gezien de tendens dat steeds meer kinderpornogebruikers gebruik maken van anonimeringstechnieken, versleuteltechnieken, steganografie en van jurisdictieverschillen moeten al snel bijzondere opsporingsbevoegdheden ingezet worden. Verkennend onderzoek is mogelijk, maar het is nog onduidelijk of een techniek als datamining daadwerkelijk een bijdrage kan leveren aan de opsporing van kinderpornogebruikers.
Men kan overgaan tot vroegsporing indien er aanwijzingen zijn dat het delict van artikel 240b Sr in georganiseerd verband wordt gepleegd. Het opsporingsonderzoek kan waardevolle informatie geven over een organisatiestructuur van een

georganiseerde bende dat kinderpornografie produceert of een besloten kinderpornonetwerk. Vervolgens kunnen de juiste verdachten worden vervolgd, zodat er een effectieve slag aan de organisatiestructuur wordt gegeven en het kindermisbruik hopelijk gestaakt wordt. In de praktijk wordt de mogelijkheid tot vroegsporing weinig toegepast en dat is zonde, want het kan een nuttige bijdrage leveren aan de bestrijding van kinderporno.

Door de hoge strafmaat van artikel 240b Sr en verwerpelijkheid van kinderpornografie mogen ter bestrijding van kinderpornografie onder omstandigheden alle bijzondere opsporingsbevoegdheden ingezet worden. Gegevens van bedrijven of instellingen kunnen een waardevolle bron van informatie voor opsporingsinstanties zijn. Soms is het verkrijgen van belangrijke gegevens voor het opsporingsonderzoek een rechtshulpverzoek noodzakelijk. Indien de verstrekking van gegevens uitblijft kan gebruik worden gemaakt van de bevoegdheid van doorzoeking ter inbeslagname van gegevens.
Een internettap kan waardevolle informatie aan opsporingsdiensten geven, maar er zijn wat praktische problemen bij de toepassing ervan. Indien het communicatieverkeer is versleuteld kunnen opsporingsdiensten met het plaatsen van een bug toch nog het communicatieverkeer van de verdachte afluisteren.

Opsporingsdiensten kunnen met verschillende instanties samenwerken teneinde kinderpornografie beter te bestrijden. Daar wordt in het volgende hoofdstuk meer over verteld.

Hoofdstuk 7: Samenwerking met andere partijen voor de bestrijding van kinderporno

De overheid onderzoekt hoe met zelfregulering en publiek-private samenwerking kinderpornografie bestreden kan worden.[348] Er zijn namelijk verschillende partijen die invloed kunnen uitoefenen op de markt van kinderpornografie.
Internet service providers zijn een interessante partner van de opsporingsdiensten voor rechtshandhaving op internet. Zij hebben een zekere machtspositie tegenover de internetgebruiker, aangezien ISP's in de gelegenheid zijn toegang tot bepaalde diensten te ontzeggen of bepaalde informatie niet aan de gebruiker door te geven.[349]
Banken en creditcardmaatschappijen spelen dikwijls een rol in het betalingsverkeer met betrekking tot kinderpornografie. Zij zijn in staat informatie te verschaffen over hun klanten en inzicht te geven in het betalingsverkeer.
Het Meldpunt Kinderporno op Internet geeft meldingen van kinderporno door aan het KLPD naar aanleiding waarvan opgespoord kan worden. Tevens is haar taakomschrijving recentelijk uitgebreid.
Tenslotte houden verschillende andere private partijen zich bezig met de bestrijding van kinderpornografie.

In dit hoofdstuk wordt nagegaan met welke partijen de overheid kan samenwerken kinderpornografie te bestrijden. Elk van deze partijen zullen hieronder afzonderlijk behandeld worden.

7.1 Internet service providers (ISP's)

De ISP kan toegang tot kinderporno aan de internetgebruiker ontzeggen. Dat is op twee manieren mogelijk. De eerste mogelijkheid is om het materiaal van haar servers te halen en de tweede mogelijkheid is door het internet te filteren. Kinderpornografie wordt dan als het ware 'eruit gefilterd'. Eenvoudig gezegd worden de kinderpornografieafbeeldingen of filmpjes dan tegengehouden en krijgt de

[348] *Kamerstukken II* 2007/08, 28 684, nr. 133 p. 17.
[349] Schellekens, Koops & Teepe 2007, p. 10.

computergebruiker ze niet te zien. Op 17 mei 2006 is er een motie aangenomen van de kamerleden Van der Staaij en Rouvoet waarin de regering opgeroepen wordt om de verdere uitbouw en toepassing van de technische mogelijkheden tot het blokkeren, filteren of afsluiten van kinderpornografisch materiaal op internet en andere media te bevorderen.[350] Uit een niet-vrijgegeven rapport van Andersson Elffers Felix[351] blijkt dat ISP's erkennen dat voor hen een duidelijke rol is weggelegd bij de bestrijding van kinderporno. Medewerking van de ISP's is onontbeerlijk voor het filteren van kinderporno op internet. In de volgende paragraaf wordt onderzocht hoe het filteren in Nederland in zijn werking gaat.

7.1.1 Filtertechnieken

Filters werken op basis van lijsten van adressen en/of codes die geblokkeerd moeten worden (*black list filtering*) of op basis van algemene criteria, zoals trefwoorden, waarmee het filterprogramma vaststelt of bepaalde informatie wel of niet kan worden doorgelaten (*dynamic filtering*).[352] Dynamic filtering leidt tot relatief veel 'overblocking' en wordt vooral in software van particuliere bedrijven toegepast. Er is sprake van overblocking als er ook legaal materiaal wordt tegengehouden. Voorbeelden van websites die onterecht werden tegengehouden bij dynamiek filtering op het zoeken naar het woord 'borst' zijn sites over seksuele voorlichting, borstkanker en minister Borst.[353]

Filteren kan op verschillende plaatsen: op de computer van de internetter, op zoekmachines, op de centrale server van de organisatie, op de server(s) van de ISP's en hostingproviders of op landelijk niveau. Dit laatste is binnen Europa niet aan de orde, maar wel bijvoorbeeld in Saudi-Arabië en China. Filteren op gebruikers- en organisatieniveau stuit niet op technische of praktische bezwaren. Het op ISP-niveau filteren van chatkanalen, P2P-netwerken, MMS- en webcamverkeer is technisch gezien aanzienlijk lastiger dan het filteren van websites op internet.[354]

---

[350] *Kamerstukken II* 2005/06, 30 300VI, nr. 160.
[351] *Publiekprivate bestrijding van kinderporno op internet, een oplossingrichting*, 6 maart 2009, Utrecht, Andersson Elffers Felix, beschikbaar via: https://www.wikileaks.org/leak/publiekprivate-bestrijding-van-kinderporno-op-internet.pdf (laatst geraadpleegd op 15 oktober 2009).
[352] Stol e.a. 2008, p. 25.
[353] Stol e.a. 2008, p. 26.
[354] Stol e.a. 2008, p. 12.

Het blokkeren op basis van een zwarte lijst kan met IP-adressen, domeinnamen, URL's, of hashcodes. Een hashcode is een soort digitale handtekening. Er wordt dan een code toegevoegd aan een afbeelding of filmpje. Indien dezelfde afbeelding of filmpje weer in het systeem van Leaseweb langskomt wordt het materiaal tegengehouden. Het is de meest fijnmazige manier van filteren en het is bekend dat hostingprovider Leaseweb hier gebruik van maakt.[355] Het filteren op hashwaarden is ook geschikt om verkeer in peer-to-peer netwerken te filteren.[356]
Het nadeel van filteren op hashwaarden is dat de hashcode gemakkelijk veranderd kan worden door de pixels in de foto aan te passen. Gezien het aantal afbeeldingen en filmpjes dat kinderpornogebruikers vandaag de dag in hun collectie hebben denk ik niet dat alle kinderpornogebruikers dit materiaal snel één voor één zullen aanpassen. De voordelen van het filteren op hashwaarden, het is de meest fijnmazige techniek en het kan ook in peer-to-peer netwerken worden toegepast, wegen mijns inziens op tegen het nadeel dat het vrij gemakkelijk te omzeilen is.

7.1.1.1 Filteren in Nederland

In 2007 is er op initiatief van het KLPD een systeem van filteren op basis van zwarte lijsten gestart door middel van domeinnamen.[357] Het KLPD sloot convenanten af met internet service providers die de ISP verplichtte domeinnamen te blokkeren die door het KLPD waren aangemerkt als websites die kinderpornografisch materiaal bevatten. De abonnee van de desbetreffende ISP werd vervolgens omgeleid naar een 'stoppagina' als een website bezocht werd die op de zwarte lijst van het KLPD stond. Op de webpagina stond dan een melding dat de desbetreffende website kinderpornografisch materiaal bevatte en daarom geblokkeerd was. In een WODC-onderzoek[358] wordt stevige kritiek op deze praktijk gegeven.

Het aangaan van convenanten met private partijen deed de KLPD ter uitvoering van een veronderstelde publiekrechtelijke taak, namelijk de daadwerkelijke handhaving

[355] P. van Ammelrooy, 'Kinderporno laat verdachte vingerafdrukken achter', *Volkskrant*, 21 maart 2009, http://www.volkskrant.nl/archief_gratis/article1168312.ece/Kinderporno_laat_verdachte_vingerafdrukken_achter
[356] Andersson Elffers Felix 2009, p. 9.
[357] *Kamerstukken II*, 28 684, nr. 133, p. 18.
[358] W.Ph. Stol e.a. *Filteren van kinderporno op internet, een verkenning van technieken en reguleringen in binnen- en buitenland*, Den Haag: Boom Juridische uitgevers 2008.

van de rechtsorde dat is vastgelegd in artikel 2 Polw 1993.[359] Aangezien het filteren en blokkeren van internetverkeer een inbreuk maakt op het grondrecht van vertrouwelijke informatie, de vrijheid van meningsuiting en de bescherming van de persoonlijke levenssfeer, zoals geregeld is in artikel 13 Gw, artikel 10 EVRM (en artikel 7 Gw) en artikel 8 EVRM, behoeft een maatregel zoals het bovenstaande een formeelwettelijke grondslag.[360] Deze grondslag is niet in te lezen in artikel 2 van de Politiewet 1993. Artikel 2 Politiewet 1993 kan namelijk niet worden ingeroepen wanneer het optreden van de politie een inbreuk maakt op door de grond of door verdragen gewaarborgde rechten en vrijheden van de burger.[361] Artikel 125o Sv en artikel 54a Sv bieden volgens de onderzoekers evenmin basis voor het filteren van internet op kinderpornografie.[362]

Geconcludeerd kan worden dat de hierboven beschreven praktijk waarbij de KLPD de websites aanleverde die een kinderpornografische inhoud bevatten en op grond van een convenant geblokkeerd moesten worden een onvoldoende formeel wettelijke grondslag had.

7.1.1.2 Effectiviteit van filteren

Het ultieme doel van het filteren van internet op kinderporno is om het misbruik van kinderen te verminderen. De gedachte is dat het blokkeren van websites een extra drempel voor gebruikers opwerpt om toegang te krijgen tot kinderporno op internet. Ook kan worden gesteld dat commerciële aanbieders hun producten minder gemakkelijk kunnen aanbieden.[363] Dit zou uiteindelijk moeten leiden tot minder misbruik van kinderen. Onderzoekers van het WODC-rapport zeggen geen aanwijzingen te hebben dat filtertechnieken dit effect bewerkstelligen.[364]

---

[359] Stol e.a. 2008, p. 49.
[360] Zie ook E. Dommering, 'Filteren is gewoon censuur en daarmee basta', 2 januari 2009, http://www.ivir.nl/publicaties/dommering/Filteren_is_gewoon_censuur_en_daarmee_basta.pdf (laatst geraadpleegd op 25 oktober 2009) en R. Chavannes, 'het wegfilteren van de uitingsvrijheid', 15 oktober 2009, http://www.nu.nl/column/1019123/het-wegfilteren-van-de-uitingsvrijheid.html (laatst geraadpleegd op 25 oktober 2009) en R. van den Hoven van Genderen en A. Lodder, 'Kinderpornosites zijn erg maar censuur is nog erger', *NRC Handelsblad*, donderdag 25 oktober 2008.
[361] Stol e.a. 2008, p. 49. Daarbij wordt gerefereerd naar de uitspraak van Rb. 's-Gravenhage 28 oktober 2003, *LJN*: AN9476.
[362] Stol e.a. 2008, p. 50 en 52.
[363] Stol e.a. 2008, p. 122.
[364] Stol e.a. 2008, p. 145.

Een andere doelstelling is om argeloze gebruikers te beschermen tegen kinderporno op internet. In het rapport wordt betwijfeld of ook deze doelstelling behaald kan worden. Volgens de wetenschappers is het vrijwel uitgesloten dat iemand per ongeluk op een website met kinderporno terecht komt.[365]
De maatregel is bovendien niet erg duurzaam. De verwijderde sites duiken snel weer op via alternatieve locaties of manieren.[366]

Belangrijk is ook het argument van het gevaar van het hellende vlak: nu gaat het om kinderporno, daarna om het blokkeren van radicaliserende sites, sites met een terroristische inhoud, sites die inbreuk maken op het auteursrecht van anderen, enzovoorts. In de literatuur wordt aangegeven dat het principiële verschil tussen het blokkeren van sites met kinderporno en het blokkeren van sites die andere strafbare content bevatten lastig is.[367] Met betrekking tot terroristische uitingen heeft de minister in dezelfde brief aangegeven dat er vooralsnog niet op terroristische uitingen wordt gefilterd. Dit omdat de ISP's alleen bereid zijn om onmiskenbaar strafbare of onrechtmatige informatie te verwijderen en bij terroristische uitingen het niet altijd *"klip en klaar is dat het om strafbare of onrechtmatige informatie gaat"*.[368] Hieruit kan worden opgemaakt dat bij de overheid wel de bereidheid bestaat om op terroristische uitingen te filteren, maar dat de ISP's hier niet aan willen.

7.1.1.3 Horizontale doorwerking van grondrechten

Grondrechten vinden niet alleen toepassing in de verhouding overheid-burger, maar ook tussen burgers onderling. Dit wordt de horizontale werking van grondrechten genoemd. In de Telecommunicatiewet (Tw) wordt dit uitgedrukt in artikel 18.13. Het doel van artikel 18.13 Tw is niet alleen om zeker te stellen dat het communicatiegeheim van artikel 13 Gw zich uitstrekt tot modernere

[365] Stol e.a. 2008, p. 146.
[366] Stol e.a. 2008, p. 122. Zie ook *Kamerstukken II* 2007-2008, 28 684, nr. 133, p. 14: *"Overigens zal de effectiviteit van maatregelen als ontoegankelijkheidsmaking of filtering bepaald niet altijd succesvol zijn. Zo kan informatie in razendsnel tempo gekopieerd en via andere (minder toegankelijke) kanalen aangeboden worden."*
[367] Bijvoorbeeld: R. van den Hoven van Genderen en A. Lodder, 'Kinderpornosites zijn erg maar censuur is nog erger', *NRC Handelsblad*, donderdag 16 oktober 2008: *"Zo'n maatregel kan bovendien een opstap zijn naar verregaande acties, zoals het blokkeren van sites die terroristische gedachten bevatten of sites waar naar waarschijnlijkheid andere wettelijke voorschriften worden overtreden."*
[368] *Kamerstukken II* 2007/08, 28 684, nr. 133, p. 22.

communicatietechnieken dan de telefoon en de telegraaf, maar vooral om aan te geven dat de aanbieder van een openbare elektronische communicatiedienst (zoals ISP's) in beginsel gehouden is tot naleving van de grondwettelijke norm ten opzichte van de gebruikers van haar dienst.[369]
Bij filteren of blokkeren van kinderporno op internet moet kennis worden genomen van het verkeer en dat is niet toegestaan op grond van artikel 18.3 Tw. De ISP's moeten daarvoor toestemming krijgen van hun gebruikers, net als dat het geval is bij het toepassen van virus en spamfilters. Dit kan via de algemene voorwaarden, aldus de auteurs van het WODC-rapport.[370]

7.1.1.4 De 'oplossing'

In het WODC-rapport komt men tot de conclusie dat filteren op basis van zwarte lijsten die door de overheid aangeleverd worden een formeelrechtelijke grondslag behoeft. De oplossing die aangedragen wordt, is om de samenstelling van de lijst waarop gefilterd wordt aan privaatrechtelijke partijen over te laten. Zo *"blijft de overheid buiten de discussie omtrent overheidscensuur en ook voor het overige zijn er geen juridische complicaties"*.[371] Door in de algemene voorwaarden een beding op te nemen dat het internet wordt gefilterd op kinderporno, kunnen de internetafnemers hieraan gebonden worden. In de brief over de voortgang van kinderpornografie[372] geeft de minister van justitie aan dat er is gewerkt aan het ondersteunen van zelfregulering en van publiek-private samenwerking. Met de direct betrokken partijen is verkend hoe een 'platform internetfiltering kinderporno' gerealiseerd kon worden. In december 2009 is afgesproken dat het Meldpunt Kinderporno op Internet de rol van dit platform op zich neemt. De taken van het meldpunt worden uitgebreid met het produceren van een blacklist die door de Internet Service Providers (ISP's) wordt gebruikt om websites te blokkeren.[373]

Er is weinig informatie voorhanden over de werkwijze van het platform. Uit een niet-vrijgegeven rapport kan ik afleiden dat de ISP's voor ogen hebben dat de

[369] Stol e.a. 2008, p. 46.
[370] Stol e.a. 2008, p. 46.
[371] Stol e.a. 2008, p. 115.
[372] Brief over de voortgang aanpak kinderpornografie 2009, p. 1.
[373] http://www.ecp.nl/kick-off-platform-internetveiligheid-intensievere-samenwerking-overheid-en-marktpartijen-voor-veilig

medewerkers van het platform getraind worden door justitie en politie en pagina's in Nederland niet gefilterd of geblokkeerd worden, omdat opsporing en vervolging door de Nederlandse opsporingsautoriteiten daarvoor mogelijk is. Dit geldt ook voor internetpagina's, die worden aangeboden vanuit landen waar de Nederlandse autoriteiten een rechtshulpverzoek kunnen indienen. De blokkering en filtering heeft dan alleen betrekking op pagina's die vanuit het buitenland worden aangeboden en opsporing en vervolging door de opsporingsautoriteiten niet mogelijk is.[374] Het bevreemt mij dat dit niet in een openbaar rapport of stuk bekend wordt gemaakt. De Nederlandse burger kan er niet vanuit gaan dat inderdaad de bovenstaande werkwijze wordt aangehouden of dat álle pagina's met kinderpornografie geblokkeerd of gefilterd worden, óók als opsporing en vervolging door de opsporingsinstanties mogelijk zijn. Voor zover ik weet zou het ook kunnen dat het Meldpunt Kinderporno alle meldingen van websites waar zich kinderporno op bevindt vluchtig bekijkt en deze vervolgens door ISP's laten blokkeren. Dat lijkt mij een weinig zorgvuldige en kwalijke werkwijze.

Steeds wordt er vanuit gegaan dat de overheid of ISP's kinderporno op internet moeten filteren. Echter, filteren is ook op gebruikersniveau mogelijk. Commerciële filters zijn al lang beschikbaar als een losstaand programma of webbrowser.[375] Van den Hoven van Genderen en Lodder zijn van mening dat een filter op gebruikersniveau geschikter is dan filteren via de ISP, omdat dit geen schending van grondrechten met zich meebrengt. De burger kiest er dan zelf voor om bepaalde informatie buiten de deur te houden.[376] De kans dat men zomaar op kinderporno stuit is erg klein (zie paragraaf 7.1.1.2). Er moet actief gezocht worden op internet om kinderporno te vinden en als men dat wilt kan men simpelweg kiezen zo'n filter niet aan te schaffen of uit te zetten. Het gaat de overheid er juist om alle mensen de toegang tot dit soort materiaal te ontzeggen. In visie van de overheid biedt een dergelijke filter daarom geen oplossing.

[374] Andersson Elffers Felix, 2009, p. 15.
[375] Zie bijvoorbeeld NetNanny (http://www.netnanny.com) en Safesurf (http://www.safesurf.com/)
[376] R. van den Hoven van Genderen en A. Lodder, 'Kinderpornosites zijn erg maar censuur is nog erger', *NRC Handelsblad*, donderdag 16 oktober 2008.

Het is de vraag of het verstandig is te filteren op basis van zwarte lijsten dat door een 'onafhankelijke' instantie wordt samengesteld. Er wordt veel macht gegeven aan het Meldpunt Kinderpornografie op Internet en het probleem van overblocking wordt niet opgelost. Waar het Meldpunt eerst nog slechts een doorgeefluik was, moet het nu beoordelen of een website kinderpornografie bevat en kan het vervolgens bewerkstelligen dat de websites uit het internetverkeer van Nederlandse ISP's gefilterd worden. De Engelse wetenschapper Akdeniz heeft stevige kritiek op de meldpunten. Volgens hem zijn deze private politieorganisaties slecht uitgerust om de illegale inhoud van materiaal op internet te beoordelen en het risico bestaat dat de medewerkers 'zelfbenoemde rechters' worden.[377] Ik onderstreep Aknediz' kritiek op de meldpunten. De medewerkers van de Meldpunten zullen heel goed opgeleid moeten worden om het materiaal goed te kunnen beoordelen. Daarnaast zouden de werkzaamheden van de Meldpunten naar mijn mening ieder jaar gecontroleerd moeten worden. Het probleem van overblocking kan alleen geminimaliseerd worden indien de lijst een paar keer per dag wordt geüpdate en vervolgens ook de ISP's zelf een aantal keren per dag de lijst controleren.[378] Dit zal een arbeidsintensief proces zijn. Bovendien neemt dit nog niet de bezwaren over de effectiviteit weg. In deze scriptie is vastgesteld dat kinderpornografie vaak via peer-to-peer netwerken wordt verspreid en daar heeft deze maatregel geen effect op. Het is naar mijn mening opmerkelijk dat er niet voor de veel fijnmaziger techniek van het filteren op hashcodes is gekozen. Het is een veel effectiever systeem, omdat de techniek al het internetverkeer kan filteren. De uiterlijke kenmerken van het verkeer wordt met deze techniek wel in de gaten gehouden, maar dat gebeurt ook al ter bestrijding van spam en virussen. Het bezwaar van ISP's is dat een dergelijk systeem te kostbaar is.[379] Wellicht wordt een dergelijk systeem wel betaalbaar door subsidieverstrekking van de overheid.

[377] Akdeniz 2008, p. 265.
[378] Zie ook de aanbeveling van ISP's in het rapport van Andersson Elffers Felix, 2009, p. 10.
[379] Andersson Elffers Felix, 2009, p. 9.

7.1.2 De Notice and Take Down (NTD) procedure

Dienstverleners op internet zijn op grond van artikel 15 van de Europese Richtlijn inzake elektronische handel[380] niet aansprakelijk voor gegevensverkeer die zij niet zelf initiëren of inhoudelijk beïnvloeden. De dienstverleners zijn niet verplicht de informatie die op hun servers staan op strafbaar of onrechtmatig materiaal te controleren, maar zij dienen wel in actie te komen indien zij wetenschap hebben of krijgen van het strafbare of onrechtmatige karakter van de informatie die zij hosten. In de praktijk houdt dat in dat het strafbare of onrechtmatige materiaal van de servers verwijderd moet worden als de dienstverleners daar over in kennis worden gebracht. In Nederland is de richtlijn omgezet in de Aanpassingswet richtlijn inzake elektronische handel.[381]

De manier waarop providers omgaan met inhoudelijke klachten over websites die zij hosten heet *notice and take down* (NTD). De provider wordt in kennis gesteld van de illegale informatie (notice) en haalt na haar eigen beoordeling het materiaal offline (take down). NTD vindt plaats als er een wettelijke basis is: de inhoud is onmiskenbaar onrechtmatig. In de algemene voorwaarden van providers staat vaak een NTD-beleid beschreven.[382] Het programma NICC is een publiek-private samenwerking bedoeld om de bestrijding van cybercrime te verbeteren en onderdeel van de ICT uitvoeringsorganisatie (ICTU).[383] In het kader van dit programma is een standaard Notice-and-take-down procedure gecreëerd. De gedragscode is gebaseerd op bestaande gedragscodes bij bedrijven, overheden en andere partijen, zoals KPN, XS4ALL, ISPConnect, Dutch Hosting Provider Association, NLKabel, Ziggo, UPC, CAIW, Zeelandnet en SIDN. Ook ministeries, politie- en opsporingsdiensten en organisaties zoals Marktplaats, eBay en de stichting BREIN hebben meegewerkt aan de totstandkoming van deze gedragscode. Met betrekking tot kinderpornografie op internet biedt een melding van prepuberale kinderporno hier goede mogelijkheden. Er zal weinig twijfel over zijn dat het om onmiskenbaar

[380] 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.
[381] Wet van 13 mei 2004, *Stb.* 2004, 210.
[382] Zie bijvoorbeeld de algemene voorwaarden van Hyves.nl: http://www.hyves.nl/useragreement/ (onderdeel 8).
[383] http://www.ictu.nl/index.php?option=com_frontpage&Itemid=1 (laatst bekeken op 26 januari 2010).

onrechtmatige informatie gaat. Op grond van artikel 4 sub a van de gedragscode kunnen opsporingsambtenaren net als ieder ander een melding van kinderpornografie doen.[384] Daarbij moet wel expliciet vermeld worden dat het geen formeel bevel betreft. In artikel 4 staan de overige eisen aan de melding.
Van den Hoven van Genderen wijst er op dat in de toelichting staat dat ook informatie kan worden verwijderd dat tussenpersonen als ongewenst beschouwen. In de toelichting staat: 'Het staat partijen vrij om daarnaast zelf te bepalen welke informatie als "ongewenst" wordt beschouwd, zonder dat er sprake is van strijd met de wet.' Onduidelijk is hoe deze bepaling zal uitwerken. Van den Hoven van Genderen wijst er op dat het zou kunnen leiden tot zelfcensuur en aanleiding kan vormen voor aansprakelijkheidsprocedures als bepaalde informatie ten onrechte wordt verwijderd.[385] De bepaling tot zelfcensuur acht ik ook onwenselijk. Een NTD-procedure is bedoeld om onmiskenbaar onrechtmatige informatie na een melding te doen verwijderen en levert geen excuus zelfcensuur toe te passen.

7.1.2.1 Artikel 54a Sr

In de situaties waar de NTD-procedure tekortschiet bij de verwijdering van onrechtmatige informatie kan gebruik worden gemaakt van de mogelijkheid om op basis van artikel 54a Sr een bevel tot verwijdering van onrechtmatige gegevens te geven. Hierin staat dat de provider niet vervolgd wordt voor het doorgeven van verboden boodschappen, indien hij voldoet aan het bevel van de officier van justitie nadat deze gemachtigd is door de rechter-commissaris en voldoende maatregelen neemt om die informatie te verwijderen of ontoegankelijk te maken. De inhoudelijke afweging of de informatie strafbaar is wordt hier dus gemaakt door de officier van justitie en de rechter-commissaris; niet meer de ISP. De Minister van Justitie geeft echter aan dat *"in de praktijk is gebleken dat artikel 54a Sr niet vanzelfsprekend een eenvoudig en snel toepasbaar middel is om tot verwijdering van ongewenste of strafbare content te komen."*[386] Dit wordt door de opstellers van een rapport[387] over

[384] De gedragscode is te downloaden op: http://www.samentegencybercrime.nl/UserFiles/File/,DanaInfo=ex01tp+NTD_Gedragscode_Opmaak.pdf (laatst bekeken op 26 januari 2010).
[385] R. van den Hoven van Genderen, 'Notice and take down (NTD-) gedragscode, gewenste censuur?', *Computerrecht* 2008, 202, p. 323.
[386] *Kamerstukken II* 2008/09, 28 684, nr. 232, p. 4 onder verwijzing naar Rb. Assen, *LJN* BD8451.

de grondslag van artikel 54a Sr voor notice-and-take-down beaamd. Bij het verwijderen van materiaal door de ISP, in plaats van de beheerder van de informatie, zal er vaak sprake zijn van bijvangst. Er wordt in dat geval meer dan het ongewenste materiaal ontoegankelijk gemaakt, wat een ongewenste situatie oplevert. De hoeveelheid bijvangst is afhankelijk van de technische mogelijkheden en de hoeveelheid moeite dat gedaan moet worden gedaan om de bijvangst te beperken. Vaak zal een heel domein geblokkeerd worden, wat de complete website inhoudt en alle (niet altijd onrechtmatige inhoud) dat daaronder hangt.[388] Daarnaast wijzen de onderzoekers er op dat het systeem niet altijd effectief is. In het geval van kinderporno ligt het niet voor de hand dat men om principiële redenen vindt dat de informatie 'online' moet blijven, maar wel is bekend dat het materiaal vaak weer opduikt op alternatieve locaties op internet.[389] Het ontoegankelijk maken van informatie leidt bovendien tot een verlies van monitoring-mogelijkheden. Er kan niet meer nagegaan worden wie de informatie bezoekt of welke veranderingen er op de pagina aangebracht worden.[390]

Het belangrijkste knelpunt is, volgens de opstellers van het rapport, dat de wettelijke grondslag voor een NTD-regime onvoldoende is. Ook het offline halen van bestanden op servers levert een inbreuk op de vrijheid van meningsuiting, waarvoor een formeelwettelijke grondslag nodig is. Op basis van tekstuele, wethistorische, wetsystematische en rechtsbeschermingargumenten is het zeer twijfelachtig of artikel 54a Sr als grondslag kan dienen.[391] Artikel 125o Sv wordt in de wetsgeschiedenis genoemd als wetsgrondslag voor het bevel tot ontoegankelijkheidsmaking als bedoelt in artikel 54a Sr, maar het artikel is slechts bruikbaar bij een doorzoeking. Het gaat bovendien in wezen uit van een ontoegankelijkheidsmaking door de officier van justitie of de rechter-commissaris en de ontoegankelijkheidsmaking dient weer opgeheven te worden zodra het belang van strafvordering zich daartegen niet meer verzet. Tenslotte biedt het geen basis

[387] 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, TILT – Centrum voor Recht, Technologie en Samenleving en Cycris – Center for Cybercrime Studies, november 2007.
[388] Schellekens, Koops & Teepe 2007, p. 13.
[389] Stol e.a. 2008, p. 122.
[390] Schellekens, Koops & Teepe 2007, p. 14.
[391] Schellekens, Koops & Teepe 2007, p. 42.

tot een *bevel* aan een derde tot ontoegankelijkheidsmaking.[392] In het rapport wordt dan ook, naar mijn mening terecht, aanbevolen de wet aan te passen. Artikel 54a Sr biedt op dit moment onvoldoende rechtsgrondslag om toegepast te worden.

7.3 Banken, creditcardmaatschappijen en online betalingsdiensten

Eerder is geconstateerd dat het aantal commerciële websites, dat zich bezighoudt met het beschikbaar stellen van kinderpornografie, toeneemt. Het geld om toegang te krijgen tot zo een website kan op verschillende manieren overgemaakt worden. Deze betalingsgegevens kunnen van grote bewijswaarde zijn. Het kan namelijk een aanwijzing opleveren dat iemand zich 'actief met kinderporno' bezig houdt en probeert toegang te verschaffen tot het illegale materiaal.

Eén manier om online betalingen te verrichten is via de creditcard. Dit is zeer populair in de Verenigde Staten, waar het betalen met de creditcard meer gemeengoed is dan in Nederland. In 2006 is in de Verenigde Staten een samenwerkingsverband van creditcardmaatschappijen gecreëerd: de 'Financial Coalition Against Child Pornography'. Zij delen informatie over websites die zich bezighouden met de commerciële exploitatie van kinderpornografie en blokkeren betalingen naar die websites.[393] Nederland neemt ook deel aan een vergelijkbaar initiatief, namelijk het European Financial Coalition (EFC).[394] Nederland draagt bij aan het EFC door de deelname van Nederlandse beleids- en politieambtenaren aan de werkgroep 'Law Enforcement'. Het EFC stelt zichzelf ambitieuze doelen. In het kamerstuk waar over het EFC wordt verteld staat: *"Vanaf september 2010 wil de EFC volledig operationeel zijn in de zin dat dan slachtoffers worden geholpen, daders worden vervolgd, het circuleren van afbeeldingen op het internet wordt verminderd en er van veel concrete samenwerking tussen stakeholders sprake is."*[395]

De kans bestaat dat banken deze gegevens op een presenteerblad aan politiediensten geven indien zij transacties naar bekende kinderpornowebsites zien. In het verleden zijn al vaker creditcardgegevens gebruikt bij de vervolging van kinderpornogebruikers. Dit is onder andere gebeurd in 'Operation Ore'. Operation

[392] Schellekens, Koops & Teepe 2007, p. 43.
[393] O'Donnell & Miller 2007, p. 61.
[394] *Kamerstukken II* 2009/10, 32 123VI, nr. 79, p. 2.
[395] *Kamerstukken II* 2009/10, 32 123VI, nr. 79, p. 2.

Ore is de grootste kinderpornografiezaak van de afgelopen tijd. Tijdens Operation Ore zijn door de FBI 7250 creditcardgegevens doorgegeven aan de Britse autoriteiten. De creditcardhouders zouden hun kaart hebben gebruikt om toegang te verschaffen tot een kinderpornowebsite van het bedrijf Landslide Productions Inc. In het Verenigd Koninkrijk zijn ongeveer 3750 aanhoudingen verricht en in totaal zijn naar schatting 6500 mensen ondervraagd. Honderd en negen kinderen die werden misbruikt, zijn gered tijdens het onderzoek.[396] Gezegd kan worden dat het gebruik van creditcardgegevens dus een nuttig hulpmiddel kan zijn bij het bestrijden van kinderpornografie.

Het probleem is wel dat door grootschalige creditcardfraude we er niet altijd meer van op aan kunnen dat de creditcardgegevens ook daadwerkelijk aan een gebruiker toebehoren. Indien een opsporingsonderzoek tegen mensen over kinderpornografie gestart wordt brengt dat een enorm sociaal stigma met zich mee.

Dit heeft te maken met het feit dat veel mensen pedofielen en kinderpornogebruikers met elkaar verwarren. Naast de straf die opgelegd kan worden voor het bezitten van kinderporno straft de maatschappij hen ook nog eens. Het is niet ongewoon dat kinderpornogebruikers vrienden, familie, status en hun baan verliezen.[397] Dat dit sociale stigma ook op de verdachten drukt, wordt goed geïllustreerd door de gevolgen die Operation Ore had voor sommige mensen. Van de 3750 mensen die in het Verenigd Koninkrijk werden gearresteerd hebben er in totaal 39 zelfmoord gepleegd.[398] In één geval stond een creditcard op naam van een bevelhebber van de Britse luchtmacht, David White, maar op zijn computer werd geen spoor van kinderporno gevonden. Het kan zijn dat David White zelf geen toegang had verschaft tot kinderporno, omdat iemand van zijn creditcard gebruik had gemaakt. Helaas was de commandant één van de mensen die zelfmoord heeft gepleegd.[399] Er moet dus voorzichtig worden om gegaan met creditcardgegevens als basis van een opsporingsonderzoek en wellicht kan het beter slechts als ondersteunend bewijs dienen.

[396] Akdeniz 2008, p. 27.
[397] O'Donnell & Miller 2007, p. 212 en 213.
[398] Akdeniz 2008, p. 26 en 27.
[399] Akdeniz 2008, p. 27.

Met de *e-currency*-bedrijven zoals genoemd in paragraaf 5.1.5 moeten inspanningen worden geleverd voor het verbeteren van de samenwerking. Bedrijven zijn misschien eerder geneigd met het opsporingsonderzoek mee te werken en de benodigde gegevens af te geven, indien er goede verhoudingen bestaan. Hetzelfde geldt voor bedrijven die proxyservers, webmail of opslagruimte (al dan niet op internet) aanbieden.

7.4 Meldpunt Kinderporno op Internet

Kinderporno kan gemeld worden bij het Meldpunt Kinderporno op Internet (dat door een stichting wordt bestuurd) en het meldpunt Cybercrime. Mensen kunnen bij het meldpunt een melding doen van kinderporno op internet, vervolgens beoordeelt het Meldpunt deze meldingen (op grond van instructie van het KLPD) en geeft meldingen van strafbare kinderporno door aan het KLPD of, als het adressen in het buitenland betreft, aan het desbetreffende land. Uit het onderzoek van Lünnemann blijkt dat in 2006 een aantal onderzoeken zijn gestart naar aanleiding van een melding.[400] Sinds kort heeft het Meldpunt ook de taak erbij gekregen om een zwarte lijst op te stellen van websites met kinderpornografie. Dit is al uitgebreid in paragraaf 7.1.1.4 beschreven.

7.5 Hulpverleningsinstanties

Instanties als de Raad van Kinderbescherming en Bureaus Jeugdzorg hebben regelmatig te maken met misbruikte kinderen. Voor zover dat nog niet gebeurt zouden de misbruikte kinderen gevraagd moeten worden of er ook foto's en films van het misbruik zijn gemaakt. Op die manier kan worden voorkomen dat het materiaal eventueel verder wordt verspreid en kan men onderzoeken wie de vervaardigers van de kinderporno zijn.

7.6 Particuliere partijen

Er zijn tal van andere organisaties en individuen die kinderpornografie op internet bestrijden. Op internet hebben zich diverse groepen georganiseerd om kinderporno te bestrijden. Mensen mogen niet zelf kinderporno verzamelen of opzoeken om dat vervolgens aan opsporingsinstanties door te geven. Deze activiteiten constitueren op zichzelf al strafwaardig gedrag op grond van artikel 240b Sr en in het verleden

[400] Lünnemann e.a. 2006, p. 121. Zie ook paragraaf 4.4.2.

zijn mensen veroordeeld ondanks het verweer dat het materiaal 'ter bestrijding van kinderpornografie' verzameld werd.[401] De kans bestaat dat het bewijsmateriaal op een presenteerblaadje aan de politie wordt aangereikt, waarna zij haar opsporingsonderzoek kan starten (de zogenaamde 'silver platter' doctrine). Dit is een onwenselijke gang van zaken, want zo blijft het onduidelijk hoe het bewijsmateriaal bemachtigd is. Het blijft exclusief de taak van opsporingsdiensten kinderporno op te sporen.
De meest bekende groep die zich bezighoudt met de bestrijding van kinderpornografie op internet zijn misschien wel de 'CyberAngels', dat uit meer dan 1000 mensen bestaat en websites, IRC, Usenet patrouilleren op kinderporno. Hackers hebben zich ook georganiseerd in clubs als de 'Phreakers & Hackers Against Child Porn' en de 'Ethical Hackers Against Porn'. Deze groepen zetten zich in om websites en andere diensten waar kinderporno wordt aangeboden niet meer te laten werken.[402] Het onwerkbaar maken van een website door het bijvoorbeeld te 'defacen'[403] of offline te brengen met een (distributed) *denial of service attack* leveren strafbare gedragingen op en zijn daarom niet toelaatbaar.[404]

Interessant is ook de ontwikkeling dat de porno-industrie steeds meer inspanningen verricht om zichzelf te distantiëren van illegale inhoud. In de Verenigde Staten is een samenwerkingsverband opgericht, de 'Association of Sites Advocating Child Protection' (ASACP). Het doel van de organisatie is om kinderporno te bestrijden door sites een certificaat te geven dat aangeeft dat er alleen legale porno wordt aangeboden. Verder willen zij voorlichting over kinderpornografie geven en een meldpunt oprichten voor als er kinderporno op een site wordt aangetroffen.[405]

Tussenconclusie
Door samen te werken met andere partijen kan kinderporno op internet effectiever bestreden worden. Internet service providers spelen hierbij de belangrijkste rol aangezien zij de internetverbinding faciliteren waarmee kinderporno zo gemakkelijk

[401] Zie bijvoorbeeld Rb. Arnhem 20 juli 2009, *LJN* BJ3015.
[402] Wall 2002, p. 172.
[403] De inhoud van een website te wissen en er zelf materiaal op te zetten.
[404] De handelingen zijn strafbaar gesteld in artikel 350a respectievelijk 138b Sr.
[405] http://www.asacp.org/

verspreid en gedownload kan worden. Een effectieve manier om kinderpornografisch materiaal ‘aan de poort’ tegen te houden is door het materiaal uit het verkeer te filteren. Op dit moment gebeurt dit door middel van zwarte lijsten die aan ISP’s en hostingproviders worden verstrekt. Naar aanleiding van die lijst worden domeinnamen geblokkeerd en niet meer aan de gebruiker verstrekt. Onderzoek heeft uitgewezen dat het filteren op domeinnamen het onwenselijke effect van overblocking met zich meebrengt en bovendien niet erg effectief is. Er zijn aanwijzingen gevonden dat het een extra drempel voor gebruikers opwerpt om toegang te krijgen tot kinderporno op internet of dat de maatregel commerciële aanbieders frustreert bij het aanbieden van hun producten. De overheid verschaft weinig transparantie over de werkwijze van het nieuwe platform internetfiltering kinderporno. Aangezien het op gespannen voet staat met de vrijheid van meningsuiting is dat zeer kwalijk. Beter zou zijn om kinderpornografie door middel van hashcodes te filteren. Op die manier wordt alleen kinderporno tegengehouden dat al eens als kinderporno is gekwalificeerd en wordt de verspreiding van kinderpornografie in peer-to-peer netwerken daadwerkelijk ingeperkt. Wel zij opgemerkt dat ook dit systeem niet waterdicht is en het kostbaarder is dan filteren op basis van zwarte lijsten. Een subsidie van de overheid is wellicht noodzakelijk om de filtertechniek mogelijk te maken.

De Notice-and-Take-Down procedure van een dienstverlener kan een positieve bijdrage leveren aan de bestrijding van kinderpornografie. Bij prepuberale kinderpornografie bestaat geen twijfel over het onmiskenbaar onrechtmatige karakter van het materiaal. Echter, het gevaar bestaat dat dienstverleners te makkelijk overgaan tot het verwijderen van materiaal van hun servers en zelfcensuur toepassen. Hier zouden aansprakelijkheidsprocedures uit kunnen voortvloeien. Het bevel tot notice-and-take down van een officier van justitie op grond van artikel 54a Sr heeft op dit moment onvoldoende wettelijke grondslag. Het artikel behoeft aanpassing om toch een bevel tot notice-and-take-down door de officier van justitie mogelijk te maken.

Bij de samenwerking met banken en in het bijzonder creditcardmaatschappijen moet er op gelet worden dat de creditcardgegevens op de juiste naam staan. Het kan wellicht beter dienen als ondersteunend bewijs bij het opsporingsonderzoek.

Bij meldpunten van kinderporno moet opgepast worden dat de medewerkers van deze organisaties niet op de stoel van de rechter gaan zitten. Om overblocking tegen te gaan moeten de zwarte lijsten meerdere keren per dag worden gecontroleerd. Dat is een erg arbeidsintensief proces. Door de belangrijke nieuwe taak dat het Meldpunt heeft gekregen is een jaarlijkse controle op de werkzaamheden raadzaam.

Particuliere groepen of individuen die zich bezig houden met de bestrijding van kinderporno handelen vaak zelf in strijd met de wet. Terecht wordt dit handelen door de rechter afgestraft. Opsporingsdiensten zouden terughoudend moeten zijn in een samenwerking met deze instanties.

Hoofdstuk 8: Conclusie

Kinderporno op internet is meer aanwezig dan ooit en het materiaal wordt steeds grover. De samenleving maakt zich dan ook grote zorgen over kinderpornografie. Onder nationale en internationale politieke druk is de delictsomschrijving van kinderpornografie door de jaren heen enorm uitgebreid. Tevens is de strafmaat van artikel 240b Sr van maximaal drie maanden verhoogd naar maximaal acht jaar. Bij kinderpornografie hoeven zelfs geen echte kinderen meer betrokken te zijn.

Kinderporno is in allerlei soorten voorhanden op internet. Het materiaal heeft zijn fysieke vorm verloren en bestaat op internet slechts uit bits en bytes. Dit heeft tot gevolg dat het materiaal met grote snelheid over het internet wordt verspreid. Vervolgens kan het materiaal gedownload worden en wordt het vaak gecategoriseerd op een harde schijf of andere gegevensdrager. Op deze manier worden hele collecties aangelegd en deze 'verzameldrift' is iets wat veel kinderpornogebruikers met elkaar gemeen hebben.

Op internet bestaan in hoofdlijnen twee verschillende circuits ten aanzien van het verspreiden van kinderporno: commerciële aanbieders met betalende klanten en 'verzamelaars' die onderling materiaal uitwisselen. Beiden circuits brengen nieuw materiaal op de markt. Commerciële vervaardigers doen dit voor financieel gewin en in besloten kinderpornonetwerken wordt het materiaal als ruilmiddel gebruikt. Het is naar mijn mening een terechte prioritering in de Aanwijzing en Richtlijn kinderpornografie om de focus te leggen op deze verspreiders en vervaardigers van kinderporno. Daarnaast wordt een focus gelegd op prepuberale kinderpornografie en extreme vormen van kinderpornografie. Wegens onvoldoende capaciteit en kennis over cybercrime bij het OM en de politie worden echter vooral 'eenvoudige bezitters' vervolgd. Deze praktijk is onwenselijk en kan naar mijn mening als 'dweilen met de kraan open' worden gekwalificeerd.

Kinderpornogebruikers maken in toenemende mate gebruik van anonimiseringstechnieken en technieken ten behoeve van cryptografie en steganografie om buiten het beeld van opsporingsdiensten te blijven. Zij lijken hier succesvol in te zijn. Tevens wordt slim gebruik gemaakt van jurisdictieverschillen teneinde de opsporing te frustreren. Om opsporingsbevoegdheden over de grens in te zetten is een rechtshulpverzoek noodzakelijk. Dit brengt altijd vertraging met zich mee en dat is door de vluchtigheid van gegevens op internet onwenselijk. Het probleem wordt gelukkig voor een deel ondervangen met het 24/7-contactpunt en de mogelijkheid een bevriezingsbevel af te geven teneinde belangrijke gegevens voor bewijsmateriaal veilig te stellen. Met een gezamenlijk opsporingsteam speelt het probleem van de vertraging bij rechtshulp in veel mindere mate.

Opsporingsbevoegdheden kunnen ook op internet toegepast worden. Proactieve opsporing op grond van artikel 3 Polw 1993 is tot zekere hoogte mogelijk, maar gezien de tendens dat steeds meer kinderpornogebruikers gebruik maken van anonimeringstechnieken, versleuteltechnieken, steganografie en van jurisdictieverschillen moeten al snel bijzondere opsporingsbevoegdheden ingezet worden. Verkennend onderzoek is mogelijk, maar het is nog onduidelijk of een techniek als datamining daadwerkelijk een bijdrage kan leveren aan de opsporing van kinderpornogebruikers.
De inzet van bijzondere opsporingsbevoegdheden op internet is vaak goed mogelijk bij de bestrijding van kinderpornografie. Wel lopen opsporingsdiensten soms tegen wettelijke grenzen aan, zoals het verbod op hacken door opsporingsdiensten. Indien de overheid deze bevoegdheid voor opsporingsdiensten mogelijk wilt maken dan moet de bevoegdheid daartoe expliciet in het Wetboek van Strafrecht worden gecreëerd. Het is onduidelijk in hoeverre de IP-tap door opsporingsdiensten wordt ingezet. Wel moet de inzet van een tap waardevolle informatie voor het opsporingsonderzoek opleveren. Daarnaast kan infiltratie in een besloten kinderpornonetwerk door een opsporingsambtenaar belangrijke informatie geven over de organisatiestructuur en het materiaal dat binnen het netwerk wordt uitgewisseld.

Het filteren van internet op grond van zwarte lijsten met domeinnamen is een weinig effectieve methode dat voor relatief veel overblocking zorgt. Het Meldpunt Kinderporno op Internet levert de lijsten aan de ISP's en hostingproviders en haar taak wordt daarmee flink uitgebreid. Hierbij ontstaat het gevaar dat het Meldpunt op de stoel van de rechter gaat zitten. Om dit probleem te ondervangen is een goede training van haar werknemers vereist. Tevens moet de zwarte lijst dagelijks meermaals geüpdate worden om overblocking tegen te gaan. Dit heeft een arbeidsintensief proces tot gevolg. Tevens zou ter controle jaarlijks een audit uitgevoerd moeten worden. Dit neemt het bezwaar nog niet weg dat filteren op basis van zwarte lijsten weinig effectief is. Er zijn in het WODC-onderzoek van 2008 geen aanwijzingen gevonden dat de maatregel een drempel opwerkt voor kinderpornogebruikers om aan het materiaal te komen of dat producenten van kinderpornografie het materiaal minder makkelijk kunnen aanbieden.

De Notice-and-Take-Down procedure is wellicht alleen geschikt voor prepuberale kinderporno. Bij dit materiaal is namelijk sprake van onmiskenbaar onrechtmatig materiaal. Opsporingsambtenaren kunnen net als een ieder een melding maken en een beroep doen op de NTD procedure van een communicatieaanbieder. Na toetsing kan het materiaal van de servers worden gehaald.
De NTD procedure werkt misschien zelfcensuur in de hand en er bestaat een kans op een toename van aansprakelijkheidsprocedures wegens het onrechtmatig verwijderen van legaal materiaal. Een NTD bevel van de officier van justitie op basis van artikel 54a Sr biedt op dit moment onvoldoende grondslag om rechtsgeldig te zijn.

Het stimuleren van de samenwerking van opsporingsinstanties met privaatrechtelijke instanties creëert mogelijkheden voor de bestrijding van kinderpornografie. Goede relaties kunnen de toepassing van opsporingsbevoegdheden wellicht vergemakkelijken. Ten aanzien van het gebruik van creditcardgegevens dienen de opsporingsinstanties terughoudend te zijn aangezien men er niet zeker van kan zijn dat er niet met de creditcardgegevens door derden is gefraudeerd. Het kan wellicht beter als ondersteunend bewijs dienen.

Particulieren die zich bezig houden met de bestrijding van kinderpornografie handelen zelf vaak ook in strijd met de wet. Opsporingsdiensten dienen in hun samenwerking met hen terughoudend te zijn. De opsporing van kinderpornografie dient bij de opsporingsinstanties te blijven.

In mijn scriptie zijn enkele aanbevelingen naar voren gekomen. Deze zijn als volgt:

1. Een andere werkwijze vergt meer kennis over cybercrime bij de politie en het OM en meer capaciteit teneinde verspreiders en vervaardigers op te sporen en te vervolgen. Het is bekend dat een verzamelaar vaak aan zijn materiaal komt door afbeeldingen en filmpjes uit te wisselen. Door niet met beperkt digitaal onderzoek genoegen te nemen maar verder te rechercheren kunnen ook verspreiders van kinderpornografie vervolgd worden. Dit kost meer capaciteit en er zullen minder zaken afgehandeld worden, maar het is veel effectiever en dat weegt op tegen de nadelen. Tevens zullen er zaken geseponeerd moeten worden die volgens de Aanwijzing en Richtlijn kinderpornografie minder prioriteit krijgen. Dit is een noodzakelijk kwaad om kinderpornografie beter te bestrijden.

2. In de loop der jaren is kinderpornografie uitgegroeid tot een ernstig misdrijf met een internationale dimensie, waarbij soms de georganiseerde misdaad in het spel is. Vanwege de vaak (technisch) complexe zaken en internationale dimensie van het probleem zou naar mijn mening kinderpornografie ondergebracht moeten worden bij het takenpakket van het Landelijk Parket van het Openbaar Ministerie. Er kunnen dan meer landelijke opsporingsonderzoeken naar commerciële verspreiders en besloten kinderpornonetwerken gestart worden.

3. Binnen gezamenlijke opsporingsteams is een vrije uitwisseling van informatie mogelijk. Tevens mogen alle leden van het team informatie verzoeken en verkrijgen van hun eigen autoriteiten. In het opsporingsteam kunnen ook derden zoals de Verenigde Staten of Rusland deelnemen. Het internationale karakter van het team is ideaal voor de grensoverschrijdende opsporing van kinderpornografie. De deelname

van Nederland aan gezamenlijke opsporingsteams dient daarom gestimuleerd te worden.

4. Opsporing naar georganiseerde verbanden bieden bepaalde voordelen ten opzichte van ‘gewone opsporing’. Men kan een criminele organisatie onderzoeken en de omvang, structuur, leden en criminele activiteiten in beeld brengen, zonder dat een concrete verdenking ten aanzien van een van de leden van het veronderstelde verband hoeft te bestaan. Vroegsporing biedt de mogelijkheid een groep van vervaardigers van kinderpornografie in kaart te brengen en uiteindelijk die verdachten te vervolgen die het meest van belang zijn. Dat kunnen bijvoorbeeld diegenen zijn die daadwerkelijk de kinderen misbruiken, diegenen die het materiaal online beschikbaar stellen of de organisatie in stand houden. Het levert daadwerkelijk een effectieve aanslag op aan de organisatiestructuur en kinderen worden hiermee uiteindelijk beschermt tegen uitbuiting door de criminele organisatie. Er wordt in de praktijk maar weinig gebruik gemaakt van vroegsporing. Het behoeft daarom aanbeveling hier in de toekomst meer gebruik van te maken.

5. Het filteren op hashwaarden biedt een goed alternatief op de huidige filterpraktijk. Het is veel fijnmaziger dan het filteren op domeinnamen. Bovendien kan het verkeer in peer-to-peer netwerken gefilterd worden wat daadwerkelijk de verspreiding van kinderpornografie frustreert. De meeste ISP’s vinden deze techniek echter te duur. Het geven van subsidie door de overheid biedt wellicht een oplossing.

De bovengenoemde maatregelen zullen geld kosten, maar gezien de consensus in de samenleving en de overheid dat kinderpornografie zo effectief mogelijk aangepakt moet worden zie ik niet in waarom dit extra geld niet beschikbaar kan worden gesteld.

Slim gebruik van techniek en jurisdictieproblemen mogen er niet toe leiden dat er alleen ‘eenvoudige downloaders’ vervolgd worden. Het officiële beleid is dan ook meer prioriteit te geven aan verspreiders en vervaardigers van kinderporno. Het wordt tijd naar dit beleid te handelen.

Literatuurlijst

Boeken:

Akdeniz 2008
Y. Akdeniz, *Internet Child Pornography and the Law, National and International Responses*, Ashgate 2008.

Britz 2009
M.T. Britz, *Computer forensics and cyber crime: an introduction,* tweede druk, Upper Saddle River NJ: Pearson 2009.

Bryant 2008
R. Bryant e.a., *Investigating Digital Crime*, Chichester: Wiley 2008.

Buruma 2001
Y. Buruma, *Buitengewone opsporingsmiddelen*, tweede druk, Deventer: Tjeenk Willink 2001.

Cleiren & Nijboer 2007
C.P.M. Cleiren, J.F. Nijboer, *Tekst & Commentaar,* Strafrecht, zevende druk, Deventer: Kluwer 2007.

Cleiren & Nijboer 2008
C.P.M. Cleiren, J.F. Nijboer, *Tekst & Commentaar,* Strafvordering, achtste druk, Deventer: Kluwer 2008.

Corstens 2008
G.J.M. Corstens, *Het Nederlands strafprocesrecht*, zesde druk, Deventer: Kluwer 2008.

Casey 2004
E. Casey, *Digital Evidence and Computer Crime, Forensic science, computers and the Internet,* tweede druk, San Diego: Elsevier Academic Press 2004.

Dasselaar 2008
A. Dasselaar, *Handboek digitale criminaliteit, over daders, daden en opsporing,* tweede druk, Culemborg: Van Duuren Media B.V. 2008.

De Hullu 2009
J. de Hullu, *Materieel strafrecht*, vierde druk, Deventer: Kluwer 2009.

Ferraro & Casey 2005
M.M. Ferraro, E. Casey, *Investigating Child Exploitation and Pornography, the internet, the law and forensic science*, Burlington: Elsevier Academic Press 2005.

Frances 2000
A. Frances, *Diagnostic and Statistical Manual of Mental Disorders*, vierde druk, Washington DC: American Psychiatric Association 2000.

Franken, Kaspersen & de Wild 2004
H. Franken, H.W.K. Kaspersen & A.H. de Wild, *Recht en Computer*, vijfde druk, Deventer: Kluwer 2004.

Gillespie 2008
A. Gillespie, *Child exploitation and communication technologies,* Dorset: Russell House Publishing 2008.

Holmes & Holmes 2009
S. Holmes, R. Holmes, *Sex Crimes: Patterns and Behavior*, derde druk, Thousand Oaks: Sage Publications 2009.

Jenkins 2001
P. Jenkins, *Beyond Tolerance, child pornography on the internet*, New York: New York University Press 2001.

Kaspersen 2007
H.W.K. Kaspersen, 'Het Cybercrime-verdrag van de Raad van Europa', in: Koops e.a. 2007, p. 137-142.

Klip 2009
A.H. Klip, *European Criminal Law, An Integrative Approach*, Ius Communitatis Series, tweede druk, Antwerp-Oxford-Portland: Intersentia 2009.

Kool 1999
R.S.B. Kool, *De strafwaardigheid van seksueel misbruik*, Sanders Instituut, Deventer: Gouda Quint 1999.

Koops e.a. 2007
B.J. Koops, *Strafrecht en ICT*, Monografieën recht en informatietechnologie, deel 1, tweede druk, Den Haag: Sdu Uitgevers 2007.

Koops & Buruma 2007
B.J. Koops, Y. Buruma, 'Formeel strafrecht en ICT', in: Koops e.a. 2007, p. 77-119.

Koops & De Roos 2007
B.J. Koops, Th.A. de Roos, 'Materieel strafrecht en ICT', in: Koops e.a. 2007, p. 23-73.

Melai & Groenhuijsen 2003
A.H. Klip, Inleidende opmerkingen, in: A.L. Melai & M.S. Groenhuijsen e.a., *Het wetboek van strafvordering, internationale en interregionale samenwerking in strafzaken* (Klip, Swart & Van der Wilt), Deventer: Kluwer 2003.

O'Donnell & Miller 2007
I. O'Donnel & C. Miller, *Child Pornography, Crime, Computers and Society*, Willen Publishing 2007

Stephenson 2000
P. Stephenson, *Investigating Computer-Related Crime*, Boca Raton: CRC Press 2000.

Taylor & Quayle 2003
M. Taylor & E. Quayle, *Child pornography: an internet crime*, Hove: Brunner-Routledge 2003.

Wall 2002
D.S. Wall, *Crime and the Internet*, London: Routledge 2002.

Warren & Streeter 2005
P. Warren & M. Streeter, *Cyber Alert, how the world is under attack from a new form of crime,* London: Vision Paperbacks 2005.

Rapporten:

Andersson Elffers Felix 2009
Publiekprivate bestrijding van kinderporno op internet, e*en oplossingsrichting,* GJ146/007a.rapportage verkenning, Utrecht 2009.
(http://wikileaks.org/leak/publiekprivate-bestrijding-van-kinderporno-op-internet.pdf)

Commissie de Melai 1980
A. Melai, *Eindrapport van de Adviescommissie Zedelijkheidswetgeving*, 's-Gravenhage: Staatsuitgeverij 1980.

Gerkens e.a. 2009
A. Gerkens, P. Smeets, F. Teeven en N. van Vroonhoven-Kok, *Auteursrechten, een rapport,* 's-Gravenhage 2009.
(http://www.tweedekamer.nl/images/Eindrapport_parlementaire_werkgroep_auteursrechten_118-189136.pdf)

Jaarverslag Meldpunt Kinderporno 2008
Stichting Meldpunt ter bestrijding van Kinderpornografie op Internet, *Jaarverslag 2008*, Amsterdam 2009.
(http://www.meldpunt-kinderporno.nl/files/Biblio/Meldpunt%20Kinderporno%20jaarverslag%202008.pdf)

Korpsmonitor Kinderporno 2009
D. Janssen & P. Reijnders, *Stand van zaken 2009, Korpsmonitor Kinderporno, Landelijk beeld*, versie 1.1., 18 november 2009. (http://parlis.nl/blg22480)

Krommendijk, Terpstra & van Kempen 2009
M. Krommendijk, J. Terpstra, P.H. van Kempen, *De Wet BOB: Titel IVa en V in de praktijk. Besluitvorming over bijzondere opsporingsbevoegdheden in de aanpak van georganiseerde criminaliteit*, Den Haag: Boom Juridische uitgevers 2009.

Lünnemann e.a. 2006
K. Lünnemann e.a. *Kinderen beschermd tegen seksueel misbruik*, *evaluatie van de partiële wijziging in de zedelijkheidswetgeving*, Utrecht: Verwey-Jonker Instituut 2006.

Oosterink & van Eijk 2006
Oosterink en Van Eijk, *Opsporing Kinderpornografie op internet*. *Een statusoverzicht,* Den Haag: Ministerie van Justitie 2006.

Savornin Lohman e.a. 1999
J. de Savornin Lohman e.a., *Wetgeving Gewogen, Evaluatie van wet- en regelgeving inzake kinderpornografie*, Utrecht: Verwey-Jonker Instituut 1999.

Schellekens, Koops & Teepe 2007.
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, TILT – Centrum voor Recht, Technologie en Samenleving en Cycris – Center for Cybercrime Studies 2007.
(http://www.cycris.nl/uploads/NTD-54a_rapport_--_30_november_2007.PDF)

Stol e.a. 2008
W.Ph. Stol e.a. *Filteren van kinderporno op internet*, *een verkenning van technieken en reguleringen in binnen- en buitenland*, WODC, Den Haag: Boom Juridische uitgevers 2008.

Stol, Treeck & van der Ven 1999.
W.Ph. Stol, R.J. van Treeck, A.E.B.M. van der Ven, *Criminaliteit in cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland.* Den Haag: Elsevier bedrijfsinformatie bv 1999.

Van der Hulst & Neve 2008
R.C. van der Hulst, R.J.M. Neve, *High-tech crime, soorten criminaliteit en hun daders*, WODC, Meppel: Boom Juridische Uitgevers 2008.

Verbeterprogramma Kinderporno 2008
Politie, landelijk project kinderporno, *Verbeterprogramma Kinderporno*, *op beeld vastgelegd seksueel misbruik van kinderen* 2008.
(http://ikregeer.nl/document/BLG19370)

Artikelen:

Alexander 2002
M. Alexander, 'The First Amendment and problems of political viability: The case of Internet pornography', *Harvard Journal of Law and Public Policy*, 2002, 25(3), p. 977-1030.

Boek 2000
J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, p. 589-593.

Buruma 2002
Y. Buruma, 'Een sleutelbegrip binnen de Wet Bijzondere Opsporingsbevoegdheden', *NJCM-Bulletin* 2002, p. 649-658.

Biddle ea. 2002
P. Biddle, P. England, M. Peinado, B. Willman, 'The Darknet and the Future of Content Distribution', *Microsoft* 2002.
(http://reference.kfupm.edu.sa/content/d/a/the_darknet_and_the_future_of_content_di_152722.pdf)

Groeneveld 2000
C.S. Groeneveld, 'Kinderporno en ontuchtzaken, problemen bij de opsporing', *Justitiële verkenningen* 2000, (6), p. 78-88.

Koops & Bekkers 2007
B.J. Koops R. Bekkers, 'Interceptability of telecommunications: is US and Dutch law prepared for the future?', *Telecommunications Policy* 2007, (31), p. 45-67.

Leukfeldt, Domenie & Stol 2009
E.R. Leukfeldt, M.M.L. Domenie, W.Ph. Stol, 'Cybercrime in Nederland: verspreiding van kinderporno en haat zaaien', *Tijdschrift voor Politie* 2009, (71), p. 25-28.

McCoy e.a. 2007
D. McCoy, K. Bauer, D. Grunwald, P. Tabriz, D. Sicker, 'Shining Light in Dark Places: A Study of Anonymous Network Usage', University of Colorado 2007.
(http://www.cs.colorado.edu/department/publications/reports/docs/CU-CS-1032-07.pdf)

Mac Gillavry 2001
E. Mac Gillavry, 'De voorstellen van de Commissie-Mevis: dwangmiddelen in de informatiemaatschappij', *NJB* 2001, (30), p. 1411-1418.

Murdoch & Danezis 2005
S.J. Murdoch, G. Danezis, 'Low-Cost Traffic Analysis of Tor', University of Cambridge, 2005. (http://www.cl.cam.ac.uk/~sjm217/papers/oakland05torta.pdf)

Popescu, Crispo & Tanenbaum 2004
B.C. Popescu, B. Crispo, A.S. Tanenbaum, 'Safe and Private Data Sharing with Turtle: Friends Team-Up and Beat the System', Vrije Universiteit, 2004. (http://www.cs.vu.nl/~ast/publications/sec_prot-2004.pdf)

Rimm 1995
Marty Rimm, 'Marketing pornography on the information superhighway', *Georgetown Law Journal* 1995, (83), p. 1839-1934.

Stevens & Koops 2009
L. Stevens & E.J. Koops, 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', *DD* 2009, (51), p. 669-696.

Stol 2004
W.Ph. Stol, 'Trends in Cybercrime', *Justitiële verkenningen* 2004, (8), p. 76-94. (http://www.wodc.nl/images/jv0408_artikel_06_tcm44-58339.pdf)

Stol e.a. 2008, *Ars Aequi*
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. 531-540.

Thoonen 2009
E.C.M. Thoonen, 'Bezit van digitale kinderpornografie', *NJB* 2009, (84), p. 2117-2122.

Van den Hoven van Genderen 2008
R. van den Hoven van Genderen, 'Notice and take down (NTD-) gedragscode, gewenste censuur?', *Computerrecht* 2008, (202), p. 323.

Van den Hoven van Genderen 2009
R. van den Hoven van Genderen, 'Inzet kinderpornofilmpjes door politie in strijd tegen kinderporno, aanvaardbaar?', 2009. (http://jurel.nl/2009/06/10/inzet-kinderpornofilmpjes-door-politie-in-strijd-tegen-kinderporno-aanvaardbaar/)

Van der Neut 2000
J.L. van der Neut, 'Kinderpornografie. De situatie in Nederland', *DD* 2000, (30), p. 108-149.

Overig:

Beleidsstukken

Aanwijzing kinderpornografie 2007
Aanwijzing kinderpornografie (artikel 240b WvSr), *Stcrt*. 2007 – 162.

Richtlijn kinderpornografie 2007
Richtlijn kinderpornografie, College van procureurs-generaal, *Stcrt*. 2007, 79.

Brief over de voortgang aanpak kinderpornografie 2009
Brief over de voortgang aanpak van kinderpornografie, Minister van Justitie, 4 juni 2009, kenmerk: DDS 5601454/09.

ITeR-publicaties:

Eshof e.a. 2002
G.L.M. van den Eshof, P.H.M. Spronck, G. Boers, J.P.G.M. Verbeek, H.J. van den Herik, *Opsporing van verborgen informatie*, 's-Gravenhage: Sdu Uitgevers, 2002 (ITeR-Reeks, nr. 56).

Kolkman, van Kralingen & Nouwt 2000
P. Kolkman, R. van Kralingen, S. Nouwt, *Privacy in bits en bytes. Privacyaspecten van electronic monitoring in netwerkomgevingen*, 's-Gravenhage: Sdu Uitgevers 2000 (ITeR-reeks, nr. 38).

Koops 2000
B.J. Koops *Verdachte en ontsleutelplicht: hoe ver reikt nemo tenetur?,* Deventer: Kluwer, 2000 *(*ITeR-Reeks, nr. 31).

Koops, Schooten & Prinsen 2006
B.J. Koops, H. van Schooten, M. Prinsen, *Recht naar binnen kijken, Een toekomstverkenning van huisrecht, lichamelijke integriteit en nieuwe opsporingstechnieken,* 's-Gravenhage: Sdu 2004 (ITeR-Reeks, nr. 80).

Schermer 2003
B.W. Schermer, *Opsporing vs. privacy in peer-to-peer netwerken*, 's-Gravenhage: Sdu 2003 (ITeR-reeks nr. 64).

Siemerink 2000
L. Siemerink, *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het internet*, Deventer: Kluwer 2000 *(*ITeR-Reeks, nr. 30).

Sietsma 2006
R. Sietsma, *Gegevensverwerking in het kader van de opsporing, toepassing van datamining ten behoeve van de opsporingstaak: afweging tussen het opsporingsbelang en het recht op privacy*, 's-Gravenhage: Sdu 2006 (*ITeR-Reeks*, nr. 80).

Dissertaties:

Schermer 2007
B.W. Schermer, *Software Agents, Surveillance, and the Right to Privacy. A legislative Framework for Agent-enabled Surveillance,* (diss. Leiden), Leiden UP 2007.

T. Cocx 2009
T. Cocx, *Algorithmic Tools for Data-Oriented Law Enforcement*, (diss. Leiden), Universiteit Leiden 2009.
(https://openaccess.leidenuniv.nl/bitstream/1887/14450/5/thesis.pdf).

Scripties:

Seeger 2008
M. Seeger, *The current state of anonymous file-sharing*, Hochschule der Medien Stuttgart 2008. (http://www.marc-seeger.de/wp-content/uploads/2008/07/thesis-the-current-state-of-anonymous-filesharing.pdf).

Bijlage

Rechtspraak met betrekking tot artikel 240b Sr

Zaak	Datum	Bezit, verspreiding of vervaardiging?	Opgelegde straf
Rb. Zutphen, LJN: BK6967	17-12-2009	bezit	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Den Bosch, LJN: BK6830	17-12-2009	bezit	120 uur taakstraf + 6 maanden voorwaardelijk
Rb. Den Haag, LJN: BK8406	9-12-2009	bezit (vrijspraak) + stalking	240 uur taakstraf
Rb. Den Bosch, LJN: BK6547	9-12-2009	bezit (vrijspraak)	vrijspraak
Rb. Rotterdam, LJN: BK6022	9-12-2009	bezit (paar miljoen) + verspreiding + vervaardiging	3 jaar + TBS
Rb. Zutphen, LJN: BK5956	9-12-2009	bezit (vrijgesproken, geen pv huiszoeking)	vrijspraak
Rb. Zutphen, LJN: BK4958	1-12-2009	vervaardiging + ontuchtelijke handelingen	24 maanden (waarvan 8 voorwaardelijk)
Rb. Utrecht, LJN: BG5250	14-11-2009	bezit	12 maanden (waarvan 6 voorwaardelijk)
Rb. Zutphen, LJN: BK3742	18-11-2009	bezit	4 maanden (voorwaardelijk) + 240 uur taakstraf
Rb. Zutphen, LJN: BK3748	18-11-2009	bezit (vrijspraak)	vrijspraak
Rb. Den Haag, LJN: BK2800	9-11-2009	bezit	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Zutphen, LJN: BK2052	4-11-2009	bezit	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Almelo, LJN: BK1906	3-11-2009	bezit + verspreiding + vervaardiging	10 maanden + TBS
Rb. Arnhem, LJN: BK1743	2-11-2009	bezit	9 maanden (4 voorwaardelijk)
Rb. Zwolle, LJN: BK7258	28-10-2009	bezit (temporary internet files) + ontuchtige handelingen (vrijspraak	240 uur taakstraf + 2790 euro boete
Rb. Middelburg, LJN: BK4618	26-10-2009	bezit	2 weken gevangenisstraf (1 voorwaardelijk)
Rb. Groningen, LJN: BK1004	22-10-2009	Bezit (duizenden afbeeldingen)	6 maanden (3 voorwaardelijk)
Rb. Zutphen, LJN: BK0673	20-10-2009	Bezit (23 afbeeldingen) + ontuchtige handelingen (niet bewezen)	4 weken gevangenisstraf
Rb. Haarlem, LJN: BJ9558	6-10-2009	bezit + ontuchtige handelingen	36 maanden, waarvan 24 maanden voorwaardelijk
Rb. Assen, LJN: BJ8750	29-9-2009	bezit	*voorwaardelijke taakstraf*
Rb. Almelo, LJN: BJ8494	18-9-2009	bezit + ontuchtige mishandeling (jongen 18, meisje 15)	90 dagen gevangenisstraf
Rb. Roermond, LJN: BJ7130	8-9-2009	bezit + ontuchtige handelingen	onvoorwaardelijke gevangenisstraf van 5 jaar
Hof Arnhem, LJN: BJ3736	24-7-2009	bezit (+ 14a, 14b, 14c, 24c, 36f, 57, 246, 248a Sr en 284 Sr. en 13 en 55 Wet wapen en munitie)	2 jaar, 1 jaar voorwaardelijk + geldboete
Rb. Arnhem, LJN: BJ3015	20-7-2009	bezit	twee maanden gevangenisstraf
Rb. Den Haag, LJN: BJ2290	10-7-2009	bezit + seksueel misbruik	9 jaar
Rb. Dordrecht, LJN: BJ2120	9-7-2009	bezit + ontuchtige handelingen	240 uur taakstraf +voorwaardelijke gevangenisstraf
Rb. Zutphen, LJN: BJ1986	8-7-2009	bezit	gevangenisstraf van 213 dagen met bijzondere voorwaarden (o.a. niet in bezit hebben van computer zonder toestemming)

Rb. Maastricht, LJN: BJ7654	6-7-2009	bezit	60 uur taakstraf + 15 dagen hechtenis
Hof Amsterdam, LJN: BJ3549	6-7-2009	bezit	6 (zes) maanden.
Rb. Amsterdam, LJN: BJ8160	3-7-2009	bezit	6 (zes) maanden met proeftijd van 2 jaar
Rb. Assen, LJN: BJ9624	26-6-2009	bezit + seksueel misbruik	van vijf jaren
Hof Den Bosch, LJN: BI9150	23-6-2009	bezit	12 maanden gevangenis,10 maanden voorwaardelijk
Rb. Roermond, LJN: BJ0054	23-6-2009	bezit	taakstraf 180 uur + 6 maanden voorwaardelijk
Rb. Middelburg, LJN: BJ1799	17-6-2009	bezit	één jaar gevangenisstraf
Rb. Rotterdam, LJN: BI7331	10-6-2009	bezit (miljoenen afbeeldingen) + vervaardiging	heropening voort horen van gedragsdeskundigen
Rb. Dordrecht, LJN: BI3715	12-5-2009	bezit + verspreiden	gevangenisstraf van twaalf (12) maanden;
Hof Den Haag, LJN: BI2591	28-4-2009	bezit + ontuchtige handelingen	2 jaar gevangenisstraf
Rb. Leeuwarden, LJN: BI2330	23-4-2009	bezit + ontuchtige handelingen	430 dagen gevangenisstraf
Rb. Roermond, LJN: BI0806	10-4-2009	bezit + vervaardiging (+ telen hennep)	geldboete € 2.500,--,
Rb. Roermond, LJN: BI0763	10-4-2009	bezit	1 maand gevangenisstraf
Rb. Zutphen, LJN: BI0514	8-4-2009	bezit + productie	3 maanden + taakstraf van 200 uur
Rb. Utrecht, LJN: BI6339	7-4-2009	bezit	twee maanden
Rb. Almelo, LJN: BI0302	7-4-2009	bezit + misbruik	3 jaar
Rb. Leeuwarden, LJN: BH9199	26-3-2009	bezit + verspreiden	zes maanden
Rb. Dordrecht, LJN: BH5894	12-3-2009	bezit + ontuchtige handelingen	42 maanden
Rb. Breda, LJN: BH4358	2-3-2009	bezit en/of verspreiding	vrijspraak
Rb. Zutphen, LJN: BH4287	27-2-2009	bezit en verspreiden (peer-to-peer)	drie maanden voorwaardelijk + 180 uur taakstraf
Rb. Utrecht, LJN: BH4911	26-2-2009	bezit + ontuchtige handelingen	gevangenisstraf 12 maanden
Rb. Alkmaar, LJN: BH3936	24-2-2009	productie + ontuchtige handelingen	4 jaar + TBS
Hof Arnhem, LJN: BH3872	24-2-2009	productie + ontuchtige handelingen	2 jaar gevangenisstraf
Rb. Assen, LJN: BH3902	24-2-2009	bezit	zes maanden
Rb. Zwolle, LJN: BH4052	19-2-2009	bezit (hoofdzakelijk 14-17 jaar) + bedreiging	taakstraf 180 uur + 2 maanden voorwaardelijk
Rb. Rotterdam, LJN: BH2361	9-2-2009	bezit	vrijspraak, niet voldaan aan 'seksuele gedraging')
Rb. Utrecht, LJN: BH6465	6-2-2009	bezit + productie + ontuchtige handelingen	4 jaar
Rb. Rotterdam, LJN: BH1711	2-2-2009	bezit	zes maanden
Rb. Middelburg, LJN: BH1254	29-1-2009	bezit	vier maanden en een taakstraf van 240 uren
Rb. Den Bosch, LJN: BH0895	27-1-2009	bezit	vrijspraak
		(niet bewust dat bestanden opgeslagen werden in "lost folders" en "unallocated folders")	
Rb. Den Haag, LJN: BH0749	23-1-2009	bezit	180 uur taakstraf + een geldboete van € 2.500
Rb. Den Bosch, LJN: BH0634	23-1-2009	bezit + ontuchtige handelingen	266 dagen gevangenisstraf + 180 uur taakstraf
Rb. Amsterdam, LJN: BH0528	21-1-2009	bezit + productie + ontuchtige handelingen	5 jaar en 3 maande
Rb. Almelo, LJN: BG8556	30-12-2008	bezit verspreiding via chat en andere delicten	achttien maanden
Rb. Den Bosch, LJN: BG9138	24-12-2008	bezit en verspreiding (via chat) (niet bewezen)	12 maanden + 84 jarige verdachte

Rb. Assen, LJN: BG9649	25-11-2008	bezit	drie maanden
Rb. Roermond, LJN: BG7851	22-12-2008	bezit	niet ontvankelijk
Rb. Utrecht, LJN: BG9937	8-12-2008	bezit + verspreiding + misbruik geestelijke gehandicapte.	zes maanden
Rb. Den Bosch, LJN: BG6094	5-12-2008	productie + verkrachting	30 maanden
Rb. Utrecht, LJN: BG6736	5-12-2008	bezit	2 maanden
Rb. Den Haag, LJN: BG6090	4-12-2008	bezit + productie (film met naakt 'jumpende' jongens)	gevangenisstraf 20 maanden
Rb. Zwolle, LJN: BG9239	2-12-2008	bezit (voorwaardelijk opzet) bijvangst, + 57 Sr	12 maanden
Rb. Utrecht, LJN: BG5730	1-12-2008	bezit + ontuchtige handelingen	12 maanden
Rb. Den Bosch, LJN: BG5404	26-11-2008	bezit	180 uur taakstraf + 6 maanden voorwaardelijk
Rb. Assen, LJN: BG9649,	25-11-2008	bezit	3 maanden gevangenisstraf
Rb. Roermond, LJN: BG4667	19-11-2008	bezit (4 afbeeldingen) + aanranding	12 maanden
HR, LJN: BF0170	18-11-2008	voldoende is "jonger ogen dan 16 jaar", geen tegenbewijs	n.v.t.
Rb. Leeuwarden, LJN: BG3632	30-10-2008	bezit + verspreiden (via mobiele telefoon)	jeugddetentie voor de duur van vier weken.
Rb. Den Bosch, LJN: BG3640	29-10-2008	bezit (voorwaardelijk opzet) (2 filmpjes)	voorwaardelijke taakstraf van 30 uur
Rb. Dordrecht, LJN: BF8894	14-10-2008	bezit + ontucht + wet wapen en munitie	36 maanden
Rb. Utrecht, LJN: BG1602	8-10-2008	bezit	2 maanden
Rb. Arnhem, LJN: BF7318	8-10-2008	bezit + ontuchtige handelingen	3 jaar
HR, LJN: BD4872,	30-9-2008	kennelijke leeftijd,	n.v.t.
Rb. Utrecht, LJN: BF5186	25-9-2008	bezit + ontucht	4 jaar
Rb. Zwolle, LJN: BF1783	11-9-2008	bezit + ontucht	18 maanden
Rb. Assen, LJN: BF0526	9-9-2008	bezit	12 maanden
Rb. Arnhem, LJN: BF0094	9-9-2008	bezit	3 maanden
Rb. Zwolle, LJN: BE9444	19-8-2008	bezit + vervaardigen	12 maanden
Rb. Arnhem,LJN: BE0049	14-8-2008	bezit + ontucht geestelijk en lichaamlijk gehandicapte	proeftijd 5 jaar wegens behandeling
Rb. Haarlemn, LJN: BD8449	24-7-2008	bezit + 138a, 246, 247, heimelijk filmen d.m.v. webcam	30 maanden
Rb. Zwolle, LJN: BE9345	17-7-2008	bezit + ontuchtige handelingen	24 maanden
Hof Den Haag, LJN: BF3925	11-7-2008	bezit	geen straf (gelet op lange duur proces en gevolgen privé-leven)
Rb. Assen, LJN: BD7143	8-7-2008	bezit + bedreiging	vier maanden.
Rb. Roermond, LJN: BD6047	2-7-2008	bezit + ontucht	4 jaar
HR, LJN: BC8645	1-7-2008	term “afbeelding van een seksuele gedraging” onvoldoende feitelijke betekenis	
Rb. Arnhem, LJN: BD5618,	27-6-2008	bezit en 248a	24 maanden
Hof Den Haag, LJN: BD9061	27-6-2008	bezit	*100 uur taakstraf*
Rb. Assen, LJN: BD7138	27-6-2008	bezit (één foto)	voorwaardelijke gevangenisstraf van 1 maand
Rb. Den Bosch, LJN: BD3643	18-6-2008	bezit + verspreiding, vrijgesproken verkrachting	4 jaar
Rb. Den Haag, LJN: BD4321	17-6-2008	bezit + productie + ontucht (40a, 240b, 245 en 249)	42 maanden

Rb. Leeuwarden, LJN: BD3768	12-6-2008	bezit + ontucht + verkrachting + aanranding,	1 jaar
Rb. Middelburg, LJN: BD3149	4-6-2008	bezit + ontuchtige handelingen	5 jaar met tbs
Rb. Den Bosch, LJN: BD4501	11-2-2008	bezit + verspreiding + ontuchtige handelingen	2 jaar gevangenisstraf + 2400 euro
Rb. Den Haag, LJN: BC7561	25-3-2008	bezit + verspreiding (peer-to-peer)	6 maanden
Rb. Den Bosch, LJN: BD4501	11-2-2008	bezit + verspreidng + 3 zedendelicten	2 jaar
Rb. Middelburg, LJN: BD3152	4-6-2008	bezit (vrijspraak) + ontuchtige handelingen	30 maanden
Rb. Maastricht, LJN: BD4797	23-5-2008	bezit (prullenbak)	10 maanden + taakstraf 120 uren
Rb. Utrecht, LJN: BC9667	16-4-2008	bezit + verspreiding + productie + ontuchtige handelingen	gevangenisstraf 300 dagen + taakstraf 240 uren
Rb. Amsterdam, LJN: BD2286	15-4-2008	bezit	10 maanden
Rb. Utrecht, LJN: BC9382	14-4-2008	bezit + vervaardiging + ontuchtige handelingen	20 maanden
Rb. Zwolle, LJN: BC9647	10-4-2008	bezit + heimelijk video opnemen	*taakstraf 240 uur (120 uur voorwaardelijk)*
Rb. Den Haag, LJN: BC7561	25-3-2008	bezit + verspreiding (peer-to-peer)	6 maanden
Rb. Den Bosch, LJN: BD4501	11-2-2008	bezit + verspreiding + drie zedendelicten	2 jaar
Rb. Den Bosch, LJN: BC3225	4-2-2008	bezit + vervaardigen + verleiding + ontuchtige handellingen	2 jaar
Rb. Zwolle, LJN: BC5441	29-1-2008	bezit	3 maanden
Rb. Groningen, LJN: BC3529	28-1-2008	bezit	*60 uur taakstraf*
Rb. Zutphen, LJN: BC2954,	24-1-2008	bezit + vervaardiging vrijspraak	vrijspraak
Rb. Zutphen, LJN: BC0013	12-12-2007	bezit + seks minderjarige (15 jaar)	24 maanden
Rb. Assen, LJN: BC0080	11-12-2007	bezit	6 maanden
Rb. Den Bosch, LJN: BB9620	10-12-2007	bezit + vervaardiging + verkrachting + ontucht + mishandeling	10 jaar
Rb. Assen, LJN: BB9587	4-12-2007	bezit + 244 (ontucht)	4 jaar
Rb. Zutphen, LJN: BB9141	30-11-2007	bezit	2 maanden + 50 uur taakstraf
Rb. Maastricht, LJN: BC1624	23-11-2007	bezit (in lost files)	vrijspraak
Rb. Den Haag, LJN: BD1920	22-11-2007	bezit + ontucht (244 en 247)	24 maanden
Rb. Den Haag, LJN: BD1919	20-11-2007	bezit + ontucht (245)	6 maanden
Rb. Den Bosch, LJN: BB7972	14-11-2007	bezit + verspreiden + vervaardigen	18 maanden
Rb. Assen, LJN: BB8187	13-11-2007	bezit	18 maanden
Rb. Den Haag, LJN: BD1906	22-10-2007	bezit + ontuchtige handelingen	48 maanden
Rb. Arnhem, LJN: BB4886	5-10-2007	bezit + vervaardigen	2 jaar
Rb. Arnhem, LJN: BB4877	5-10-2007	vervaardigen + prostitueren minderjarige jongens	3 jaar en zes maanden
Rb. Maastricht, LJN: BB2405	28-08-2007	bezit + ontuchtige handelingen + wet wapens en munitie	vrijspraak ontucht, zes maanden
Rb. Arnhem, LJN: BB4879	5-10-2007	bezit + ontuchtige handelingen	2 jaar gevangenisstraf
Rb. Den Bosch, LJN: BB4213	26-9-2007	bezit + vervaardigen + stelselmatige verkrachting	10 jaar
Rb. Amsterdam,LJN: BB4237	25-9-2007	bezit + ontuchtige handleingen	4 jaar
Rb. Breda, LJN: BB3922	20-9-2007	bezit + vervaardiging	60 uur taakstraf + 25 dagen jeugddetentie

Rb. Breda, LJN: BB3906	20-9-2007	bezit + medeplegen verkrachting + vrijheidsberoving	gevangenisstraf 210 dagen + taakstraf 200 uren
Rb. Utrecht, LJN: BB4221	17-9-2007	bezit + verspreiding + ontuchtige handelingen + poging tot afdreiging	240 taakstraf + 12 maanden voorwaardelijk
Rb. Den Haag, LJN: BB3919	14-9-2007	bezit + 242 en 245	21 maanden
HR, LJN: BA6316	11-9-2007	"opzet op bezit" kinderporno	n.v.t.
Rb. Maastricht, LJN: BB2405	28-8-2007	bezit + ontuchtige handelingen + wet wapens en munitie	6 maanden
Rb. Den Haag, LJN: BB2033	20-8-2007	bezit 73a (oud), 273f	36 maaanden + schadevergoeding 5140 euro
Rb. Dordrecht, LJN: BB0510	26-7-2007	bezit + vervaardiging + ontuchtige handelingen	3 jaar en zes maanden
Rb. Dordrecht, LJN: BB0292	26-7-2007	bezit + vervaardiging + ontuchtige handelingen	20 maanden (verminderd toerekeningsvatbaar)
Rb. Maastricht, LJN: BB0271	24-7-2007	bezit + vervaardiging + verkrachting	9 jaar
Rb. Breda, LJN: BB0089	23-7-2007	bezit + webcamseks (248a)	zes maanden
Rb. Utrecht, LJN: BA9146	10-7-2007	bezit + verspreiding + vervaardigen + ontuchtige handelingen	4 jaar
Rb. Utrecht, LJN: BA5521	22-5-2007	bezit + ontuchtige handelingen	3 jaar en zes maanden
Rb. Leeuwarden, LJN: BA4878	8-5-2007	bezit + verspreiden	240 uur taakstraf + 1 maand gevangenisstraf
Rb. Zutphen, LJN: BA3253	18-4-2007	bezit + verspreiden	6 maanden + 120 uur taakstraf
Hof Den Haag, LJN: BA3188	17-4-2007	bezit + vervaardiging + ontuchtige handelingen	36 maanden
Hof Den Bosch, LJN: BA2386	6-4-2007	bezit + begraven van lijk (151) + vrijspraak moord	2 jaar
Rb. Den Haag, LJN: BA3173	6-4-2007	bezit + verspreiden	12 maanden + tbs
Rb. Maastricht, LJN: BA2122	3-4-2007	bezit + 242, 246 en 300	9 maanden
Rb. Zutphen, LJN: BA1597	28-3-2007	bezit	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Arnhem, LJN: BA1508	26-3-2007	bezit (vrijspraak) + ontuchtige handleingen	18 maanden
Rb. Alkmaar, LJN: BA1776	21-3-2007	bezit + vervaardiging + ontuchtige handelingen	6 maanden + 1000 euro schadevergoeding
Rb. Zutphen, LJN: AZ9741	1-3-2007	bezit + vervaardiging + ontucht (249)	20 maanden gevangenisstraf
Rb. Groningen, LJN: AZ9383	27-2-2007	bezit + ontuchtige handelingen	36 maanden
Hof Den Bosch, LJN: AZ9818	27-2-2007	bezit + verspreiding + vervaardiging + bedreiging	12 maanden + taakstraf 240 uur
Rb. Zwolle, LJN: AZ7613	1-2-2007	bezit (1 afbeelding) + ontuchtige handelingen	30 maanden en TBS
Hof Den Bosch, LJN: AZ8027	25-1-2007	bezit (o.a. unallocated files) + ontuchtelijke handelingen	4 jaar + 6000 euro
HR, LJN: AZ0221	16-1-2007	seksuele gedraging	n.v.t.
Rb. Alkmaar, LJN: AZ4422	13-12-2006	verspreiding	ontneming wederrechtelijk verkregen voordeel
Rb. Alkmaar, LJN: AZ4431	13-12-2006	verspreiding	ontneming wederrechtelijk verkregen voordeel
Rb. Alkmaar, LJN: AZ4419	13-12-2006	verspreiding	ontneming wederrechtelijk verkregen voordeel
Rb. Maastricht, LJN: AZ4183	14-11-2006	bezit	12 maanden+ 240 uur taakstraf
Rb. Alkmaar, LJN: AZ3173	28-11-2006	bezit + ontuchtige handelingen + vertoning seksfilm	15 maanden
Rb. Leeuwarden, LJN: AZ2144	14-11-2006	bezit + ontuchtige handelingen	20 maanden
Hof Den Bosch, LJN: AZ1421	30-10-2006	bezit + ontuchtige handelingen	12 maanden
Rb. Alkmaar, LJN: AZ1161	24-10-2006	bezit + medeplegen verspreiden + openlijke vertoning	3 maanden + 120 uur taakstraf

Rb. Alkmaar, LJN: AZ1122	24-10-2006	bezit + medeplegen verspreiden + openlijke vertoning	geen straf of maatregel
Rb. Alkmaar, LJN: AZ1144	24-10-2006	bezit + medeplegen verspreiden + openlijke vertoning	9 maanden + 240 uur
Rb. Alkmaar, LJN: AZ0743	24-10-2006	bezit + medeplegen verspreiden + openlijke vertoning	6 maanden + 180 uur
Rb. Den Bosch, LJN: AY9815	11-10-2006	bezit + verspreiding + vervaardiging + verkrachting	4 jaar en zes maanden + TBS
Rb. Utrecht, LJN: AY9796	10-10-2006	bezit + verspreiding	196 dagen gevangenisstraf
Rb. Middelburg, LJN: AY5948	9-8-2006	bezit + vervaardiging + verkrachting	6 jaar
Rb. Breda, LJN: AY5686	4-8-2006	bezit + vervaardiging + ontuchtelijke handelingen	27 maanden + 1500 euro
Rb. Den Haag, LJN: AY5348	31-7-2006	bezit + verspreiding	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Zwolle, LJN: AY5104	11-7-2006	bezit	1 maand + 100 uur taakstraf
Rb. Roermond, LJN: AX9921	7-7-2006	bezit	240 uur taakstraf + 12 maanden voorwaardelijk
Rb. Zutphen, LJN: AY0321	5-7-2006	bezit + ontuchtelijke handelingen	30 maanden gevangenisstraf en TBS
Rb. Zutphen, LJN: AY0409	5-7-2006	bezit + ontuchtelijke handelingen	15 maanden gevangenisstraf
Rb. Den Haag, LJN: AY0283	16-6-2006	bezit + ontuchtige handelingen (248a, 245, 249)	gevangenisstraf 36 maanden + 4500 euro
Rb. Den Bosch, LJN: AX9637	30-6-2006	bezit + doodslag + lijk begraven en verbergen	12 jaar
Rb. Haarlem, LJN: AX8978	16-6-2006	bezit + heimelijk filmen + ontuchtige handelingen	120 uren taakstraf + 3 maanden voorwaardelijk
Rb. Leeuwarden, LJN: AX5820	30-5-2006	bezit	240 uren taakstraf + 4 maanden voorwaardelijk
Rb. Zutphen, LJN: AW5516	28-4-2006	bezit	6 maanden
Rb. Zutphen, LJN: AW5462	28-4-2006	bezit + verspreiden (KaZa)	gevangenisstraf 9 maanden
Hof Arnhem, LJN: AW3267	24-4-2006	bezit (5 afbeeldingen, 2 video's 14 t/m 16 jaar)	voorwaardelijk 1 maand gevangenisstraf
Rb. Groningen, LJN: AW3140	24-4-2006	bezit + mishandeling	180 uur taakstraf + 2 maanden voorwaardelijk
HR, LJN: AV4193	11-4-2006	"seksuele gedraging" moet schadelijk voor de jeugdige zijn	
Rb. Assen, LJN: AV9485	7-4-2006	bezit	200 uur taakstraf + 4 maanden voorwaardelijk
Rb. Utrecht, LJN: AV7354	27-3-2006	bezit + vervaarding + verkrachting	4 jaar
Rb. Den Haag, LJN: AV6320	21-3-2006	bezit + verspreiding (Peer-to-peer) + openlijke tentoonstelling	24 maanden gevangenisstraf
Rb. Assen, LJN: AV5184	21-3-2006	bezit	240 uur taakstraf + 6 maanden voorwaardelijk
HR, LJN: AU9104	28-2-2006	bezit en opzet, slechts bezit indien opzet	n.v.t.
Rb. Groningen, LJN: AV2491	23-2-2006	bezit + oplichting	24 maanden
Hof Den Haag, LJN: AV2588	23-2-2006	bezit + 248a oud, 248ter oud, 249 oud en 249	30 maanden
Rb. Breda, LJN: AV2458	22-2-2006	bezit	150 uur taakstraf + 3 maanden voorwaardelijk
Rb. Breda, LJN: AV2996	22-2-2006	bezit (vrijspraak, unallocated clusers en tijdelijke bestanden)	
Hof Arnhem, LJN: AV2184	22-2-2006	bezit + 285, 300, 302, 310 en 312 + wet wapens en munitie	8 maanden
Rb. Breda, LJN: AV1470	10-2-2006	Bezit + verspreiding + vervaardiging + aanranding (webcam)	12 maanden
Rb. Groningen, LJN: AV0559	31-1-2006	bezit + verspreiding + Misbruik van overwicht	12 maanden
Rb. Maastricht, LJN: AV0178	24-1-2006	bezit + ontuchtelijke handelingen geestelijk gehandicapten	6 jaar

Rb. Dordrecht, LJN: AV0174	19-1-2006	bezit	taakstraf 200 uur + 6 maanden voorwaardelijk
Rb. Den Haag, LJN: AU9492	11-1-2006	bezit (gemanipuleerde foto) + ontuchtelijke handelingen	6 weken gevangenisstraf
Rb. Breda, LJN: AU7651	8-12-2005	bezit + ontuchtelijke handelingen + ontvoering	3 jaar gevangenisstraf
Rb. Utrecht, LJN: AU7307	1-12-2005	bezit + verspreiding (uitwisseling cd-roms)	6 maanden
Rb. Zwolle, LJN: AU5739	8-11-2005	bezit + ontucht	18 maanden
Rb. Breda, LJN: AU5780	7-11-2005	bezit + verkrachting	30 maanden gevangenisstraf + 2279,72 euro
Rb. Almelo, LJN: AU5638	1-11-2005	bezit + 239 + 247	3 jaar
Rb. Utrecht, LJN: AU4848	24-10-2005	bezit + verleiding + ontuchtelijke handelingen	3 jaar
Rb. Dordrecht, LJN: AU4724	20-10-2005	bezit + vervaardiging + aanranding (via MSN)	15 maanden gevangenisstraf
Hof Amsterdam, LJN: AU4229	12-10-2005	bezit + 307 en 309	180 dagen gevangenisstraf + 240 uur taakstraf
Hof Den Bosch, LJN: AU4032	5-10-2005	bezit + verspreiding (d.m.v. KaZaa)	240 uur taakstraf + 51 dagen gevangenisstraf
Rb. Den Haag, LJN: AU3675	3-10-2005	bezit + verspreiding (uploaden nieuwsgroepen)	100 uur taakstraf + 4 maanden voorwaardelijk
Rb. Zwolle, LJN: AU2067	6-9-2005	bezit + ontuchtelijke handelingen	30 maanden gevangenisstraf
Rb. Zutphen, LJN: AU1918	2-9-2005	bezit + moord + diefstal + mishandeling	14 jaar
Rb. Zwolle, LJN: AU1861	1-9-2005	bezit (in prullenbak vrijgesproken) + ontuchtelijke handelingen	50 uur taakstraf (+ voorwaardelijk 4 maanden jeugddetentie)
Hof Leeuwarden, LJN: AU0797	8-8-2005	bezit	15 maanden (waarvan 5 voorwaardelijk)
Rb. Dordrecht, LJN: AU0249	21-7-2005	bezit	12 maanden (waarvan 6 voorwaardelijk)
Rb. Utrecht, LJN: AT8591	1-7-2005	bezit	1 jaar gevangenisstraf
HR, LJN: AT7301	28-6-2005	"seksueel binnendringen" is onvoldoende feitelijke beschrijving	
Rb. Utrecht, LJN: AT7126	7-6-2005	bezit + ontuchtelijke handelingen + bedreiging + aanranding	36 maanden (waarvan 6 voorwaardelijk)
Rb. Almelo, LJN: AT5847	17-5-2005	bezit + ontuchtelijke handelingen (vrijspraak)	18 maanden (waarvan 6 voorwaardelijk)
Rb. Arnhem, LJN: AT4918	29-4-2005	bezit (1,2 miljoen) (verweer: verzamelen proefschrift)	24 maanden
HR, LJN: AS5874	22-3-2005	seksuele gedraging	n.v.t.
Hof Leeuwarden,LJN: AT6636	22-3-2005	bezit + verspreiding (via MSN-group)	1 maand voorwaardelijk + 750 euro
Rb. Middelburg, LJN: AT6872	16-3-2005	bezit + ontucht	30 maanden waarvan 6 voorwaardelijk
Rb. Arnhem, LJN: AS3632	20-1-2005	bezit + openlijke tentoonstelling (261)	180 uur taakstraf + 1000 euro
HR, LJN: AR5741	4-1-2005	ontrekking rechtsverkeer gegevensdragers met kinderporno	
Rb. Arnhem, LJN: AR8201	23-12-2004	bezit (foto's van naakte kinderen, kunstenaar-verweer)	gevangenisstraf 245 dagen, 180 voorwaardelijk
Rb. Alkmaar, LJN: AR7614	15-12-2004	bezit + diefstal + brandstichting	36 maanden gevangenisstraf, 6 voorwaardelijk
HR, LJN: AQ8936	7-12-2004	"kennelijke leeftijd" niet noodzakelijk dat de werkelijke leeftijd onder 16 jaren ligt	
Rb. Utrecht, LJN: AR6673	30-11-2004	bezit + dood door schuld	18 maanden, waarvan 6 voorwaardelijk
Rb. Arnhem, LJN: AR5780	17-11-2004	Bezit + ontuchtelijke handelingen	2 jaar + 1000 euro
Rb. Arnhem, LJN: AR3696	13-10-2004	bezit + (in prullenbak, geen opzet aangenomen)	vrijspraak
Rb. Leeuwarden, LJN: AR5373	12-10-2004	bezit + verspreiding (MSN-group)	120 uur taakstraf + 4 maanden voorwaardelijk

HR, LJN: AQ3710	28-9-2004	"een ontuchtige handeling" is van onvoldoende feitelijke betekenis	
Rb. Leeuwarden, LJN: AR4924	23-9-2004	bezit	240 dagen gevangenisstraf, 127 voorwaardelijk + 240 uur taakstraf
Rb. Leeuwarden, LJN: AQ9972	2-9-2004	bezit	*80 uur taakstraf*
Rb. Groningen, LJN: AQ6334	5-8-2004	bezit + opiumwet + wet wapens en munitie	18 maanden
Rb. Zutphen, LJN: AQ0554	2-7-2004	bezit	*150 uren, waarvan 75 voorwaardelijk*
Rb. Leeuwarden, LJN: AQ2471	24-6-2004	bezit + verspreiding (uploaden naar website)	geldboete 750 euro
Rb. Arnhem, LJN: AP1705	16-6-2004	bezit + verspreiding + ontuchtelijke handelingen	3 jaar
Rb. Den Haag, LJN: AP1332	10-6-2004	bezit + verspreiding	15 maanden, waarvan 5 voorwaardelijk
Rb. Breda, LJN: AO8758	29-4-2004	bezit + verspreiding (via "een box" op internet) + poging ontuchtelijke handelingen	18 maanden, waarvan 6 voorwaardelijk
Rb. Arnhem, LJN: AO8245	22-4-2004	bezit + sigarettensmokkel	30 maanden, waarvan 6 voorwaardelijk
Rb. Den Haag, LJN: AO6995	2-4-2004	bezit + ontuchtelijke handelingen (in slaap ex-vriendin)	120 uur taakstraf (+voorwaardelijke gevangenisstraf)
Rb. Arnhem, LJN: AO6240	25-3-2004	bezit	2500 euro (+ voorwaardelijke gevangenisstraf)
Rb. Dordrecht, LJN: AO3821	17-2-2004	bezit + verspreiding	24 maanden waarvan 6 voorwaardelijk
Rb. Dordrecht, LJN: AO3832	17-2-2004	bezit + verspreiding	30 maanden, waarvan 6 voorwaardelijk
Rb. Dordrecht, LJN: AO3817	17-2-2004	bezit	12 maanden, waarvan 6 voorwaardelijk
Rb. Almelo, LJN: AO3589	10-2-2004	bezit + stalking	24 maanden
Rb. Dordrecht, LJN: AO2649	29-1-2004	bezit + vervaardiging + verkrachting + hennep kwekerij	6 jaar
Hof Den Bosch, LJN: AO1915	19-12-2003	bezit	24 maanden, waarvan 6 voorwaardelijk
Rb. Dordrecht, LJN: AO1399	18-12-2003	bezit + verspreiding + vervaardiging + ontuchtelijke handelingen	4 jaar
Rb. Den Bosch, LJN: AN9804	2-12-2003	bezit	12 maanden
Rb. Den Bosch, LJN: AN9846	2-12-2003	bezit + 245 en 248b	12 maanden + 240 uur taakstraf (120 uur voorwaardelijk)
Rb. Den Bosch, LJN: AN9276	2-12-2003	bezit + ontuchtelijke handelingen	15 maanden
Rb. Den Haag, LJN: AM3308,	27-10-2003	bezit + schennis eerbaarheid	2 maanden
Rb. Den Haag, LJN: AL1187	18-9-2003	bezit + verspreiding	18 maanden
Rb. Almelo, LJN: AJ6859	9-9-2003	bezit + verspreid	1 jaar voorwaardelijk onder voorwaarde behandeling
Rb. Den Bosch, LJN: AI1728	2-9-2003	bezit + jeugdprostitutie	14 maanden waarvan 6 voorwaardelijk
Rb. Maastricht, LJN: AH9793	10-7-2003	bezit + ontuchtige handelingen	6 maanden en 80 dagen
Hof Den Haag, LJN: AI0999	1-7-2003	bezit + ontuchtige handelingen + schending vd eerbaarheid	6 jaar
Rb. Zutphen, LJN: AH8581	18-6-2003	bezit + ontuchtige handelingen	120 dagen gevangenisstraf, 25 voorwaardelijk
HR, LJN: AF6437	10-6-2003	naakte kinderen op strand geen seksuele gedraging	vrijspraak

Rb. Almelo, LJN: AF6834	1-4-2003	bezit + vervaardigen + ontuchtelijke handelingen	4 jaar
Rb. Middelburg, LJN: AF4981	12-2-2003	bezit	240 uur taakstraf, 4 maanden voorwaardelijk
Hof Den Haag, LJN: AF0684	15-11-2002	bezit	voorwaardelijk 2 maanden gevangenisstraf
Rb. Maastricht, LJN: AE9367	23-10-2002	bezit + verspreiding	18 maanden
Rb. Alkmaar, LJN: AE5198	10-7-2002	verspreiding (via e-mailadressen op internet gezet)	80 uur taakstraf + 3 maanden voorwaardelijk
Hof Leeuwarden, LJN: AE4138	3-6-2002	bezit + verspreid (via nieuwsgroep)	240 uur taakstraf + 6 maanden voorwaardelijk
Rb. Dordrecht, LJN: AE2876	21-5-2002	bezit + ontuchtelijke handelingen	30 maanden, waarvan 8 voorwaardelijk
Rb. Alkmaar, LJN: AE1918	24-4-2002	bezit + verspreiding	160 uur taakstraf, 9 maanden voorwaardelijk
Rb. Assen, LJN: AE1790	23-4-2002	bezit	18 maanden, waarvan 6 voorwaardelijk
Rb. Maastricht, LJN: AE0507	18-3-2002	bezit + ontuchtige handelingen	32 maanden, waarvan 10 voorwaardelijk
Hof Den Bosch, LJN: AD8158	6-12-2001	bezit (geen opzet, schijf geformatteerd)	vrijspraak
Rb. Maastricht, LJN: AD6284	27-11-2001	vervaardigen + 139f + opiumwet	200 uur taakstraf + 100 dagen gevangenisstraf
Rb. Dordrecht, LJN: AD4074	4-10-2001	bezit + schennis eerbaarheid	voorwaardelijk vier maanden + 1000 gulden
Rb. Den Bosch, LJN: AB2182	19-6-2001	bezit + ontuchtelijke handelingen	3 jaar, waarvan 1 voorwaardelijk
Rb. Den Haag, LJN: AB1907	31-5-2001	bezit + ontuchtelijke handelingen	15 maanden, waarvan 5 voorwaardelijk
Rb. Breda, LJN: AA8997	7-12-2000	bezit + verspreiding	30 maanden waarvan 6 voorwaardelijk
Hof Den Bosch, LJN: AA8226	8-11-2000	bezit	2000 gulden, 1 maand voorwaardelijk
Rb. Roermond, LJN: AA5850	15-5-2000	bezit (deel op account bij ISP, niet op PC en deel in prullenbak)	(vrijspraak)
Rb. Leeuwarden, LJN: AA5273	28-3-2000	bezit + verspreiding (via nieuwsgroepen)	18 maanden, waarvan 6 voorwaardelijk
Rb. Amsterdam, LJN: AA1022	14-6-1999	bezit (niet aangenomen, geen onnatuurlijke houding)	klaagschrift gegrond

Statistieken				
				+ Ontuchteli
Jaar:	**Bezit**	**+ Verspreiding**	**+ Vervaardiging**	**handelingen**
2009 (61 zaken)	29	6	9	16
2008 (50 zaken)	14	11	7	13
2007 (43 zaken)	5	5	11	19
2006 (42 zaken)	10	11	3	10
2005 (22 zaken)	4	4	0	7
2004 (21 zaken)	7	7	1	4
2003 (13 zaken)	4	3	2	6
2002 (9 zaken)	3	4	0	2
2001 (5 zaken)	1	0	1	2
2000 (4 zaken)	2	2	0	0

Jaar:	Totaal:	"Kale" taakstraf - alleen bezit	Taakstraf + gevangenisstraf - alleen bezit	
2009	61	1	12	
2008	50	3	2	
2007	43	0	2	
2006	42	0	8	
2005	22	0	0	
2004	21	2	1	
2003	13	0	2	
2002	9	0	1	
2001	5	0	0	
2000	4	0	0