19. Binnenkort moet het Hof Den Haag beslissen over bijzondere persoonsgegevens in de context van verwijderverzoeken.[19] Verder zijn er Franse vragen gesteld aan het HvJ EU over dit soort situaties, waarin Google verwijst naar websites met bijzondere persoonsgegevens (zie *Computerrecht* 2017/128 in de rubriek Privacybescherming in deze aflevering).[20] Maar, zoals gezegd, het bijzondere-persoonsgegevens-probleem komt niet aan de orde in dit arrest van de Hoge Raad.

20. We sluiten af. De Hoge Raad heeft de zaak van Arthur van M voor verdere behandeling terugverwezen naar het Gerechtshof Den Haag. Daarbij moet het gerechtshof de voorrangsregel toepassen: in vergeetrecht-zaken weegt het recht op privacy in principe zwaarder dan het recht op vrijheid van meningsuiting. Het gerechtshof kan overigens tot ongeveer hetzelfde eindoordeel komen als in het vernietigde arrest. Het hof zal dan wel moeten uitleggen waarom de zoekresultaten niet verwijderd hoeven te worden, en daarbij ingaan op de rol die de crimineel in het openbare leven speelt.

Mr. S. Kulk en dr. F.J. Zuiderveen Borgesius

Computerrecht 2017/103

Rechtbank Amsterdam 16 maart 2017, nr. 13/995008-13
(Mrs. K.A. Brunner, C.F. de Lemos Benvindo en M. Woerdman)
m.nt. mr. dr. J.J. Oerlemans[1]

Art. 138ab Sr (computervredebreuk), art. 139d Sr (bezit van malware), art. 225 Sr (Valsheid met geschrifte), art. 240b Sr (kinderporno), art. 246 Sr (aanranding), art. 248a Sr (aanzetten tot ontuchtelijke handelingen), art. 318 Sr (afdreiging) en art. 326 Sr (bedrog)

ECLI:NL:RBAMS:2017:1627

Deze zaak betreft de veroordeling van "webcamafperser" Aydin C. De verdachte is met betrekking tot 34 meisjes veroordeeld voor kinderporno, (poging tot) aanranding en/of verleiding en met betrekking tot één man veroordeeld voor afdreiging. In de zaak is software gebruikt teneinde bewijs vanaf de computer van de verdachte te verzamelen.

Vonnis van de Rechtbank Amsterdam, meervoudige strafkamer, in de strafzaak tegen
[verdachte],
geboren te [geboortegegevens] 1978,
zonder vaste woon- of verblijfplaats in Nederland,
gedetineerd in de Penitentiaire Inrichting '[PI]' te [plaats].

Uitspraak (ingekort)[2]

1 Het onderzoek ter terechtzitting

Dit vonnis is op tegenspraak gewezen naar aanleiding van het onderzoek op de terechtzittingen op 21 maart, 1 en 29 april, 2 mei, 6 juli, 16 september en 9 en 21 november 2016 en 25, 26 en 30 januari, 1, 6, 9, 13 en 15 februari en 2 maart 2017.

De rechtbank heeft kennisgenomen van de vordering van de officieren van justitie, mrs. A.C. Kramer en J. Weening (hierna: officier van justitie), en van wat verdachte en zijn raadslieden, mrs. C. Grijsen en R. Malewicz, naar voren hebben gebracht.

2 Tenlastelegging

2.1 Verdachte wordt er – samengevat – van beschuldigd dat hij
- een gewoonte heeft gemaakt van het vervaardigen, verwerven, verspreiden, openlijk tentoonstellen en/of in bezit hebben van kinderporno van 28 minderjarige meisjes;
  (art. 240b van het Wetboek van Strafrecht (Sr));
- 33 minderjarige meisjes heeft aangerand of verleid, of dat heeft geprobeerd;
  (art. 246 Sr of art. 248a Sr);
- vier meerderjarige mannen heeft afgedreigd of opgelicht en één meerderjarige man heeft geprobeerd af te dreigen of op te lichten;
  (art. 318 Sr of art. 326 Sr)
- computervredebreuk heeft gepleegd en een computerprogramma voorhanden heeft gehad om computervredebreuk te plegen;
  (art. 138ab Sr en art. 139d Sr)
- negen mensen heeft opgelicht;
  (art. 326 Sr)
- documenten heeft vervalst en van die vervalste documenten gebruik heeft gemaakt;
  (art. 225 Sr)
- 1.500 gram DMT aanwezig heeft gehad.
  (art. 2 van de Opiumwet)

2.2. De tenlastelegging is op de zitting van 11 januari 2016 nader omschreven en daarna op de zittingen van 9 november 2016 en 6 februari 2017 gewijzigd.

2.3. De tekst van de volledige tenlastelegging zoals die nu geldt, is opgenomen in bijlage 1 bij dit vonnis. Die bijlage hoort bij het vonnis.

(...)

19 Er is hoger beroep ingesteld in deze zaak: Rechtbank Rotterdam 29 maart 2016, ECLI:NL:RBROT:2016:2395 (*Computerrecht* 2016/126).

20 Zie: https://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted.

1 Jan-Jaap Oerlemans is als onderzoeker verbonden aan eLaw, het centrum voor Recht en Technologie van de Universiteit Leiden.

2 Deze uitspraak is sterk ingekort vanwege de zeer uitgebreide tenlastelegging van de officier van justitie en de uitgebreide overwegingen van de rechtbank. Slechts de (voor de noot) relevante overwegingen van de rechtbank worden opgenomen.

4 **Inleiding**

Facebookrapporten

Het strafrechtelijk onderzoek 'Disclosure' werd gestart naar aanleiding van een intern onderzoek van Facebook. De Nederlandse politie ontving op 13 mei 2013 een rapport van Facebook en op 6 september een aanvulling daarop.

Volgens Facebook zou een onbekende persoon met minimaal 86 onderling verbonden Facebookaccounts zich bezig houden met het verzamelen, produceren en verspreiden van beelden van kinderuitbuiting. Die persoon zou ook tientallen minderjarige meisjes chanteren, waarbij gebruik gemaakt werd van die afbeeldingen van kinderuitbuiting.

Verder zou deze persoon een aantal mannen chanteren. Hij legde beelden vast waarop deze mannen masturbeerden terwijl zij aan het webcammen waren met – zo dachten ze – minderjarige jongens. Vervolgens eiste deze persoon dat er geld zou worden betaald, omdat anders de opgenomen beelden zouden worden verspreid onder vrienden en familie van de meerderjarige man.

De gebruiker van dit netwerk van Facebookaccounts maakte gebruik van valse identiteitsgegevens, afgeschermde IP-adressen en afgeschermde internetverbindingen. Facebook achterhaalde informatie die erop wees dat de gebruiker actief was vanuit Nederland: hij maakte gebruik van een Nederlands IP-adres ([IP-adres]) en hij gebruikte bij de registratie van één van de Facebookaccounts een Nederlands mobiel telefoonnummer ([telefoonnummer]).

IP-adres [IP-adres]

Na de ontvangst van het tweede Facebookrapport in september 2013 startte de Nederlandse politie met een onderzoek. Het IP-adres [IP-adres] hoorde bij een woning op het bungalowpark [bungalowpark 1] aan de [adres 3] in Oisterwijk. Dit IP-adres (hierna: IP-adres [bungalowpark 1]) was in de politiesystemen bekend uit een oplichtingszaak in Rotterdam (politie-onderzoek met de naam 'Sleutel', zie feit 69). In die zaak zijn verschillende mensen opgelicht, toen zij in januari 2011 de woning aan de [adres 1] in Rotterdam wilden huren. Zij betaalden de eerste maand huur en een borgsom, maar konden vervolgens de gehuurde woning niet in. De oplichter maakte gebruik van IP-adres [bungalowpark 1]. In het onderzoek Sleutel had de politie het ernstige vermoeden dat het verdachte was die achter de oplichtingen zat.

Telefoonnummer [telefoonnummer]

Het telefoonnummer uit het Facebookrapport, [telefoonnummer], kwam ook voor in de Nederlandse politiesystemen in het kader van een aangifte van woningoplichting. Deze keer ging het om een melding van 31 mei 2011 en ging het om het verhuren van de woning aan de [adres 2] te Rotterdam (feit 70). De werkwijze van deze oplichter leek sterk op die van de oplichter in het onderzoek Sleutel. Op foto's die door de oplichter van de [adres 2] werden gebruikt op valse paspoortkopieën was dezelfde persoon te zien als op de foto's op de valse paspoortkopieën in het onderzoek Sleutel.

Vervolgonderzoek door de Nederlandse politie

Tijdens het vervolgonderzoek bleek dat verdachte op dat moment verbleef op bungalowpark [bungalowpark 2] in Oost-, West- en Middelbeers. Eind november 2013 verhuisde verdachte vanaf dat bungalowpark naar het bungalowpark [bungalowpark 3] in Oisterwijk. [bungalowpark 3] ligt direct naast het eerdergenoemde bungalowpark [bungalowpark 1]. Nadat verdachte naar [bungalowpark 3] verhuisde, werd een IP-tap geplaatst op IP-adres [bungalowpark 1]. Het internetverkeer kon meestal niet goed worden gevolgd, omdat het internetgedrag werd afgeschermd via een 'Virtual Private Network'-verbinding (VPN-verbinding). De politie stelde na de aanhouding van verdachte vast dat de computers in de woning van verdachte verbonden waren met de router die hoorde bij IP-adres [bungalowpark 1].

Onderzoek naar betalingen

Het Nederlandse onderzoeksteam ontving via de Engelse politie informatie over betalingen die door meerderjarige mannen waren gedaan via Skrill/Moneybookers (hierna: Skrill) en Western Union.
Eén van de Skrill-accounts stond op naam van verdachte. Een ander Skrill-account werd benaderd via het eerdergenoemde IP-adres [bungalowpark 1]. In de woning van verdachte trof de politie van verschillende van deze Skrill-accounts documenten of Mastercards aan. Deze Skrill-accounts stonden op naam van slachtoffers van de (pogingen tot) woningoplichting (feit 69 en 70) die aan de oplichter een kopie van hun paspoort hadden verstrekt.

Via Western Union werd in twee jaar tijd meer dan € 30.000 overgemaakt op naam van verdachte. Een deel van dat geld was afkomstig van mannelijke slachtoffers in deze strafzaak. Het geld werd opgehaald met een paspoort van verdachte, dat na zijn aanhouding ook in zijn woning werd aangetroffen. Van één geldopname waren camerabeelden beschikbaar waarop politiemedewerkers verdachte hebben herkend.

Technisch hulpmiddel

Verdachte werd in het onderzoek Sleutel aangehouden op 20 december 2013. Op 23 december 2013 werd hij weer vrijgelaten. In de tussenliggende periode heeft het onderzoeksteam in de zaak waarvoor verdachte nu terechtstaat (onderzoek 'Disclosure') de woning van verdachte op bungalowpark [bungalowpark 3] in het geheim betreden en doorzocht. Daarbij werd op de desktopcomputer en de laptop in die woning een technisch hulpmiddel geïnstalleerd. Dit technisch hulpmiddel registreerde toetsaanslagen en maakte schermafbeeldingen wanneer op die desktop of laptop gebruik werd gemaakt van communicatieprogramma's zoals Skype of een internetbrowser. Hierdoor kreeg het onderzoeksteam inzicht in het internetgedrag op deze computers en kon de afscherming door het gebruik van een VPN-verbinding worden omzeild.

Aanhouding Disclosure, doorzoeking en digitaal onderzoek

Op 13 januari 2014 werd verdachte aangehouden in zijn woning. Na de aanhouding van verdachte is de woning voor een tweede keer doorzocht. De desktopcomputer en de laptop werden in beslag genomen. Daarnaast nam de politie een aantal (losse) harde schijven in beslag. Tijdens het digitale onderzoek trof de politie, verspreid over verschillende harde schijven, een grote hoeveelheid informatie aan die verband houdt met de feiten waarvan verdachte nu wordt verdacht. Ook trof de politie veel informatie aan over mogelijke slachtoffers. Geprobeerd is om deze slachtoffers, die uit binnen- en buitenland afkomstig zijn, te identificeren. Wanneer dat mogelijk was, verhoorde de lokale politie hen en werd er onderzoek verricht op hun computers. Een aantal van de deeldossiers in deze strafzaak werd op deze wijze samengesteld.

Daarnaast liepen er verschillende politieonderzoeken in binnen- en buitenland naar aanleiding van meldingen van slachtoffers. Tijdens het onderzoek Disclosure werd een verband gelegd tussen sommige van die meldingen en de bevindingen in Disclosure. In een aantal van die zaken zijn de strafdossiers daarom overgedragen aan het Nederlandse onderzoeksteam van Disclosure en van die zaken werden ook deeldossiers samengesteld.

5 Technisch hulpmiddel – rechtmatigheid en betrouwbaarheid

5.1 *Inleiding*

Zoals al in de inleiding is opgemerkt, is in het onderzoek Disclosure gebruik gemaakt van een technisch hulpmiddel, dat is ingezet op de desktop en de laptop in de woning van verdachte. De verdediging betoogt dat dat middel onrechtmatig is toegepast en dat de resultaten van het hulpmiddel niet betrouwbaar zijn en daarom niet mogen worden gebruikt voor het bewijs.
Voor de vraag of dit verweer kan slagen is het Besluit technische hulpmiddelen strafvordering van 20 oktober 2006 (hierna: het Besluit)[3] van belang. Het Besluit heeft tot doel de betrouwbaarheid en herleidbaarheid te waarborgen van de gegevens die met de desbetreffende apparatuur zijn verkregen. Het hulpmiddel moet voldoen aan technische eisen; van de keuring moet door een keuringsdienst een rapport worden opgemaakt en de keuring moet plaatsvinden overeenkomstig een goedgekeurd keuringsprotocol.

Hierbij zijn verder de uitgangspunten van de Hoge Raad in de uitspraken van 12 juli 2011[4] en 16 juni 2015[5] van belang. In die zaken ging het om het gebruik van een technisch hulpmiddel dat was goedgekeurd overeenkomstig het in die zaken nog geldende Besluit technische hulpmiddelen bijzondere opsporingsbevoegdheden (hierna: Bthbo). Het Bthbo is ingetrokken bij het Besluit van 20 oktober 2006.

De Hoge Raad oordeelde in die zaken, kort gezegd, dat de rechter ervan moet uitgaan dat het technisch hulpmiddel aan de wettelijke eisen voldeed als daarvoor een verklaring van goedkeuring is gegeven.

In het dossier bevindt zich een Keuringsrapport OVC van 24 maart 2009 met betrekking tot het in de onderhavige zaak ingezette technische hulpmiddel THv030+102 dat geldig is tot 1 april 2014. Ook bevindt zich in het dossier een op 7 januari 2014 door de Keuringsdienst van de Politie/Landelijke Eenheid afgegeven conformiteitsverklaring. Het technisch hulpmiddel is ingezet van 22 december 2013 tot en met 13 januari 2014.

Op basis van de eerdergenoemde twee uitspraken van de Hoge Raad moet, gelet op de goedkeuring van het gebruikte technisch hulpmiddel, er (in beginsel) van worden uitgegaan dat de apparatuur aan de wettelijke eisen voldeed.

(…)

5.3. *Geldt de regel van de Hoge Raad ook voor softwarematige hulpmiddelen?*

De verdediging wijst erop dat de zaken waarover de Hoge Raad zich uitsprak, gingen over apparatuur. Daarom is de lijn van de Hoge Raad niet zonder meer toepasbaar op technische hulpmiddelen die bestaan uit software. De verdediging betwist verder dat het Besluit gelijke eisen stelt aan hardwarematige en softwarematige hulpmiddelen.

Naar het oordeel van de rechtbank geldt het Besluit voor zowel hardware als software. In het besluit wordt tussen beide geen onderscheid gemaakt, maar wordt enkel over ‘technisch hulpmiddel’ gesproken. Aparte regels voor software worden niet gegeven. De nota van toelichting spreekt (ook) over apparatuur, maar met dat begrip is niet alleen hardware bedoeld. Uit de nota van toelichting is bovendien op te maken dat onder ogen is gezien dat ook softwarematige hulpmiddelen kunnen worden ingezet:

> “In de tweede plaats kan de officier van justitie bepalen dat een technisch hulpmiddel wordt ingezet dat zich naar zijn aard niet leent voor keuring voorafgaand aan de inzet. (…) Bij technische hulpmiddelen die zich naar hun aard niet lenen voor keuring vooraf kan bijvoorbeeld worden gedacht aan het gebruik van softwareprogrammatuur als onderdeel van een technisch hulpmiddel. Deze softwareprogrammatuur dient in veel gevallen speciaal op maat te worden gemaakt voor de inzet in een specifiek geval. Bij de inzet van software zal het veelal noodzakelijk zijn om bij of tijdens de inzet aanpassingen te maken aan het technische hulpmiddel om het correct te laten functioneren. Een keuringsprocedure van het technische hulpmiddel als geheel, voorafgaand aan de inzet, zal in deze gevallen praktisch onmogelijk zijn en

3 *Stb.* 2006, 524 laatstelijk gewijzigd *Stb.* 2013, 49.
4 ECLI:NL:HR:2011:BP4650 en ECLI:NL:HR:2011:BP4651.
5 ECLI:NL:HR:2015:1663.

een effectieve inzet van dit technische hulpmiddel belemmeren."

(...)

De rechter-commissaris heeft de heer J.G.J. Kulker (hierna: Kulker), teamleider bij de Keuringsdienst, als getuige-deskundige gehoord. Hij heeft verklaard dat hij zelf de keuring van het gebruikte technische hulpmiddel heeft gedaan en dat het volgens hem niet een hulpmiddel betreft dat volgens het besluit achteraf moet worden gekeurd. Het middel wordt niet aangepast bij de installatie. Het is een vaststaand softwarepakket en bij de installatie worden er instellingen aangevinkt. Er worden geen wijzigingen in de broncode aangebracht. De Keuringsdienst maakt ook een handleiding voor het gebruik. Daarin staat welke vinkjes en instellingen moeten worden aangezet, aldus Kulker.

Dat instellingen van het technisch hulpmiddel bij de installatie moeten worden aangevinkt betekent naar het oordeel van de rechtbank niet dat het middel zich niet zou lenen voor keuring vooraf. Het middel kan immers worden gekeurd met inbegrip van de (mogelijk) aan te vinken opties. Uit de verklaring van Kulker is op te maken dat dat in dit geval ook gebeurd is.

Tussenconclusie rechtbank

Gelet op de vóóraf gegeven goedkeuring moet er van worden uitgegaan dat het ingezette technische hulpmiddel aan de wettelijke eisen voldeed. In zoverre is geen sprake van een verzuim.

5.5. ***Nuancering rechtbank: onregelmatigheden***

Op de zojuist gegeven conclusie moet naar het oordeel van de rechtbank een nuancering gemaakt worden indien zou blijken dat onregelmatigheden zijn geconstateerd voorafgaand of na afloop van de inzet van een technisch hulpmiddel. In dit verband is van belang de nota van toelichting op het besluit waarin onder 1.3 onder meer het volgende wordt vermeld:

> "Voorafgaand en na afloop van de inzet stelt het besluit verschillende procedurele eisen om manipulatie van de geregistreerde gegevens te voorkomen en de authenticiteit te waarborgen. Indien onregelmatigheden worden geconstateerd wordt een proces-verbaal opgemaakt en naar de officier van justitie gezonden. De officier van justitie en de rechter kunnen op grond van het proces-verbaal beoordelen in hoeverre de geconstateerde onregelmatigheden afbreuk doen aan de authenticiteit en bewijskracht van de vastgelegde waarnemingen."

De in de nota van toelichting genoemde onregelmatigheden kunnen zowel een verzuim opleveren in de zin van artikel 359a van het Wetboek van Strafvordering, als afbreuk doen aan de betrouwbaarheid van de waarnemingen. De rechtbank dient daarom te beoordelen of van dergelijke onregelmatigheden sprake is.

De verdediging voert aan dat zich zes onregelmatigheden hebben voorgedaan.

1. Verschillen tussen schermafbeeldingen en geregistreerde toetsaanslagen

De verdediging heeft gewezen op (chat-)teksten die wel te zien zijn op de door het technisch hulpmiddel gemaakte schermafbeeldingen, maar die niet terugkomen in de geregistreerde toetsaanslagen. Weliswaar is in het proces-verbaal opgemerkt dat dat verschil verklaard kan worden doordat gebruik is gemaakt van de functies *kopiëren* en *plakken*, maar daarmee kunnen niet alle verschillen worden verklaard, aldus de verdediging.

Met de officier van justitie is de rechtbank van oordeel dat een aanmerkelijk deel van de teksten op de schermafbeeldingen wel is te herleiden tot geregistreerde toetsaanslagen. De resterende verschillen tussen beiden levert op zichzelf geen aanwijzing op dat er abnormaal gebruik zou zijn gemaakt van het technisch hulpmiddel, en evenmin dat de *wel* doorgestuurde informatie niet authentiek zou zijn.

2. en 3. Technisch hulpmiddel niet meer aanwezig op de desktop

Het technisch hulpmiddel werd na de aanhouding van verdachte niet meer op de desktopcomputer aangetroffen. Wat de reden daarvan is, is niet geheel opgehelderd. De verdediging meent dat de manier van verwijdering van het technisch hulpmiddel iets zegt over de betrouwbaarheid ervan. Daarom had naar die verwijdering nader onderzoek moeten plaatsvinden. Nu dat onderzoek niet is toegestaan kan volgens de verdediging geen beslissende waarde worden toegekend aan de resultaten van het hulpmiddel.

De rechter-commissaris heeft over de verwijdering van het hulpmiddel vragen gesteld. Uit de beantwoording van die vragen door Kulker, in de aanvullende processen-verbaal van 22 en 23 oktober 2015 is af te leiden dat het niet mogelijk is dat het technisch hulpmiddel op afstand kan worden geplaatst, bediend, bestuurd, onderhouden, verwijderd of geactiveerd tot zelfvernietiging. Hiervoor is volgens Kulker fysieke toegang tot de computer noodzakelijk.

De verdediging heeft vraagtekens gezet bij de in de aanvullende processen-verbaal genoemde mogelijke scenario dat het technisch hulpmiddel is verwijderd door de installatie en toepassing van een virusscanner, echter dat betekent niet dat nader onderzoek naar de werking van het technisch hulpmiddel plaats moet vinden. Tegenover de beantwoording door Kulker heeft de verdediging namelijk onvoldoende onderbouwd waarom het verwijderd zijn van het technisch hulpmiddel op de desktop computer na de inzet afbreuk doet aan de authenticiteit en bewijskracht van de vastgestelde waarnemingen.

4. Verschillen tussen IP-tap en keylogger

De verdediging wijst erop dat het technisch hulpmiddel, heeft gefunctioneerd tot 6 januari 2014, 18:21 uur, en dat

deze al vanaf 18.07 uur verminderd werkte, vóórdat de virusscan werd uitgevoerd. Het hulpmiddel moet volgens de verdediging dan ook door een andere oorzaak minder goed zijn gaan functioneren en dat moet consequenties hebben voor de betrouwbaarheid van de resultaten.

De rechtbank verwerpt ook dit verweer. De verdediging heeft namelijk niet onderbouwd, en de rechtbank kan dat ook niet inzien, hoe het minder functioneren van het hulpmiddel tot de conclusie moet leiden dat de uitkomsten daarvan niet betrouwbaar zijn. Dat geldt des te sterker omdat wel vast staat dat de gebruiker van de desktop (waarvan verdachte heeft verklaard dat die van hem is) kennelijk die avond bezig was met het opschonen van die computer. Verdachte heeft nagelaten te verklaren:
a. of hij dat was;
b. zo ja, wat hij dan voor handelingen heeft verricht;
c. zo nee, wie er dan van de desktop gebruik maakte.

Ook ontbreekt iedere aanwijzing dat sprake is van een vormverzuim door de opsporingsautoriteiten.

5. Uitschakelen VPN-verbinding

Volgens de verdediging startte de desktop vóór de aanhouding van verdachte op 20 december 2013 altijd direct een VPN-verbinding op, maar na terugkomst op 23 december 2013 gebeurde dat niet meer automatisch. Dat vormt een aanwijzing dat het technisch hulpmiddel ook op andere dan de ingestelde programma's invloed heeft. Dat moet volgens de verdediging gevolgen hebben voor de betrouwbaarheid van de resultaten.

Dit verweer faalt alleen al omdat de rechtbank niet inziet op welke manier de betrouwbaarheid van de verkregen resultaten nadelig beïnvloed zou kunnen worden door het gestelde neveneffect van het hulpmiddel. Ieder aanknopingspunt voor die bewering ontbreekt.

6. Technisch hulpmiddel legde teveel vast

De verdediging betoogt dat uit schermafdrukken blijkt dat het technisch hulpmiddel meer opnam dan de toegestane communicatie.

De rechtbank volgt de verdediging daarin niet. Op de print van een schermafdruk op p. D22-246 lijkt slechts een deel van het scherm te zien te zijn. Op de schermafdrukken op p. A01-02341 en p. A01-2342 zijn verschillende tabbladen te zien, waaronder toegestane applicaties. Dat op schermafdrukken meer is te zien dan alleen de ingestelde programma's, maakt naar het oordeel van de rechtbank nog niet dat sprake is van een verzuim.

Eindconclusie rechtbank

Het technisch hulpmiddel was goedgekeurd. Er is geen aanwijzing dat bij het gebruik van het hulpmiddel sprake is geweest vaneen vormverzuim en ook niet dat de resultaten van het middel onbetrouwbaar zouden zijn. Het technisch hulpmiddel is dus bruikbaar voor het bewijs.

6 Waardering van het bewijs (1): de grote lijn

6.1. Het standpunt van de officier van justitie

Volgens de officier van justitie zijn alle 72 ten laste gelegde feiten bewezen. Als sprake is van een 'primair/subsidiair'-tenlastelegging gaat de officier van justitie steeds uit van de primair ten laste gelegde variant, behalve bij feit 15 en de feiten 62 tot en met 66. Bij die feiten vinden zij de subsidiaire variant bewezen.

6.2. Het standpunt van de verdediging

De verdediging verzoekt vrijspraak van alle 72 feiten. In het scenario van de verdediging wordt een belangrijke rol toegekend aan een door verdachte genoemde persoon, [persoon 1]. Deze [persoon 1] zou de oorspronkelijke eigenaar zijn van een aantal harde schijven die de politie in de woning van verdachte in beslag nam.[6] [persoon 1] zou ook de eigenaar zijn van een versleutelde gegevensdrager en van de laptop. Ook niet-digitale voorwerpen die de politie onder verdachte in beslag nam, waren volgens de verdediging van [persoon 1], waaronder de Skrill Mastercards en de aangetroffen harddrugs. Daarnaast gebruikte [persoon 1] verdachte om zelf bij zijn criminele activiteiten buiten beeld te kunnen blijven. Zo gaf verdachte voor [persoon 1] rondleidingen in de woning in de [adres 1] en nam hij geldbedragen in ontvangst. De oplichtingen betreffende de woning in de [adres 2] heeft [persoon 1] alleen gepleegd, dus zonder dat verdachte daarbij een rol heeft gespeeld.

Ten aanzien van de minderjarige slachtoffers (feiten 1 tot en met 61) maakt de verdediging gebruik van terugkerende redeneringen. Op basis daarvan is betoogd dat verdachte niet de gebruiker kan zijn geweest van de verschillende – onderling verbonden – accounts. Het gaat daarbij om vijf redeneringen, door de verdediging aangeduid als 'ontkoppelingsmethoden':
1. Verdachte is niet te koppelen aan een deel van de IP-adressen waarvan Facebook in haar rapport stelde dat accounts van de dader daarvan gebruik maakten.
2. Het telefoonnummer uit het Facebookrapport dat de dader van de oplichting van de [adres 2] gebruikte kan niet met verdachte in verband gebracht worden.
3. Wanneer de verdediging kijkt naar het laatste contact tussen de dader en het slachtoffer, constateert zij dat in die periode geen koppelingen met verdachte beschikbaar waren op de harde schijven in de woning van verdachte, omdat de data dan al waren verwijderd op de harde schijf.
4. De twee harde schijven waarop het belastend materiaal is aangetroffen waren niet van verdachte, maar van [persoon 1].
5. De versleutelde harde schijf was eveneens van [persoon 1].

6 Het zou uiteindelijk gaan om de volgende harde schijven: OI013.02.02.002 (*Maxtor*); OI013.04.01.002 (*Hitachi*); OI013.04.01.005 (*Western Digital*).

6.3. ***Het oordeel van de rechtbank***

(…)

Tussenconclusie:
Het bestaan van [persoon 1] (als persoon die een rol speelt bij de tenlastegelegde feiten) is niet aannemelijk geworden. Ook heeft verdachte geen handvatten gegeven die verder onderzoek naar de identiteit van [persoon 1] mogelijk maken.
Bij de verdere beoordeling van de feiten wordt er dan ook van uitgegaan dat de door verdachte opgevoerde [persoon 1] niet bestaat.

6.3.2. ***Heeft verdachte de accounts gebruikt?***

Inleiding
De zedenfeiten werden via internet gepleegd. De vraag die moet worden beantwoord, is of verdachte de persoon is achter de accounts die daarvoor werden gebruikt. De verschillende accounts die gebruikt zijn, lijken door één persoon te zijn gebruikt. De accounts lijken bij elkaar te horen, wanneer het ene account verwijst naar het andere account. Daarmee lijken die accounts een netwerk te vormen. Op verschillende plaatsen kan een verband gelegd worden tussen de online accounts en de fysieke, echte wereld. Dat zijn ook de plaatsen waar gekeken kan worden welke persoon achter die accounts zit.

(…)

Technisch hulpmiddel
De politie installeerde op de desktopcomputer in de woning van verdachte een technisch hulpmiddel. Verdachte verklaarde in april 2015 bij de rechter-commissaris dat hij in principe de enige gebruiker was van de desktop. Het technisch hulpmiddel registreerde dat de gebruiker van die computer was ingelogd op het Yahoo-account [account 8]. '[alias 4]' gaf op een eerder moment via dit e-mailadres aan D35 de opdracht om via Western Union geld aan verdachte over te maken.

Het technisch hulpmiddel registreerde ook het gebruik van het e-mailadres [account 9]. [alias 5] is de naam die verdachte gebruikte om zijn woning op het park [bungalowpark 2] te huren.

Tussenconclusie:
Verdachte was de gebruiker van de desktopcomputer en hij verrichtte de handelingen die door het technisch hulpmiddel zijn vastgelegd. Verdachte is de persoon achter '[account 8]' en '[alias 4]'.

[account 10]
Het technisch hulpmiddel registreerde ook het gebruik van het Skype-account ' [account 10] '. Geregistreerd werd dat [account 10] een seksueel getinte chat voerde met een jong meisje. Ook had [account 10] contact met een Skype-account van D15 op momenten dat een Britse undercoveragent daarvan gebruik maakte. Dat contact vond plaats op 10 januari 2014, tussen 16.09 en 16.25 uur (Engelse tijd), en 13 januari 2014, tussen 20.48 en 20.58 uur (Engelse tijd).
Op beide tijdstippen was verdachte in zijn woning aanwezig.

Op 10 januari 2014 is de communicatie in de woning gedurende bijna drie uur opgenomen. In de periode waarin de chat tussen de undercoveragent en [account 10] plaatsvond, zijn er toetsaanslagen te horen. Ook is er af en toe gemompel en gevloek van verdachte te horen. Uit het procesverbaal van de opname kan op geen enkele manier worden afgeleid dat behalve verdachte nog een andere persoon in de woning aanwezig was en verdachte heeft daarover ook niet verklaard. Daarom neemt de rechtbank aan dat verdachte toen alleen in de woning was.
Op 13 januari 2014 stond de woning van verdachte vanaf 18.00 uur (Nederlandse tijd) onder observatie. Die observatie duurde tot aan het moment dat de politie de woning van verdachte binnenviel en verdachte om 22.00 uur (Nederlandse tijd) werd aangehouden. Tussen 18.00 uur en 22.00 uur zag het observatieteam geen personen aankomen of weggaan bij de woning van verdachte. Verdachte was de enige persoon in de woning ten tijde van de aanhouding en hij was dus ook tijdens de chat op 13 januari 2014 (die tot twee minuten voor zijn aanhouding voortduurde) alleen in de woning.

Het Skype-account [account 10] staat ook in verband met andere onderzoeksgegevens. Zo werd op de laptop uit de woning van verdachte een verwijzing naar het account aangetroffen. Ook gaven de Hotmailaccounts [account 11] en [account 12] aan dat andere gebruikers hen op Skype konden toevoegen via het account [account 10]. De contactenlijsten van deze Hotmailaccounts zijn weer aangetroffen op de Western Digital harde schijf. Het Facebookaccount ' [alias 6] ' zond in mei 2013 als statusbericht dat zij een nieuw Skype-account heeft: [account 10]. Eerder noemde [alias 6] [account 12] als haar (zijn) MSN-account. [alias 6] gaf ook door dat contact opgenomen moest worden met [alias 3] via het e-mailadres [account 3]. Dat was het e-mailadres dat hoorde bij het Skrill-account waarna D38 en D39 geld moesten overmaken.

Tussenconclusie:
Verdachte was de gebruiker van het Skype-account [account 10]. De verankering op verschillende gegevensdragers laat zien dat die bij elkaar horen en één gebruiker hebben: verdachte. De koppeling met [account 3] laat ook zien dat de [account 10 t/m 12]-aliassen (typerend voor het chanteren van jonge meisjes) en de [alias 3]-aliassen (typerend voor het chanteren van mannen) bij elkaar horen en door verdachte gebruikt worden.

Virtuele webcams
Uit de registraties van het technisch hulpmiddel blijkt dat de dader gebruik maakte van een virtuele webcam. Op

verschillende gegevensdragers die in de woning van verdachte zijn aangetroffen, vond de politie programma's voor een virtuele webcam. Zo werd het programma 'Manycam' aangetroffen op de laptop, de desktop en de Hitachi harde schijf. Daarnaast werd op de Hitachi harde schijf, de Western Digital harde schijf en de laptop het programma 'WebcamMax' aangetroffen. Daarnaast werden op weer een andere harde schijf[7] installatieprogramma's aangetroffen van zowel Manycam als Webcammax. Het gebruik van een virtuele webcam door de dader bleek uit de registraties van het technisch hulpmiddel. Ook bleek dit uit een opname die werd aangetroffen op de Western Digital harde schijf.

Tussenconclusie:
Het op verschillende gegevensdragers aantreffen van dezelfde virtuele webcams ondersteunt de conclusie dat die gegevensdragers één gebruiker hebben en dat die gegevensdragers onder meer werden gebruikt voor het chanteren van jonge meisjes en mannen.

(…)

Conclusie: verdachte is de gebruiker van de accounts en de gegevensdragers
Het voorgaande laat zien dat verschillende belastende gedragingen en verschillende gegevensdragers met belastende informatie met elkaar verbonden zijn. Steeds als er een *echt* persoon in beeld komt, is dat verdachte. Verdachte stond op camerabeelden bij een Western Union-transactie, verdachte lichtte huurders van de [adres 1] op, de harde schijven en de documenten van Skrill lagen in de woning van verdachte, en het technisch hulpmiddel op de desktopcomputer van verdachte registreerde een seksueel getinte chat met een jonge vrouw.
Voor zover verdachte over deze omstandigheden verklaarde, verklaarde hij dat niet hij, maar [persoon 1] de dader was. Maar de rechtbank gaat ervan uit dat [persoon 1] niet bestaat. Ook verder zijn er geen omstandigheden die erop wijzen dat verdachte niet degene was die achter het netwerk van accounts zit. Bij de verdere beoordeling van de feiten wordt er dan ook vanuit gegaan dat verdachte de persoon achter het netwerk van accounts is. Dat geldt temeer omdat bij chats van 10 en 13 januari 2014 met het account van één van de minderjarige slachtoffers, verdachte degene moet zijn geweest die chatte.

6.3.3. ***Handvatten om de omvang van het netwerk van accounts vast te stellen***

Inleiding
De volgende vraag die beantwoord moet worden is welke accounts onderdeel uitmaken van het netwerk van verdachte. Daarbij wordt ervan uitgegaan dat verdachte de enige gebruiker is geweest van de harde schijven in zijn woning en de in deze zaak relevante accounts. Op zichzelf hoeft het niet zo te zijn dat de harde schijf of een account slechts door één persoon wordt gebruikt, maar het dossier bevat geen aanwijzingen dat naast verdachte ook anderen hiervan gebruik hebben gemaakt. In het bijzonder bevat het dossier geen aanwijzingen dat een ander (een deel van) de belastende berichten verstuurde of de belastende berichten op de harde schijven zette. Van een verdachte mag in zo'n situatie worden verwacht dat hij een concrete inhoudelijke verklaring geeft als hij slechts een deel van de berichten zou hebben verstuurd. Verdachte heeft zo'n verklaring niet gegeven. Zijn verklaring over [persoon 1] is dat in elk geval niet.

(…)

Eindconclusie
Op basis van het dossier moet worden vastgesteld dat verdachte de gebruiker is van de in zijn woning aangetroffen gegevensdragers en dat hij de gebruiker is van een groot netwerk van accounts. De ontkoppelingsmethoden van de verdediging kunnen de accounts niet van het netwerk losmaken. Het door de rechtbank vastgestelde netwerk van accounts die steeds naar verdachte zijn te herleiden blijft dan ook in stand.

(…)

8 **Juridische kaders strafbaarstellingen**

8.1. ***Feitelijke aanranding van de eerbaarheid (artikel 246 Sr)***

8.1.1 Het standpunt van de verdediging
Er is geen sprake van aanrandingen of pogingen tot aanranding, omdat geen sprake is van lichamelijk contact tussen dader en slachtoffer. Bij '*hands off*'-delicten is alleen in uitzonderlijke gevallen sprake van dwang en dat is nu niet het geval. Die dwang vereist namelijk onvrijwilligheid en onvermijdbaarheid aan de kant van het slachtoffer. Met name de onvermijdbaarheid is moeilijk voorstelbaar wanneer de dader en het slachtoffer alleen op afstand contact hebben gehad. Daarom moet verdachte worden vrijgesproken van de ten laste gelegde (pogingen tot) aanranding.

8.1.2. Het standpunt van de officier van justitie
De (pogingen tot) aanranding kan worden bewezen. De officier van justitie wijzen ter ondersteuning op een arrest van het gerechtshof Arnhem-Leeuwarden.[8] In die zaak veroordeelde het gerechtshof de verdachte voor vergelijkbare feiten. Ook in die zaak moesten de slachtoffers ontuchtige handelingen voor de webcam plegen en werd gedreigd 'alles op internet te zetten'. Die uitspraak is definitief geworden, nadat de Hoge Raad de bezwaren van verdachte tegen die uitspraak verwierp.[9]

7 OI013.03.03.001 (*Maxtor*).

8 ECLI:NL:GHARL:2015:9221.

9 ECLI:NL:HR:2017:39, conclusie van de advocaat-generaal bij deze zaak: ECLI:NL:PHR:2016:1392.

8.1.3 Het oordeel van de rechtbank

In deze zaak gaat het steeds om (pogingen tot) aanranding op afstand. Het gaat ook om seksuele handelingen waarbij lichamelijk contact tussen de dader en het slachtoffer niet nodig is. De slachtoffers moesten immers seksuele handelingen bij zichzelf verrichten. Die handelingen waren via een webcam voor verdachte zichtbaar. Als het slachtoffer die handelingen niet wilde verrichten, dreigde verdachte via internet een seksueel getinte afbeelding van het slachtoffer te verspreiden in haar (sociale) omgeving. Ook daarvoor is het niet nodig dat sprake is van lichamelijk contact tussen de dader en het slachtoffer. Omdat zowel de seksuele handelingen als het dreigen in deze zaak kan plaatsvinden zonder dat lichamelijk contact noodzakelijk is, kan sprake zijn van aanranding.

Juist omdat het slachtoffer niet bij verdachte was, had zij geen enkele mogelijkheid om te verhinderen dat de dader de afbeelding zou verspreiden. Voor het slachtoffer was het daarom onvermijdbaar dat het dreigement (het verspreiden van de foto/video) zou worden uitgevoerd, als zij niet zou toegeven aan de dader. Het slachtoffer verkeerde in een onmogelijke positie: zij kon slechts kiezen uit twee opties die zij beiden niet wilde: of zij moest (opnieuw) bij zichzelf seksuele handelingen voor de webcam verrichten, of een seksueel getinte afbeelding van haar werd in haar omgeving verspreid als zij niet deed wat verdachte zei. De uitspraak waarnaar de officier van justitie verwijst, bevestigt bovendien dat een feitencomplex zoals dat in deze zaak aan de orde is, aanranding kan opleveren.

(…)

9 **Bewezenverklaring**

De rechtbank acht de feiten bewezen zoals die in de bewezenverklaring zijn opgenomen. De bewezenverklaring is als bijlage 2 aan dit vonnis gehecht en geldt als hier ingevoegd. Voor zover in de tenlastelegging taal- en/of schrijffouten voorkomen, zijn deze in de bewezenverklaring verbeterd. Verdachte is hierdoor niet in zijn verdediging geschaad.

10 **Bewijs**

De rechtbank baseert haar beslissing dat verdachte de bewezen geachte feiten heeft begaan op de feiten en omstandigheden die in de bewijsmiddelen zijn opgenomen. Het overzicht van de bewijsmiddelen is als bijlage 3 aan dit vonnis gehecht en geldt als hier ingevoegd.

Omdat de bewijsconstructie van de verschillende feiten sterk met elkaar samenhangt, worden de bewijsmiddelen gebruikt voor alle feiten.

11 **De strafbaarheid van de feiten**

De bewezen geachte feiten zijn volgens de wet strafbaar. Het bestaan van een rechtvaardigingsgrond is niet aannemelijk geworden.

12 **De strafbaarheid van verdachte**

Er is geen omstandigheid aannemelijk geworden die de strafbaarheid van verdachte uitsluit. Verdachte is dan ook strafbaar.

13 **Motivering van de gevangenisstraf**

13.1. ***De eis van de officier van justitie***

De officier van justitie gaat bij de strafeis uit van de 72 door haar bewezen geachte feiten. Zij vorderen dat verdachte wordt veroordeeld tot de maximale straf die op die feiten is gesteld: een gevangenisstraf van tien jaar en acht maanden, met aftrek van voorarrest.

Voor het opleggen van een minder zware straf ziet de officier van justitie geen ruimte. Daarbij kijken zij in de eerste plaats naar de ernst en de hoeveelheid strafbare feiten die verdachte heeft gepleegd. Ook wegen zij de proceshouding van verdachte mee; in het bijzonder dat verdachte geen verantwoording over zijn daden heeft willen afleggen en dat verdachte niet heeft willen meewerken aan het psychologisch en psychiatrisch onderzoek. De noodzakelijke bescherming van de maatschappij kan dan alleen worden bereikt door verdachte zo lang mogelijk vast te zetten.

13.2. ***Het standpunt van de verdediging***

De verdediging verzoekt een fors lagere straf op te leggen dan de straf die door de officier van justitie is geëist. Daarbij heeft zij verwezen naar uitspraken van andere rechtbanken en gerechtshoven.

13.3. ***Het oordeel van de rechtbank***

Het heeft erg lang geduurd voordat deze zaak op zitting kon worden behandeld, en voordat er uitspraak kon worden gedaan. Verdachte is op 13 januari 2014 aangehouden en op 16 maart 2017 is de uitspraak. Dat is onwenselijk, niet alleen voor verdachte maar ook voor de slachtoffers en de samenleving. De lange duur is allereerst het gevolg van het grote onderzoek en van de internationale kant ervan. Dat het einddossier in mei 2015 aan de rechtbank en de verdediging is gegeven, is dan ook niet onredelijk lang. Daarna heeft nog onderzoek plaatsgevonden op verzoek van de verdediging. De inhoudelijke zitting zou plaats vinden vanaf 1 april 2016. Die zitting kon echter niet doorgaan omdat verdachte een andere advocaat wilde. De zaak kon pas vanaf januari 2017 inhoudelijk worden behandeld. Er is geen sprake van schending van de redelijke termijn waarbinnen zaken moeten worden afgedaan, en er is ook geen reden om in de strafmaat rekening te houden met het tijdsverloop.

Deze zaak is bijzonder, in de eerste plaats omdat verdachte anderen heeft geschaad ten behoeve van zijn eigen behoeften en van zijn eigen geldelijk gewin, en dat op grote schaal en op niets ontziende wijze.

Dat heeft verdachte allereerst gedaan door mensen die een woning dachten te huren, geld te laten betalen, terwijl zij

de woning vervolgens niet kregen, en door de gegevens van slachtoffers van die oplichtingen dan weer te gebruiken om bankrekeningen op hun naam te openen.
Verder heeft verdachte ingebroken op het wifi-verbinding van een ander, waarmee verdachte zelf onder de radar bleef. De officiële gebruiker van dat WiFi-adres komt daardoor als mogelijke verdachte in beeld tijdens het politie-onderzoek, terwijl die onwetend is over het illegale gebruik van zijn internetverbinding.

Verdachte heeft daarnaast geld buitgemaakt door zich op chatsites eerst voor te doen als een puberjongen, die seksueel getint contact zocht met volwassen mannen, en door vervolgens een van die mannen te chanteren met opnamen die verdachte van dat contact had gemaakt.
Maar bovenal is verdachte chatcontacten aangegaan met tientallen jonge meisjes, waarbij hij zich als jongen of meisje voordeed en hun vertrouwen wist te winnen. En dat vertrouwen misbruikte verdachte vervolgens. In veel gevallen wist hij die meisjes ertoe te brengen voor de webcam seksuele handelingen te verrichten. Later legde hij dan weer contact met de meisjes en eiste nieuwe 'shows' voor de webcam, want anders zou hij mensen in hun omgeving beeldmateriaal toesturen of de beelden op pornosites plaatsen. Soms lukte het om de meisjes op die manier te misbruiken. Maar als een meisje niet op zijn eisen inging, deinsde verdachte er niet voor terug om daadwerkelijk seksuele beelden aan de familie en vrienden van het slachtoffer te sturen of op het web te plaatsen. Het laat zich raden welke grote en beschadigende impact dit kan hebben op de persoonlijke ontwikkeling van jonge meisjes.

De rechtbank hecht eraan om op te merken dat de meisjes enkel en alleen slachtoffer zijn. Zij zijn door een geraffineerde en doortrapte volwassen man in de val gelokt. Verdachte richtte zich speciaal op chatsites voor (jonge) pubers, en het is algemeen bekend dat die vaak onzeker en kwetsbaar zijn. Sommige slachtoffers waren aanvankelijk zelfs niet ouder dan negen of tien jaar.
Het dossier geeft een indringend beeld hoe groot de druk was die verdachte met zijn dreigementen uitoefende op de meisjes. Verdachte dreigde vaak expliciet dat hij het leven van het meisje zou ruïneren.

(…)

Het is verbijsterend dat verdachte, als een meisje niet ingaat op zijn dreigementen, het materiaal daadwerkelijk openbaar maakt met alle verwoestende gevolgen voor het jonge leven van de meisjes van dien. Hoewel de kans niet groot lijkt dat het slachtoffer na die openbaarmaking alsnog zal doen wat hij wil, is het kennelijk voor verdachte belangrijker dat het meisje door hem 'gestraft' wordt en lijdt. Hier schiet ieder inlevingsvermogen in de denkwereld van verdachte tekort.
Uit de verklaringen van de meisjes blijkt hoe bang zij zijn geweest en soms nog zijn. Ook is duidelijk geworden hoe ingrijpend de gevolgen van het handelen van verdachte zijn geweest en nog steeds zijn voor de slachtoffers, maar ook voor hun families.

Het geheel van de gepleegde feiten is zodanig schokkend, dat uit een oogpunt van vergelding alleen een gevangenisstraf van vele jaren op zijn plaats is.

Op de bewezen feiten staan verschillende maximale gevangenisstraffen, waarvan de hoogste acht jaar is. Volgens het Nederlandse recht is het niet toegestaan om de straffen voor de individuele feiten eenvoudigweg bij elkaar op te tellen. De straf voor alle bewezen feiten samen mag niet meer bedragen dan de hoogste maximale straf die op de feiten is gesteld, en dan vermeerderd met een derde daarvan. In dit geval levert dat een maximale straf op van tien jaar en 243 dagen.
De rechtbank heeft geprobeerd inzicht te krijgen hoe verdachte tot dergelijke feiten heeft kunnen komen. Dat inzicht is niet ontstaan. Verdachte heeft niet willen meewerken aan onderzoek door gedragsdeskundigen en hij heeft ook maar heel weinig over zichzelf willen verklaren. Hij heeft verder de feiten kortweg ontkend en heeft nooit enige uitleg gegeven of verantwoording afgelegd.
Uit het dossier komt wel het volgende beeld van verdachte naar voren:

Verdachte probeerde in de maatschappij anoniem te leven. Hij was niet bij een gemeente ingeschreven maar woonde in wisselende vakantiehuisjes, onder valse namen. Hij staat bij zijn (enige twee) vrienden bekend als een filosoof en natuurmens, die geen belangstelling heeft voor seks. Verdachte heeft echter veel gezichten, hij kan zich beleefd en charmant voordoen, bijvoorbeeld op het vakantiepark en tegenover de oplichtingsslachtoffers. Hij kan zich voordoen als een betrouwbare chatvriendin, bijvoorbeeld [account 10 t/m 12], maar als webcamafperser lijkt verdachte plezier te beleven aan de vernedering en de angst van de meisjes, en hij lijkt daardoor ook seksueel opgewonden te worden. (…)

Hij wekt de indruk niet gehinderd te worden door zijn geweten en ook niet door geldende wetten.
Nu niet is vastgesteld dat verdachte – kort gezegd – een stoornis heeft, is hij volledig verantwoordelijk voor zijn daden. Er is dus geen reden voor strafvermindering. Maar dat betekent ook dat verdachte niet kan worden veroordeeld tot opname en behandeling, omdat oplegging van de Tbs-maatregel is uitgesloten als er geen sprake is van een stoornis.

Omdat verdachte makkelijk mensen misbruikt als hem dat uitkomt en hij kennelijk (ook) gedreven wordt door seksuele motieven, maakt de rechtbank zich zorgen dat verdachte na invrijheidstelling nieuwe, ernstige strafbare feiten zal plegen. Ook die omstandigheid is een reden om verdachte zo lang mogelijk uit de maatschappij te verwijderen.

De bovenstaande overwegingen van de rechtbank kunnen maar tot één conclusie leiden. Verdachte wordt veroordeeld

tot de maximale gevangenisstraf, te weten tien jaar en 243 dagen.

(...)

Noot

1. In 2012 leidt de zelfmoord van de 15-jarige Amanda Todd tot wereldwijde aandacht.[10] Amanda beroofde zichzelf van het leven nadat ze met blootfoto's werd gechanteerd door een onbekende. Deze persoon bleek 'Aydin C.' te heten, woonachtig in Nederland. Op 31 maart 2017 is hij voor deze vorm van online aanranding en andere delicten door de Rechtbank Amsterdam veroordeeld tot de maximale gevangenisstraf van tien jaar en 243 dagen. Daarnaast heeft de Hoge Raad op 4 april 2017 beslist dat de verdachte mag worden uitgeleverd naar Canada.[11] Amanda Todd had de Canadese nationaliteit.

Vanuit juridisch perspectief is deze uitspraak om drie redenen interessant. Deze zijn als volgt:
- De zaak biedt inzicht in de *modus operandi* van online zedendelinquenten en opsporingsautoriteiten in cybercrimezaken.
- In deze zaak komt voor het eerst naar voren dat de politie *software* gebruikt voor het vastleggen van gedragingen van de verdachte achter zijn computer.
- De zaak geeft duidelijkheid over de juridische kwalificatie van *online aanranding*.

In deze noot worden deze drie aspecten uitgelicht.

Modus operandi

2. In de uitspraak wordt uitgebreid beschreven hoe de verdachte is opgespoord door de politie. Een belangrijk probleem voor de opsporing in cybercrimezaken is dat de verdachte relatief anoniem kan blijven op internet. De politie moet bewijzen dat een verdachte achter zijn toetsenbord zat ten tijde van de gedragingen. In het geval van Aydin C. nam de verdachte verschillende maatregelen om anoniem te blijven. Hij maakte gebruik van verschillende huisjes in bungalowparken en een VPN-verbinding om zijn netwerkverkeer langs een andere server te routeren, om op die wijze zijn IP-adres en fysieke locatie te verhullen.[12] Ook heeft hij paspoorten van andere mensen misbruikt ten behoeve van de registratie voor een online betalingsdienst (Skrill). Ten slotte heeft hij van Western Union gebruikgemaakt voor het ophalen van de bedragen (in totaal meer dan € 30.000) die hij door webcamafpersing heeft verkregen. Met slechts enkele gegevens kunnen mensen via Western Union wereldwijd geld overmaken. De geldtransferdienst is ook welbekend bij drugsdealers en witwassers.[13]

3. Tijdens zijn communicatie met minderjarige meisjes en volwassen mannen deed Aydin C. zich voor als een minderjarige jongen om de betrokkenen te verleiden tot het plegen van seksuele handelingen. Daarvoor maakte hij onder andere gebruik van verschillende Facebook accounts. Deze activiteiten zijn Facebook niet ontgaan en dit bedrijf heeft een belangrijke bijdrage aan de zaak geleverd door gegevens van de verdachte, waaronder zijn IP-adres en telefoonnummer, met de Nederlandse autoriteiten te delen. Het IP-adres leidde naar een adres op een bungalowpark nabij Oisterwijk. Een IP-tap op de router leverde weinig bruikbare informatie op. Kenmerkend aan een VPN-verbinding is dat deze anonimiseringsdienst tevens het netwerkverkeer versleutelt, waardoor de inhoud van het verkeer onleesbaar wordt. Daarop besloot de politie tijdens een doorzoeking speciale software te installeren, waarbij op afstand informatie over het computergedrag van de verdachte kan worden vergaard. De software bleek cruciaal, omdat daarmee een directe link werd gelegd tussen de communicatie van de verdachte met zijn slachtoffers in combinatie met de strafbare gedragingen.[14] De pogingen van de verdediging om voor elke tenlastegelegde gedraging in twijfel te trekken dat Aydin C. achter de computer zat, heeft voor enkele gedragingen tot vrijspraak geleid. Voor de meeste ten laste gelegde delicten werd echter voldoende bewijs verzameld op basis van (1) aanwijzingen uit andere strafzaken waar Aydin C. bij betrokken was; (2) gegevens die door de Engelse opsporingsautoriteiten zijn versterkt over transacties met Skrill en Western Union; (3) gegevens die zijn verkregen met de geplaatste software; en (4) gegevens op de laptop en gegevensdragers van de verdachte die na een doorzoeking in beslag zijn genomen.

Technisch hulpmiddel – *Software*

4. De zaak is omstreden vanwege het gebruik van de eerder genoemde software door de politie. Al eerder deed de media bericht van het gebruik van een '*keylogger*', waarvan de rechtmatigheid in twijfel werd getrokken.[15] Keyloggers leggen toetsaanslagen vast. Op deze wijze kan communicatie van de verdachte worden vastgelegd, waaronder ingevoerde wachtwoorden. Al 20 jaar geleden werd in de memorie van toelichting van de Wet bijzondere opsporings-

10 Zie bijvoorbeeld: BBC, 'Amanda Todd: Memorial for teenage cyberbullying victim', 17 oktober 2012. Beschikbaar op: www.bbc.co.uk/newsbeat/article/19960162/amanda-todd-memorial-for-teenage-cyberbullying-victim, Zembla, 'De dood van Amanda Todd', 4 december 2014 (documentaire). Beschikbaar op: https://zembla.vara.nl/dossier/uitzending/de-dood-van-amanda-todd en Nos.nl, 'Harddisk vermoedelijke afperser Amanda Todd nog niet gekraakt', 25 januari 2017. Beschikbaar op: https://nos.nl/artikel/2154807-harddisk-vermoedelijke-afperser-amanda-todd-nog-niet-gekraakt.html (laatst geraadpleegd op 9 april 2017).

11 HR 4 april 2017, ECLI:NL:HR:2017:586.

12 Zie voor een meer uitgebreide beschrijving van het anonimiteitsprobleem in cybercrimezaken: J.J. Oerlemans, *Investigating Cybercrime*, diss. Leiden, Amsterdam: Amsterdam University Press 2017, p. 37-41.

13 Zie J.J. Oerlemans e.a., 'Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware', WODC, Onderzoek en Beleid, nr. 319, Meppel: Boom Criminologie 2016, p. 74-75.

14 Het gebruik van Skype en webmail van Yahoo! werd bijvoorbeeld geregistreerd. Zie r.o. 6.2.3.

15 Zie bijvoorbeeld Joost Schellevis, 'Openbaar Ministerie plaatste malware op pc verdachte', *Tweakers*, 24 juni 2014. Beschikbaar op: https://tweakers.net/nieuws/96922/openbaar-ministerie-plaatste-malware-op-pc-verdachte.html (laatst geraadpleegd op 9 april 2017).

bevoegdheden aangegeven dat het plaatsen van keyloggers mogelijk is op basis van de bijzondere opsporingsbevoegdheid 'direct afluisteren'.[16] In 2014 stelde de toenmalige Minister van Veiligheid en Justitie in een Kamerbrief dat het gebruik van '*spyware*' is toegestaan onder de bijzondere bevoegdheid van direct afluisteren, voor zover de software 'fysiek wordt geïnstalleerd' (dus niet op afstand via een hack).[17] Er gelden strenge eisen voor de inzet van deze bijzondere opsporingsbevoegdheid, waaronder een machtiging van een rechter-commissaris.[18] Bovendien moet de inzet van het 'technische hulpmiddel' zijn goedgekeurd op basis van het Besluit technische hulpmiddelen strafvordering.[19]

5. De verdediging voerde aan dat het gebruik van de keylogger onrechtmatig was. Een belangrijk verweer betrof dat de software niet betrouwbaar zou zijn en meer functionaliteiten zou hebben dan slechts het loggen van de '*keystrokes*'. De rechtbank heeft alle verweren verworpen. Mijns inziens heeft zij zich daarbij weinig kritisch getoond. De rechtbank beargumenteerd goed dat uit het Besluit technische hulpmiddelen strafvordering kan worden afgeleid dat een technisch hulpmiddel niet altijd uit een (hardwarematig) apparaat hoeft te bestaan, maar ook uit software kan bestaan. Ook stelt de rechtbank vast dat de software door de inspectie is gekomen en is goedgekeurd. Maar het ontbreekt volgens de verdediging hen aan de mogelijkheid om de opsporingsactiviteiten en de vergaarde gegevens voldoende te controleren.[20] In plaats daarvan is slechts één deskundige van de politie gehoord. Het is vanuit opsporingsperspectief begrijpelijk dat de software zelf niet bekend wordt gemaakt en gecontroleerd kan worden. Het moet echter wel helder zijn van welke functionaliteiten van de software precies gebruik is gemaakt en welke gegevens zijn vergaard, om zowel de *betrouwbaarheid* als de *reikwijdte van de inzet van het middel* te kunnen controleren. In de uitspraak wordt de – ongetwijfeld gevoelige – informatie gedeeld dat het technisch hulpmiddel uit een softwarepakket bestaat, waarbij 'vinkjes kunnen worden aangeklikt' om van de verschillende functionaliteiten gebruik te maken.[21] Op het moment dat bepaalde programma's worden gestart, zoals Skype, treed het programma in werking. Daarbij worden niet alleen toetsaanslagen geregistreerd, maar ook *schermafbeeldingen* gemaakt. Let wel: het gaat dus helemaal niet alleen om een keylogger, maar om een heel softwarepakket met een scala aan mogelijkheden om 'bij de bron' de activiteiten van de verdachte achter zijn computer te monitoren.

6. Mijns inziens dringt nu de vraag zich op of het maken van schermafbeeldingen een functionaliteit is die de wetgever in 1997 voor ogen had toen de bevoegdheid voor het direct afluisteren van communicatie in het Wetboek van Strafvordering werd geregeld.[22] Als dat niet het geval is hoeft dat niet tot bewijsuitsluiting te leiden, maar op deze vraag is nu door de rechtbank niet ingegaan. In de Wet computercriminaliteit III wordt dit vraagstuk overigens opgelost door onomstotelijk vast te stellen dat de software verschillende functionaliteiten mag bevatten, waaronder het maken van schermafbeeldingen.[23] Onder de voorgestelde regeling in de Wet computercriminaliteit III moeten de wenselijke functionaliteiten van de software expliciet in het bevel tot inzet van de hackbevoegdheid worden genoemd en worden de gedragingen van de software nauwlettend vastgelegd.[24] De rechter kan tijdens een strafzaak beslissen tot nader onderzoek van de gelogde gegevens, al dan niet op verzoek van de verdachte of raadsman of verdachte.[25] Daarbij zou mijns inziens de mogelijkheid moeten bestaan om voor dat onderzoek een onafhankelijk deskundige aan te wijzen.

Online aanranding?

7. Ten slotte is de zaak van belang, omdat de rechtbank ingaat op de vraag of aanranding op het internet eigenlijk wel mogelijk is. De verdediging voert aan dat geen sprake kan zijn van aanranding of pogingen tot aanranding, omdat geen sprake is van lichamelijk contact tussen de dader en het slachtoffer. In repliek stelt de officier van justitie dat op basis van vergelijkbare feiten in een andere zaak, poging tot aanranding eerder is bewezen.[26] Ook in die zaak moesten de slachtoffers ontuchtige handelingen voor de webcam plegen en werd gedreigd 'alles op internet te zetten.' De rechtbank bevestigt de aangehaalde zaak en maakt duidelijk dat het hier gaat om (pogingen tot) aanranding *op afstand*; lichamelijk contact tussen de dader en het slachtoffer is daarbij niet noodzakelijk. De slachtoffers moesten seksuele handelingen verrichten, onder dreiging van verspreiding van al eerder door verdachte opgenomen beelden. Omdat zowel de seksuele handelingen als het dreigen in deze zaak kan plaatsvinden zonder dat lichamelijk contact noodzakelijk is, kan sprake zijn van aanranding. Juist omdat het slachtoffer niet bij verdachte was, had zij geen enkele mogelijkheid om te verhinderen dat de dader de afbeelding zou verspreiden. Voor het slachtoffer was het daarom onvermijdbaar dat het dreigement (het verspreiden van de foto/video) zou worden uitgevoerd, als zij niet zou toegeven aan de dader. Daarmee is er sprake van (poging tot) aanranding op afstand.

8. De Wet computercriminaliteit III stelt ook expliciet een dergelijk feitencomplex strafbaar, waarbij slachtoffers worden gedwongen door een 'webcamafperser' om seksuele handelingen te verrichten.[27] Deze vorm van *sextortion*

16 *Kamerstukken II* 1996/97, 25403, 3, p. 35-37.
17 J.J. Oerlemans, 'Antwoord Kamervragen over het gebruik van omstreden spionagesoftware', *Computerrecht* 2014/211.
18 Zie art. 126l Sv voor alle voorwaarden voor inzet van de bijzondere opsporingsbevoegdheid.
19 *Stb* 2006, 524.
20 Zie ook C.T.W. van Dijk, 'De slager die zijn eigen keylogger keurt', *TPWS* 2015/26.
21 Zie r.o. 8.1.2.
22 Één van de advocaten van Aydin C., Van Dijk, stelt in zijn artikel duidelijk dat de software wat hem betreft een stap te ver gaat. C.T.W. van Dijk, 'De slager die zijn eigen keylogger keurt', *TPWS* 2015/26.
23 *Kamerstukken II* 2015/16, 34372, 3, p. 20.
24 *Kamerstukken II* 2015/16, 34372, 3, p. 102.
25 Zie *Kamerstukken II* 2016/17, 34372, 6, p. 59.
26 Zie Gerechtshof Arnhem-Leeuwarden 8 december 2015, ECLI:NL:GHARL:2015:9221, m.nt. Tina van der Linden-Smit en Kea Kroeks-de Raaij in UDH:IR/13054.
27 *Kamerstukken II* 2015/16, 34372, 3, p. 68.

wordt strafbaar gesteld in het voorgestelde artikel 248a Sr. Op deze manier kan deze groeiende vorm van cybercrime eenvoudiger worden vervolgd. De Aydin C.-zaak laat zien dat de politie ook succesvol de meer geraffineerde cybercriminelen kan opsporen. Daarbij is van een innovatief middel gebruikgemaakt dat in de toekomst ongetwijfeld vaker zal worden ingezet onder de nieuwe hackbevoegdheid.

Mr. dr. J.J. Oerlemans