de Rechtspraak

Art. 240b Sr

Juridische en digitaal-technische aspecten van strafvervolging wegens gedragingen met digitaal kinderpornografisch materiaal

Kenniscentrum Cybercrime

versie 4.0 (2023)

mr. J.W. van den Hurk, senior raadsheer/onderzoeker
mr. R.J.A. Klaar, juridisch adviseur/onderzoeker
mr. J.J. Mossink, senior gerechtsjurist

cybercrime@rechtspraak.nl

Colofon

Art. 240b Sr
Juridische en digitaal-technische aspecten van strafvervolging wegens gedragingen met digitaal kinderpornografisch materiaal

Dit is een uitgave van het Kenniscentrum Cybercrime voor de Rechtspraak.

Correspondentieadres:
Postbus 20302, 2500 EH Den Haag
Telefoon secretaris: 06-25656510
E-mailadres: cybercrime@rechtspraak.nl
Website: Wiki Juridica Kenniscentrum Cybercrime

Bezoekadres:
Prins Clauslaan 60, 2595 AJ Den Haag

Art. 240b Sr

Juridische en digitaal-technische aspecten van strafvervolging wegens gedragingen met digitaal kinderpornografisch materiaal

HOOFDSTUK 1: INLEIDING

1.1. Waarom dit e-book?

Jaarlijks worden er grote aantallen zaken[1] bij de strafrechter aangebracht die - kort gezegd - gaan over gedragingen met betrekking tot kinderpornografische[2] afbeeldingen. Vrijwel altijd gaat het daarbij om kinderpornografische afbeeldingen die zijn aangetroffen op een computer of mobiel apparaat (zoals: een smartphone, of een tablet), of om materiaal dat zou zijn verzonden vanaf (of ontvangen op) een computer of mobiel apparaat. Een computer of mobiel apparaat die/dat bovendien veelal weer onderdeel uitmaakt van een netwerk dat in verbinding staat met het internet. Veel gebruikers hebben echter slechts een beperkte kennis van het functioneren van hun computer of mobiel apparaat.

Terzijde merken wij op dat ten behoeve van de leesbaarheid in dit boek regelmatig het woord 'computer' of 'device[3]' wordt gebruikt in plaats van de juridische aanduiding 'geautomatiseerd werk' en/of 'gegevensdrager'. Als de tekst daarom vraagt gebruiken wij een specifieke feitelijke omschrijving van het apparaat. Bovendien mag waar over 'computer' wordt gesproken in beginsel ook 'device' worden gelezen, en vice versa, tenzij anders aangegeven.

Het enkele aantreffen van kinderpornografisch materiaal op een computer of mobiel apparaat zegt bepaald niet alles over wat nu de intentie van de betreffende gebruiker van deze computer of dit mobiel apparaat was met betrekking tot dat materiaal, of hij nog daadwerkelijk kon beschikken over dat materiaal en zelfs niet zonder meer of hij zich van de aanwezigheid van dat materiaal bewust was of had moeten zijn. Dit is van belang omdat het bezit (etc.) van kinderporno alleen strafbaar is, indien dat *opzettelijk* plaatsvindt, waarvoor in de regel onder meer wetenschap van en beschikkingsmacht over het betreffende materiaal is vereist.

Naast deze aspecten van wetenschap, intentie en beschikkingsmacht met betrekking tot gegevens op een computer is ook het gegeven van belang dat computers tegenwoordig eigenlijk standaard onderdeel uitmaken van een (al dan niet draadloos) netwerk, en via een internetaansluiting ook verbonden zijn met het internet. De jurisprudentie laat gevallen zien waarin (onbevoegd) gebruik is gemaakt van de internetaansluiting van een ander, waardoor het lijkt of bepaald gegevensverkeer van de normale gebruiker van die verbinding afkomstig is, terwijl dat in werkelijkheid door de "inbreker" werd verzonden.[4] Technisch is het bovendien mogelijk dat een ander dan de eigenaar/primaire gebruiker zich (direct of via internet) toegang verschaft tot een bepaalde computer en met die computer handelingen, zoals bijvoorbeeld het downloaden van kinderporno, verricht. Dat kan bijvoorbeeld via het - al dan niet met speciale software - op afstand "inbreken" op die computer, maar het kan ook een huisgenoot of collega zijn die het voor het gebruik van die computer vereiste wachtwoord of de toegangscode kent.

---

[1] Er zijn geen exacte cijfers bekend, omdat kinderpornografiezaken niet als aparte delictgroep worden geregistreerd en art. 240b-feiten daarnaast ook wel tegelijkertijd met andere (zeden)feiten ten laste worden gelegd. Uit de rapportages van Team bestrijding kinderporno en kindersekstoerisme (TBKK) van de Nationale Politie (meest recent over het jaar 2019) volgt dat in 2019 193 onderzoeken zijn verricht naar vervaardigers en misbruikers. Verder zijn er 632 onderzoeken naar bezitters dan wel verspreiders van kinderporno uitgevoerd.

[2] Het CBS rapporteert jaarlijks het aantal misdrijven, door de politie vastgelegd in een proces-verbaal van aangifte of in een ambtshalve opgemaakt proces-verbaal. In 2022 en 2021 is in de categorie "pornografie", breder dan kinderpornografie *sec* omdat het de artikelen 240 tot en met 240b Sr betreft, een totaalaantal van respectievelijk 460 en 450 zaken geregistreerd, waarbij wordt vermeld dat het gaat om voorlopige cijfers.

[3] Denk bijvoorbeeld aan tablets, camera's, smart tv's en -telefoons etc.

[4] HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.

Genoemde voorbeelden maken duidelijk dat zelfs als kinderpornografisch materiaal aan een bepaalde computer of internetaansluiting gelinkt kan worden, daarmee nog niet gegeven is dat de normale gebruiker van die computer strafrechtelijk verantwoordelijk is voor de handelingen die kennelijk met dat materiaal via zijn computer(verbinding) zijn verricht. De praktijk heeft geleerd dat voor een goede beoordeling van de (bewijs)vraag of sprake is van strafbare betrokkenheid bij, of opzet op, handelingen met digitale kinderpornografische afbeeldingen minimale kennis van een aantal meer technische ICT-aspecten onontbeerlijk is. Omdat dergelijke kennis niet vanzelfsprekend onderdeel uitmaakt van de opleiding van juridische beroepsbeoefenaren, en daarover in de praktijk bovendien veel vragen blijken te bestaan, is vanuit het Kenniscentrum Cybercrime voor de Rechtspraak besloten een publicatie te maken die speciaal op dit onderwerp is gericht.

1.2. Beoogde doelgroep, gekozen beperkingen en 'disclaimer'

Deze publicatie is bewust zo opgezet dat er naast de bespreking van de juridische aspecten ook nadrukkelijk ruimte is ingeruimd voor het toelichten van een aantal ICT-technische aspecten. Daarbij gelden echter wel een aantal voorbehouden.

Allereerst kunnen door de snelle en brede ontwikkelingen op dit gebied in de toelichtingen slechts een beperkt aantal onderwerpen worden besproken en zal daarbij ook nooit de volledige actualiteit kunnen worden verzekerd. Voorts is van belang zich te realiseren dat in deze uitgave nadrukkelijk gekozen is voor een uitleg die is toegesneden op een overwegend niet ICT-technisch onderlegde doelgroep. Dat betekent dat, waar dat zou kunnen bijdragen aan een vergroting van het begrip, bijvoorbeeld ook gebruik wordt gemaakt van voorbeelden uit de analoge wereld. Ook is gepoogd ICT-technisch vakjargon tot een minimum te beperken. Deze keuzes kunnen betekenen dat "echte" ICT-deskundigen de technische toelichtingen te algemeen en/of niet 100% precies of volledig zullen vinden en dat het dus goed mogelijk is dat ze daarin gelijk hebben. De uitleg van technische begrippen in deze uitgave is derhalve geschikt noch bedoeld om als vervanging te dienen voor de inbreng in een concrete zaak van een deskundige en dient dan ook niet als zodanig te worden gebruikt. Wil men de betreffende informatie wel bij een individuele zaak betrekken, dan zal een en ander langs de geëigende strafvorderlijke weg, *en in de specifieke context van de betreffende zaak*, aan een ICT-deskundige moeten worden voorgelegd en/of door deze moeten worden bevestigd.

Wel wordt met deze publicatie beoogd de juridische doelgroep een beter algemeen begrip te geven van voor de beoordeling van dossiers, deskundigenrapporten en verweren in kinderpornozaken mogelijk relevante ICT-technische en juridische aspecten, zodat de dialoog met partijen en deskundigen over hetgeen in de individuele zaak voorligt op een kwalitatief hoger niveau kan worden gevoerd en beslissingen beter onderbouwd kunnen worden.

In het kader van deze uitgave zijn behalve relevante literatuur ook vele honderden uitspraken op rechtspraak.nl en de digitale database van het Kenniscentrum Cybercrime aanwezige uitspraken op het gebied van "digitale kinderpornografie" geanalyseerd. Waar in de tekst naar wets- en verdragsbepalingen, uitspraken of literatuur wordt verwezen, zijn deze zoveel mogelijk ook (en soms ook daarbuiten) via op het open internet en binnen de digitale rechtspraakomgeving werkende hyperlinks direct benaderbaar gemaakt.[5]

[5] Daartoe zal men wel aangemeld moeten zijn op Legal Intelligence en/of Kluwer Navigator. Voor een aantal hyperlinks geldt dat deze alleen bruikbaar zijn voor hen werkzaam bij De Rechtspraak.

Met betrekking tot de technische informatie zijn voor elk onderwerp diverse bronnen geraadpleegd en zijn de teksten ook voorgelegd aan diverse deskundigen. In aanvulling op de toelichting van een aantal ICT-technische aspecten in deze publicatie zij ook verwezen naar het Cybersecurity Woordenboek. In deze uitgave zijn vele technische begrippen op heldere wijze en in begrijpelijk Nederlands uitgelegd. De woordenlijst is omvangrijk en met name gericht op de bespreking van de terminologie van cybersecuritybegrippen. Voor een meer op cybercrime, digitale opsporing en digitaal bewijs gerichte begrippenlijst zij verwezen naar de cyberbegrippenlijst op de (besloten) Wiki Juridica-pagina van het Kenniscentrum Cybercrime.

1.3. De verdere opzet van dit e-book

De opzet van dit e-book is als volgt. In hoofdstuk 2 wordt een kort overzicht gegeven van de relevante nationale en internationale regelgeving, en van de belangrijkste wetsbepalingen. Incidenteel zal ook aandacht worden besteed aan komend recht.
In hoofdstuk 3 wordt nader ingezoomd op (de bestanddelen van) art. 240b van het Wetboek van Strafrecht (hierna: 'Sr'), de voor de strafrechtelijke praktijk in het kader van kinderpornozaken veruit meest belangrijke delictsomschrijving. In hoofdstuk 4 wordt specifiek ingegaan op de kwestie van (voorwaardelijk) opzet in de context van dit type zaken. In hoofdstuk 5 komen schuld- en strafuitsluitingsgronden en andere aspecten met betrekking tot (mogelijk) ontslag van rechtsvervolging aan de orde en in hoofdstuk 6 een aantal kwesties over het (digitale) forensisch onderzoek en digitaal bewijs. Een aantal strafvorderlijke aspecten, waaronder de wijze van tenlastelegging in geval van grote hoeveelheden kinderpornografisch materiaal, zijn het onderwerp van hoofdstuk 7 en de voorlopige hechtenis en de straftoemeting (inclusief een bespreking van specifieke en algemene strafverzwarende en strafmatigende omstandigheden) worden tot slot in hoofdstuk 8 besproken.

HOOFDSTUK 2: WETTELIJK- EN VERDRAGSRECHTELIJK KADER

2.1. Nationale bepalingen: de artt. 240b en 248 Sr.

Gedragingen met kinderpornografisch materiaal zijn in zeer veel landen strafbaar gesteld. In Nederland vinden wij de strafbaarstelling in art. 240b Sr. Deze bepaling luidt als volgt:

Art. 240b Sr
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.

In art. 248, leden 1-6 Sr is voorts bepaald dat de op overtreding van art. 240b Sr gestelde maximum gevangenisstraffen met een derde worden verhoogd, indien:
- het feit wordt gepleegd door twee of meer verenigde personen;
- de schuldige het feit begaat tegen zijn kind, een kind over wie hij het gezag uitoefent, een kind dat hij verzorgt of opvoedt als behorend tot zijn gezin, zijn pupil, een aan zijn zorg, opleiding of waakzaamheid toevertrouwde minderjarige of zijn minderjarige bediende of ondergeschikte;
- de schuldige het feit begaat tegen een persoon bij wie misbruik van een kwetsbare positie wordt gemaakt;
- de schuldige het feit begaat tegen een persoon beneden de leeftijd van achttien jaar bij wie misbruik van een kwetsbare positie wordt gemaakt;
- het feit is voorafgegaan, vergezeld of gevolgd van geweld;

Uit art. 248, leden 7 en 8 Sr volgt dat, indien het in art. 240b Sr omschreven misdrijf zwaar lichamelijk letsel ten gevolge heeft of daarvan levensgevaar voor een ander te duchten is, een gevangenisstraf van ten hoogste vijftien jaren (of geldboete van de vijfde categorie) kan worden opgelegd. Heeft de overtreding van art. 240b Sr de dood ten gevolge, dan kan een gevangenisstraf van ten hoogste achttien jaren (of een geldboete van de vijfde categorie) worden opgelegd.

Opvallend genoeg lijkt art. 248 Sr in de rechtspraktijk door het Openbaar Ministerie nogal veronachtzaamd te worden. Ook indien de feiten daartoe aanleiding lijken te geven, worden de in art. 248 Sr genoemde strafverzwarende omstandigheden namelijk veelal niet expliciet in de tenlastelegging opgenomen.[6] Dat heeft dan tot gevolg dat de strafrechter bij de

[6] De reden daarvan is vermoedelijk dat in die situaties veelal tevens andere zedenmisdrijven, of het misdrijf van mensenhandel, ten laste zijn/is gelegd, welke misdrijven aanmerkelijk hogere strafmaxima kennen dan art. 240b Sr. Opstellers van tenlasteleggingen lijken dan nog al eens het opnemen van de strafverzwarende omstandigheden in de tenlastelegging voor art. 240b Sr overbodig te vinden. Nochtans lijken er goede argumenten te zijn om bijvoorbeeld indien sprake is van de vervaardiging van kinderpornografisch materiaal in combinatie met (veelal lastig bewijsbare) mensenhandel - en/of loverboypraktijken -, ook de eventueel toepasselijk strafverzwarende omstandigheden (denk bijvoorbeeld aan "het misbruik maken van een kwetsbare positie") mee te nemen in de tenlastelegging met betrekking tot art. 240b Sr.

strafbepaling ook niet de in art. 248 Sr bepaalde hogere strafmaxima kan toepassen.[7]

Uit de rechtspraak van de Hoge Raad blijkt voorts dat art. 240b Sr geen *lex specialis* vormt ten opzichte van art. 416 Sr (heling)[8] en evenmin ten opzichte van art. 249 Sr (ontucht met eigen kind).[9] Art. 240b Sr kan dus (ook als het hetzelfde materiaal betreft of afbeeldingen betreft van voormelde ontucht) apart naast deze feiten ten laste worden gelegd.

Art. 240b Sr is de afgelopen decennia herhaaldelijk gewijzigd. Die wijzingen weerspiegelen de veranderende nationale en internationale opvattingen ten opzichte van de schadelijkheid van kinderpornografisch materiaal.[10] Illustratief voor de mate waarin deze opvattingen de laatste 30 jaar zijn gewijzigd is het feit dat pas sinds 1986 (en deels na internationale druk) gedragingen met kinderpornografische materiaal expliciet strafbaar zijn gesteld. Op deze feiten werd toen echter nog een maximum gevangenisstraf gesteld van 3 maanden. In 1996 werd de maximum gevangenisstraf voor verspreiding, openlijk tentoonstellen, vervaardigen, in-, door- of uitvoer of bezit van kinderporno echter al aanzienlijk verhoogd en wel tot 4 jaar.

De veranderde maatschappelijke opvattingen werkten ook door bij de relatief ingrijpende wijziging van art. 240b Sr per 1 oktober 2002, waarbij onder meer de leeftijdsgrens werd verhoogd van 16 naar 18 jaar en ook virtuele kinderporno werd verboden. Bij deze wetswijzing kwam veel meer dan voorheen het belang en de bescherming van minderjarigen tegen seksuele exploitatie op de voorgrond te staan, en aanmerkelijk minder het belang van "vrije" (seksuele) expressie. Zo blijkt bijvoorbeeld uit de wetsgeschiedenis (2001) dat art. 240b Sr ertoe strekt(e) te voorkomen dat:

a. een jeugdige in een situatie wordt gebracht waarin hij/zij wordt gebruikt voor het op beeldmateriaal vastleggen van een seksuele gedraging in de zin van art. 240b Sr waarbij hij/zij alleen of met een ander/anderen is betrokken;
b. beeldmateriaal dat onder het bereik van art. 240b Sr valt, na vervaardiging (verder) wordt verspreid, openlijk wordt tentoongesteld, of in bezit gehouden wordt;
c. jeugdigen worden aangemoedigd of verleid om deel te nemen aan seksueel gedrag en gedrag dat deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.[11]

Nog korter gezegd: art. 240b Sr beoogt strafbaar te stellen gedragingen die - als ze zijn of worden vastgelegd - schadelijk zijn voor een minderjarige, hetzij omdat het tot die gedraging brengen al schadelijk is, hetzij de publicatie daarvan direct of indirect schadelijk is.[12]

Na 2002 is art. 240b Sr echter nog meerdere malen gewijzigd. Zo werd in 2009 de maximumstraf op overtreding van art. 240b, lid 2, Sr verhoogd van 6 naar 8 jaar, werd in 2010 een aantal nieuwe strafverzwarende omstandigheden in art. 248 Sr opgenomen, alsook een extraterritoriale rechtsmacht voor de vervolging van Nederlandse verdachten van deze

---

[7] De rechter kan en mag echter ook dan met deze omstandigheden wel rekening houden bij de straftoemeting, zij het dat hij daarbij dan niet mag uitgaan van de hogere strafmaxima van art. 248 Sr, maar de strafmaxima van art. 240b moet aanhouden. Vgl. HR 30-5-2006, ECLI:NL:HR:2006:AW0475.
[8] HR 1-12-1998, *NJ* 1999/470 (m.nt. 't Hart).
[9] HR 20-1-1998, *NJ* 1998/336.
[10] Vervolgens werd in 2009 met name het strafvorderlijk kader aangescherpt, en werd per 1 januari 2012 ook onder meer het zich via een geautomatiseerd werk toegang verschaffen tot kinderporno strafbaar gesteld.
[11] Memorie van Toelichting, Kamerstukken II 2001/02, 27745, nr. 3; Nota naar aanleiding van het verslag, Kamerstukken II 2001/02, 27745, nr. 6.
[12] Nota naar aanleiding van het verslag, Kamerstukken II 2001/02, 27745, nr. 6. (onder de subkop "kinderpornografie").

feiten gecreëerd en werd per 1 januari 2010 ook het zich via een geautomatiseerd werk[13] of een communicatiedienst toegang verschaffen tot (en/of het aanbieden en verwerven van) kinderporno strafbaar gesteld.

2.2. Verdragsrecht

De wijzigingen in het laatste decennium zijn in belangrijke mate ingegeven door internationale ontwikkelingen, zoals de inwerkingtreding van het Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik[14] (verder te noemen: het *Verdrag van Lanzarote*), Richtlijn 2011/92/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie[15] en het Facultatief Protocol inzake de verkoop van kinderen, kinderprostitutie en kinderpornografie[16] bij het Internationaal Verdrag inzake de Rechten van het Kind (hierna: 'IVRK').
Met name voor de opsporing zijn ook de bepalingen van het Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken[17] (beter bekend als het *Cybercrimeverdrag* of het *Verdrag van Boedapest*) van groot belang.

De inhoud van laatstgenoemde internationale rechtsinstrumenten is door de Nederlandse wetgever grotendeels geïmplementeerd in art. 240b Sr[18], terwijl daarnaast bij de uitleg van 240b Sr aan de inhoud van die instrumenten groot gezag wordt toegekend. Om deze reden en vanwege het praktische karakter van deze uitgave, zal hier niet een uitgebreide beschrijving worden gegeven van de inhoud en achtergronden van genoemde internationale instrumenten. Daartoe wordt verwezen naar meer algemene rechtsliteratuur. Waar dit van belang is, zoals bij de bespreking van de interpretatie van de bestanddelen van art. 240b Sr, zal vanzelfsprekend wel tevens aandacht aan de betekenis van voormelde internationale instrumenten worden besteed.

De totstandkoming en inhoud van deze internationale instrumenten reflecteert niet alleen de al eerder genoemde gewijzigde inzichten en kennis omtrent de schadelijkheid van gedragingen met kinderpornografisch materiaal (en de daaruit voortvloeiende noodzaak tot bescherming van minderjarigen), maar ook dat deze schadelijkheid als gevolg van de mondiale digitalisering een veel grotere en veelal ook ernstiger dimensie heeft gekregen dan voorheen. Het gevolg daarvan is dat thans veel meer gedragingen met seksuele of geseksualiseerde afbeeldingen van minderjarigen strafbaar zijn dan bijvoorbeeld eind jaren '80 van de vorige eeuw.

---

[13] In dit boek worden, afhankelijk van de context, naast de overkoepelende term "geautomatiseerd werk", ook begrippen als "computer", "smartphone", "tablet" en "device" gebruikt. Tenzij anders vermeld zijn deze alle aan te merken als "geautomatiseerd werk". Zie hierover nader par. 3.5.4.
[14] Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, Lanzarote, 25 oktober 2007, Trb. 2008, 58.
[15] Richtlijn 2011/92/EU ter bestrijding van seksueel misbruik en seksuele uitbuiting van kinderen en kinderpornografie (en ter vervanging van Kaderbesluit 2004/68/JBZ) van 13 december 2011, Publicatieblad EU, 2011, L 335/1.
[16] Facultatief Protocol inzake de verkoop van kinderen, kinderprostitutie en kinderpornografie bij het Verdrag inzake de Rechten van het Kind, New York, 25 mei 2000 (i.w.tr. voor Nederland: 23-9-2005), Trb. 2001, 130.
[17] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken; Boedapest, 23 november 2001, Trb. 2004, 290.
[18] Opmerking hierbij verdient wel dat met name de implementatie van het Verdrag van Lanzarote niet altijd even zorgvuldig en doordacht lijkt te hebben plaatsgevonden, waardoor er thans in art. 240b Sr bestanddelen zijn opgenomen welke elkaar in betekenis overlappen, of waartussen anderszins moeilijk onderscheid valt te maken.

Genoemde gewijzigde opvattingen maken ook dat de (oorspronkelijke) wetsgeschiedenis op onderdelen als bron van rechtsvinding al snel gedateerd kan zijn. In de praktijk blijkt dan ook de uitleg van de Hoge Raad al dan niet in combinatie met internationaalrechtelijke opvattingen over de uitleg van een aantal specifieke of mede op de bestrijding van kinderpornografie gerichte internationale verdragen meer van belang te zijn voor de juridische betekenis en invulling van art. 240b Sr dan de wetsgeschiedenis betreffende deze bepaling.

2.3. Wat de toekomst brengen gaat

Zelfs nu de Wet Computercriminaliteit III per 1 maart 2019 in werking is getreden kunnen we er allerminst van uitgaan dat qua wetgeving sprake is van rustiger vaarwater.
Hoewel het Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering (versie: 20 maart 2023)[19] geen specifieke nieuwe bepalingen op het gebied van kinderpornografie bevat, is er wel sprake van een grondige herziening van wat we gemakshalve 'digitale opsporingsbevoegdheden' kunnen noemen. Een aantal van deze digitale opsporingsbevoegdheden is in een versneld traject terecht gekomen na opname in de op 1 oktober 2022 in werking getreden Innovatiewet Strafvordering.[20]
Uit een oogpunt van digitale opsporing gezien zijn de bepalingen over het vastleggen van gegevens uit een inbeslaggenomen geautomatiseerd werk (art. 556 van het Wetboek van Strafvordering (hierna: 'Sv')), het onderzoek in een elders aanwezig geautomatiseerd werk (art. 557 Sv) en het ongedaan maken van biometrische vergrendeling van een geautomatiseerd werk (art. 558 Sv) relevant.
Gezien het stadium waarin het moderniseringsproces zich bevindt en het inhoudelijk algemene karakter van de overige voorziene wijzigingen voert het te ver om er hier uitgebreider op in te gaan en volstaan we met een verwijzing naar het kennisdossier dat hierover wordt bijgehouden.

[19] Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering (op 20 maart 2023 ingediend bij de Tweede Kamer; zie: Kamerstukken II, 36 327, nr. 2).
[20] Besluit van 15 september 2022 tot vaststelling van het tijdstip van de inwerkingtreding van de Innovatiewet Strafvordering en het Besluit innovatiewet.

HOOFDSTUK 3: DE BESTANDDELEN VAN ART. 240B SR NADER BESCHOUWD

Zoals in hoofdstuk 2 al aangegeven spelen internationale verdragen wel een belangrijke rol in het politieke- en wetgevingstraject met betrekking tot de strafbaarstelling en vervolging van gedragingen met kinderpornografisch materiaal, maar hebben deze slechts een indirecte betekenis waar het gaat om de beoordeling van concrete strafzaken op dit terrein.

In de rechtspraktijk spitst het debat zich in de overgrote meerderheid van de zaken toe op de duiding van de verschillende bestanddelen van art. 240b Sr. De tenlasteleggingen zijn ook altijd toegesneden op deze bepaling.[21]

Art. 240b Sr luidt – zoals reeds eerder vermeld - voluit als volgt[22]:

> *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.*

Uit de plaatsing van art. 240b Sr in titel XIV, boek II, van het Wetboek van Strafrecht genaamd 'Misdrijven tegen de zeden', volgt dat overtreding van art. 240b Sr door de wetgever als (zeden)*misdrijf* is gekwalificeerd. Deze kwalificatie betekent onder meer dat dit misdrijf alleen strafbaar is als het *opzettelijk* is begaan, en – gezien de daarop gestelde maximale strafbedreiging – ook dat daarvoor in beginsel voorlopige hechtenis kan worden bevolen.[23]

In dit hoofdstuk zullen de verschillende bestanddelen van de specifieke strafbaarstelling van art. 240b Sr nader worden besproken. Meer algemeen-juridische aspecten rondom deze strafbaarstelling (zoals de voor de rechtspraktijk op dit gebied even belangrijke als soms lastig te beantwoorden vraag naar de invulling van het begrip opzet) worden in het volgende hoofdstuk 4 behandeld. Daarbij zal overigens soms sprake zijn van een zekere overlap tussen het in dit hoofdstuk en het in hoofdstuk 4 gestelde. Dat is om systematische redenen welhaast onontkoombaar, en vanwege de didactische meerwaarde van "herhaling" (zij het dan veelal in een iets andere context) van bepaalde aspecten van dit lastige onderwerp, onzes inziens zelfs gewenst.

---

[21] Voor de bepaling van de maximale strafbedreiging is daarnaast ook het gestelde in art. 248 Sr van belang. Deze bepaling zal verder in hoofdstuk 8 worden besproken.
[22] Wettekst zoals deze luidt sinds 1 oktober 2010.
[23] Zie art. 67, lid 1, Sv.

3.1. "Afbeelding of gegevensdrager[24] bevattende een afbeelding"

Het begrip "afbeelding" wordt in het Wetboek van Strafrecht noch in de wetsgeschiedenis bij art. 240b Sr nader gedefinieerd. In de Van Dale wordt het echter omschreven als: "*weergave, met name geschilderd, getekend of grafisch beeld van iets dat in werkelijkheid of in de gedachte bestaat*". Aangenomen moet dan ook worden dat niet alleen (al dan niet bewerkte) foto's en videomateriaal als "afbeelding" in de zin van art. 240b Sr moeten worden beschouwd, maar bijvoorbeeld ook (realistische[25]) tekeningen, schilderijen, montages en collages. Het is daarbij niet van belang of de afbeeldingen zelf centraal staan of dat zij een (beoogde) secundaire functie als bijvoorbeeld illustratiemateriaal hebben.[26]

Minder duidelijk ligt dit ten aanzien van digitale foto's, films en dergelijke. Dat zijn namelijk *gegevens*bestanden. Dergelijke digitale bestanden worden in art. 240b Sr niet (expliciet) genoemd. Met een beroep op de wetsgeschiedenis[27] zou daarom betoogd kunnen worden dat digitale bestanden in de systematiek van het Wetboek van Strafrecht als zodanig geen "afbeeldingen" zijn als bedoeld in art. 240b Sr.[28] Gegevens als zodanig zijn immers niet stoffelijk of tastbaar.

Uit de rechtspraak blijkt echter dat in ieder geval gegevensbestanden, die een kinderpornografische "afbeelding" behelzen en die op een gegevensdrager[29, 30] zijn vastgelegd, algemeen worden beschouwd als een "afbeelding" als bedoeld in art. 240b Sr. Incidenteel wordt dit "probleem" bij de bewezenverklaring ook wel omzeild door bewezen te verklaren: "een gegevensdrager, bevattende een afbeelding".[31] Hoewel daarvoor in de kern

---

[24] In de (juridische) praktijk worden de begrippen 'gegevensdrager' en 'computer' niet altijd zuiver gebruikt. Waar het gaat om de opslag van gegevens is een gegevensdrager vereist. Bij computers is altijd sprake van tenminste één ingebouwde gegevensdrager waarop gegevens worden bewaard, ook als de computer is uitgeschakeld (in de vorm van een 'hard disk drive' en steeds vaker een 'solid state drive', hierna doorgaans aan te duiden als: 'harde schijf'). Daarnaast kunnen met behulp van een computer gegevens worden opgeslagen op externe harde schijven, dvd's, USB-sticks etc. Waar in dit boek over opslag van gegevens op een computer wordt gesproken, wordt daarmee gedoeld op opslag op in die computer ingebouwde gegevensdragers. Gaat het over niet-permanent van een computer deel uitmakende gegevensdragers dan gebruiken we de generieke term gegevensdrager of noemen we de technische benaming.

[25] Zie voor de "realiteitseis" bij kinderpornografische afbeeldingen van virtuele minderjarigen, verder hierna onder 3.3.2.

[26] RB Midden-Nederland 24-4-2015, ECLI:NL:RBMNE:2015:2846 (foto's bij seksadvertentie). Zie voor de zogenaamde wetenschaps- of kunstexceptie hierna onder 5.2.

[27] Kamerstukken II 1991/92, 21 551, nr. 11, Nota naar aanleiding van het verslag, p. 4.

[28] Vgl. bijv. Kamerstukken II 1991/92, 21 551, nr. 11, Nota naar aanleiding van het verslag, p. 4.

[29] Een gegevensdrager is (ruim) gedefinieerd als "*een voorwerp waarop gegevens kunnen worden of zijn opgeslagen*" (Kamerstukken II 1991/92, 21 551, nr. 11, Nota naar aanleiding van het verslag, p. 4). Daaronder valt elk medium waarop digitale gegevens kunnen worden vastgelegd, zoals een harde schijf, een dvd, een geheugenkaart enz.

[30] Interessant is dat in het concept-wetsvoorstel modernisering Strafvordering (nog niet openbaar) afbeeldingen op papier fundamenteel identiek worden benaderd als afbeeldingen die digitaal zijn vastgelegd. Het papier wordt daarbij als de gegevensdrager gezien. Pregnant komt dit naar voren in het voorgestelde art. 2.7.39, lid 3 Sv., waar wordt gesproken over het geval dat analoog vastgelegde gegevens worden omgezet in digitale gegevens. Blijkens de Memorie van Toelichting bij het Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering (versie: 20 maart 2023) (p. 610-611/1497 dig.) moet daarbij gedacht worden aan het inscannen van aangetroffen papieren. Aldus beschouwd is een fysieke afbeelding niet meer dan op een bepaalde wijze verdeelde inkt of toner op een papieren gegevensdrager en is er alleen al daarom geen goede reden om digitale afbeeldingen anders te behandelen dan afbeeldingen in inkt of toner.

[31] Vgl. bijv. RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735, onder 4. Kwalificatie en bewezenverklaring dienen wel overeen te stemmen. Vgl. Rb. Gelderland, 22 december 2022, ECLI:NL:RBGEL:2022:7420 (kwalificatie: "een gegevensdrager bevattende een afbeelding (…)", terwijl 'gegevensdragers' in de bewezenverklaring zijn weggestreept).

een niet geheel logische redenering nodig is[32], behoeft er niet aan getwijfeld te worden dat het overeenkomstig de bedoeling van de wetgever is om digitale en fysieke afbeeldingen in dit opzicht gelijk te stellen.[33] Men zou derhalve kunnen stellen dat het begrip "afbeelding" in art. 240b Sr vooral *inhoudelijk* moet worden geduid (in de zin van: behelst het bestand de weergave van...) en dat het *format* (digitaal[34] of analoog) van deze afbeelding daarbij van sterk ondergeschikt belang wordt geacht.[35]

Het voorgaande wil echter niet zeggen dat zich geen problemen (kunnen) voordoen rond de inpassing in art. 240b Sr van (digitale) gegevensbestanden die kinderpornografisch materiaal bevatten. Daarbij moet bedacht worden dat in de zich snel ontwikkelende internetomgeving steeds minder digitaal materiaal op gegevensdragers van de gebruikers zelf wordt opgeslagen (en steeds meer in de cloud) en dat steeds meer gebruik wordt gemaakt van bijvoorbeeld "streaming video". Voorstreaming video is het niet noodzakelijk dat het bekeken materiaal ook op een aan een verdachte toebehorende gegevensdrager wordt vastgelegd. Het (opzettelijk) (al dan niet live) bekijken van kinderpornografische videobeelden (streamingdienst) was dan ook tot relatief recent niet strafbaar. Er werden immers geen afbeeldingen opgeslagen, waardoor deze niet in het bezit waren gekomen. Ook andere begrippen van art. 240b Sr dekten de gedragingen niet. Per 1 januari 2010 is art. 240b Sr echter gewijzigd, waarbij ook strafbaar werd gesteld het zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst verschaffen van de toegang tot kinderpornografische afbeeldingen.

Niet alle vragen lijken daardoor echter al te zijn opgelost. Zo is het de vraag of, en zo ja in hoeverre, ook databestanden met kinderpornografische inhoud die zonder interventie van de ontvanger, en zonder vastlegging op een gegevensdrager van deze ontvanger, worden doorgezonden (bijv. automatische doorgeleiding van *streaming video*) nog wel als "afbeelding" in de zin van art. 240b Sr kunnen gelden. Het lijkt dan namelijk om loutere communicatie van *gegevens* te gaan. In die zin besliste het Hof Leeuwarden in 2013 in een geval waarin de getoonde beelden via een live-webcamverbinding enkel op het moment zelf te zien waren. Het Hof stelde vast dat deze beelden niet werden opgeslagen, zodat zij niet op een later tijdstip (nogmaals) bekeken konden worden. Daaruit volgde dat die beelden geen 'afbeelding, voorwerp en/of gegevensdrager' in de zin van art. 240a Sr waren.[36]

---

[32] Een digitaal fotobestand is op zichzelf geen afbeelding maar een gegevensbestand (en nog feitelijker: slechts een verzameling van "enen en nullen"). Logisch doorredenerend is dan een digitaal fotobestand op een gegevensdrager op zichzelf ook geen afbeelding en dientengevolge is de gegevensdrager evenmin een gegevensdrager bevattende een afbeelding.

[33] Daarbij dient bedacht te worden dat de delictsomschrijving in art. 240b Sr grotendeels in 1991 vorm heeft gekregen, in welke tijd er nog slechts in beperkte mate middelen beschikbaar waren voor digitale fotografie en video.

[34] Zie voor een beknopte beschrijving van gangbare digitale bestandsformaten van foto's en video's par. 3.5.2 en bijlage 3 van "Terug naar de bestanden, technische toelichting over identificeren, verbergen en verwijderen van bestanden", Nederlands Forensisch Instituut 22 juni 2019.

[35] In deze zin is het ook niet relevant of een afbeelding bijvoorbeeld groot of klein is; zodat ook bijvoorbeeld de zogenaamde *thumbnails* (miniatuurweergaven van webpagina's, afbeeldingen etc) als afbeelding in de hier bedoelde zin kunnen gelden; bij thumbnails kunnen zich dan wel problemen voordoen omtrent de opzet op het bezit, omdat dergelijke thumbnails vrijwel altijd automatisch door een browser of besturingssysteem worden aangemaakt en dan veelal ook nog op een voor een gemiddelde computergebruiker niet-toegankelijke en/of niet kenbare locatie. Zie ook Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (bezit aangenomen m.b.t geüploade thumbnail met kinderpornografische afbeelding) en hierna onder 4.2.1.4.

[36] Hof Leeuwarden 27-3-2012, ECLI:NL:GHLEE:2012:BW0103.

Eind 2019 is in lagere rechtspraak geoordeeld dat livestreams wel een "afbeelding" de zin van art. 240b Sr kunnen zijn.[37] De rechtbank Zeeland-West-Brabant overwoog dat een afbeelding in de zin van genoemd artikel het weergeven van een werkelijkheid door middel van een technisch hulpmiddel is waardoor deze werkelijkheid door (veel) anderen door middel van gebruik van techniek bekeken kan worden.

Wij vragen ons af of dit niet een stap te ver is. Het wezen van een afbeelding is immers traditioneel een vastlegging van iets visueels. In het onderhavige geval is (voor zover uit het vonnis kan worden afgeleid) niets vastgelegd. Waarin verschilt deze livestream, die kennelijk door een verbalisant is bekeken en vervolgens beschreven, van een fysieke observatie? Scherper gesteld, als deze opvatting juist zou zijn, dan zou ook het zonder tussenkomst van technische apparatuur waarnemen van een handeling of situatie als een afbeelding aangemerkt kunnen worden. Het valt immers niet goed te beredeneren waarom het gebruik van die apparatuur een constitutief element vormt in deze overweging; deze vormde slechts het medium waarlangs de observatie plaatsvond maar voegt niets wezenlijks aan het afbeeldingskarakter toe. De omstandigheid dat een livestream een potentieel groot bereik heeft moet onzes inziens los worden gezien van de beoordeling of sprake is van een afbeelding. Een foto is een afbeelding, of deze nu al jaren in een oude schoenendoos zit of op de voorpagina van een krant staat. Vervang in deze casus het technisch hulpmiddel (de telefoon waarmee gefilmd werd en het apparaat waarmee de gestreamde beelden werden uitgekeken) door het raam van het vertrek waarin de seksuele handelingen plaatsvonden. De kans dat in een dergelijk geval een afbeelding in de zin van art. 240b Sr aanwezig wordt geacht schatten wij in op nihil.

In dit licht lijkt het ook vanuit het oogpunt van de wetgevingssystematiek de voorkeur te hebben, indien de wetgever zich (alsnog) zou beraden op het expliciet strafbaar stellen van de in art. 240b Sr omschreven gedragingen, niet alleen voor zover deze betrekking hebben op "afbeeldingen (enz.)", maar ook indien zij betrekking hebbende op "gegevens inhoudende afbeeldingen (enz.)". Met het wetsvoorstel Wet seksuele misdrijven heeft de wetgever die handschoen opgepakt.[38] Door de term 'afbeelding' te vervangen voor 'visuele weergave', en met in de Memorie van Toelichting de nadere overweging dat hieronder mede *live*streams moeten worden begrepen[39], heeft de wetgever aandacht aan dit punt geschonken. Of dit evenwel een afdoende oplossing voor het hier beschreven probleem is zal moeten blijken.

3.2. "Seksuele gedraging"

3.2.1. (Rechts)historische opvattingen

Een van de meer centrale vragen bij de interpretatie en toepassing van art. 240b Sr is de vraag wanneer van een afbeelding ook gezegd kan worden dat deze een "seksuele gedraging" inhoudt. Waar het gaat om uitersten zal er over het algemeen geen discussie zijn. Genitaal seksueel contact waarbij een minderjarige betrokken is zal zeker onder de noemer "seksuele gedraging" vallen. Evenzo zal bij een familiefoto van een op het strand spelende naakte peuter

---

[37] Rb Zeeland-West-Brabant 10-12-2019, ECLI:NL:RBZWB:2019:5546: "*Er is sprake van een afbeelding in de zin van art. 240b Sr indien via een livestream mogelijk wordt gemaakt dat anderen een weergave van de werkelijke seksuele gedragingen van kinderen kunnen zien door middel van streamen en volgen.*"

[38] Wijziging van het Wetboek van Strafrecht en andere wetten in verband met de modernisering van de strafbaarstelling van verschillende vormen van seksueel grensoverschrijdend gedrag (Wet seksuele misdrijven). Dit wetsvoorstel is op 10 oktober 2022 ingediend bij de Tweede Kamer.

[39] Memorie van Toelichting bij de Wet seksuele misdrijven, Kamerstukken II 2022-2023, 36 222, nr. 3., p. 75: "Niet-limitatieve voorbeelden van visuele weergaven zijn foto's, filmmateriaal, live streaming beeldmateriaal en streams die reeds bestaand beeldmateriaal bevatten".

geen sprake zijn van een afbeelding van een "seksuele gedraging". Daartussen ligt echter een aanzienlijk grijs gebied, waarvan de juridische grenzen blijken mee te bewegen met nieuwe (internationale) regelgeving en veranderende maatschappelijke opvattingen over de schadelijkheid van kinderpornografisch materiaal en het belang van de bescherming van kinderen.

De wetsgeschiedenis met betrekking tot art. 240b Sr geeft hierbij weinig concrete aanknopingspunten. In het kader van de invoering van deze bepaling in 1986 werd het begrip seksuele gedraging beperkt uitgelegd als verwijzend naar gedragingen welke tevens seksueel misbruik van kinderen inhielden. In de rechtspraak werd deze uitleg echter al tamelijk snel verbreed. Zo accepteerde de Hoge Raad in 1990 onder meer de uitleg van het Amsterdamse Hof dat "onder afbeelding van een seksuele gedraging in de zin van art. 240b Sr mede moet worden begrepen de afbeelding (van iemand die kennelijk de leeftijd van 16 jaren[40] nog niet heeft bereikt, al dan niet alleen) in een zodanige houding dat daarmee kennelijk het opwekken van seksuele prikkeling wordt beoogd."[41] Duidelijk is dat daarmee een groter aantal afbeeldingen, namelijk ook die waarin geen sprake is van direct seksueel contact of van meerdere betrokken personen, maar wel van poseren met bijvoorbeeld expliciete aandacht voor de geslachtsdelen, onder het bereik van art. 240b Sr werd gebracht.[42] Of de afbeeldingen tot stand waren gekomen als gevolg van seksueel misbruik is bovendien geen *conditio sine qua non* meer voor het kwalificeren van een afbeelding als inhoudende een seksuele gedraging.

In het kader van de wijziging in 1995 van art. 240b Sr[43] codificeerde de wetgever deze ontwikkeling, maar ging daarbij ook nog een stap verder. Bij de beoordeling of sprake is van een seksuele gedraging in de zin van art. 240b Sr werd het criterium van de *schadelijkheid voor de minderjarige* (welke bijvoorbeeld gelegen kan zijn in het brengen van de minderjarige in een bepaalde houding of pose, of in de gevolgen van publicatie van de afbeelding) veel sterker op de voorgrond geplaatst.[44] Het gegeven dat een afbeelding primair wordt vervaardigd en in omloop wordt gebracht met het oogmerk anderen seksueel te prikkelen werd daarbij als "bijzaak"[45] of zelfs als "niet relevant"[46] gezien.
In zoverre week men dus nadrukkelijk af van de lijn van de Hoge Raad, die de – al dan niet zinnenprikkelende – indruk die de afbeelding maakte op een waarnemer wel (mede) als

---

[40] In 1990 was de wettelijke leeftijdsgrens nog 16 jaar in plaats van de huidige 18 jaar.
[41] HR 6-3-1990, *NJ* 1990/667 (*Mader)* r.o. 5.1. e.v. m.nt. 't Hart. Vgl. ook HR 1-12-1998, *NJ NJ* 1999/470 m.nt. 't Hart (art. 240b Sr richt zich ook op die situaties waarin geen sprake is van een voorafgaand misdrijf, met andere woorden een zedenmisdrijf is geen noodzakelijke voorwaarde voor het van toepassing zijn van art. 240b Sr).
[42] Vgl. ook HR 4-12-1990, *NJ NJ* 1991/312 m.nt. 't Hart (niet vereist dat sprake is van minstens twee deelnemers; enkele naaktheid is geen voldoende voorwaarde voor de kwalificatie van een bepaalde afbeelding als zijnde een seksuele afbeelding. "*Het seksuele karakter blijkt in casu uit de wijze van poseren waarbij het geslachtsdeel op een bepaalde wijze en in een zekere toestand is gefotografeerd*". In zijn noot bij dit arrest merkt 't Hart op dat de uitleg van de rechtbank die wordt gesauveerd door de Hoge Raad verschilt van de wijze waarop de Hoge Raad in HR 6-3-1990, *NJ* 1990/667 de uitleg van het Amsterdamse Hof goedkeurde. In voormeld arrest werd het seksuele karakter van de afbeelding namelijk hoofdzakelijk afgeleid uit de seksuele prikkeling die zij teweeg kan brengen bij de toeschouwer (extern), terwijl in deze zaak het seksuele karakter van de afbeelding wordt afgeleid uit de aard van de zaak zelf (intern).
[43] Wet van 13 november 1995 tot wijziging van art. 240b Sr (Stb. 1995, 575).
[44] Zie Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 9.
[45] Aldus de Minister in de Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 9.
[46] Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 9 ("*Niet relevant is dat de afbeelding een seksuele prikkeling teweeg kan brengen, maar dat de afbeelding, afgezien van haar eventuele seksueel prikkelende karakter, kennelijk het gevolg is van seksuele exploitatie van een jeugdige"*).

criterium bezigde bij de beoordeling of een afbeelding een seksuele gedraging als bedoeld in art. 240b Sr inhield.

In de Nota naar aanleiding van het verslag[47] werden door de toenmalige minister Sorgdrager vier categorieën van afbeeldingen genoemd die binnen het bereik van art. 240b Sr zouden vallen, te weten:

- de gedragingen strafbaar gesteld in de artt. 242 e.v. Sr;
- seksuele gedragingen waarbij uitsluitend de jeugdige is betrokken;
- seksuele gedragingen waarbij de jeugdige een 'uitdagende houding' aanneemt;
- gedragingen waarbij de onnatuurlijke ambiance, veroorzaakt door het vastleggen van bijkomende onnatuurlijke ingrediënten, aan de afbeelding van een geheel of gedeeltelijk naakte jeugdige een voor deze jeugdige schadelijke seksuele connotatie geeft. Deze "onnatuurlijke ambiance" kan bijvoorbeeld blijken uit bepaalde voorwerpen die op een foto staan of de wijze van aankleding van het kind.[48]

Opvallend[49] was ook de opmerking in dezelfde Nota naar aanleiding van het verslag dat ter zake van afbeeldingen van seksuele gedragingen bij de vervaardiging waarvan niet een echt kind betrokken is geweest, vervolging achterwege dient te blijven[50]. Ook als het met moderne computertechnieken gegenereerde afbeeldingen betrof die niet of nauwelijks van echt te onderscheiden, dan wel "levensecht" waren.[51]

De hiervoor weergeven opvattingen van de wetgever omtrent het bereik van art. 240b Sr vonden ook weerklank in de rechtspraak. In het zogenaamde "Holland festival"-arrest uit 2000 oordeelde de Hoge Raad over een op dit festival geëxposeerde foto.[52] Op deze foto werd een zittende naakte man met een erectie getoond die een zeer jong kind op zijn arm heeft. Onder nadrukkelijke verwijzing naar de (recente) wetsgeschiedenis oordeelde de Hoge Raad dat de betreffende foto in deze zaak haar onnatuurlijke ambiance (de weergegeven erectie en het afgebeelde jonge kind) verliest door zowel de familiale relatie (de man is namelijk de vader van het kind) als doordat de man en het kind niet herkenbaar in beeld zijn gebracht. De Hoge Raad concludeert dat er geen sprake is van een uit de afbeelding naar voren komende ambiance die schadelijk is voor het kind, en kwalificeert de betreffende afbeelding mitsdien niet als een van een "seksuele gedraging".
De Hoge Raad lijkt hier derhalve - anders dan hij voorheen in bijvoorbeeld het arrest van 6 maart 1990[53] deed - de schadelijkheid van het gedrag voor het kind op de voorgrond te plaatsen en niet (meer) het beogen van een seksuele prikkeling.

Het geheel buiten beschouwing laten van de (seksuele) intenties van de vervaardiger c.q. de waarneming van bepaalde afbeeldingen van minderjarigen leidde echter tot nieuwe rechtsvragen en problemen. Zo ging het in de zaak die leidde tot het arrest van de Hoge Raad van 10 juni 2003[54] om videobeelden die waren gemaakt van foto's die een vijfjarige naakte jongen en negenjarig naakt meisje te zien gaven, waarbij langdurig op hun geslachtsdelen was

---

[47] Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 9 e.v..
[48] Handelingen II 1994/95, 6 april 1995, 67-4006 e.v.
[49] Zie par. 3.3.2.
[50] Tegelijkertijd werd daarbij echter erkend dat naar de letter van de wet onder het bereik van art. 240b Sr valt. Zie Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 10 en Handelingen II 1994/95, 6 april 1995, 67-4006.
[51] Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 10.
[52] HR 26-9-2000, *NJ* 2001, 61 (*Holland Festival*) m. nt. De Hullu.
[53] HR 6-3-1990, *NJ* 1990, 667.
[54] HR 10-6-2003, ECLI:NL:HR:2003:AF6437, *NJ* 2003, 609.

ingezoomd. De Hoge Raad oordeelde – anders dan het Bossche Hof en anders dan AG Machielse – met een beroep op de tekst van art. 240b Sr en de wetsgeschiedenis dat hier geen sprake was van een "seksuele gedraging". De foto's van de kinderen bevatten immers geen afbeeldingen van een seksuele gedraging conform art. 240b Sr en "*evenmin lagen daaraan seksuele gedragingen ten grondslag waartoe de betrokken kinderen waren gebracht*".

Dit arrest werd direct al kritisch ontvangen, waarbij de kritiek zich met name richtte tegen de (beperkte) invulling die door de Hoge Raad aan het criterium "bescherming van het kind" was gegeven. De wetsgeschiedenis gaf namelijk een ruimer kader om dit criterium in te vullen dan alleen de bescherming tegen de schadelijkheid van het brengen van het kind tot een seksuele gedraging. Met zoveel woorden werd daarin namelijk ook de bescherming tegen *de schadelijkheid van de publicatie van de seksuele gedraging* genoemd.[55] Dit aspect werd door de Hoge Raad echter geheel onbesproken gelaten, hetgeen gezien de leeftijd van de kinderen en het inzoomen op hun geslachtsdelen toch opmerkelijk genoemd kan worden. Evenzeer liet de Hoge Raad de vraag onbeantwoord in hoeverre door het (langdurig) inzoomen op de geslachtsdelen de afbeelding niet een zodanig "onnatuurlijke ambiance" krijgt, dat ook om die reden gesproken zou kunnen worden van een seksuele gedraging.[56]

Ondertussen had zich ook een aantal verdragsrechtelijke ontwikkelingen voorgedaan.
Op 23 september 2005 respectievelijk 1 juli 2010 waren namelijk het Facultatief protocol bij het IVRK en het Verdrag van Lanzarote in werking getreden. Beide bevatten een definitie van het begrip kinderpornografie te weten: "*elke afbeelding, op welke wijze dan ook, van een kind dat betrokken is bij, werkelijke of gesimuleerd expliciete seksuele gedragingen of elke afbeelding van de geslachtsorganen van een kind voor primair seksuele doeleinden*", respectievelijk "*elk materiaal dat een visuele weergave behelst van een kind dat betrokken is bij werkelijke of gesimuleerde expliciete seksuele gedragingen of elke afbeelding van de geslachtsorganen van een kind voor primair seksuele doeleinden*".

Richtlijn 2011/92/EU hanteert een meer complexe, maar met betrekking tot dit punt wel vergelijkbare definitie van kinderpornografie, namelijk:

i. *alle materiaal dat de visuele weergave behelst van een kind dat deelneemt aan echte of gesimuleerde expliciete seksuele handelingen;*
ii. *elke weergave voor primair seksuele doeleinden van de geslachtsorganen van een kind;*
iii. *alle materiaal dat de visuele weergave behelst van een persoon die er als een kind uitziet en die deelneemt aan echte of gesimuleerde expliciete seksuele gedragingen of elke weergave voor primair seksuele doeleinden van de geslachtsorganen van een persoon die er als een kind uitziet, of*
iv. *realistische afbeeldingen van een kind dat deelneemt aan expliciete seksuele gedragingen, of realistische afbeeldingen voor primair seksuele doeleinden van de geslachtsorganen van een kind."*

---

[55] Vgl. hieromtrent ook de (niet door de Hoge Raad gevolgde) conclusie van AG Machielse (ECLI:NL:PHR:2003:AF6437) bij dit arrest, waarin hij onzes inziens met kracht van argumenten aangaf dat uit de wetsgeschiedenis (Nota naar aanleiding van het verslag, Kamerstukken II 1994/95, 23 682, nr. 5, blz. 9) kan worden afgeleid dat art. 240b Sr ook ziet op de bescherming van het kind tegen schadelijkheid van *de publicatie* van de afbeelding.
[56] Zoals hiervoor aangegeven is dat namelijk blijkens de wetsgeschiedenis nadrukkelijk een aspect dat een afbeelding kan maken tot een afbeelding als bedoeld in art. 240b Sr.

Hieruit volgt onzes inziens dat, verdragsrechtelijk gezien, het kennelijk met een seksuele intentie of met een primair seksueel doel tonen/afbeelden/weergeven van de geslachtsdelen van kinderen in ieder geval naar internationaalrechtelijke standaarden als kinderpornografie dient te worden beschouwd.

3.2.2. Het beoordelingskader van de Hoge Raad sinds 2010

Naar mag worden aangenomen mede onder invloed van deze verdragsrechtelijke ontwikkelingen is dan ook vanaf ongeveer 2009 een kentering zichtbaar in de rechtspraak. Met name afbeeldingen waarbij – kennelijk met een seksuele intentie – was ingezoomd op de geslachtsdelen van kinderen werden vanaf die tijd steeds vaker als "afbeeldingen van een seksuele gedraging" gekwalificeerd.[57] In 2010 ging ook de Hoge Raad om.[58] In zijn arrest van 7 december 2010 oordeelde de Hoge Raad dat art. 240b Sr:

a. ziet op een afbeelding van een gedraging van expliciet seksuele aard, zoals die aan de hand van de afbeelding zelf kan worden vastgesteld[59], waaronder begrepen het op zinnenprikkelende wijze tonen van de geslachtsdelen of de schaamstreek. Het gaat dan om een gedraging die reeds door haar karakter strekt tot het opwekken van seksuele prikkeling; en voorts
b. ziet op een afbeelding die weliswaar niet een gedraging van expliciet seksuele aard in de hiervoor aangegeven zin toont, maar die, gelet op de wijze waarop zij tot stand is gekomen eveneens strekt tot het opwekken van seksuele prikkeling. Hierbij kan het gaan om een afbeelding van iemand in een houding of omgeving die weliswaar op zichzelf of in andere omstandigheden 'onschuldig' zouden kunnen zijn, maar die in het concrete geval een onmiskenbaar seksuele strekking heeft.[60]

---

[57] Vgl. echter Hof Arnhem 15-4-2009, ECLI:NL:GHARN:2009:BJ7530 (de omstandigheid dat de borsten en schaamstreek van het minderjarige meisje in beeld zijn vormt geen voldoende voorwaarde om te oordelen dat sprake is van een afbeelding van een seksuele gedraging in de zin van art. 240b Sr; er is pas sprake van een seksuele gedraging als de schaamstreek en borsten uitdrukkelijk in beeld zouden zijn gebracht waarmee het opwekken van een seksuele prikkeling werd beoogd).

[58] HR 7-12-2010, ECLI:NL:HR:2010:BO6446.

[59] Zie in dit verband ook RB Zutphen 7-10-2011, ECLI:NL:RBZUT:2011:BT7059 (op beeld vastleggen van masturberende jongen van 13-14 jaar oud valt onder art. 240b Sr).

[60] Dit criterium is nog vrij vaag en niet makkelijk toepasbaar. Het College van Procureurs-Generaal had echter in de van 1 januari 2011 tot en met 1 mei 2016 geldende Aanwijzing Kinderpornografie 2010 tamelijk gedetailleerde nadere criteria neergelegd voor de beoordeling door leden van het Openbaar Ministerie van afbeeldingen als zijnde al dan niet kinderpornografisch. Daarbij worden vooral *het karakter van de afbeelding* (ontuchtige handeling; onnatuurlijke en/of geregisseerde houding of pose in seksuele zin (blijkende uit o.m. erotische kleding, camerapositie, niet bij de leeftijd passende seksuele attributen); nadruk op de geslachtsdelen) en *de context van de afbeelding* (kleding met een erotiserende karakter die niet bij de leeftijd past; zichtbaarheid/gebruik voorwerpen en seksuele attributen; afbeelding in seksuele sfeer of sfeer van prostitutie). Voormelde criteria zijn nagenoeg ongewijzigd overgenomen in de Aanwijzing Kinderpornografie (2016) van het College van Procureurs-Generaal d.d. 1 mei 2016, met dien verstande dat daarbij als nieuw aanvullend beoordelingscriterium is opgenomen *de wijze van totstandkoming* van de afbeelding, waardoor een afbeelding een "kennelijk seksuele strekking" heeft gekregen. Ter toelichting worden daarbij genoemd het bewerken van beelden door toevoegen van (gesproken) teksten, samenvoegen van beelden, uitsnijden van delen, weghalen van oorspronkelijke elementen en achtergronden, waardoor een seksuele strekking is verkregen. Ook wordt in dit verband gerefereerd aan het (al dan niet heimelijk) maken van opnames, waarbij het standpunt van de camera, de regievoering door de verdachte of het inzoomen op een slachtoffer de nadruk legt op bepaalde lichaams- of geslachtsdelen of handelingen.
Hoewel deze OM-Aanwijzingen vanzelfsprekend de strafrechter niet binden, kan het daarin gestelde wel ook aanknopingspunten bieden voor de rechterlijke beoordeling of bepaalde afbeeldingen kinderpornografisch van aard zijn.

Belangrijk is ook de overweging van de Hoge Raad in ditzelfde arrest dat het voor de toepassing van art. 240b Sr niet noodzakelijk is dat vaststaat dat de jeugdige (concreet) is geschaad.[61]

Hoewel dit arrest zeker werkbare aanknopingspunten voor de beoordeling van het al dan niet kinderpornografisch karakter van afbeeldingen geeft, resteert er een aantal probleemcategorieën. De meest in het oog springende is die waarin sprake is van (veelal heimelijk gemaakte) opnamen van naakte dan wel deels ontklede kinderen in een niet onnatuurlijke omgeving als een kleedkamer, douche of naaktstrand. Met name spitst het juridisch debat zich hier toe op de vraag in hoeverre de intentie van de vervaardiger een rol speelt, dan wel dient te spelen bij de beoordeling of het materiaal moet worden aangemerkt als een afbeelding van een seksuele gedraging, dan wel dit louter mag worden afgeleid uit hetgeen op de afbeelding zelf zichtbaar is.

Het Hof Den Bosch kende in de zaak van de zwemleraar Benno L. zeer veel gewicht toe aan de intentie van de verdachte bij het vervaardigen van de afbeeldingen. Hij wilde deze namelijk aan zijn voyeuristische collectie toevoegen.[62] Annotator Schalken is bepaald kritisch over dit arrest. Hij meent dat het Hof teveel aandacht heeft besteed aan de intentie van de verdachte en betoogt dat het uitgangspunt van de intentie van de vervaardiger niet voldoende is voor de vaststelling dat sprake is van kinderpornografie. Zijns inziens moet reeds in de afbeelding zelf een deel van de strafbaarheid besloten liggen. Pas bij de digitale bewerking van de afbeelding (waarbij wordt beoogd een seksuele prikkeling teweeg te brengen) kan in bepaalde ten laste gelegde gevallen volgens Schalken tot een plaatsing in de categorie kinderpornografie conform art. 240b Sr worden gekomen.

Dit roept echter – zeker in het licht van voormelde verdragsbepalingen en het belang van de bescherming van het kind – de vraag op of Schalken hier de lat niet te hoog legt. Daarbij kan worden opgemerkt dat het Bossche Hof evenzeer bij zijn afwegingen heeft betrokken dat de verdachte bij het maken van zijn opnamen de vagina van de betrokken meisjes uitdrukkelijk in beeld bracht. Zowel vanuit de optiek van een verdragsconforme interpretatie van art. 240b Sr, als bezien vanuit het arrest van de Hoge Raad van 7 december 2010, is het oordeel van het Bossche Hof om – mede gelet op de wijze en het (seksuele) doel waarop zij tot stand zijn gekomen – de betreffende opnamen als afbeeldingen van een seksuele gedraging te kwalificeren derhalve goed verdedigbaar.

Onzes inziens zit ook de Hoge Raad meer op deze laatste lijn. In zijn arrest van 10 juni 2014 liet de Hoge Raad namelijk het oordeel van het Hof Den Bosch van 9 oktober 2012 in stand dat de in de tenlastelegging genoemde afbeeldingen van de geslachtsdelen van een minderjarige jongen, mede gelet op de wijze waarop deze zijn tot stand gekomen,

---

[61] HR 10-6-2014, ECLI:NL:HR:2014:1359, r.o. 3.5; zie in dezelfde zin HR 7-12-2010, ECLI:NL:HR:2010:BO6446 r.o. 3.4. en Hof Den Haag 2-4-2012, ECLI:NL:GHSGR:2012:BW0675. Vgl. ook RB Rotterdam 22-11-2017, ECLI:NL:RBROT:2017:9328 (consensuele pornografische foto's gemaakt van een kind van (bijna) 16 jaar). Gelet op het grote verschil in leeftijd tussen het slachtoffer en de verdachte (een jongen van (bijna) 16 jaar en een man van 49 jaar) is gehandeld in strijd met een sociaal-ethische norm; bewezenverklaard dat foto's kinderpornografisch zijn in de zin van art. 240b Sr). De ouderdom van de beelden lijkt bij de beoordeling of materiaal kinderpornografisch van aard is evenmin relevant: zie bijv. RB Midden-Nederland 9-12-2016, ECLI:NL:RBMNE:2016:7765 (verweer dat de ouderdom van het materiaal afdoet aan de aard en strafbaarheid daarvan verworpen).

[62] Hof 's-Hertogenbosch 26-5-2011, ECLI:NL:GHSHE:2011:BQ6181, *NJ* 2011/397 (*zaak Benno L.*) m.nt. Schalken.

onmiskenbaar strekten tot het opwekken van seksuele prikkeling.[63] Daarbij overwoog de Hoge Raad onder meer dat het hof uit de gebezigde bewijsmiddelen heeft kunnen afleiden dat verdachte de focus van de camera, waarmee de afbeeldingen zijn vervaardigd, (nagenoeg) op de hoogte van de geslachtsdelen van de minderjarige jongen heeft afgesteld, hij de jongen vervolgens heeft opgedragen zich te gaan douchen waarbij filmopnames zijn gemaakt van de ontblote geslachtsdelen van de jongen en hij de filmpjes vervolgens op zijn computer heeft overgebracht en bekeken. Evenmin onbegrijpelijk oordeelde de Hoge Raad het oordeel van het hof dat verdachte gebruik heeft gemaakt van de pose waarin de jongen in de gegeven omstandigheden voor de camera heeft gestaan.

Uit het voorgaande blijkt dat in situaties waarbij afbeeldingen van (geheel dan wel gedeeltelijk naakte) kinderen zijn gemaakt in een min of meer natuurlijke of huiselijke omgeving, zowel verdragsrechtelijk als in de jurisprudentie grote waarde wordt toegekend aan het al dan niet focussen op de geslachtsdelen. Is daarvan sprake, dan wordt als regel aangenomen dat de afbeeldingen een seksuele gedraging inhouden als bedoeld in art. 240b Sr. Is dat niet het geval, dan volgt veelal vrijspraak.[64]

---

[63] HR 10-6-2014, ECLI:NL:HR:2014:1359 r.o. 3.5.; vgl. ook: RB Midden-Nederland 29-4-2015, ECLI:NL:RBMNE:2015:2846 (foto's van poserend meisje in "kerstpakje", waarbij door de positie van de camera en de houding van de vrouw de nadruk wordt gelegd op de (bedekte) geslachtsdelen); foto's o.m. bij seksadvertentie op kinky.nl geplaatst; veroordeling).

[64] Zie bijv. RB Noord-Holland 17-3-2015, ECLI:NL:RBNHO:2015:2161 (Heimelijk in kleedkamers van hockeyverenigingen gemaakte filmopnamen van (gedeeltelijk) naakte minderjarige (13-14 jaar oud) meisjes zijn geen kinderporno; geen bewijs van "pedoseksuele neigingen" van verdachte en/of dat de filmopnamen eerst en vooral strekten tot het opwekken van seksuele prikkeling) en Hof Amsterdam 14-10-2015, ECLI:NL:GHAMS:2015:4209 waarbij de hiervoor genoemde uitspraak werd vernietigd onder meer omdat het Hof vaststelde "*dat door de wijze waarop de opnamen werden gemaakt, de nadruk kwam te liggen op hun naaktheid en in voorkomend geval ook op hun billen, hun (ontluikende) borsten en/of de schaamstreek*" ; Zie verder ook: RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (afbeeldingen van leerlingen waarbij gericht werd gefilmd/ingezoomd op de geslachtsdelen/het kruis, strekten kennelijk tot seksuele prikkeling en vallen mitsdien onder art. 240b); RB Den Haag 11-10-2017, ECLI:NL:RBDHA:2017:11522 (Op de desbetreffende foto is behalve een naakt geslachtsdeel van een minderjarige, te zien dat een volwassen persoon diens hand heeft geplaatst op korte afstand van het geslachtsdeel van deze minderjarige op een intieme plaats van haar lichaam die zich dicht bij haar geslachtsdeel bevindt, te weten haar lies. Daardoor wordt de aandacht op onnatuurlijke, kennelijk zinnenprikkelend bedoelde wijze op het geslachtsdeel van de minderjarige gevestigd); RB Noord-Nederland 29-6-2017, ECLI:NL:RBNNE:2017:2349 (afbeeldingen gemaakt van driejarige dochter. Op deze foto's zijn onder meer het ontblote geslachtsdeel en de billen van voornoemde dochter te zien, waarbij zij gezien haar leeftijd een onnatuurlijke houding aanneemt. Deze foto's heeft verdachte tijdens seksueel geladen en/of prikkelende chatgesprekken via de WhatsApp naar een derde gestuurd. Afbeeldingen zijn kinderpornografisch); RB Oost-Brabant 25-9-2017, ECLI:NL:RBOBR:2017:5059 (Het verweer dat foto 1 in het procesdossier geen seksuele strekking of onnatuurlijk camerastandpunt of pose heeft, nu het slachtoffer in zijn geheel is te zien is en zijn geslachtsdeel nauwelijks, wordt verworpen nu bij het bewijs wordt betrokken dat verdachte twee foto's heeft gemaakt waarop de broek van het slachtoffer nog omhoog is en de bovenzijde van zijn penis boven de broekrand uitkomt); RB Gelderland 30-4-2018, ECLI:NL:RBGEL:2018:1994 (de rechtbank stelt – na uitvoerig onderzoek van regelgeving en jurisprudentie - vast dat 240b Sr mede omvat elke weergave voor primair seksuele doeleinden van de geslachtorganen van een kind en kwalificeert vervolgens alle afbeeldingen waarop geslachtsorganen van een kind te zien zijn (ook die waar niet daarop is ingezoomd) als kinderpornografisch "*aangezien er steeds sprake is geweest van het maken van meerdere afbeeldingen van de betreffende kinderen in één sessie*."), bevestigd door het Hof Arnhem-Leeuwarden, 13-5-2019, ECLI:NL:GHARL:2019:4494 (met overname van deze fraaie overwegingen) en Rb Limburg 18-5-2018, ECLI:NL:RBLIM:2018:4685 (14 afbeeldingen van wisselende seksuele aard, de rechtbank stelt ten aanzien van foto's waarvan de seksuele aard minder nadrukkelijk naar voren komt: "*Doordat deze foto's deel uitmaken van een reeks waarbij ook foto's werden gemaakt die expliciet seksueel van aard waren, hebben ook deze foto's een onmiskenbaar seksuele strekking*."

De drempel voor het bestanddeel "*afbeelding van seksuele gedraging, waarbij iemand die kennelijk leeftijd van 18 jaren nog niet heeft bereikt, is betrokken*" is onlangs nog lager komen te liggen. De feitenrechter krijgt van de Hoge Raad nog meer ruimte. Een ten opzichte van de voorgaande zaak spiegelbeeldige situatie deed zich namelijk voor in de zaak die leidde tot het arrest van de Hoge Raad van 1 september 2020.[65] Er waren diverse '*selfies*' aan de orde waarop de stijve penis van de verdachte zichtbaar was dan wel door de verdachte in zijn hand wordt gehouden. Op deze selfies zijn telkens een of twee van zijn jonge kinderen in directe nabijheid herkenbaar in beeld. De foto's zijn kennelijk genomen in huiselijke sfeer, namelijk voor een commode, in een badkamer en op een bank. Het hof heeft uit de aard van de afbeeldingen vastgesteld dat blijkt dat de aanwezigheid van de kinderen niet min of meer toevallig is, maar dat zij (deels) het onderwerp vormen van de foto's. Daarnaast heeft het hof vastgesteld dat de foto's telkens onmiskenbaar een seksuele lading hebben. Het oordeel van het hof dat telkens sprake is van een afbeelding van een seksuele gedraging waarbij iemand is betrokken die de leeftijd van achttien jaar nog niet heeft bereikt, geeft volgens de Hoge Raad geen blijk van een onjuiste rechtsopvatting en is evenmin onbegrijpelijk. Daar voegt de Hoge Raad nog aan toe dat de enkele omstandigheid dat de kinderen op deze foto's niet naakt zijn afgebeeld en daarop zelf geen seksuele handelingen verrichten, niet aan een dergelijk oordeel in de weg hoeft te staan.

3.2.3. Seksuele intentie als relevante factor bij de beoordeling van afbeeldingen

Men kan zich de vraag stellen in hoeverre zeker in een tijd waarin digitale camera's, beeldbewerkingstechnieken, ongekende en onomkeerbare verspreidingsmogelijkheden via *social media* en internet en technische ontwikkelingen als gezichtsherkenning (waardoor afbeeldingen van personen veel sneller te herleiden zijn tot degenen van wie zij zijn gemaakt) een grote vlucht hebben genomen, laatstgenoemde jurisprudentie nog wel in voldoende mate invulling geeft aan de – ook verdragsrechtelijk vastgelegde – verplichting tot bescherming van minderjarigen tegen – kort gezegd – exploitatie voor seksuele doeleinden. Met het oplopende risico van identificatie door middel van gezichtsherkenning wordt bovendien de kans op reële (reputatie)schade als gevolg van publicatie (eventueel op een aanmerkelijk later moment) ook groter.

Niet geheel duidelijk is in hoeverre de Hoge Raad ruimte lijkt te willen geven om in gevallen waarin de seksuele intentie van de vervaardiger of bezitter van de afbeeldingen van kinderen in een natuurlijke omgeving duidelijk is, deze intentie toch bij de beoordeling van het seksuele karakter van het materiaal te betrekken. In dit kader is met name van belang dat de Hoge Raad in zijn arrest van 10 juni 2014 onder meer overweegt dat art. 240b Sr ziet op een afbeelding die weliswaar niet een gedraging van expliciet seksuele aard toont, "*maar die, gelet op de wijze waarop zij tot stand is gekomen eveneens strekt tot het opwekken van seksuele prikkeling"*.[66]

In dit kader is het niet ondenkbaar dat de gebleken intentie om dergelijke afbeeldingen te vervaardigen met bijvoorbeeld de (kennelijke) bedoeling deze toe te voegen aan een kinderpornografische collectie, of om deze te verspreiden binnen een kinderpornonetwerk, als een relevante omstandigheid door de strafrechter mag worden betrokken bij de beoordeling of die afbeelding "gelet op de wijze waarop deze tot stand is gekomen eveneens strekt tot het opwekken van seksuele prikkeling". Veelal zal dan overigens juist door deze specifieke context duidelijk zijn dat dergelijke afbeeldingen – zowel voor de verdachte als de afgebeelde persoon – een onmiskenbaar seksuele strekking hebben.

---

[65] HR 1-9-2020, ECLI:NL:HR:2020:1347.
[66] HR 10-6-2014, ECLI:NL:HR:2014:1359.

Een dergelijke – meer context-gerelateerde – uitleg van het begrip "afbeelding van een seksuele gedraging" lijkt ook de meest verdragsconforme te zijn. Zowel het Facultatief protocol bij het IVRK als het Verdrag van Lanzarote als Richtlijn 2011/92/EU definiëren kinderpornografie immers (onder meer) als "elke afbeelding van de geslachtsorganen van een kind *voor primair seksuele doeleinden*" (*curs. auteurs*). Deze definitie betrekt derhalve ook de intentie waarmee een afbeelding is gemaakt bij de beoordeling of deze als kinderpornografisch dient te worden aangemerkt.
Ook een dergelijke meer context-gerelateerde invulling van het begrip afbeelding van een seksuele gedraging is echter niet probleemloos. Zo zal in deze gevallen voor een ander dan de oorspronkelijke vervaardiger of gerichte verspreider het seksuele c.q. kinderpornografische karakter van de afbeelding niet altijd aanstonds duidelijk (behoeven te) zijn. Het antwoord op de vraag of een bepaalde afbeelding een seksueel gedraging weergeeft, is dan immers niet louter afhankelijk van hetgeen op de afbeelding zelf te zien is, maar ook van de context waarin de gedraging ten opzichte van deze afbeelding plaatsvindt. Dat impliceert een zekere mate van rechtsonzekerheid. Dit komt echter vaker in het strafrecht voor, en rechters blijken daarin gewoonlijk hun weg wel te kunnen vinden. Zo is het bijvoorbeeld niet ondenkbaar dat het bezit van een afbeelding van een naakt kind op het strand in zijn algemeenheid langs deze weg niet onder het bereik van art. 240b Sr wordt gebracht, maar de plaatsing van diezelfde afbeelding op een kinderpornowebsite bijvoorbeeld wel.

Anderzijds zou ook kunnen worden betoogd dat waar de Hoge Raad in zijn arrest van 10 juni 2014 refereert aan "de wijze waarop de afbeelding tot stand is gekomen", dit college slechts het oog heeft gehad op de (fysieke) wijze waarop de afbeelding is vervaardigd, dus derhalve op zaken als camerapositie, cameragebruik, het bewust plaatsen van kinderen in bepaalde posities etc. De intentie van de maker zou dan geen rol (mogen) spelen bij de kwalificatie van een afbeelding als zijnde al dan niet van een seksuele gedraging (van een minderjarige).[67] Welke jurisprudentiële lijn uiteindelijk zal worden gevolgd, zal de tijd moeten leren.

3.2.4. Kunnen afbeeldingen door (digitale) bewerking een kinderpornografisch karakter krijgen?

Een bijzonder vraagpunt wordt nog gevormd door de kwestie in hoeverre een afbeelding die in zijn oorspronkelijke vorm niet als kinderpornografisch wordt aangemerkt, door (digitale) bewerkingen als bijvoorbeeld selecteren, isoleren, vergroten en inzoomen alsnog een dergelijk karakter zouden kunnen krijgen. De Hoge Raad wilde daar blijkens zijn arresten van 31 januari 2012 en 10 juni 2003 niet van weten.[68] Daarin werd geoordeeld dat een filmopname die zélf geen afbeelding van een seksuele gedraging in de zin van art. 240b Sr vormt, niet door het enkele selecteren, isoleren en vastleggen van een bepaald beeld daarop, kan worden tot een afbeelding van seksuele gedraging(en). In casu ging het om het knippen en apart vastleggen van fragmenten uit een documentaire, op welke fragmenten de geslachtsdelen van 2 jongens in close-up zichtbaar waren.

---

[67] Vgl. ook RB Amsterdam 11-4-2017, ECLI:NL:RBAMS:2017:2294 (afbeeldingen van (jonge) vrouw in beslagen douchecabine. Afbeeldingen zijn vaag. Lichaamscontouren zijn zichtbaar. Houding is dusdanig dat schaamstreek of borsten niet in beeld zijn. Geen sprake van een "uitdagende houding". "*Verder ontbreekt de onnatuurlijke ambiance die de afbeeldingen een seksuele connotatie zou kunnen geven. De rechtbank deelt niet de stelling van de officier van justitie dat de seksuele bedoeling waarmee verdachte de foto's heeft gemaakt reeds maakt dat deze foto's kinderpornografisch zijn*." Geen afbeelding van seksuele gedraging. Vrijspraak.
[68] HR 31-1-2012, ECLI:NL:HR:2012:BT1822; in dezelfde zin HR 10-6-2003, ECLI:NL:HR:2003:AF6437 en RB Noord-Holland 17-03-2015, ECLI:NL:RBNHO:2015:2161 (apart vastgelegde stills van filmopnamen in kleedkamer waarbij nadrukkelijk is gekozen voor beelden waarop meisjes naakt zijn te zien geen afbeeldingen van seksuele gedragingen).

Onzes inziens heeft de Hoge Raad in voormelde arresten bedoeld te zeggen, dat een oorspronkelijk niet-kinderpornografische film *zelf* niet kinderpornografisch wordt door het enkele feit dat delen daaruit zijn of worden geïsoleerd, bewerkt enz.[69]
Deze uitleg van de rechtspraak van de Hoge Raad van 31 januari 2012 lijkt zich goed te verhouden tot zowel het Facultatief protocol bij het IVRK als het Verdrag van Lanzarote waarin, zoals hiervoor ook reeds aangegeven kinderpornografie onder meer wordt gedefinieerd als "*elke afbeelding van de geslachtsorganen van een kind voor primair seksuele doeleinden*" (*curs. auteurs*).[70] In dat kader lijkt het meer voor de hand te liggen om een afbeelding die bijvoorbeeld is gemaakt door digitaal in te zoomen op de geslachtsdelen van kinderen op een "normale" foto, en welke bewerkte afbeelding vervolgens apart op een gegevensdrager is opgeslagen, als een (zelfstandige) afbeelding bevattende een seksuele gedraging aan te merken.

Het lijkt blijkens het arrest van de Hoge Raad van 18 november 2014[71] aannemelijk dat ook de Hoge Raad deze visie deelt. In die zaak betrof het foto's van zeer jonge naakte meisjes, waarbij hun geslachtsdelen (deels prominent) in beeld waren. Van die foto's waren uitsneden gemaakt waardoor de foto's ook van de natuurlijke achtergrond waren ontdaan. De aldus bewerkte foto's werden bij elkaar in collagevorm op een ondergrond bevestigd. De raadsman voerde een op voormelde HR-uitspraken gestoeld verweer. Het Hof oordeelde dat gelet op de wijze waarop de collages tot stand waren gekomen, deze strekten tot het opwekken van seksuele prikkeling en in dit concrete geval een onmiskenbaar seksuele strekking hebben en kwalificeerde ze als kinderpornografisch. Overeenkomstig de conclusie van de Advocaat-Generaal hield de Hoge Raad dit oordeel in stand.

Wij zien dan ook een parallelle beweging ten aanzien van deze jurisprudentiële lijn van de Hoge Raad inzake de beoordeling van afbeeldingen waarbij na (*digitale*) bewerking van oorspronkelijk niet kinderpornografisch materiaal de nadruk wordt gelegd op de geslachtsdelen, en die welke is neergelegd in het reeds hiervoor besproken arrest van 10 juni 2014. Daarin wordt immers de omstandigheid dat "de verdachte de focus van de camera, waarmee de afbeeldingen zijn vervaardigd, (nagenoeg) op de hoogte van de geslachtsdelen van de minderjarige jongen heeft afgesteld" relevant geacht voor de beoordeling of de wijze waarop afbeeldingen tot stand zijn gekomen, onmiskenbaar strekken tot het opwekken van seksuele prikkeling. Hierin kan steun worden gevonden voor de gedachte dat het inzoomen op de geslachtsdelen in dat verband eveneens een relevante factor kan zijn. Inhoudelijk zijn er geen goede gronden om daarbij *digitaal* inzoomen op een afbeelding anders te benaderen dat *hardwarematig* inzoomen.[72] Te meer niet omdat digitaal inzoomen hetzelfde effect kan

---

[69] Opmerking verdient hier overigens wel dat een "gewone" filmopname wel kinderpornografisch kan worden wanneer daaraan prikkelende aspecten worden toegevoegd. In deze zin ook: RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564.

[70] Wellicht speelt hier mee dat de feiten die in het arrest van 31 januari 2012 aan de orde waren, zich hadden voorgedaan in een periode die ruim ligt voor de datum van inwerkingtreding voor Nederland van het Verdrag van Lanzarote (1-7-2010). De bepalingen van dit verdrag kon daardoor bezwaarlijk bij de interpretatie van het in die zaak aan de orde zijn art. 240b Sr worden betrokken. Daar staat echter tegenover dat ten tijde van de tenlastegelegde gedragingen het Facultatieve Protocol inzake de verkoop van kinderen (etc.) bij het IVRK al wel voor Nederland in werking was getreden (namelijk op 23-09-2005).

[71] HR 18-11-2014, ECLI:NL:HR:2014:3304.

[72] Bij hardwarematig inzoomen kan worden gedacht aan het dichter op het onderwerp plaatsen van een camera, of het gebruik van een (zoom)lens die het onderwerp optisch uitvergroot. Bij digitaal inzoomen is een digitale afbeelding uitgangspunt. Daar wordt een uitsnede van gemaakt die vervolgens wordt uitvergroot tot (doorgaans) het formaat van de oorspronkelijke afbeelding. In dezelfde zin begrijpen wij ook: Noyon-Langemeijer-Remmelink, Wetboek van Strafrecht, aant. 5, onder c bij art. 240b Sr: "*Ook het manipuleren met*

hebben als *hardware*matig inzoomen.[73] Bovendien heeft de wijze van inzoomen geen consequenties voor de schadelijkheid (ook in verband met (verdere) publicatie) voor de afgebeelde minderjarige. Dit zou slechts anders kunnen zijn indien digitaal inzoomen leidt tot een zodanige vervaging van de afbeelding dat de voor de kwalificatie als kinderpornografische afbeelding vereiste elementen niet meer voldoende zichtbaar zijn.

Het is dan ook goed verdedigbaar dat hier als onderscheidend criterium kan worden gehanteerd of kan worden gezegd dat als gevolg van de bewerking en vastlegging van de oorspronkelijke afbeelding, voor primair seksuele doeleinden *een nieuwe, zelfstandige afbeelding* is vervaardigd c.q. dat gezien de wijze waarop de vanuit het oorspronkelijk materiaal vervaardigde afbeelding tot stand is gekomen, deze kennelijk strekt tot het opwekken van seksuele prikkeling.

3.3. "Waarbij kennelijk iemand die de leeftijd van 18 jaar nog niet heeft bereikt is betrokken of schijnbaar is betrokken"

3.3.1. Kennelijk de leeftijd van 18 jaar nog niet bereikt
Uit de tekst van art. 240b Sr volgt reeds dat pas sprake kan zijn van strafbare gedragingen met betrekking tot afbeeldingen van seksuele gedragingen, indien daarbij *kennelijk* iemand is betrokken of schijnbaar is betrokken, die de leeftijd van *18 jaar* nog niet heeft bereikt. Het criterium is derhalve of de afgebeelde personen *kennelijk* de leeftijd van 18 jaar nog niet hebben bereikt. Nog anders gezegd: of aan de hand van de uit de afbeelding blijkende lichaamskenmerken kan worden bewezen dat de betrokkene jonger *oogt* dan 18 jaar.[74]
De *werkelijke* leeftijd van de afgebeelde persoon is in die benadering dus voor de bewezenverklaring irrelevant en behoeft (dus) ook niet uit de bewijsmiddelen te blijken.[75] Evenmin behoeft *wetenschap* bij de verdachte van de (kennelijke) minderjarigheid bewezen te worden, nu deze leeftijd een geobjectiveerd bestanddeel van de delictsomschrijving van art.

---

beeldbewerkingsprogramma's, waardoor men uit wellicht een samenstel van foto's die op zichzelf ieder nog geen kinderpornografie inhouden, een nieuw geheel maakt dat wel als kinderpornografie zal hebben te gelden, is als vervaardigen aan te merken, ook al komt er in feite geen kind meer aan te pas".

[73] In het Amerikaanse Rittenhouse-proces werd door de verdediging betoogd dat bij handmatig inzoomen op een iPad sprake zou zijn van beeldmanipulatie ten gevolge van door Apple gebruikte A.I.-technieken. Het is echter algemeen bekend dat door in- en/of uitzoomen op een iPad geen intrinsieke veranderingen optreden in de afbeelding zelf. Niettemin werd naar aanleiding van dit verweer bepaald dat de jury slechts kennis mocht nemen van de niet ingezoomde videobeelden. Zie Judge buys Rittenhouse lawyer's insane argument that Apple's pinch-to-zoom manipulates footage - The Verge en Apple "Pinch To Zoom" Can't Add Things That Aren't There (forbes.com).

[74] Zie o.m. HR 18-11-2008, ECLI:NL:HR:2008:BF0170 die voortbouwt op HR 7-12-2004, ECLI:NL:HR:2004:AQ8936.

[75] Aldus HR 6-4-2010, ECLI:NL:HR:2010:BL8772 en HR 18-11-2008, ECLI:NL:HR:2008:BF0170; zie ook Kamerstukken II 2001/2002, 27 745, nr. 3, p. 4. Als de leeftijd echter wel bekend is, en deze beneden de 18 jaren ligt, dan is het echter niet relevant of betrokkene er op de afbeeldingen wellicht ouder dan 18 jaar uit ziet en hoeft dus ook niet uit de bewijsmiddelen te blijken dat de afgebeelde persoon jonger oogt dan 18 jaar; Aldus ook HR 27-9-2016, ECLI:NL:HR:2016:2185, Hof Arnhem-Leeuwarden 14-6-2017, ECLI:NL:GHARL:2017:5020, Hof Arnhem-Leeuwarden 20-5-2016, ECLI:NLGHARL:2016:3907; RB Noord-Holland 2-11-2021, ECLI:NL:RBNHO:2021:9625; en Kamerstukken II 2001/2002, 27 745, nr. 6. Blijkt de leeftijd van de afgebeelde persoon boven de 18 jaar te zijn, maar *oogt* de afgebeelde persoon jonger, dan zit men eveneens in het strafbare domein (zie ook de conclusie van AG Machielse (ECLI:NL:PHR:2008:BF0170) bij HR 18-11-2008, ECLI:NL:HR:2008:BF0170. O.i. problematisch is dus: RB Den Haag 26-4-2017, ECLI:NL:RBDHA:2017:4273 (heimelijke filmopnamen in kleedhokjes; "*De rechtbank heeft niet kunnen vaststellen wie de meisjes of vrouwen zijn die op vijf bij de man aangetroffen filmpjes staan en of zij jonger zijn dan achttien jaar. De rechtbank spreekt de man daarom vrij van het maken van kinderporno*"), de rechtbank heeft immers niet overwogen dat zij (ook) niet kon vaststellen dat de afgebeelde personen jonger *oogden* dan 18 jaar.

240b Sr vormt.[76] Gezien de irrelevantie daarvan is er dus ook geen plaats voor het (laten) doen van nader (tegen)onderzoek naar de werkelijke leeftijd van de afgebeelde persoon. Wel zal uit het proces-verbaal c.q. de processtukken moeten blijken *op grond waarvan* tot het oordeel is gekomen dat sprake is van een persoon die kennelijk de leeftijd van 18 jaar nog niet heeft bereikt. Ontbreekt een dergelijke onderbouwing, dan zal een door de verbalisant of rapporteur gegeven oordeel omtrent de leeftijd van de afgebeelde persoon niet mogen bijdragen aan het bewijs.[77]

Het gaat derhalve om een verantwoorde schatting, op grond van kenmerken die in het algemeen in de beschouwing kunnen en plegen te worden betrokken bij de schatting van de leeftijd van een bepaalde persoon, waarbij onder meer gedacht kan worden aan de lengte en de lichamelijke ontwikkeling.[78]

De beoordeling of bepaalde afbeeldingen een *kinder*pornografisch karakter hebben wordt primair gedaan door daartoe speciaal opgeleide en gecertificeerde rechercheurs. In de praktijk vindt die schatting van de leeftijd plaats aan de hand van de op de afbeelding zichtbare lichaamskenmerken van de afgebeelde persoon. Tot de leeftijd van 12 jaar levert dit doorgaans geen problemen op. Bij vermoedelijk oudere personen is deze vaststelling echter minder eenvoudig. Om deze reden wordt in dergelijke situaties de leeftijd doorgaans door (politie)deskundigen beoordeeld aan de hand van de zogenaamde Tanner-schaal, dan wel aan de hand van mede aan deze schaal ontleende criteria.[79] Dit gebruik is niet onomstreden, met name omdat deze schalen voor medische en niet voor forensische toepassingen zijn ontwikkeld. Ook de ontwikkelaar zelf, dr. James Tanner, heeft het gebruik van zijn schaal voor leeftijdsschattingen ontraden, omdat de schaal slechts bedoeld is om ten behoeve van kinderartsen ontwikkelingsstadia te beschrijven en niet om leeftijden te schatten.

Over het gebruik en de bewijsrechtelijke waarde van de Tanner-schaal wordt al langere tijd gediscussieerd.[80] Recent onderzoek toont echter aan dat, indien met behulp van de Tanner-schaal een Tannerstadium 3 of 4 wordt vastgesteld, dit "zeer diagnostisch" (in meer juridisch

---

[76] Aldus ook o.m. RB Overijssel, 15-9-2015, ECLI:NL:RBOVE:2015:4299. Minder juist lijkt derhalve RB Oost-Brabant 18-11-2016**,** ECLI:NL:RBOBR:2016:6439 (Vrijspraak bezit kinderporno, sprake van zich toegang verschaffen tot**,** "*maar de rechtbank kan niet vaststellen dat verdachte op dat moment wist of redelijkerwijs diende te vermoeden dat de afbeeldingen op een website afbeeldingen betrof van een persoon onder de 18 jaar*." I.c. betrof het een door het (14-jarige) slachtoffer zelf op een website voor - volgens de site zelf - alleen volwassenen geplaatste afbeeldingen, terwijl het slachtoffer in haar profiel op die website had aangegeven ouder dan 20 te zijn en volgens de Rb ook qua uiterlijk en kleding voor een volwassene kon doorgaan). Zie echter ook hierna onder 5.4 met betrekking tot een eventueel ontslag van rechtsvervolging (vanwege het ontbreken van alle schuld), wat ook in laatstgenoemde situatie mogelijk meer voor de hand had gelegen. Zie met betrekking tot de objectivering van de leeftijd (maar dan in relatie tot art. 245 en art. 247 Sr) ook: RB Gelderland 15-6-2017, ECLI:NL:RBGEL:2017:3152 (minderjarigheid vormt een geobjectiveerd bestanddeel. Dit bestanddeel is bewezen als objectief komt vast te staan dat de minderjarige tussen de 12 en 16 jaar oud was. Wetenschap van de leeftijd is niet van belang voor een bewezenverklaring. De leeftijd is als geobjectiveerd bestanddeel opgenomen ter bescherming van minderjarigen in zedenzaken).
[77] Aldus o.m. HR 7-12-2004, ECLI:NL:HR:2004:AQ8936.
[78] HR 7-12-2004, ECLI:NL:HR:2004:AQ8936; HR 8-5-2001, ECLI:NL:HR:2001:AB1517; Zie ook Kamerstukken II 2001/2002, 27 745, nr. 6. En vgl. RB Overijssel 24-06-2013, ECLI:NL:RBOVE:2013:1506 (bewijs persoon kennelijk jonger dan 18 jaar; toepassing van o.m. Tanner-criteria in pv; bewezenverklaring).
[79] Zie o.m. RB Amsterdam 18-10-2011, ECLI:NL:RBAMS:2011:BT8424 (in het proces-verbaal van politie is voldoende duidelijk beschreven op grond waarvan ((geslachts)ontwikkeling en lichaamsbouw) de verbalisant tot de conclusie is gekomen dat de afbeeldingen kinderpornografisch van aard zijn); zie ook hierna onder 6.2.7.
[80] Zie hierover onder meer S. van der Zee en C. Groeneveld, *Kinderpornografisch beeldmateriaal;* In: Van Wijk e.a., *Facetten van zedencriminaliteit*, Elsevier 2007, p. 235-236.

taalgebruik: “een sterke aanwijzing”) is voor een leeftijd beneden de 18 jaar.[81] Uitgaande van de juistheid van deze bevindingen kan aan een dergelijke vaststelling in het kader van de vraag of sprake is van *een kennelijke leeftijd beneden de 18 jaar* derhalve met name in grensgevallen mogelijk een grotere bewijswaarde worden toegekend, dan tot op heden in de rechtspraktijk het geval is geweest. Zeker gezien bovenvermelde beoordelingsproblematiek is het derhalve ook voor de rechterlijke beoordeling en bewijswaardering van belang dat de beoordelaars bij de politie in hun proces-verbaal aangeven welke kwalificaties zij in dit opzicht hebben, welke criteria zij hebben gehanteerd en hoe en op welke afbeeldingen zij vervolgens die criteria hebben toegepast.[82]

3.3.2. Virtuele kinderpornografische afbeeldingen

Het huidige art. 240b Sr vereist niet dat wordt bewezen dat de betrokken afbeelding een “echt” kind weergeeft. Ook gedragingen met virtuele afbeeldingen van een seksuele gedraging van een kind, zoals bijvoorbeeld afbeeldingen die met behulp van computersoftware zijn gegenereerd, of die in de vorm van tekeningen, schilderijen, collages, montages[83] enz. kunnen tegenwoordig[84] strafbaar zijn. Dit komt in de delictsomschrijving tot uitdrukking in de woorden “schijnbaar betrokken”.
Deze strafbaarstelling van virtuele kinderporno vloeit voort uit de implementatie van internationaalrechtelijke instrumenten als het Cybercrimeverdrag, het Verdrag van Lanzarote en Richtlijn 2011/92/EU. In al deze internationaalrechtelijke instrumenten worden onder het begrip kinderpornografie tevens begrepen “realistische afbeeldingen” van seksuele handelingen waarbij minderjarigen zijn betrokken.[85]

Uit de wetsgeschiedenis van art. 240b Sr blijkt dat virtuele afbeeldingen pas strafbaar zijn als het gaat om realistische afbeeldingen, en wel in de zin van “niet van echt te onderscheiden” c.q. “levensecht”.[86]

In het verleden heeft het openbaar ministerie wel (conform de Aanwijzing Kinderpornografie 2010 het standpunt ingenomen dat het verbod op bezit van kinderporno tevens alle afbeeldingen (van seksuele gedragingen waarbij (schijnbaar) kinderen betrokken zijn) zou omvatten die “niet evident levensecht zijn”.[87]

---

[81] Zie M.J. Hoogendoorn, *De waarde van Tannerschalen bij de bepaling van de kennelijke leeftijd van een model*, *DD* 2014/9 (afl. 2, p. 90-107), waarin o.m. ook wordt gesteld: “*Wij kunnen dus ook zeggen dat alle Tannerstadia 3 duiden op een kennelijke leeftijd onder de 18*”. Daarbij kan worden opgemerkt dat het bij de Tanner-stadia 1 en 2 veelal evident is dat sprake is van minderjarigheid.

[82] Vgl. in dit opzicht ook onder meer: RB Noord-Holland 24-11-2014, ECLI:NL:RBNHO:2014:11709 (“*De verbalisanten die het materiaal hebben beoordeeld maken deel uit van een team dat gespecialiseerd is in de beoordeling van kinderporno en bezitten de expertise die hiervoor nodig is. In hun proces-verbaal van bevindingen is door een zedenrechercheur en een gecertificeerde selecteur kinderpornografie, beschreven hoe zij hebben vastgesteld dat het om minderjarige personen gaat. De rechtbank heeft mede gelet op het ontbreken van een nadere onderbouwing door de verdediging, geen reden om aan die bevindingen van de zedenrechercheurs te twijfelen en verwerpt het verweer*”) en HR 7-12-2004, ECLI:NL:HR:2004:AQ8936.

[83] Zie bijv. RB Utrecht 9-11-2010, ECLI:NL:RBUTR:2010:BO3818 (op foto’s van seksuele handelingen drie hoofden van actoren digitaal vervangen door die van 3 kinderen; zodanig van kwaliteit dat nauwelijks te zien is dat deze zijn gemanipuleerd; veroordeling).

[84] Deze strafbaarstelling is op 1 oktober 2012 in werking getreden.

[85] Zie o.m. art. 2, sub c onder III en IV van Richtlijn 2011/92/EU, Publicatieblad EU, 2011, L 335/1, art. 9, lid 2, onder c van het Cybercrimeverdrag, Trb. 2004, 290 en art. 20 lid 4 van het Verdrag van Lanzarote, Trb. 2008, 58, met dien verstande partijen bij dit laatste verdrag een reservering kunnen maken met betrekking tot deze uitbreiding van de definitie van kinderpornografie.

[86] Zie Kamerstukken II 2001/2002, 27445, nr. 6, p. 14.

[87] Deze stelling was vervat in het requisitoir van de advocaat-generaal die bij het hof de zaak behandelde die leidde tot HR 12-3-2013, ECLI:NL:HR:2013:BY9719 en is weergegeven in de conclusie van AG Vellinga bij laatstgenoemd arrest.

In lijn met hetgeen daaromtrent al overwegend in de lagere rechtspraak was geoordeeld[88], heeft de Hoge Raad deze ruimere OM-uitleg echter in 2013 verworpen.[89] De Hoge Raad overwoog daarbij met zoveel woorden dat: "*noch uit de ontstaansgeschiedenis noch uit de tekst van het Facultatief Protocol (inzake de verkoop van kinderen, kinderprostitutie en kinderpornografie bij het Verdrag inzake de Rechten van het Kind) volgt dat de daarin gegeven definitie van 'child pornography' ook betrekking heeft op niet realistische afbeeldingen van niet-bestaande kinderen*."
In de betreffende zaak ging het om zogenaamde Hentai-afbeeldingen[90] die geheel digitaal op de computer waren vervaardigd en die een artificieel karakter hadden. Omdat de desbetreffende afbeeldingen niet realistisch waren, vielen zij zowel volgens het Hof Den Bosch[91] als volgens de Hoge Raad niet onder de reikwijdte van art. 240b Sr. De technische mogelijkheden voor de vervaardiging van computeranimaties zijn de laatste jaren steeds geavanceerder geworden. De computeranimaties krijgen een steeds groter realiteitsgehalte.[92] Of in het concrete geval aan de realiteitseis wordt voldaan is ter beoordeling van de feitenrechter.

Van groot belang voor de feitelijke invulling van de realiteitseis zijn voorts de overwegingen van de Hoge Raad in twee arresten van 8 december 2015.[93] De Hoge Raad overwoog daarbij onder meer:

> *4.3.2. De Hoge Raad heeft in zijn arrest van 12 maart 2013, ECLI:NL:HR:2013:BY9719, NJ 2013/403, ten aanzien van virtuele kinderpornografie op grond van de wetsgeschiedenis van art. 240b Sr geoordeeld dat het bestanddeel 'schijnbaar betrokken' in de delictsomschrijving van art. 240b Sr meebrengt dat onder deze strafbepaling ook begrepen is een realistische afbeelding van een niet-bestaand kind in de zin dat de afbeelding niet van echt is te onderscheiden. In dat arrest werd het oordeel van het hof dat virtuele afbeeldingen van kinderpornografie niet als realistisch in deze zin zijn aan te merken niet onbegrijpelijk geacht, gelet op de vaststellingen van het hof dat de afgebeelde personen "geen echte kinderen" zijn en dat voor "de gemiddelde kijker (...) aanstonds blijkt dat het gaat om gemanipuleerde afbeeldingen".*
>
> *4.3.3. De enkele omstandigheid dat aanstonds blijkt dat niet sprake is van een fotografische maar van een geschilderde realistische weergave van een seksuele gedraging waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is*

---

[88] Zie o.m. Hof Amsterdam 09-1-2013, ECLI:NL:GHAMS:2013:BY8414 (appel inzake RB Amsterdam ECLI:NL:RBAMS:2010:BO9296, schilderijen met realistische kinderpornografische scenes worden beschouwd als afbeeldingen in de zin van art. 240b Sr, ondanks het feit dat sommige kinderen zijn afgebeeld met engelenvleugels); Hof Arnhem 12-04-2012, ECLI:NL:GHARN:2012:BW3415 bevestiging vrijspraak i.v.m. het niet-realistisch zijn van 5 Hentai-afbeeldingen), Hof Den Bosch 14-4-2011, ECLI:NL:GHSHE:2011:BQ1179;; RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (o.a. vrijspraak bezit virtuele kinderporno nu de afbeeldingen niet als realistisch zijn aan te merken); anders: Hof Arnhem 25-01-2012, ECLI:NL:GHARN:2012:BV2126 (appel inzake RB Utrecht 9-11-2010, ECLI:NL:RBUTR:2010:BO3818 (afbeeldingen waarbij het hoofd van een overduidelijk minderjarige is gebruikt op het lichaam van een (jong)volwassene zijn als kinderpornografie aan te merken. "*Voor een buitenstaander is niet zonder meer duidelijk dat de beelden bewerkt zijn*").
[89] HR 12-3-2013, ECLI:NL:HR:2013:BY9719.
[90] Zie hiervoor bij noot 69.
[91] Hof Den Bosch 14-4-2011, ECLI:NL:GHSHE:2011:BQ1179.
[92] Illustratief voor dit realiteitsgehalte is bijvoorbeeld het door Terre des Hommes in het kader van het verkrijgen van aandacht voor seksueel kindertoerisme via de webcam ingezette geheel digitale kind "Sweetie". Klik hier om de video hiervan te zien.
[93] HR 8-12-2015, ECLI:NL:HR:2015:3483 en ECLI:NL:HR:2015:3484. Vgl. voor toepassing van het beoordelingskader van de Hoge Raad, en uitvoerige verwijzingen naar de wetsgeschiedenis Hof Amsterdam, 4 maart 2021, ECLI:NL:GHAMS:2021:647.

betrokken, staat op zichzelf niet aan de toepasselijkheid van art. 240b, eerste lid, Sr in de weg. Ook de omstandigheid dat ondergeschikte onderdelen van zo'n afbeelding een niet-werkelijkheidsgetrouwe weergave van een kind zijn, bijvoorbeeld doordat - zoals in het onderhavige geval - op de rug van het afgebeelde kind vleugels zijn aangebracht, heeft niet zonder meer tot gevolg dat de afbeelding van het kind als geheel niet kan worden aangemerkt als een realistische afbeelding zoals bedoeld in art. 240b Sr.

4.3.4. Wel zal vanwege het bijzondere karakter van zo een onder art. 240b Sr te rubriceren geschilderde realistische afbeelding uit de motivering van het oordeel van de feitenrechter duidelijk moeten blijken waarop is gebaseerd dat de afbeelding een zodanig realiteitsgehalte heeft dat de afbeelding van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, niet van echt is te onderscheiden. Dat sluit ook aan bij eerdere rechtspraak van de Hoge Raad over virtuele kinderpornografie.

Een en ander impliceert dat het in dergelijke gevallen aan de rechter zal zijn om via de eigen waarneming[94] te oordelen in hoeverre hij bepaalde virtuele afbeeldingen "niet van echt te onderscheiden" acht[95], waarbij echter vermenging van realistische met niet-realistische elementen er niet zonder meer aan in de weg staat dat afbeeldingen als geheel toch als zodanig worden gekwalificeerd. Gezien het voorgaande zal daarbij de lat waarschijnlijk wel relatief hoog dienen te worden gelegd. Omkeringen in de trant van "*het is voor een waarnemer niet aanstonds duidelijk dat de beelden bewerkt zijn*"[96] zijn dan ook cassatietechnisch gezien waarschijnlijk risicovol.

3.4. "Verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezit heeft"

Art. 240b Sr omschrijft een groot aantal (strafbare) gedragingen met betrekking tot kinderpornografisch materiaal. Deze opsomming van gedragingen is echter weinig systematisch en ten aanzien van bepaalde gedragingen is sprake van – soms aanzienlijke – overlap. De verklaring hiervoor is dat een aantal gedragingen in het kader van de implementatie van internationaalrechtelijke instrumenten (vooral het Verdrag van Lanzarote) rechtstreeks uit die instrumenten is overgenomen. De omvang van de opsomming maakt echter duidelijk dat de wetgever beoogd heeft vrijwel elke handeling met betrekking tot kinderpornografisch materiaal als een strafbare gedraging aan te merken.[97] Deze duiding en reikwijdte van deze gedragingen worden hierna apart besproken.

---

[94] Zie omtrent de rol van de eigen rechterlijke waarneming r.o. 4.3.4 bij de in de vorige noot genoemde arresten.
[95] Vgl. bijv. RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 ("*Gemanipuleerde afbeeldingen en films vallen onder de reikwijdte van art. 240b Sr als deze op het eerste gezicht niet van echt zijn te onderscheiden. Dit criterium heeft de rechtbank ook gehanteerd in raadkamer bij het bestuderen van de afbeeldingen*"; Vrijspraak voor deel van de afbeeldingen); RB Utrecht 9-11-2010, ECLI:NL:RBUTR:2010:BO3818 (op foto's van seksuele handelingen drie hoofden van actoren vervangen door die van 3 kinderen; resultaat digitaal opgeslagen; zodanig van kwaliteit dat nauwelijks te zien is dat deze zijn gemanipuleerd; veroordeling vervaardigen virtuele kinderporno); RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (de afdrukken die door de rechtbank zijn waargenomen, zijn niet als realistisch in die zin aan te merken; vrijspraak).
[96] Zoals in Hof Arnhem 25-1-2012, ECLI:NL:GHARN:2012:BV2126 wordt overwogen.
[97] Een uitzondering is het louter "(mee)kijken" naar kinderpornografisch materiaal. De wetgever heeft dit niet zelfstandig strafbaar willen stellen, tenzij sprake is van kijken naar afbeeldingen waartoe men zich via een geautomatiseerd werk toegang heeft verschaft (zie verder hierna onder 3.5).

3.4.1. "verspreidt"

De wetsgeschiedenis bevat geen bijzondere aanknopingspunten voor hetgeen in deze context onder "verspreiden" moet worden begrepen. Van Dale omschrijft verspreiden als: "*in allerlei richtingen, over een oppervlakte of door een ruimte, plaatsen, uitzenden, strooien*". Hieruit kan worden afgeleid dat het bij verspreiden moet gaan om het *verplaatsen* van zaken, goederen, informatie of gegevens.[98]

Deze laatste constatering is van belang, omdat tot op heden in de rechtspraak het onderscheid tussen het (actief) digitaal verplaatsen van bijvoorbeeld afbeeldingen en het op een andere wijze ter kennis brengen van het bestaan van (en/of het toegang verschaffen tot) dergelijke afbeeldingen, dan wel het (passief) aanbieden van afbeeldingen niet altijd even systematisch en juist wordt gemaakt. Dit klemt te meer nu bij de straftoemeting aan verspreiden een zwaarder gewicht wordt toegekend dan aan bijvoorbeeld (enkel) bezit.

Kinderpornografisch materiaal wordt op zeer grote schaal gedeeld, zowel door commerciële criminele organisaties als binnen netwerken en tussen "geïnteresseerde" individuen. In het kader van art. 240b Sr is echter de omvang van de verspreiding en de omvang van het verspreide materiaal niet van belang. De verspreiding kan mitsdien zowel meerdere afbeeldingen betreffen als meerdere exemplaren van een en dezelfde afbeelding. Gezien het beschermde belang volstaat voor de bewezenverklaring van verspreiden namelijk al de verzending (etc.) van één afbeelding.[99] Evenmin is vereist dat het verspreiden heeft plaatsgevonden naar meerdere personen. Toezending aan één andere persoon volstaat om van verspreiding te kunnen spreken.[100] De titel waaronder (bijv. koop, ruil) of reden waarom (wraak, lid kunnen worden van een forum) kinderpornografisch materiaal wordt verspreid is voor de bewezenverklaring van het bestanddeel "verspreiden" irrelevant.[101]

Niet elke vorm van delen impliceert echter ook "verspreiden" in de hier genoemde zin. Een aantal vormen van delen van computerbestanden impliceert (voor zover er opzettelijk is gedeeld)[102] eveneens verspreiding.[103] Gedacht kan hierbij allereerst worden aan situaties waarin afbeeldingen worden ge-upload/gezonden naar een nieuws[104]-, forum[105]-, chat[106]- of

---

[98] Dit impliceert dat het aantreffen van kinderpornografisch materiaal in een "gewone" map op een computer, ongeacht of deze map door de benaming doet vermoeden dat de inhoud daarvan bedoeld is voor verspreiding, onvoldoende is om zulks als verspreiden te kwalificeren. Zie ook: RB Amsterdam 1-8-2017, ECLI:NL:RBAMS:2017:5532 (vrijspraak voor het verspreiden en aanbieden van kinderpornografisch materiaal. De enkele omstandigheid dat er een map op de computer is aangetroffen met de bestandsnaam 'Trade' brengt niet zonder meer met zich dat verdachte daadwerkelijk heeft gehandeld of geruild met de inhoud van die map. Ook een e-mail met het voorstel kinderpornografisch materiaal te ruilen leidt niet zonder meer tot diezelfde conclusie).

[99] Aldus begrijpen de auteurs ook Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht*, art. 240b Sr, aantekening 5, onder a.

[100] Aldus ook o.m. RB Gelderland 25-11-2013, ECLI:NL:RBGEL:2013:4849 (versturen filmpje van 15-jarige ex-sekspartner naar 1 persoon).

[101] Zie bijv. RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735 (bewezenverklaring *verspreiding;* Verdachte heeft verklaard dat hij bestanden die kinderporno bevatten heeft *geruild* met anderen); Hof Arnhem-Leeuwarden 14-6-2017, ECLI:NL:GHARL:2017:5020 (veroordeling voor bezit, verspreiden en openlijk tentoonstellen van kinderporno. Uit *wraak* één foto van (ex-)vriendin op Facebook geplaatst).

[102] Voor alle in art. 240b Sr genoemde handelingen is immers ook (voorwaardelijk) opzet vereist; zie hierover verder hoofdstuk 4.

[103] Zie specifiek over "verspreiding" van kinderpornografische afbeeldingen via chatgroepen par. 3.4.1.3.

[104] Zie o.m. RB Utrecht 21-5-2010, ECLI:NL:RBUTR:2010:BM8666; RB Den Haag 3-10-2005, ECLI:NL:RBSGR:2005:AU3675 en RB Utrecht 21-5-2010, ECLI:NL:RBUTR:2010:BM8666.

[105] Hof Arnhem-Leeuwarden 26-8-2016, ECLI:NL:GHARL:2016:6883 (verspreiden d.m.v. plaatsen op forum)

[106] RB Noord-Nederland 29-5-2017, ECLI:NL:RBNNE:2017:1929 (afbeeldingen verspreid via Tumblr);.

WhatsAppgroep[107], of (ook) voor andere personen toegankelijke websites[108], (cloud)opslagdiensten als Dropbox[109], SkyDrive (de voorganger van OneDrive[110]) en OneDrive[111], of waarin afbeeldingen worden gedeeld via social media-accounts als bijvoorbeeld Facebook, Instagram en Snapchat en Kik (Messenger).[112] Ook het verzenden of doorzenden van een afbeelding – al dan niet als bijlage bij bijvoorbeeld een e-mailbericht – aan een of meer personen valt (uitzonderingen daargelaten)[113] onder "verspreiding".[114] Voor zover sprake is van het delen van kinderpornografisch materiaal in chatgroepen, zoals WhatsApp- of Telegram-groepen, verdient in het bijzonder aandacht dat de kring van personen die daarvan kennis konden nemen (door het delen) moet zijn vergroot.[115]

Eerst recent is in de jurisprudentie de vraag aan de orde gekomen in hoeverre er ook sprake is van verspreiding indien men kinderpornografische afbeeldingen vastlegt op, of zendt/uploadt naar locaties waartoe de verdachte *alleen zelf* toegang heeft. Hoewel strikt feitelijk het materiaal dan wel is verspreid, is er dan geen sprake van vergroting van de kring van personen die kennis kunnen nemen van de betreffende afbeeldingen. Betoogd kan dan ook worden dat in dit geval *de jure* eerder sprake is van een situatie van "in bezit hebben" dan van "verspreiden". De Rechtbank Oost-Brabant oordeelde in 2017 ook in deze zin.[116]

In de rechtspraak is tevens de vraag aan de orde gekomen in hoeverre het zenden (of publiceren) van een *hyperlink* die leidt naar een weblocatie met kinderpornografische afbeeldingen kan worden gelijkgesteld met het versturen/verspreiden van die afbeelding zelf. Enerzijds kan worden betoogd dat daarvoor goede gronden bestaan, immers "*met het verstrekken van de sleutel verschaf je een ander ook de toegang*".[117] Weliswaar ziet de wettelijke strafbaarstelling op het verspreiden van een *afbeelding*, niet (ook) op die van

---

RB Arnhem 27-6-2008, ECLI:NL:RBARN:2008:BD5618 (verspreiden via MSN); RB Oost-Brabant 26-04-2013, ECLI:NL:RBOBR:2013:CA3587 (delen kinderpornografisch materiaal via MSN); RB Zutphen 09-2-2011, ECLI:NL:RBZUT:2011:BP3790 (verspreiden kinderporno tijdens chatsessies).

[107] Zie nader par. 3.4.1.3.

[108] RB Rotterdam 1-6-2017, ECLI:NL:RBROT:2017:5192 (plaatsing kinderpornografie op diverse websites, waaronder twitter.com); RB Zwolle 13-10-2011, ECLI:NL:RBZLY:2011:BT7560 (uploaden kinderpornografisch materiaal naar de community site Dreamboard); RB Midden-Nederland 24-2-2014, ECLI:NL:RBMNE:2014:705 (verspreiden kinderporno "via plaatsing op internet").

[109] RB Roermond 22-4-2011, ECLI:NL:RBROE:2011:BQ3544 (uitwisseling via Dropbox).

[110] RB Oost-Brabant 26-4-2013, ECLI:NL:RBOBR:2013:CA3587 (delen kinderpornografisch materiaal door plaatsing in de cloud via online backup- en opslagprogramma SkyDrive).

[111] RB Oost-Brabant 17-12-2015, ECLI:NL:RBOBR:2015:7343 (verspreiden via e-mail en door het plaatsen in een digitale opslagruimte van Microsoft).

[112] Vgl. RB Gelderland, 21-5-2021, ECLI:NL:RBGEL:2021:2737 (verspreiden door eenmalige plaatsing via en in het chatprogramma Kik). RB Den Haag 14-9-2017, ECLI:NL:RBDHA:2017:10941 (bezit/verspreiden/aanbieden van 17 kinderpornografische afbeeldingen via *Twitter:* **"***De verdachte heeft zich, door foto's die als kinderpornografisch kunnen worden aangemerkt op een twitteraccount met 100 tot 200 volgers te plaatsen, schuldig heeft gemaakt aan het bezit en het verspreiden van die foto's*"); RB Noord-Holland 25-11-2016**,** ECLI:NL:RBNHO:2016:9771 (openbaar maken d.m.v. plaatsen van filmpjes op *Snapchat*).

[113] RB Midden-Nederland 11-11-2020, ECLI:NL:RBMNE:2020:4883 (partiële vrijspraak verspreiden/aanbieden, weliswaar e-mail met als bijlage enkele kinderpornografische afbeeldingen verzonden aan voormalig werkgever, maar niet gebleken van daadwerkelijke bedoeling tot verspreiding).

[114] Zie o.m. RB Gelderland 25-11-2013, ECLI:NL:RBGEL:2013:4849 (versturen kinderpornografisch filmpje naar 1 persoon); RB Den Bosch 18-6-2012, ECLI:NL:RBSHE:2012:BW9037 (e-mailen van naaktfoto's);

[115] Zie hierover meer uitvoerig par. 3.4.1.3 ("verspreiden" via chatgroepen; WhatsApp/Telegram).

[116] RB Oost-Brabant 4-5-2017, ECLI:NL:RBOBR:2017:2471 (vrijspraak van verspreiding van kinderporno via Whatsapp, aannemelijk dat verdachte via zijn ene telefoon naar zijn andere telefoon met behulp van Whatsapp de kinderpornografische afbeeldingen doorzond, en de kring van personen die van de kinderpornografische afbeeldingen kennis konden nemen daarmee niet heeft vergroot).

[117] RB Amsterdam 23-7-2012, ECLI:NL:RBAMS:2012:BX2325 (verspreiden van een link naar een afbeelding kan worden beschouwd als het versturen van die afbeelding).

hyperlinks of wachtwoorden[118], maar daar staat tegenover dat het qua praktische uitwerking niet veel verschil maakt of iemand een of meer afbeeldingen uit zijn eigen cloudopslag per mail naar een ander stuurt of deze afbeeldingen aan die ander ter beschikking stelt door deze een hyperlink naar die bestanden toe te sturen (en doorgaans daarmee samenvallend die ander machtigt om daarvan kennis te nemen).

In een zaak waarin art. 261, tweede lid, Sr ten laste werd gelegd (verspreiding van een smadelijk geschrift en/of -afbeelding) oordeelde de Hoge Raad op 13 maart 2018:

> *2.5. Uit de bewijsmiddelen blijkt dat de inhoud van het bericht op de website www.stopkinderseks.com van de verdachte afkomstig is. Voorts blijkt uit de bewijsmiddelen dat de verdachte een hyperlink naar voormeld bericht op haar Facebookpagina heeft gedeeld en dat zij daarbij anderen heeft verzocht het bericht verder te delen. Gelet hierop en in aanmerking genomen dat het Hof tevens heeft vastgesteld dat door het delen van die hyperlink op haar Facebookpagina het bericht waar die hyperlink naartoe leidde voor iedere willekeurige bezoeker van de Facebookpagina van de verdachte zichtbaar was en dat het bericht vervolgens ook daadwerkelijk door derden verder is gedeeld, geeft het oordeel van het Hof dat de verdachte zich schuldig heeft gemaakt aan "verspreiding van een geschrift en/of afbeelding" niet blijk van een onjuiste rechtsopvatting en is het toereikend gemotiveerd.*[119]

Gezien deze laatste overweging(en) lijkt het niet erg waarschijnlijk dat de Hoge Raad in art. 240b Sr-zaken moeite zou hebben met de juridische gelijkstelling van hyperlinks naar locaties met afbeeldingen van kinderporno met die van de afbeeldingen zelf.

In de lagere rechtspraak is soortgelijk geoordeeld in relatie tot het verstrekken van wachtwoorden aan anderen die toegang gaven tot beveiligde mappen met kinderpornografische afbeeldingen op een bepaald netwerk.[120]

3.4.1.1. "verspreiden" via peer-to-peer (P2P) software?

In de digitale wereld wordt voor het verspreiden en delen van bestanden nog altijd gebruik gemaakt van zogenaamde peer-to-peer (P2P) programma's. Er is een aantal van dergelijke programma's in omloop.

Technisch lemma: peer-to-peer (P2P)-programma's

---

[118] Het verspreiden van hyperlinks en wachtwoorden welke toegang geven tot kinderpornografisch materiaal kan overigens wellicht ook onder het bereik van "aanbieden" en/of van "openlijk tentoonstellen" vallen.

[119] HR 13-3-2018, ECLI:NL:HR:2018:331 (conform ook de conclusie van AG Bleichrodt (ECLI:NL:PHR:2017:1587), die in par. 18 uitvoeriger ingaat op de betekenis en duiding van het begrip "verspreiden" in het digitale tijdperk), recentelijk bevestigd in HR 7-7-2020, ECLI:NL:HR:2020:1213.

[120] RB Midden-Nederland 28-9-2016, ECLI:NL:RBMNE:2016:5203; Opvallend in dit kader is ook Hof Amsterdam 4-5-2016, ECLI:NL:GHAMS:2016:1891 ("*Het hof stelt voorop dat alleen dan kan worden gesproken van het verspreiden van kinderpornografisch materiaal, indien niet alleen komt vast te staan dat de verdachte een ander de mogelijkheid heeft geboden om met gebruikmaking van een wachtwoord kinderpornografisch materiaal van zijn computer te downloaden, maar tevens dat die ander daadwerkelijk gebruik heeft gemaakt van deze geboden mogelijkheid*"; i.c. is dit laatste slechts bij 7 afbeeldingen gebleken, voor de overige afbeeldingen vrijspraak). Het Amsterdamse hof lijkt hier het onderscheid tussen verspreiden en aanbieden/tentoonstellen wat uit het oog te hebben verloren.

Hoe werken peer-to-peer (P2P)-programma's?[121]
Een peer-to-peer (P2P)-programma is een programma dat computers met elkaar in verbinding brengt met het doel onderling bestanden uit te wisselen. Men spreekt dan ook veelal over P2P-netwerken. P2P-programma's zijn in beginsel legaal en zeer eenvoudig (en veelal gratis) via internet te downloaden. Ook het gebruik van dergelijke programma's is eenvoudig. P2P-programma's worden veelal gebruikt om games, muziek- en videobestanden (waaronder die welke kinderpornografische afbeeldingen bevatten) uit te wisselen.

Downloaden via een P2P-programma
Het downloaden via een P2P-programma gaat fundamenteel anders dan bij bijvoorbeeld downloaden vanaf een website, waar een bestand in zijn geheel vanaf één locatie kan worden gedownload (het zogenaamde client-server model). Een P2P-netwerk kent namelijk een geheel ander model: elke computer die is aangesloten op het P2P-netwerk gaat zich gedragen als een server. Via een gedeelde map (shared folder) kunnen door die computers bestanden worden aangeboden aan de andere gebruikers in het P2P-netwerk. Deze andere gebruikers kunnen de aangeboden bestanden vinden via een zoekmachine in het P2P-programma.

Dit model heeft als belangrijk voordeel ten opzichte van het client-server model dat de gebruiker een gegevensbestand in delen kan verkrijgen van meerdere aanbieders tegelijk en zo een hogere downloadsnelheid kan bereiken. Daarnaast is het model niet afhankelijk van de bereikbaarheid van één downloadlocatie. Gedownload materiaal wordt bij de bestandsopvragende gebruiker (zo nodig) bij elkaar gevoegd en opgeslagen op een bij de installatie van het P2P-programma (al dan niet na autorisatie van de programmagebruiker) automatisch aangemaakte map, dan wel op een door de gebruiker specifiek opgegeven locatie (die ook hier de gedeelde map/shared folder wordt genoemd) op de harde schijf van zijn computer. Dit is een permanente map, die dus ook niet van de computer verdwijnt door de computer af te sluiten en opnieuw op te starten. Gedownload materiaal blijft dus in de gedeelde map/shared folder aanwezig tot het actief door de gebruiker wordt verwijderd.

Er zijn verschillende P2P-netwerken met bijbehorende programma's. Zo werkt GigaTribe met het GigaTribe-netwerk, eMule op het eDonkey-netwerk en BitTorrent op het BitTorrent-netwerk. Dit laatste netwerkt wijkt af van doorsnee-P2P-programma's. Gebruikers van dit protocol wisselen bestanden onderling uit met tussenkomst van zogenaamde trackers, een soort servers. De tracker (een bestand met de extentie .torrent) weet wie van de gebruikers een bepaald bestand heeft en brengt de vragende en aanbiedende partij in contact. Een tracker kan een vragende partij in contact brengen met meerdere aanbieders, die elk een deel van het bestand naar de vragende partij sturen. Wanneer een gebruiker een bestand downloadt van andere gebruikers, kan datzelfde bestand nog voordat het in zijn geheel is gedownload in kleine deeltjes worden aangeboden aan andere gebruikers. De software plaatst de ontvangen stukjes van het bestand bij elkaar als alle stukjes zijn ontvangen. Recentelijk is het BitTorrent-protocol doorontwikkeld en zijn op een server geplaatste trackers niet langer noodzakelijk. Gebruikers van het BitTorrent-protocol delen in dat nieuwe model onderling die informatie.

Beschikbaarheid voor derden van via P2P-programma's gedownloade bestanden
Het is afhankelijk van de gebruikte instellingen of hetgeen wordt gedownload ook weer direct beschikbaar is voor andere gebruikers van hetzelfde P2P-programma. Omdat het succes van dergelijke bestandsuitwisselingsprogramma's afhangt van de bereidheid van deelnemers om zoveel mogelijk te delen is bij vele van deze programma's de standaardinstelling dat ontvangen bestanden ook (nog voordat deze in hun geheel zijn ontvangen) beschikbaar zijn voor anderen. Veel programma's bieden evenwel de mogelijkheid om uitwisseling volledig te blokkeren dan wel te beperken in bandbreedte. Daarnaast kunnen gebruikers ook een gedeelde map/shared folder selecteren waar geen bestanden in aanwezig zijn.

Trackers zoals torrent-bestanden worden veelal via daartoe bestemde websites aangeboden. Soms is de toegang tot die websites pas mogelijk na aanmelding en registratie, of alleen op uitnodiging van eerdere gebruikers. Deze websites houden via de trackers bij door welke gebruikers wordt gedownload en of zij en hoeveel bestanden zij weer aanbieden (een shared rate). In sommige gevallen worden gebruikers die enkel downloaden na enige tijd uitgesloten van verder gebruik van de via het platform aangeboden .torrents. Aldus wordt actief gestimuleerd dat gebruikers zelf ook zoveel mogelijk delen.

[121] Zie voor een uitvoerig overzicht van welke bekende/veel gebruikte P2P-programma's, -netwerken, -protocollen en -applicaties er zoal zijn o.m.: https://nl.wikipedia.org/wiki/Peer-to-peer.

Het is derhalve veelal eigen aan het gebruiken van een P2P-programma dat de gebruiker via een gedeelde map/shared folder gegevens ter beschikbaar stelt aan anderen, en dat hij van de gedeelde mappen/shared folders van anderen materiaal kan downloaden, welk materiaal dan vervolgens via hem ook weer voor anderen beschikbaar komt. Aldus vormen de gebruikers van een P2P-programma een netwerk dat is gebaseerd op gelijkwaardigheid en directe uitwisseling van en tussen computers. Vandaar ook de aanduiding "peer-to-peer"-netwerk.

Uit het voorgaande volgt dat het nagenoeg eigen is aan het gebruik van een peer-to-peer programma, dat niet alleen kan worden gedownload, maar ook dat (en ook tegelijk) ander op de shared map of shared drive aanwezig materiaal wordt gedeeld met anderen. Het komt ons dan ook voor dat tegenwoordig nagenoeg elke gebruiker van P2P-software wel van dit feit op de hoogte zal zijn. De werking van P2P-programma's (en derhalve ook dit specifieke aspect) is thans immers breed bekend en deze informatie is thans ook voor een ieder bijvoorbeeld via internet op eenvoudige wijze toegankelijk.

Besloten peer-to-peer (friend-to-friend/F2F)-netwerken / darkweb
De meest gebruikte P2P-programma's (zoals µTorrent en Gigatribe) kunnen vrijelijk worden gedownload, ook dus door bijvoorbeeld opsporingsdiensten. Het is bekend dat opsporingsdiensten actief onderzoeken of kinderpornografisch materiaal wordt aangeboden via deze programma's. Hoewel het langs deze weg aanbieden van kinderpornografisch materiaal nog steeds lijkt voor te komen, is aannemelijk dat de meeste verspreiders van kinderpornografisch materiaal andere plaatsen verkiezen. Ook bepaalde netwerken die alleen toegankelijk zijn voor 'friends', bekenden van de bestaande deelnemers, zijn wat dat betreft voor veel gebruikers niet langer veilig door intensivering van de controle door opsporingsdiensten. Het uitwisselen van kinderpornografisch materiaal lijkt zich steeds meer te hebben verplaatst naar het darkweb, zie 3.4.1.2.

Uit het voorgaande blijkt dat het bij het gebruik van P2P-software vaker voorkomt dat bestanden die men downloadt of die anderszins worden geplaatst in de voor het gebruik van dat P2P-programma ingestelde "*shared*" map *op de eigen computer* geheel of gedeeltelijk ook beschikbaar stelt voor andere gebruikers van het betreffende P2P-programma. Het digitale materiaal wordt derhalve wel toegankelijk voor andere gebruikers, maar niet *actief* door de gebruiker van de shared drive naar hen of naar een ander geautomatiseerd werk of andere gegevensdrager dan die op de eigen computer verzonden. Het is derhalve twijfelachtig of de plaatsing (al dan niet "automatisch") met gebruikmaking van P2P-software van kinderpornografisch materiaal op een gegevensdrager van de gebruiker *de jure* wel kan worden aangemerkt als *verspreiding* van dat materiaal.[122] De eveneens in de delictsomschrijving van art. 240b Sr opgenomen begrippen "aanbieden" of "openlijk tentoonstellen" lijken hier meer passend.[123]
Vanuit strafvorderlijk oogpunt blijft bij de beoordeling of, en zo ja: in hoeverre, aan deze onderscheiden bestanddelen is voldaan overigens wel van eminent belang dat uit het dossier voldoende blijkt dat de op de tenlastelegging vermelde bestanden zich daadwerkelijk op de *shared drive* bevonden.[124]

[122] Dit onderscheid en de eigenlijke werking van P2P-software worden regelmatig onvoldoende onderkend, zoals bijv. in RB Noord-Nederland 21-11-2017, ECLI:NL:RBNNE:2017:4460 ("Bij het downloaden van dit materiaal maakte verdachte onder meer gebruik van Peer2Peer programma's en bij het gebruik van dergelijke downloadprogramma's *worden tegelijkertijd met het downloaden van bestanden ook bestanden ge-upload* en zo met anderen gedeeld. Hoewel verdachte zich hier wellicht niet (altijd) van bewust was heeft hij daarnaast ook bewust kinderpornografisch materiaal met een ander gedeeld en zich aldus meerdere malen schuldig gemaakt aan het *verspreiden* van kinderpornografisch materiaal). Daarnaast kan er discussie bestaan over de vraag in hoeverre bij "delen" via een shared drive sprake is van opzet; zie hierover verder onder 4.1.3.2.
[123] Voor de strafmaat zal dit overigens waarschijnlijk weinig verschil maken; zie hierna onder 8.3.3.1.
[124] Zie bijv. ook: RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (vrijspraak voor verspreiden van kinderporno via Gigatribe. Niet kan worden vastgesteld dat verdachte een of meer in de tenlastelegging genoemde bestanden via Gigatribe daadwerkelijk heeft gedeeld. Weliswaar blijkt uit chats dat er bestanden zijn gedeeld met anderen, maar niet blijkt om *welke* bestanden dit gaat).

Nochtans kan worden geconstateerd dat in de rechtspraak het via P2P-software voor anderen (mede)toegankelijk maken van kinderpornografisch materiaal op de eigen computer zeer veelvuldig als "verspreiden" is aangemerkt[125], hoewel zulks meer recentelijk ook wel als "aanbieden" is gekwalificeerd.[126]

3.4.1.2. "verspreiden" via het dark web

Met name vanwege de hoge mate van anonimiteit die het dark web biedt, is de uitwisseling van kinderpornografisch materiaal de laatste jaren in grote mate verplaatst naar speciaal daarvoor ingerichte internetpagina's op het dark web.[127]

Technisch lemma: het dark web

Wat is het dark web?
Waar gesproken wordt over het dark web worden veelal websites bedoeld die niet via zoekmachines vindbaar zijn, maar enkel te benaderen zijn via speciale software. Voor hier dieper op in te gaan, is het goed de positie van het dark web helder te krijgen. Het totale internet is grofweg op te delen in drie terreinen. Het "clear web" of "surface web", bestaande uit reguliere websites zoals nrc.nl en knmi.nl, maakt slechts ongeveer 4% van het totale internet uit. Veruit het grootste gedeelte van het internet bestaat uit wat ook wel het "deep web" wordt genoemd. Dat zijn die websites en gegevens die niet toegankelijk zijn voor iedereen, zoals bijvoorbeeld het gedeelte van websites waarvoor inloggen is vereist (een LinkedIn-pagina van een collega), een database of afgeschermde online omgevingen zoals het intranet (binnen de Rechtspraak aangeduid als Intro). Het derde terrein wordt gevormd door het "dark web" en kan worden gezien als een (overigens zeer klein) onderdeel van het hiervoor genoemde deep web. Dit gedeelte van het internet maakt wel gebruik van de infrastructuur van het internet, maar vereist specifieke software en configuraties om de websites op dat netwerk te kunnen bereiken. De meest bekende software is de Tor-browser, maar er zijn ook andere netwerken zoals Freenet, I2P en Riffle, die elk hun eigen software of configuraties vereisen. In het onderstaande wordt verder slechts ingegaan op de werking van het Tor-netwerk, dat veruit het meest populaire netwerk is. Deze netwerken zijn ontworpen om de gebruikers daarvan een hoge mate van anonimiteit te verschaffen.

Wat is Tor?
Tor is een afkorting en staat voor The Union Router.[128] Het is een netwerk dat slechts te benaderen is via de Tor-browser[129], een flink aangepaste versie van de browser Mozilla Firefox. De websites die enkel via de Tor-browser te benaderen zijn hanteren als domeinnaam het domein ".onion" en worden ook wel *hidden services* genoemd. De links naar deze websites worden gevormd door een voor de mens niet te onthouden reeks cijfers en letters, zoals bijvoorbeeld https://3g2upl4pq6kufc4m.onion/ dat verwijst naar zoekmachine DuckDuckGo. Overigens is het daarnaast ook mogelijk websites op het clear web te benaderen.

---

[125] Zie o.m. RB Oost-Brabant 7-9-2017, ECLI:NL:RBOBR:2017:4706 (bewezenverklaard dat verdachte 134 afbeeldingen heeft *verspreid*, door deze in het kader van het P2P-programma beschikbaar te stellen aan anderen); RB Overijssel 18-3-2014, ECLI:NL:RBOVE:2014:1339 (verspreiding, omdat verdachte zijn computer "open zette" in de wetenschap dat ook anderen dan de daarop aanwezige kinderporno konden binnenhalen); RB Gelderland 27-8-2013, ECLI:NL:RBGEL:2013:2580; RB Arnhem 5-3-2013, ECLI:NL:RBONE:2013:BZ3290; RB Middelburg 04-02-2013, ECLI:NL:RBZWB:2013:BZ5657;
RB Zutphen 6-9-2011, ECLI:NL:RBZUT:2011:BR6814; RB Dordrecht 10-8-2010, ECLI:NL:RBDOR:2010:BN3858; enz.

[126] Zie RB Gelderland 10-3-2014, ECLI:NL:RBGEL:2014:1541 (vrijspraak *verspreiden* via clouddienst SkyDrive, en via P2P-programma Shareaza, wel *aanbieden* van kinderporno via P2P-programma Shareaza); RB Gelderland 1-5-2015, ECLI:NL:RBGEL:2015:2897 (*aanbieden* van kinderporno via (P2P-programma) Gigatribe).

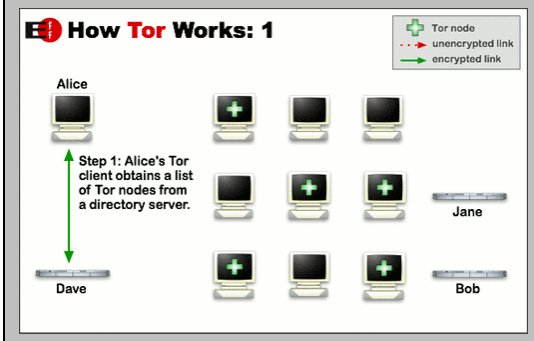
[127] Zie nader Georganiseerde kinderpornonetwerken op het darkweb, M. van der Bruggen, Justitiële verkenningen 2018/5.4.

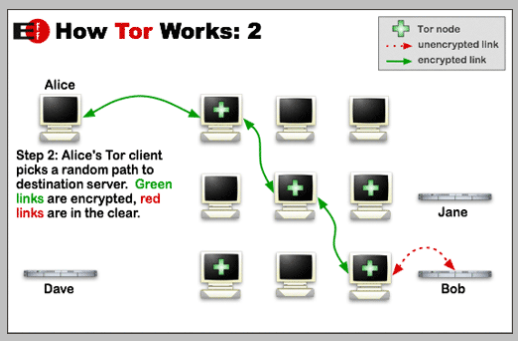
[128] In het onderstaande wordt geput uit informatie afkomstig uit de documentatie van het Tor Project, te bereiken via https://2019.www.torproject.org/docs/documentation.html.en.

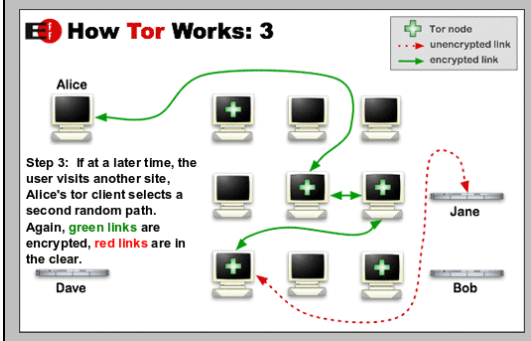
[129] Te downloaden via de website van het Tor Project.

Hoe werkt Tor?
Bij het gebruik van de normale internetbrowser worden na het geven van de opdracht naar een website te navigeren achter de schermen pakketjes met gegevens uitgewisseld tussen de server waarop de website staat en het device van de gebruiker. Die pakketjes volgen een directe route tussen de server en de gebruiker. Dat maakt dat de server identificerende informatie kan ontvangen van de gebruiker, zoals zijn IP-adres en gegevens over het gebruikte device.

De bedoeling van Tor is om bij het benaderen van een website (een *hidden service* of reguliere website) een route te kiezen die door de bevraagde website onmogelijk te reconstrueren is. Dat zorgt voor een hoge mate van anonimiteit. In onderstaande afbeeldingen wordt de werkwijze van Tor uiteengezet aan de hand van een voorbeeld: Alice wil een website bezoeken. De computer van Alice volgt bij het benaderen van die website geen directe route, maar een route over zogenaamde 'Tor Nodes' (servers die deel uitmaken van het Tor netwerk). Elke Tor-Node ziet alleen de gegevens van de verbinding met de voorgaande tor-node en niet de gegevens van de verbindingen van de volgende Tor-Nodes in het netwerk.. De verbindingen zijn telkens versleuteld, totdat het verzoek de laatste node verlaat op weg naar de server van de website.







De verwijzing naar de ui is niet toevallig. De gegevens die heen en weer worden gestuurd om de gegevens van de website op het scherm van Alice te kunnen tonen kunnen samen gezien worden als een ui. De ui wordt door elke node schil voor schil afgepeld. Elke node kan – door de gebruikte versleuteling – alleen de buitenste schil van de ui afpellen. Vervolgens kan de node zien waar de rest van de ui vervolgens naar toe moet worden gestuurd. De server van de website die wordt bezocht ziet daarmee enkel het IP-adres van de laatste node en kan het IP-adres van Alice niet zien.

Verspreiding van kinderpornografisch materiaal op het darkweb
De uitwisseling van kinderpornografisch materiaal op het dark web vindt met name plaats via fora die zijn ingericht op een gelijke wijze als op het clear web. Toegang wordt verkregen door aanmelding met een *nickname* en wachtwoord. Er wordt met elkaar gecommuniceerd binnen *threads* waarin de gebruikers berichten kunnen plaatsen. De kinderpornografische afbeeldingen worden veelal via links naar *file hosters* aangeboden aan andere gebruikers op het betreffende forum. Gebruikers verkrijgen op sommige fora al naar gelang hun inbreng een hogere status, bijvoorbeeld als zij nieuw materiaal delen. Bij een hogere status kan soms een gesloten deel van het forum worden ontsloten, waar meer specifiek of ander materiaal verkregen kan worden.[130] Opgemerkt moet worden dat in vergelijking met de p2p-netwerken die hiervoor zijn beschreven deze vorm van uitwisseling van kinderpornografisch materiaal op een veel anoniemere wijze plaatsvindt. Daarnaast zijn gebruikers in staat om intensiever met elkaar te communiceren.

Het in de vorige paragraaf omschreven vraagstuk welke in de delictsomschrijving van art. 240b Sr opgenomen begrippen ("verspreiding", "aanbieden" of "openlijk tentoonstellen") van toepassing zijn, speelt ook ten aanzien van het darkweb. Daar waar op een forum op het darkweb een hyperlink wordt geplaatst naar het elders te downloaden materiaal kan deze gedraging op zichzelf beoordeeld worden als de "verspreiding" van kinderpornografisch

[130] Zie nader Georganiseerde kinderpornonetwerken op het darkweb, M. van der Bruggen, Justitiële verkenningen 2018/5.4.

materiaal. Er valt echter – gelet op bovenstaande argumenten – meer voor te zeggen deze gedraging te brengen onder "aanbieden", nu de daadwerkelijke verplaatsing naar de ontvanger plaatsvindt op de externe site. Een keuze voor allebei is ook voorstelbaar.[131]

In die gevallen waarin een verdachte wordt vervolgd voor (onder meer) de verspreiding van kinderpornografisch materiaal door hyperlinks op een forum op het darkweb te plaatsen, zal de tenlastelegging een omschrijving van een of meer van die kinderpornografische afbeeldingen moeten inhouden. Het is van groot belang dat het dossier dan ook een afdoende omschrijving bevat van de inhoud van de betreffende afbeeldingen, waardoor het voor verbalisanten tijdens het onderzoek nodig zal zijn om enkele afbeeldingen via die links naar de externe sites te downloaden.

Ook andere feitelijke handelingen op het darkweb dan het plaatsen van hyperlinks naar een externe site kunnen worden gebracht worden onder "verspreiding", te denken valt aan het fungeren als moderator op een kinderpornografisch forum op het darkweb[132] of het hosten van een dergelijk platform.[133] In die gevallen kan sprake zijn van het medeplegen van "verspreiding' van kinderpornografisch materiaal.

3.4.1.3 "Verspreiden" via chatgroepen (WhatsApp/Telegram)

Kinderpornografische afbeeldingen wordt niet zelden gedeeld via chatapplicaties, bijvoorbeeld in WhatsApp- of Telegramgroepen.[134] De Europese Commissie heeft in mei 2022 een voorstel[135] gedaan om communicatiediensten[136], waaronder chatdiensten, te verplichten om de inhoud van berichten en foto's die door gebruikers worden gedeeld te scannen op gevallen van seksueel misbruik van kinderen. Het op geautomatiseerde wijze controleren van de inhoud van op het apparaat van de gebruiker aanwezige chatberichten

---

[131] Zie bijvoorbeeld RB Rotterdam 27-1-2020, ECLI:NL:RBROT:2020:501, waarbij zowel "verspreiden" als "aanbieden" bewezen zijn verklaard ten aanzien van een verdachte die beheerstaken uitvoerde op een dark web chatsite *"en zodoende mede kinderporno heeft verspreid en aangeboden"*.

[132] Zie o.m. Hof Den Haag, 9-2-2021, ECLI:NL:GHDHA:2021:193 (verdachte is gedurende een periode van vijf jaren actief geweest als moderator en gedurende zekere tijd ook als administrator van drie elkaar opvolgende chatsites/websites waarop kinderpornografisch materiaal werd gedeeld). RB Rotterdam 14-7-2020, ECLI:NL:RBROT:2020:7646 (verdachte heeft gedurende ruim 1,5 jaar twee chatsites gehost, beveiligingsscripts geschreven en voor de toegankelijkheid van de chatrooms gezorgd. Tevens was verdachte moderator van beide chatsites).

[133] RB Overijssel 3-3-2020, ECLI:NL:RBOVE:2020:913. Veroordeling wegens onder meer verspreiding van kinderpornografisch materiaal via drie verschillende chatrooms op het darkweb (feit 1). De verdachte was hoofdadministrator van twee van de drie chatrooms. Van de derde chatroom was hij oprichter en administrator. Hoewel uit het dossier niet volgt dat de verdachte zelf kinderpornografisch materiaal heeft gedeeld via de chatrooms wordt hij wel veroordeeld voor de verspreiding daarvan nu kan worden vastgesteld dat hij opzet had op de verspreiding van kinderpornografisch materiaal via de chatrooms. Uit het vonnis is overigens niet op te maken of is vastgesteld dat het kinderpornografisch materiaal opgenomen in de tenlastelegging daadwerkelijk is verspreid via de chatrooms. De rechtbank lijkt genoegen te hebben genomen met de vaststelling dat kinderpornografisch materiaal is gedeeld via de chatrooms. Vgl. met het hiervoor genoemde vonnis RB Rotterdam 27-1-2020, ECLI:NL:RBROT:2020:501, waarover dezelfde opmerking kan worden gemaakt.

[134] Vgl. bijv. 'Kinderporno veel gedeeld op WhatsApp' | Tech | AD.nl (20/12/2018). Zie o.m.: RB Midden-Nederland, 24-3-2020, ECLI:NL:RBMNE:2020:1098 (o.a. bewezenverklaard: *"(...) heeft verspreid door het verzenden via WhatsApp-gesprekken het delen in chat-groepen (...)"*);

[135] Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, COM(2022) 209, (11 mei 2022).

[136] In art 1, par. 1 sub a-e, van het voorstel worden 4 categorieën normadressaten onderscheiden: "providers of relevant information society services", "providers of hosting services", "providers of interpersonal communication services" en "providers of internet access services". Onduidelijk is met name welke rechtspersonen/entiteiten onder de eerstgenoemde categorie vallen.

(‘*client-side device scanning’*) is door onder meer Bits of Freedom uitvoerig bekritiseerd.[137] Nu niet elke vorm van delen kan worden aangemerkt als “verspreiden”, kan men de vraag stellen in hoeverre en zo ja, onder welke voorwaarden het delen van kinderpornografisch materiaal via chatgroepen als “verspreiden” in art. 240b Sr kan worden aangemerkt.

Vooropgesteld moet worden dat voor een bewezenverklaring van “verspreiden” op het moment van het delen sprake moet zijn van een vergroting van de kring van personen die kennis konden nemen van de afbeeldingen.[138] De beoordeling of sprake is van “verspreiden” lijkt in principe niet problematisch, wanneer kan worden vastgesteld dat door de verdachte kinderpornografische afbeeldingen zijn gedeeld in een groepschat waaraan op het moment van delen tenminste één andere gebruiker (de groepsbeheerder) deelnam. Ook het via de groepschat terugsturen van daarin (ongewenst) ontvangen kinderpornografische afbeeldingen naar de afzender zal onder omstandigheden als “verspreiding” kunnen worden aangemerkt, nu niet slechts de afzender maar ook andere groepsdeelnemers daarvan kennis kunnen nemen.[139] Problematisch is evenwel dat het dossier veelal niet of nauwelijks informatie bevat op basis waarvan kan worden beoordeeld of op het moment van het ‘terugsturen’ van de afbeeldingen in een groepschat sprake is van een vergroting van de kring van personen die kennis konden nemen van de afbeeldingen. Daarvoor kunnen onder meer relevant zijn: de activiteiten in de betreffende groepschat (in het bijzonder het tijdsverloop tussen de momenten waarop de afbeeldingen in de groepschat werden gedeeld, en de vraag of op het moment van delen sprake was van (nieuwe) groepsdeelnemers)), de handelingen die de verdachte met de betreffende chatapplicatie heeft verricht, en (voor zover relevant) de applicatieversie en de instellingen van de betreffende chatapplicatie op het apparaat van de gebruiker.[140] In de praktijk zijn dergelijke aspecten (vooralsnog) met name relevant in relatie tot de chatapplicaties WhatsApp en Telegram Messenger.[141]

---

[137] Zie: Jouw berichtjes zijn alleen voor jou en je gesprekspartner – en niemand anders - Bits of Freedom (9/5/2022). Vgl. ook: Diensten als WhatsApp en Gmail moeten van de EU actief jagen op kinderporno, privacy-experts vrezen gevolgen (volkskrant.nl) (11/5/2022) en Online privéberichten scannen? - Achtergrond - Tweakers (1/6/2022).

[138] Vgl. in die zin ook: Noyon/Langemeijer/Remmelink, “Wetboek van Strafrecht”, art. 240b Sr, aant. 5. “De delictshandelingen” (commentaar prof. mr. A.J. Machielse, bijgewerkt t/m 15-8-2018), over “verspreiden”: “*Toch is voorstelbaar dat het overhandigen van één exemplaar als verspreiden zal kunnen worden beschouwd, wanneer het de bedoeling van het uit handen geven is dat bijvoorbeeld de gegevensdrager wordt vermenigvuldigd. Voorts dringt zich de vraag op of de bescherming van de jeugdige niet ook gediend is als een uniek exemplaar door ‘liefhebbers’ onderling wordt doorgegeven*.”

[139] Zie anders: Gerecht van Eerste Aanleg in Aruba, 3-3-2022, ECLI:NL:OGEAA:2022:88: “*Ervan uitgaande dat de verdachte videoafbeelding(en) als voorbeeld van ongewenste berichten heeft ‘teruggestuurd’ naar de leden van de groepschat, kan niet gezegd worden dat hij deze opzettelijk (verder) heeft verspreid.*” De tenlastelegging bood onzes inziens evenwel ruimte om het terugsturen van de kinderpornografische afbeeldingen als “verspreiding” aan te merken. Wel kan de vraag worden gesteld of door het terugsturen sprake is van een vergroting van de kring van personen die kennis konden nemen van de afbeeldingen.

[140] Dat lijkt niet het geval te zijn geweest in o.m.: Hof Arnhem-Leeuwarden, 22-7-2021, ECLI:NL:GHARL:2021:7281 (“*Anders dan de rechtbank acht hof onvoldoende aanknopingspunten in het dossier aanwezig om te komen tot een bewezenverklaring van (…) verspreiden (…). Het dossier biedt voor een andersluidende conclusie onvoldoende concrete en ondubbelzinnige aanknopingspunten*.”; en Hof Den Haag, 28-1-2021, ECLI:NL:GHDHA:2021:254 (wel bewezen: verspreiden door het plaatsen van kinderpornografische afbeeldingen op de internetsite ‘Chatgirl’, maar niet: verspreiden door het verzenden van WhatsApp-berichten).Vgl. ook: RB Midden-Nederland, 25-4-2022, ECLI:NL:RBMNE:2022:1578 (“*Het file path van de foto’s 1, 36 en 37 lijkt er voorts op te wijzen dat de foto’s via WhatsApp zijn ontvangen. Het file path van foto 38 lijkt er op te wijzen dat deze is ontvangen via Telegram*”). De Rb. kan hieraan geen duidelijke conclusie(s) verbinden.

[141] Dergelijke aspecten kunnen ook relevant zijn voor de beoordeling of in een chatgroep gedane uitlatingen in het openbaar zijn gedaan, bijvoorbeeld in de context van opruiing (art. 131 Sr).

WhatsApp

Voor WhatsApp geldt dat de beheerder van een WhatsApp-groep een uitnodigingslink kan genereren die gedeeld kan worden met andere WhatsApp-gebruikers.[142] Let wel: een uitnodigingslink kan door de ontvanger zonder medeweten van de groepsbeheerder worden doorgestuurd aan derden. Anders dan bij Telegram bestaat niet de mogelijkheid om het delen van uitnodigingslinks voor te behouden aan de groepsbeheerder. Het toevoegen of verwijderen van groepsdeelnemers is voorbehouden aan de groepsbeheerder.[143] Nadat op de uitnodigingslink is geklikt wordt de betreffende WhatsApp-gebruiker lid van de WhatsApp-groep, en is het in principe mogelijk om bestanden, zoals afbeeldingen, te delen. Aan een WhatsApp-groepschat kunnen maximaal 256 gebruikers deelnemen.[144] Het archiveren van een WhatsApp-groep door de beheerder laat onverlet dat daarin nog steeds bestanden kunnen worden gedeeld, maar deelnemers van de groepschat ontvangen daarvan geen notificaties meer (tenzij in het bericht rechtstreeks naar een of meer groepsdeelnemers wordt verwezen, of wordt geantwoord op een bericht van een andere groepsdeelnemer).[145]

Telegram

Voor Telegram geldt dat onderscheid moet worden gemaakt tussen Telegram-kanalen en Telegram-groepen. Telegram-kanalen zijn bedoeld om informatie te delen met abonnees ('subscribers'). Het aantal abonnees van een Telegram-kanaal is ongelimiteerd.[146]
In relatie tot Telegram-groepen kan onderscheid worden gemaakt tussen privé-groepen en openbare groepen.[147] Voor openbare groepen geldt, evenals voor WhatsApp-groepen, dat gebruikers ontvangen uitnodigingslinks zonder medeweten van de groepsbeheerder kunnen doorsturen aan derden.[148] Voor privé-groepen geldt dat alleen de beheerder van de groep uitnodigingslinks kan verzenden. Anders dan voor WhatsApp-groepen en voor openbare Telegram-groepen geldt dat de ontvanger van een door de maker of beheerder van de Telegram-groep gedeelde uitnodigingslink, die link niet kan doorsturen aan derden.[149]
Door te klikken op een uitnodigingslink wordt de betreffende Telegram-gebruiker lid van de Telegram-groep, en is het in principe mogelijk om bestanden, zoals afbeeldingen, te delen. Aan een Telegram-groepschat kunnen maximaal 200 gebruikers deelnemen.[150]
Het archiveren van een Telegram-groepschat heeft, evenals voor WhatsApp geldt, geen invloed op de mogelijkheid voor groepsdeelnemers om bestanden te delen. Anders dan voor WhatsApp geldt, kan de beheerder van een Telegram-groep de zichtbaarheid van de chatgeschiedenis voor nieuwe groepsleden beperken.[151]

---

[142] Een groep aanmaken en deelnemers uitnodigen | FAQ WhatsApp.
[143] Groepsdeelnemers toevoegen en verwijderen | FAQ WhatsApp.
[144] Een groep aanmaken en deelnemers uitnodigen | FAQ WhatsApp.
[145] Een chat of groep archiveren of dearchiveren | FAQ WhatsApp.
[146] What is the difference between groups and channels - FAQ Telegram.
[147] Zie bijv. Private Telegram Groups vs Public Telegram Groups | Respond.io. Zgn. Telegram-supergroepen blijven hier buiten beschouwing; zie nader: Admins, Supergroups and More (telegram.org).
[148] Een groep aanmaken en deelnemers uitnodigen | FAQ WhatsApp: "*Let op: (...) Iemand kan de link doorsturen naar andere mensen, die dan zonder goedkeuring van de groepsbeheerder kunnen deelnemen aan de groep.*"
[149] Private Telegram Groups vs Public Telegram Groups | Respond.io: "*In private Telegram groups, only the creator of the group or the admin can invite people to the group. (...) Only the creator or the admin has access to the t.me Telegram link.*"
[150] What is the difference between groups and channels - FAQ Telegram. Telegram-supergroepen ondersteunen max. 5000 deelnemers; zie nader: Admins, Supergroups and More (telegram.org).
[151] De beheerder van een Telegram-groep heeft de mogelijkheid om via de groepsinstellingen de optie om de chatgeschiedenis zichtbaar te maken voor nieuwe groepsleden te selecteren.

Onzes inziens geldt dat het delen van afbeeldingen in een chatgroep als "verspreiding" kan worden aangemerkt, voor zover kan worden vastgesteld dat voorafgaand aan of op het moment van delen één (of meer) nieuwe groepsdeelnemer(s) lid werden van de betreffende groepschat. Onder meer de beperkte zichtbaarheid van de chatgeschiedenis voor nieuwe leden en/of de ontoegankelijkheid van een chatgroep voor buitenstaanders, zijn redenen dat relevante informatie hierover veelal ontbreekt in het dossier.

3.4.2. "aanbiedt"

De term "aanbieden" is in art. 240b Sr opgenomen in het kader van de implementatie van het Verdrag van Lanzarote.[152] Zoals hiervoor onder 3.4.1.1. reeds is aangegeven, lijkt "aanbieden" vooral aan de orde in situaties waarin men digitale kinderpornografische afbeeldingen – al dan niet met of door gebruik van P2P-software – vanaf de eigen computer beschikbaar stelt voor downloaden of bekijken door derden.[153] Dat kan eveneens gebeuren door het beschikbaar stellen van een hyperlink dat een ander leidt naar een downloadlocatie om dergelijk materiaal te downloaden, zoals hiervoor besproken.
Naar zijn aard zal aanbieden dus veelal samenvallen met bezit, maar zal vanwege het deels andere karakter van de gedraging, "aanbieden" ook naast "bezit" als een aparte gedraging kunnen worden gekwalificeerd. "Aanbieden" wordt bovendien in de regel ook als een ernstiger strafrechtelijke gedraging aangemerkt dan (alleen) het bezit.

3.4.3. "openlijk tentoonstelt"

Van openlijk tentoonstellen kan worden gesproken als er met betrekking tot kinderpornografisch materiaal sprake is geweest van een actieve handeling gericht op het (kunnen) kennisnemen door derden van dat materiaal.[154] In concreto kan daarbij bijvoorbeeld gedacht worden aan het plaatsen van kinderpornografisch materiaal op een eigen website, een ook voor derden toegankelijk account op Facebook[155], Twitter, Instagram (etc.) of een mededeling dat bepaald materiaal kan worden gedownload vanaf aan de betrokkene toebehorende computers en/of gegevensdragers in combinatie met het daadwerkelijk daartoe "openzetten" van die computers c.q. gegevensdragers. Het louter voorhanden hebben kwalificeert derhalve niet tevens als "openlijk tentoonstellen".[156]

Het moge duidelijk zijn dat "openlijk tentoonstellen" voor een groot deel samen zal en kan vallen met aanbieden en/of verspreiden en/of in bezit hebben.[157] Waarschijnlijk wordt om die reden dit bestanddeel maar zelden zelfstandig bewezenverklaard.

De term "openlijk" impliceert overigens niet dat het materiaal ook op een openbare plaats ter beschikking moet zijn gesteld. Analoog aan de jurisprudentie met betrekking tot art. 113 Sr (verspreiding c.a. van voor de Koning beledigende afbeeldingen) lijkt aannemelijk dat "openlijk" hier ruim moet worden opgevat, in de zin dat reeds volstaat indien het materiaal

---

[152] Kamerstukken II, 2008/2009, 31810, nr. 3, p. 3.
[153] In deze zin ook Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht*, art. 240b Sr, aant. 5, onder f.
[154] Aldus Cleiren e.a. *Tekst en Commentaar Strafrecht*, 10e druk, art. 240b Sr, aant. 7.
[155] Hof Arnhem-Leeuwarden 14-6-2017, ECLI:NL:GHARL:2017:5020 Veroordeling wegens o.m. openlijk tentoonstellen van kinderporno. Uit *wraak* één foto van (ex-)vriendin op Facebook geplaatst.
[156] Vgl. RB Leeuwarden 10-11-2009, ECLI:NL:RBLEE:2009:BK2796 m.b.t. het begrip vertonen.
[157] Niettemin verdient het onzes inziens aanbeveling om telkens kritisch te bezien in hoeverre naast "openlijk tentoonstellen" andere modaliteiten, zoals "verspreiden" en "aanbieden" bewezen dienen te worden verklaard. Zie bijvoorbeeld RB Oost-Brabant 19-10-2021, ECLI:NL:RBOBR:2021:5487, waarin het plaatsen van kinderpornografische afbeeldingen op een internetsite zowel als "verspreiden" als als "openlijk tentoonstellen" (en "aanbieden") is bewezenverklaard, hoewel (voor wat betreft de hiervoor beschreven handeling) volstaan had kunnen worden met bewezenverklaring van "openlijk tentoonstellen".

voor derden zichtbaar was.[158] Of derden het materiaal ook daadwerkelijk hebben gezien is in dit kader hoogstwaarschijnlijk irrelevant.

3.4.4. "vervaardigt"

Onder het vervaardigen van kinderporno wordt verstaan het maken van kinderpornografische afbeeldingen. In de regel zal het daarbij gaan om het maken van afbeeldingen met behulp van webcams[159], videocamera's en fotocamera's[160] (al dan niet als onderdeel van een computer of smartphone). Kinderporno kan echter – indien en voor zover het realistische afbeeldingen betreft – ook vervaardigd worden door tekenen, schilderen, het maken van collages[161] of computerbewerking van afbeeldingen.[162, 163]

Het vervaardigen behoeft niet altijd direct door de verdachte zelf te hebben plaatsgevonden.[164] In de rechtspraak wordt namelijk aangenomen dat, indien iemand een actieve rol (bijvoorbeeld als regisseur, dan wel vanwege participatie of feitelijk overwicht) heeft bij de totstandkoming van kinderpornografische afbeeldingen, maar de feitelijke opnameapparatuur daarbij wordt bediend door een ander, bewezenverklaring voor "vervaardigen" kan plaatsvinden.[165] Voor een bewezenverklaring van "vervaardigen" lijkt evenmin vereist dat de verdachte daadwerkelijk in de ruimte aanwezig was ten tijde van de opname(s), bijvoorbeeld

---

[158] Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht* verwoordt het in aant. 4 bij art. 113 Sr als volgt: "*Openlijk is: voor het aangezicht van een ieder die zien wil; dat behoeft dus niet te zijn op een openbare plaats, maar kan zijn bijv. achter een venster aan de openbare weg*." Zie m.b.t. openlijk tentoonstellen op internet ook Cleiren c.s., *Tekst en Commentaar Strafrecht*; aant. 8, onder g, bij art. 113 Sr: "*Aannemelijk is dat tentoonstellen ook op het internet kan geschieden*." Zie ook RB Gelderland 27-2-2015, ECLI:NL:RBGEL:2015:1293 Veroordeling wegens o.m. openlijk tentoonstellen van kinderpornografische filmpjes. Filmpjes werden getoond tijdens chatgesprekken.

[159] Zie bijvoorbeeld RB Roermond 22-4-2011, ECLI:NL:RBROE:2011:BQ3544 (vervaardigen van kinderporno, d.m.v. via de webcam maken van afbeeldingen en video's van minderjarige meisjes).

[160] RB Noord-Nederland 29-6-2017, ECLI:NL:RBNNE:2017:2349 (maken van kinderpornografische foto's van 3-jarige dochter; o.m. bewezenverklaard: vervaardigen); RB Noord-Holland 29-6-2017, ECLI:NL:RBNHO:2017:5546 (heimelijk opnemen van 11-jarige die seksuele handelingen met zichzelf verricht is vervaardigen kinderporno); RB Haarlem 31-8-2011, ECLI:NL:RBHAA:2011:BS1673 (maken van foto's van eigen ontucht met minderjarige is vervaardigen kinderporno).

[161] Zie o.m. HR 18-11-2014, ECLI:NL:HR:2014:3304 (cassatie verworpen tegen oordeel hof dat door de verdachte gemaakte collages bestaande uit uitsneden van diverse foto's van zeer jonge kinderen (waarbij ook de geslachtsdelen prominent in beeld komen) moeten worden aangemerkt als vervaardigen van kinderpornografisch materiaal).

[162] Zie bijv. RB Utrecht 9-11-2010, ECLI:NL:RBUTR:2010:BO3818 (op foto's van seksuele handelingen hoofden van actoren vervangen zodat het leek alsof verdachte seksuele handelingen verrichte met drie minderjarige meisjes; resultaat digitaal opgeslagen; zodanig van kwaliteit dat nauwelijks te zien is dat deze zijn gemanipuleerd; veroordeling voor vervaardigen virtuele kinderporno); In deze zin ook Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht*, art. 240b Sr, aant. 5, onder c bij art. 240b: "*Ook het manipuleren met beeldbewerkingsprogramma's, waardoor men uit wellicht een samenstel van foto's die op zichzelf ieder nog geen kinderpornografie inhouden, een nieuw geheel maakt dat wel als kinderpornografie zal hebben te gelden, is als vervaardigen aan te merken, ook al komt er in feite geen kind meer aan te pas*".

[163] Zie over de vraag of dan nog sprake is van 'betrokken of schijnbaar is betrokken' par. 3.3.2.

[164] Een opmerkelijk geval betreft RB Rotterdam 1-10-2020, ECLI:NL:RBROT:2020:8992 (vrijspraak van vervaardigen, nu het geschetste alternatieve scenario dat een andere persoon die eveneens toegang had tot de woning, camera en de computer van verdachte en die persoon een ongebruikelijke (liefdes)relatie had met het slachtoffer - gelet op alle feiten en omstandigheden van het geval - niet zonder meer als onaannemelijk kan worden verworpen).

[165] Het participeren/feitelijk overwicht van verdachte werd behoorlijk opgerekt in: RB Zeeland-West Brabant 10-12-2019, ECLI:NL:RBZWB:2019:5546. ("*Het filmpje is opgenomen met de telefoon van verdachte en is onder zijn account op [Naam 1] beschikbaar gekomen. Bovendien is het filmpje in zijn schuur opgenomen. Voorts is het filmpje kort gemaakt na het eerste filmpje in de auto en had verdachte [Slachtoffer] op dat moment onder zijn hoede. Het kan daarom niet anders dan dat verdachte betrokken was bij het vervaardigen van dat filmpje*."), Vgl. ook: Hof Den Bosch 3-8-2016, ECLI:NL:GHSHE:2016:3477; RB Den Haag 19-2-2016, ECLI:NL:RBDHA:2016:1611.

indien er via een beeld- en geluidverbinding sprake is van interactie tussen de verdachte en degene die daadwerkelijk een opname maakt.[166]

Door de rechtbank Den Haag is geoordeeld dat slechts van "vervaardiging" sprake kan zijn, indien het gaat om "nieuwe" (in de zin van *inhoudelijk/qua content* nog niet eerder bestaande) kinderpornografische afbeeldingen.[167] In deze opvatting zou bijvoorbeeld derhalve het (ongewijzigd) geheel of gedeeltelijk kopiëren van reeds bestaande kinderpornografische afbeeldingen niet als "vervaardigen" kunnen worden gekwalificeerd. In zijn algemeenheid lijkt ons deze opvatting te eng, reeds omdat het niet ondenkbaar lijkt dat het kopiëren en bijvoorbeeld vervolgens in een bepaalde samenstelling presenteren van bepaalde kinderpornografische afbeeldingen een zodanig nieuwe afbeelding of set van afbeeldingen oplevert dat deze moet(en) worden beschouwd als te zijn "vervaardigd" in de zin van art. 240b Sr. De rechtbank Rotterdam lijkt die opvatting ook te zijn toegedaan[168] waar het vervaardigen van kinderporno bewezen wordt verklaard: "*Anders dan de raadsvrouw is de rechtbank van oordeel dat het gebruik van bestaande kinderporno om daarmee nieuwe afbeeldingen te maken die seksueel van aard zijn en waarop die oude afbeeldingen ook nog steeds zichtbaar zijn, moet worden gekwalificeerd als het vervaardigen van kinderporno*." Het vonnis geeft helaas weinig inzicht in wat de verdachte feitelijk had gedaan.

Dat is anders in de interessante casus die zich voordeed in het arrest van de Hoge Raad van 22 januari 2019.[169] Het ging hier in de eerste plaats om het vervaardigen van een videobestand waarop opnamen van een computerbeeldscherm te zien waren waarop een webcamchatgesprek plaatsvond. Omdat er onvoldoende aanwijzingen voorhanden waren dat sprake was van een livesessie nam het hof als uitgangspunt dat in de webcamchatapplicatie bestaande beelden van een meisje werden afgespeeld, die vervolgens werden opgenomen met zogenaamde videocapturing-software. Daarnaast was de verdachte met een seksuele handeling en het chatgesprek in beeld. Gezamenlijk gaf dit de indruk van een rechtstreekse, expliciete, seksuele interactie van de verdachte met het meisje. Het hof was van oordeel dat dit een nieuwe afbeelding van een seksuele gedraging was, waarbij het minderjarige meisje betrokken of schijnbaar betrokken was die wezenlijk verschilde van de beelden waarop alleen het meisje te zien was, zodat sprake was van het vervaardigen van kinderporno.
Dit lag anders bij de overige in de tenlastelegging genoemde videobestanden. Ook daar ging het om schermopnamen van bestaande beelden van kinderporno, van andere kinderporno en/of van een chatgesprek dat gevoerd leek te worden met het zichtbare kind of met een andere aanbieder van kinderporno. Dat bestaande beelden[170] werden gecombineerd was voor het hof onvoldoende om te spreken van vervaardigen. In cassatie was alleen de vrijspraak ten

---

[166] RB Noord-Holland 24-12-2021, ECLI:NL:RBNHO:2021:11936 (o.a. bewezenverklaring van medeplegen van het vervaardigen van kinderpornografische afbeeldingen: *"(...) dat [verdachte] [slachtoffer 2] (en de andere vrouwen) regelmatig uitleg gaf over hoe ze de prostitutiewerkzaamheden moest verrichten, dat het niet anders kan dan dat [medeverdachte 1] [verdachte] aan de telefoon had en dat [verdachte] via de Yoosee camera meekeek en de seksfilmpjes tussen [slachtoffer 2] en de minderjarige jongens via de Yoosee app op haar telefoon heeft opgenomen*.").
[167] RB Den Haag 31-5-2017, ECLI:NL:RBDHA:2017:5839 (korte opnames met behulp van een tablet gemaakt van op een televisiescherm afgespeeld reeds bestaand kinderpornografisch materiaal. "*Hoewel er door de gedragingen van verdachte nieuwe bestanden zijn ontstaan met daarop kinderpornografisch materiaal, kan er naar het oordeel van de rechtbank niet gesproken worden van nieuw materiaal nu er enkel sprake is van het selecteren en opnemen van fragmenten van reeds bestaand materiaal. Er is dan ook geen sprake van het vervaardigen zoals bedoeld in art. 240b, eerste lid, van het Wetboek van Strafrecht*". Vrijspraak).
Zie nader voor een vergelijking 3.2.4.
[168] RB Rotterdam 26-7-2018, ECLI:NL:RBROT:2018:6130.
[169] HR 22-1-2019, ECLI:NL:HR:2019:93.
[170] Kennelijk heeft het hof vastgesteld dat ook de andere kinderporno en/of de chatgesprekken bestaande beelden betroffen. Dat blijkt echter niet expliciet uit dit arrest.

aanzien van deze overige videobestanden aan de orde. De Hoge Raad stelt vast dat het oordeel van het hof geen blijk gaf van een onjuiste uitleg van art. 240b, eerste lid, Sr.

Opmerking verdient voorts dat – zoals uit het voorgaande blijkt – wanneer (delen van) op zichzelf beschouwd onschuldige afbeeldingen worden gemanipuleerd/bewerkt tot een kinderpornografische afbeelding dit in ieder geval wel als "vervaardigen" als bedoeld in art. 240b Sr kan worden beschouwd.

Bij het vervaardigen van kinderporno zal veelal sprake zijn van samenloop met zedendelicten zoals verkrachting, ontucht met minderjarigen, "grooming", etc. Die gedragingen (waaronder verkrachting en ontucht) worden met aanzienlijk hogere strafmaxima bedreigd (zes tot twaalf jaar gevangenisstraf) dan het enkele vervaardigen van kinderporno als bedoeld in art. 240b, eerste lid, Sr (maximaal vier jaar gevangenisstraf). Als het vervaardigen van kinderporno gepaard gaat met deze overige zedendelicten zijn daarop de samenloopbepalingen van toepassing. Bij meerdaadse samenloop wordt de maximumstraf met een derde verhoogd.

3.4.5. "invoert", "doorvoert"[171] *en "uitvoert"*

In het geval van "invoert", "doorvoert" en "uitvoert" gaat het om het binnen of (weer) buiten het grondgebied van Nederland brengen van kinderpornografisch materiaal. Onder invoer, doorvoer en uitvoer van kinderpornografisch materiaal vallen in ieder geval die gedragingen waarbij sprake is van een *fysieke beweging* van dat materiaal (prints, drukwerk, maar ook gegevensdragers als dvd's en usb-sticks met daarop dergelijk materiaal) binnen of (weer) over de grenzen van Nederland.[172]
De wetgever zwijgt over de vraag in hoeverre er bij internationale uitwisseling van louter digitale kinderporno (geen fysiek object dus, maar alleen gegevens) via internet ook sprake is van invoer, doorvoer en uitvoer. In de rechtspraak is dit echter al een aantal malen aangenomen[173] en ook Noyon/Langemeijer/Remmelink lijkt dit bepaald niet uit te sluiten.[174] Vanwege de zich doorgaans voordoende samenloop met verspreiden en/of in bezit hebben, en de mogelijk extra bewijsrechtelijke complicaties die verband houden met het bewezen (kunnen) verklaren van invoeren, doorvoeren en uitvoeren, worden deze laatste bestanddelen maar zelden (zelfstandig) bewezenverklaard.

3.4.6. "verwerft"

Onder het "verwerven" van kinderporno moet worden begrepen het verkrijgen van beschikkingsmacht over de kinderpornografische afbeeldingen. De term "verwerven" is in het

---

[171] Een vermoedelijk vooral academisch interessante vraag is of sprake is van invoer etc. indien een verdachte kinderpornografisch materiaal up- en/of downloadt naar en van een cloudserver in het buitenland.
[172] Zie RB Haarlem 22-3-2011, ECLI:NL:RBHAA:2011:BQ1647 (invoeren van kinderporno, vastgelegd op twee cd-roms en een dvd).
[173] Zie o.m. RB Overijssel 19-10-2017, ECLI:NL:RBOVE:2017:3926 (verzending van kinderpornografische foto's via Bullchat aan getuige (woonachtig in België). "*Dit in combinatie met onder meer het karakter van de website Bullchat die ook in landen buiten Nederland te raadplegen is, maakt dat de rechtbank wettig en overtuigend bewezen acht dat verdachte zich tevens schuldig heeft gemaakt aan de uitvoer van kinderporno*"); RB Zutphen 7-10-2011, ECLI:NL:RBZUT:2011:BT7059 (invoeren van kinderporno d.m.v. downloaden (uit vermoedelijk Zwitserland); RB Arnhem 21-02-2011, ECLI:NL:RBARN:2011:BP5151 (invoeren kinderporno d.m.v. downloaden uit Wit-Rusland); RB Zwolle 13-10-2011, ECLI:NL:RBZLY:2011:BT7560 (invoeren van kinderporno d.m.v. downloaden van community site Dreamboard).
[174] Zie Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht*, art. 240b Sr, aantekening 5 bij art. 240b: "*Als het geoorloofd is dit bestanddeel ruim uit te leggen, biedt ook hier het internet weer onverwachte mogelijkheden. Het downloaden van kinderpornografisch materiaal uit een gedeelde map van een individuele internetter aan de andere kant van de oceaan is dan immers een strafbaar grensoverschrijdend handelen*".

kader van de implementatie van art. 20 van het Verdrag van Lanzarote in art. 240b Sr terecht gekomen. Daarbij werd geen nadere invulling gegeven aan deze uitvoeringshandeling.
De meerwaarde van de opname van "verwerven" in art. 240b Sr is beperkt, nu deze uitvoeringshandeling in de praktijk feitelijk ook al onder het bereik zal vallen van bijvoorbeeld "bezit" en "zich toegang verschaffen" van respectievelijk tot kinderpornografisch materiaal. Nochtans meende de wetgever om "systematische redenen" deze bepaling uit het Verdrag van Lanzarote toch over te moeten nemen in art. 240b Sr.

Bij verwerven gaat het concreet om handelingen als het aannemen/kopen van fysieke goederen, zoals bijvoorbeeld gegevensdragers (geheugenkaarten, USB-sticks, dvd's enz.) indien daarop kinderpornografische afbeeldingen zijn geplaatst en drukwerk.
Het lijkt in de rechtspraak echter onomstreden dat het zich laten toezenden van afbeeldingen[175] en downloaden van afbeeldingen (al dan niet tegen betaling) eveneens een wijze van "verwerven" is.[176] De verdachte moet ook feitelijk in staat zijn om de gedownloade afbeeldingen (bijvoorbeeld door middel van speciale software) te kunnen bekijken. Een aardig voorbeeld van een casus waarin het verwerven een zelfstandige rol speelde is het geval waarin een verdachte via Skype op zijn telefoon een videobestand ontving. Niet bewezen kon namelijk worden dat verdachte dit bestand (in Nederland) in zijn bezit had (gehad), nu het op het moment van onderzoek van de telefoon daarop niet meer aanwezig was maar alleen via de Dropbox-applicatie bereikbaar was.[177]

Technisch lemma: thumbnails

Wat zijn thumbnails?
In kinderpornografiezaken worden regelmatig afbeeldingen in de tenlastelegging opgenomen die een gecomprimeerde weergave (ook wel: voorvertoning of miniatuur) van een kinderpornografische afbeelding betreffen. Thumbnails zijn verkleinde weergaven (postzegelformaat) van afbeeldingen, die de gebruiker in staat stellen om kennis te nemen van de inhoud van een bronafbeelding zonder deze te openen. Een thumbnail kan tevens dienen als snelkoppeling naar een afbeelding. Deze beschrijving impliceert dat thumbnails voor zedendelinquenten in principe geen interessant verzamelobject zijn. Nu thumbnails een verkleinde weergave zijn van een afbeelding, kan men de vraag stellen of thumbnails in juridische zin wel als 'afbeeldingen' als bedoeld in art. 240b Sr kunnen worden aangemerkt. In de jurisprudentie is dit aspect (vooralsnog) niet geproblematiseerd.[1]

[175] Zie bijv. RB Midden-Nederland 15-6-2017, ECLI:NL:RBMNE:2017:2872 (verwerven van kinderpornografische afbeeldingen d.m.v. het zich door 15-jarige onder valse beloften laten toezenden van naaktfoto's en -filmpjes); idem: RB Gelderland 15-6-2017, ECLI:NL:RBGEL:2017:3152; *zie echter ook*: RB Gelderland 30-10-2017, ECLI:NL:RBGEL:2017:5674 (via de applicatie Snapchat kinderpornografische foto's ontvangen. Gelet op de bijzondere eigenschappen van deze applicatie heeft verdachte deze foto's *niet* in bezit gehad of *verworven,* maar zich wel met gebruikmaking van een geautomatiseerd werk en/of communicatiedienst de toegang tot de foto's verschaft). Men kan zich echter bij deze laatste uitspraak de vraag stellen of het juist is om bij "verwerven" (waarbij de strafbare gedraging betreft het verkrijgen van beschikkingsmacht over kinderpornografische afbeeldingen) dezelfde eisen voor wat betreft de tijd van de beschikbaarheid te stellen als bijvoorbeeld bij "in bezit hebben" (waar de strafbare gedraging veeleer in de sfeer van het kunnen uitoefenen van beschikkingsmacht over kinderpornografische afbeeldingen).
[176] Zie o.m. RB Overijssel, 10-10-2020, ECLI:NL:RBOVE:2020:4213 (verwerven d.m.v. downloaden via Instagram). RB Rotterdam 12-4-2017, ECLI:NL:RBROT:2017:3051 (verwerven d.m.v. downloaden); RB Gelderland 27-2-2015, ECLI:NL:RBGEL:2015:1293 (verwerven d.m.v. downloaden en opslaan in digitale verzameling); RB Zwolle 13-10-2011, ECLI:NL:RBZLY:2011:BT7560 (verwerven d.m.v. downloaden).
[177] Hof Den Haag 22-1-2020, ECLI:NL:GHDHA:2020:286.

Hoe kunnen thumbnails ontstaan?
Thumbnails kunnen op verschillende manieren, zowel automatisch als door een handeling van de gebruiker, ontstaan. Van belang is om daarbij vast te stellen dat een thumbnail altijd[1] een verkleinde kopie van een andere afbeelding is. Onjuist is de opvatting dat thumbnails per definitie ontstaan na verwijdering van de oorspronkelijke afbeeldingen. Wel kunnen thumbnails na verwijdering van de oorspronkelijke afbeeldingen achterblijven op een gegevensdrager.[1]
Thumbnails kunnen automatisch ontstaan door bestandsindexering bij opslag van afbeeldingen in een bestandsmap. In Windows worden voorvertoningen/miniaturen van afbeeldingen standaard automatisch opgeslagen[1] in een niet direct toegankelijk databasebestand (een bestand met de naam: "thumbs.db"[1]). In dergelijke databases opgeslagen thumbnails en de metadata daarvan kunnen alleen met speciale computerprogramma's[1] worden bekeken.
Thumbnails kunnen, afhankelijk van de browserinstellingen, ook ontstaan door websitebezoek. Afbeeldingen die onderdeel zijn van een webpagina worden door de meeste browsers standaard tijdelijk opgeslagen[1] in de tijdelijke internetbestanden (ook wel: browser cache, of web cache). De bestaansreden van de browsercache is om een webpagina bij herhaald bezoek sneller te kunnen laden. In de browsercache worden de afbeeldingen niet in oorspronkelijk bestandsformaat (zoals: .jpg, .jpeg, .mov, .mpeg, etc.), maar in een niet direct toegankelijk databasebestand (ook wel: thumbcache) opgeslagen[1]. In de browser cache opgeslagen thumbnails en de metadata daarvan kunnen alleen met speciale computerprogramma's[1] worden bekeken.
Ten slotte kunnen thumbnails ook ontstaan door het gebruik van (chat)applicaties, zoals WhatsApp of Telegram. Afhankelijk van (de instellingen van) de (chat)applicatie, kunnen thumbnails lokaal (op de betreffende gegevensdrager) dan wel in de cloud worden opgeslagen. De mogelijkheden voor digitaal-forensisch onderzoek naar (eventuele) thumbnails in de lokale cache van (chat)applicaties zijn soms (zeer) beperkt, bijvoorbeeld omdat de cache (vrijwel) voortdurend automatisch wordt gewist. Digitaal-forensisch onderzoek naar (sporen van) thumbnails in (chat)applicaties is bewerkelijk, nu bruikbare onderzoeksbevindingen slechts na analyse van gegevens in verschillende databases van een (chat)applicatie kunnen worden verkregen.

Juridische aandachtspunten in relatie tot "bezit".
Nu thumbnails en andere cachebestanden zonder gebruikmaking van speciale software voor de computergebruiker niet toegankelijk zijn, is het enkele aantreffen van thumbnails in een database-bestand in beginsel onvoldoende voor de conclusie dat de gebruiker gedurende (een deel van) de tenlastegelegde periode beschikkingsmacht over de thumbnails heeft gehad en dat sprake is van "bezit".[1] Er kan evenwel sprake zijn van bijzondere omstandigheden waaruit kan worden afgeleid dat de gebruiker gedurende (een deel van) de tenlastegelegde periode beschikkingsmacht over de thumbnails heeft uitgeoefend, zoals:
-het aantreffen van sporen van naar kinderpornografisch materiaal verwijzende hyperlinks/URL's in de tijdelijke internetgegevens;
-de aanwezigheid van computerprogramma's waarmee thumbnail-databasebestanden kunnen worden bekeken in combinatie met andere aanwijzingen dat de thumbnails door de gebruiker zijn benaderd en;
-het aantreffen van sporen waaruit blijkt dat de gebruiker herhaaldelijk thumbnails met kinderpornografische inhoud uit de (browser)cache heeft verwijderd.
Bovendien kan het aantreffen van thumbnails, bijvoorbeeld als kan worden vastgesteld dat deze zijn ontstaan door bestandsindexering bij opslag van bestanden, een aanwijzing zijn dat de gebruiker van het apparaat die bestanden op een bepaald moment heeft opgeslagen, hetgeen weer een aanwijzing kan zijn voor bijvoorbeeld het bezit van die afbeeldingen op dat moment. Bij een dergelijke bewijsconstructie dient iedere stap vanzelfsprekend goed te worden uitgelegd en een solide basis in het strafdossier te hebben.

3.4.7. "in bezit heeft"

In nagenoeg alle zaken waarin art. 240b Sr ten laste is gelegd is (tevens) het "in bezit hebben" van kinderpornografisch materiaal ten laste gelegd. Tot 1 januari 2002 sprak art. 240b Sr nog van "in voorraad hebben". De Hoge Raad oordeelde dat het bezit van één afbeelding – ook al is deze voor eigen gebruik – al kwalificeerde als "in voorraad hebben".[178] Het leidt geen twijfel dat zulks ook thans ten aanzien van "in bezit hebben" heeft te gelden.[179]

In de rechtspraak (b)lijken geen al te hoge eisen te worden gesteld aan *hoelang* een persoon over een afbeelding moet hebben beschikt alvorens gesproken kan worden van "in bezit hebben". Weliswaar wordt wel verlangd dat op enige wijze blijkt dat de afbeeldingen in ieder geval gedurende een zekere periode beschikbaar moeten zijn geweest.[180] Het op de dag van inbeslagneming van de gegevensdrager aanwezig zijn van afbeeldingen, kan al voldoende zijn voor bezit.[181] Zo is bijvoorbeeld het (zeer) kortstondig op een telefoon via Snapchat zichtbaar zijn van een afbeelding wel als bezit aangemerkt[182], en is ook uit het gedurende een periode van in ieder geval enkele uren verspreiden en uploaden van afbeeldingen afgeleid dat die afbeeldingen dus ook in bezit van betrokkene waren.[183] Hoewel in het overgrote deel van de art. 240b-zaken daadwerkelijk kinderpornografische afbeeldingen zijn aangetroffen op een *device* van een verdachte, is ook wel aangenomen dat dit niet een conditio sine qua non is voor het bewezen kunnen verklaren van "in bezit hebben". Dan zal echter de aanwezigheid en het karakter van de betreffende afbeeldingen wel uit andere bewijsmiddelen moeten blijken.[184]

---

[178] HR 21-4-1998, ECLI:NL:1998:ZD1030 (n.g.); *NJ* 1998/782 m. nt. 't Hart; HR 23-6-1959, *NJ* 1960/72.
[179] Zie in dit licht o.m. ook de conclusie van AG Jorg bij HR 6-4-2010, ECLI:NL:HR:2010:BL8772, par 13-16.
[180] Zie o.m. RB Amsterdam 26-1-2017, ECLI:NL:RBAMS:2017:537 ("*Nu de bestanden verwijderd zijn, kan worden aangenomen dat deze bestanden op enig moment wel te openen en voor verdachte zichtbaar zijn geweest. Voor bewezenverklaring van het in het bezit hebben van de bestanden is echter vereist dat verdachte de beelden gedurende een zekere periode beschikbaar voor zich heeft gehouden. Het dossier biedt geen duidelijkheid met betrekking tot de vraag hoeveel tijd er heeft gezeten tussen de binnenkomst van het betreffende bestand en het verwijderen daarvan. Het kan daarom niet worden uitgesloten dat verdachte de bestanden onmiddellijk na binnenkomst als ongewenst heeft verwijderd.*"; vrijspraak).
[181] Zie o.m. RB Midden-Nederland, 9 december 2021, ECLI:NL:RBMNE:2021:5984 ("*Naar het oordeel van de rechtbank kan (...) slechts bewezen worden dat hij deze foto's op één dag in zijn bezit heeft gehad, te weten (...), de dag dat de usb-stick in beslag genomen is*.").
[182] Zie o.m. RB Noord-Nederland, 23-2-2023, ECLI:NL:RBNNE:2023:611 (bezitten, verwerven en zich de toegang verschaffen tot 4 kinderpornografische video's (snaps) die via Snapchat werden ontvangen en met de app Du Recorder zijn vastgelegd. Uit het vonnis wordt overigens niet duidelijk of de vastgelegde snaps voor verdachte toegankelijk waren). RB Amsterdam 23-4-2021, ECLI:NL:RBAMS:2021:2011 (hoewel dossier geen duidelijkheid biedt over hoe lang de bestanden op de telefoon van verdachte stonden, is de Rb. van oordeel dat uit het geheel aan bewijs in onderlinge samenhang bezien wel degelijk volgt dat verdachte de bestanden gedurende een periode beschikbaar moet hebben gehad). RB Midden-Nederland 30-8-2016, ECLI:NL:RBMNE:2016:4869 (kortstondig op telefoon hebben a.g.v. toezending met Snapchat is *bezit* in de zin van art. 240b Sr). *Anders echter:* RB Gelderland 30-10-2017, ECLI:NL:RBGEL:2017:5674 (via de applicatie Snapchat kinderpornografische foto's ontvangen. Gelet op de bijzondere eigenschappen van deze applicatie heeft verdachte deze foto's niet in bezit gehad of verworven, maar zich wel met gebruikmaking van een geautomatiseerd werk en/of communicatiedienst de toegang tot de foto's verschaft).
[183] RB Den Haag 19-2-2016, ECLI:NL:RBDHA:2016:1611.
[184] Zie bijv. RB Midden-Nederland 25-10-2017, ECLI:NL:RBMNE:2017:5362 (seksueel getint contact via Wordfeud en later via Whatsapp. Veroordeling voor bezit kinderporno, ondanks het feit dat er geen kinderpornografisch materiaal onder verdachte is aangetroffen. Op grond van de verklaring van het slachtoffer, de verklaring van verdachte ter zitting en de inhoud van het telefoongesprek dat verdachte voerde met de politie en een sms-bericht dat verdachte verstuurde aan het slachtoffer, heeft verdachte deze afbeeldingen en films naar oordeel van de rechtbank in zijn bezit gehad); RB Midden-Nederland 2-8-2017, ECLI:NL:RBMNE:2017:4010 (in chatcontact op Bullchat 20 tot 30 kinderpornografische foto's ontvangen, welke 2 maanden zijn bewaard. De rechtbank veroordeelt verdachte voor het bezit van deze foto's op basis van zijn eigen verklaring bij politie en ter zitting en de inhoud van een aantal chats, ook al zijn op de bewuste gegevensdragers van verdachte deze afbeeldingen niet meer aangetroffen).

AG Knigge stelde in zijn conclusie bij het arrest van de Hoge Raad van 28 februari 2006[185], dat bezit uit drie elementen dient te bestaan: vastlegging, opslag en beschikkingsmacht. Deze driedeling is daarna in rechtspraak en literatuur breed overgenomen.
De begrippen vastleggen (in de zin van: op een gegevensdrager *plaatsen*) en opslag (in de zin van: de (bestanden op de) gegevensdrager *bewaren*) spreken voor zich en behoeven hier dan ook geen nadere toelichting.

De duiding van het begrip "beschikkingsmacht" vereist zeker in de relatie tot kinderpornografische afbeeldingen meer toelichting. Die beschikkingsmacht vertaalt zich *in digitalis* in het *kunnen uitvoeren* van allerlei handelingen, zoals openen (hier in de zin van: het zichtbaar maken), verzenden, uploaden, kopiëren, vernietigen etc., met betrekking tot een op een gegevensdrager vastgelegd bestand dat een kinderpornografische afbeelding bevat, dan wel met betrekking tot die gegevensdrager zelf. Aangenomen moet worden dat het enkele (online) op afstand kunnen bekijken van de kinderpornografische inhoud van een bestand, terwijl men verder niet over dat bestand kan beschikken, niet heeft te gelden als bezit.[186] Dit laatste zal echter sinds 1 januari 2010 nagenoeg altijd wel vallen onder het eveneens in art. 240b Sr voorkomende bestanddeel "zich toegang verschaffen door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst".[187]

Discussie kan erover bestaan in hoeverre het opslaan van digitale afbeeldingen elders dan op de "eigen" computer of andere gegevensdragers van de gebruiker zelf in deze ook als "in bezit hebben" kan gelden. Hierbij kan gedacht worden aan fenomenen als opslag in de *cloud*[188], gebruikmaking van bijvoorbeeld *FTP-servers*[189], *hosting sites*[190], *social media accounts*[191] en *web-based e-mail accounts*.[192] Ons uitgangspunt is dat, indien het onderzoek uitwijst dat de

---

[185] Conclusie AG Knigge (onder pt. 15), ECLI:NL:PHR:2006:AU9104 bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104.
[186] Kamerstukken II, 2001/2002, 27745, nr. 14, p. 16 en nr. 15, p. 2; in deze zin ook Noyon/Langemeijer/Remmelink, *Wetboek van Strafrecht*, art. 240b Sr, aantekening 5 onder e bij art. 240b en Cleiren, *Tekst en Commentaar Strafrecht*, art. 240b, aantekening 7.
[187] Zie hierna onder 3.5.
[188] Cloud is hier te lezen als een (gewoonlijk via internet benaderbare) externe opslaglocatie, welke normaliter wordt beheerd door een andere partij dan de eigenaar van de gegevens. In HR 12-5-2020, ECLI:NL:HR:2020:799 heeft de Hoge Raad benadrukt dat onderscheid moet worden gemaakt tussen de digitale opslagruimte en de digitale gegevensdrager waarop de digitale opslagruimte zich bevindt. Dit onderscheid wordt soms nog miskend; vgl. RB Noord-Holland, 29 november 2022, ECLI:NL:RBNHO:2022:10515 (bewezenverklaring feit 2: *"(...) gegevensdragers (te weten(...) en digitale opslagruimte van OneDrive*)."
[189] FTP = *File Transfer Protocol*. FTP is een protocol dat op het internet wordt gebruikt voor het verspreiden en uitwisselen van bestanden. De meeste internetgebruikers hebben op hun device ook standaard een programma geïnstalleerd gekregen dat verbinding kan maken met servers die dit protocol gebruiken (de zogenaamde *FTP-servers*). Deze programma's worden bijvoorbeeld gebruikt bij het uploaden van bestanden naar een website. Met behulp van een FTP-programma kunnen bestanden die op een FTP-server zijn geplaatst worden gelezen of daarop vanaf een device worden geplaatst en/of aangepast.
[190] Een *hosting site* is de ruimte op een via het internet toegankelijke server waarop men een website kan plaatsen die dan vervolgens (normaliter tegen een vergoeding) technisch beheerd wordt door de bedrijf of persoon (de "*host*", of "*hosting provider*") die de betreffende serverruimte heeft aangeboden.
[191] Vele sociale media-app's bevatten namelijk ook de mogelijkheid om afbeeldingen te uploaden naar de – al dan niet openbare - "eigen" account, die zich dan echter bevindt in de digitale omgeving (lees: een server) van de communicatiedienstaanbieder; zie in dit verband bijv. ook Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (Bewezenverklaring bezit van thumbnailafbeelding, die door verdachte op zijn niet openbare Twitter account is geüpload, een handeling die enkel kan worden verricht als verdachte *beschikkingsmacht* heeft over de afbeelding en zich van de aanwezigheid op de computer bewust is).
[192] *Web-based e-mail* (ook wel "*webmail*" genoemd) is een e-mailfaciliteit in de vorm van een emailprogramma dat draait op een *web server* (en dus niet zoals bijvoorbeeld bij gebruik van Outlook uit het MS Officepakket op de eigen computer van de gebruiker). De e-mails zelf staan dan ook op deze webserver en niet op de computer

betreffende bestanden ook op die locaties door de verdachte zelf zichtbaar (te maken) zijn en/of door hem kunnen worden verwijderd, aan het vereiste van beschikkingsmacht is voldaan en dat dan sprake is van "in bezit hebben".[193] Er bestaat wat de elementen die bepalend zijn voor het bezit van gegevens immers geen wezenlijk verschil tussen deze vormen van gegevensopslag en de opslag op gegevensdragers waar verdachte zelf de fysieke beschikkingsmacht over heeft. Wel dient men zich te realiseren dat in het geval van gegevensopslag in – kort gezegd – de cloud onduidelijk kan blijven waar ter wereld de afbeeldingen feitelijk zijn opgeslagen.[194]

Digitale kinderpornografische afbeeldingen worden weliswaar in toenemende mate "op afstand" opgeslagen op externe dataopslagmedia (zoals in de cloud), maar ook nog steeds op de eigen computerharddisk van de gebruiker of op andere gegevensdragers zoals bijvoorbeeld dvd's, USB-sticks en de geheugenkaarten in smartphones en digitale fotocamera's. De digitale recherche kan dergelijke afbeeldingen met speciale software opsporen, ook nadat deze door de gebruiker zelf zijn "verwijderd". Alleen met speciale software of door vernietiging van de gegevensdragers kunnen sporen definitief worden gewist.[195] In nagenoeg alle zaken waarin het bezit van kinderporno ten laste is gelegd wordt – gegeven de uitkomsten van het verrichte forensisch digitale onderzoek – de aanwezigheid van bepaald kinderpornografisch materiaal op een gegevensdrager veelal door alle partijen als een gegeven beschouwd. De discussie spitst zich hier vooral toe op de vraag of de gegevensdrager aan de verdachte toebehoort, dan wel op de vraag in hoeverre de verdachte *opzet* had op het bezitten van voormelde afbeeldingen. Volgens vaste rechtspraak is immers het in bezit hebben van een afbeelding of gegevensdrager als bedoeld in art. 240b Sr slechts strafbaar, indien sprake is van (voorwaardelijk) opzet.[196]

In het licht van het opzetvereiste is het goed zich te realiseren dat het kan voorkomen dat kinderpornografische afbeeldingen onbedoeld met het downloaden van andere bestanden zijn binnengekomen en vastgelegd op de harde schijf van de computer van de downloader (men spreekt in dat geval van bijvangst). Ook kan een ander dan de eigenlijke gebruiker bijvoorbeeld kinderpornografische afbeeldingen op een computer hebben gedownload. Evenzo kan zich de situatie voordoen dat een gebruiker serieus gepoogd heeft kinderpornografisch materiaal te verwijderen, en meent daarin ook geslaagd te zijn, maar dat zulks toch nog aanwezig blijkt te zijn.

De jurisprudentie laat dan ook zien dat in zeer veel strafzaken niet zozeer het *feitelijke* bezit, maar de *opzet* op dat bezit wordt betwist. De relatie tussen feitelijk bezit en strafbaar bezit (waarvoor opzet is vereist) is complex, omdat zulks mede samenhangt met de technische wijze waarop de vastlegging en opslag is geschied en het antwoord op de vraag in hoeverre

---

van de gebruiker zelf. Het bekendste voorbeeld van web-based e-mail is Gmail, maar in Nederland bieden ook alle grote internetproviders (zoals Ziggo, UPC etc.) web-based e-mail aan als onderdeel van de in hun internet pakket aangeboden emaildienst. Het is wellicht goed om te weten dat informatie (zoals digitale kinderpornografie) ook uitgewisseld kan worden door deze te plaatsen in bijvoorbeeld concept-mailberichten van een web-based e-mail-account. Deze worden nimmer verzonden, maar kunnen wel met anderen gedeeld worden door die anderen de toegangsgegevens tot het betreffende mailaccount te verstrekken.

[193] Zie ook RB Rotterdam 5-4-2016, ECLI:NLRBROT:2016:2538 (De rechtbank merkt het in een e-mailaccount bewaren van e-mails waarbij kinderporno is gevoegd aan als het *in bezit hebben* van kinderporno) en Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (Bewezenverklaring bezit van thumbnailafbeelding die door verdachte naar zijn niet-openbare twitter-account is geupload).

[194] Zie nader over de technische werking van cloudopslag paragraaf 2 van "Cybercrime", J.W. van den Hurk en S.J. de Vries, *Strafblad* 2019/37.

[195] Zie verder hierover ook hierna onder 4.2.1.2., 4.2.1.5. en 4.3.2.

[196] Zie o.m. HR 28-2-2006, ECLI:NL:HR:2006:AU9104 en de hierna in hoofdstuk 4 besproken jurisprudentie.

kan worden gezegd dat de verdachte daarvan wetenschap had en/of in dat kader zelf handelingen heeft verricht.

Evenzo hangen de beschikkingsmacht en het opzetvereiste samen. Zijn kinderpornografische afbeeldingen bijvoorbeeld wel digitaal vastgelegd en opgeslagen, maar voor een normale gebruiker niet (meer) toegankelijk, dan wordt in de rechtspraak veelal geoordeeld dat de gebruiker daarover geen beschikkingsmacht (meer) had. Gaat het echter niet om een normale gebruiker, maar om een persoon met meer dan gemiddelde kennis van computers, dan zal beschikkingsmacht wellicht eerder kunnen worden aangenomen.[197] Wordt op de betreffende computer forensische software aangetroffen waarmee de "niet toegankelijke bestanden" wel weer benaderd en geopend kunnen worden, dan zal weer wel beschikkingsmacht kunnen worden aangenomen.

Gezien de veelvormigheid en complexiteit van de relatie tussen *feitelijk* bezit en het voor *strafbaar* bezit vereiste opzet wordt deze thematiek verder in hoofdstuk 4 apart besproken.

3.5. Zich toegang tot kinderpornografisch materiaal verschaffen door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst (sinds 1 januari 2010)

Technisch lemma: hoe communiceren computers via internet

De infrastructuur van internet
Het internet is feitelijk een netwerk van honderden miljoenen met elkaar verbonden *devices*. Om te communiceren via het internet moet een apparaat eerst verbinding makenmet het internet. Daarvoor heeft men de hulp nodig van een zogenoemde Internet Service Provider (ISP). In Nederland zijn dat onder meer Ziggo, UPC en KPN. Desgevraagd levert een ISP (in ieder geval aan particulieren) 'een kastje' dat wordt aangesloten op een glasvezel- of coaxkabel of een koperen telefoonlijn die geschikt is gemaakt voor het internet (DSL).

Jaren geleden leverden ISP's niet één maar twee verschillende kastjes aan particulieren die een internetaansluiting wensten, namelijk een modem en een router. Tegenwoordig echter zijn deze twee verschillende kastjes in één apparaat ondergebracht. Door velen wordt dit apparaat nu 'een router' genoemd, een aanduiding die strikt genomen niet volledig is. Om de technische achtergrond van de communicatie van computers via internet te kunnen uitleggen, is het van belang de functies van een modem en een router eerst te schetsen.

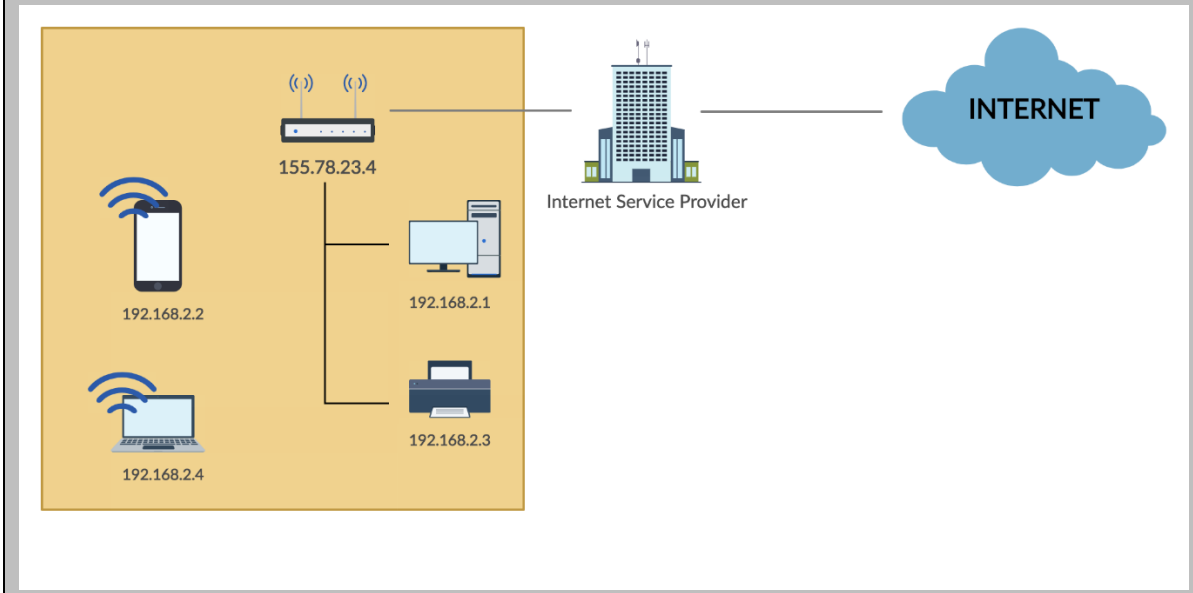
Een modem verbindt de computer thuis met de computers van de provider. Het zijn deze laatste computers die vervolgens – via de computers van andere ISP's en via internetknooppunten – verbinding maken met andere met het internet verbonden computers en andere *devices*.

Een router kan je zien als een soort verdeelkastje, dat ervoor zorgt dat niet één, maar meerdere computers, tablets of ander apparaten van het betreffende huishouden of bedrijf (via de modem) verbinding kunnen maken met het internet. Een router creëert feitelijk een netwerk in huis, een thuisnetwerk dus.

De twee functies van de router en het modem zijn zoals hierboven uitgelegd tegenwoordig ondergebracht in één 'kastje'. Dat kastje heeft nog een derde functionaliteit: het fungeert als wifi-access point. Het is met die functionaliteit mogelijk om computers en *devices* binnen het thuisnetwerk draadloos aan te sluiten op het kastje.

Hieronder ziet u een voorbeeld van een typisch thuisnetwerk, waarin een desktopcomputer en printer bekabeld zijn aangesloten op wat hierboven is aangeduid als 'het kastje'. Daarnaast zijn via een draadloze netwerkverbinding een smartphone en een laptop aangesloten. Op de numerieke aanduidingen van de apparaten wordt hieronder nader ingegaan. Het thuisnetwerk is via de ISP verbonden met het internet.

[197] Aldus ook (onder punt 16) AG Knigge in zijn conclusie (ECLI:NL:PHR:2006:AU9104) bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104.



Opmerking verdient dat alles wat hier wordt gesteld over een thuisnetwerk geldt voor ieder met het internet verbonden subnetwerk. Ook door bedrijven en instellingen gecreëerde netwerken (vaak aangeduid als 'Intranet') werken grosso modo volgens hetzelfde principe.

Hoe herkennen computers elkaar?
Bovenstaande infrastructuur vormt derhalve als het ware het internetwegennet dat nodig is om vanaf een huis of bedrijf gegevens van elders binnen te halen of naar elders weg te brengen. Maar hoe krijgt een computer deze gegevens nu op de goede plaats? Daarvoor zijn internationale afspraken, protocollen, gemaakt. Bijna alle landen en fabrikanten hebben zich ook bij deze protocollen aangesloten. Het werkt – vanzelfsprekend op hoofdlijnen – als volgt.

MAC-adres
Op het laagste niveau werkt de verbinding tussen apparaten op basis van MAC-adressen. Een MAC-adres (de afkorting MAC staat voor: "Media Access Control", ofwel hardware-adres of fysiek adres van een netwerkkaart die onderdeel is van een apparaat) is een (vrijwel)[198] uniek identificatienummer dat aan een apparaat wordt toegekend, veelal door de leverancier van de hardware die zorgt voor de verbinding.
Aan elkaar aangesloten apparaten wisselen elkaars MAC-adres uit en slaan deze op. Het MAC-adres is alleen bekend bij direct aangesloten apparaten. Zo zal uw 'kastje' ofwel wifi-router thuis de MAC-adressen kennen van uw iPad, de laptop van uw echtgeno(o)t(e) en eventueel de smartphones van uw kinderen. De registratie van een MAC-adres van een apparaat in een ander apparaat geeft dus tevens aan dat deze twee apparaten verbonden zijn (geweest). Deze laatste omstandigheid kan voor digitaal forensisch onderzoek van belang zijn, bijvoorbeeld voor de beantwoording van de vraag met welke specifieke computer (c.q. welk *device*) op een gegeven moment via een wifi-router contact is geweest met internet.

IP-adres
Extern IP-adres
Hiervoor is al aangegeven dat een MAC-adres vooral van belang is voor de gegevensuitwisseling tussen *devices* die direct met elkaar zijn verbonden. Het moge duidelijk zijn dat dit maar voor een extreem klein aantal van met het internet verbonden computers het geval is. Om die reden wordt ter aanduiding en identificatie van een internetaansluiting (en de daarop aangesloten apparaten) gebruik gemaakt van een zogenaamd IP (Internet Protocol)-adres. Het externe IP-adres wordt aan een gebruiker (c.q. een

[198] Het MAC-adres wordt meestal in hexadecimale vorm aangeduid, bijvoorbeeld 00:0C:6E:D2:11:E6. In deze door een internationale standaard (IEEE 802) bepaalde nummering (MAC48) zijn er 281.474.976.710.656 (256^6) unieke mogelijkheden. In principe dient elk apparaat een uniek MAC-adres te hebben en mogen er geen twee dezelfde zijn in een netwerk. Dit wordt bereikt door aan elke fabrikant van netwerkapparatuur een verschillend bereik van adressen toe te kennen. De fabrikanten mogen elk adres ook maar eenmaal gebruiken. De kans dat een MAC-adres behalve aan een bepaalde geïdentificeerd apparaat ook zou toebehoren aan een onbekend ander apparaat kan derhalve als bijzonder klein worden ingeschat. Aan de eerste 24 bits van een MAC-adres kan de fabrikant van de apparatuur worden afgeleid, hetgeen onder omstandigheden ook forensisch van belang kan zijn.

internetaansluiting) toegekend door de ISP.[199] Een extern IP-adres is in zoverre een uniek adres dat in een bepaalde periode slechts één internetaansluiting een bepaald IP-adres heeft. Ingevolge het thans nog zeer veel gebruikte IPv4-protocol bestaat een IP-adres uit een (decimaal) getal, dat wordt weergegeven in vier secties van maximaal drie cijfer ieder gescheiden door punten. Een IP-adres ziet er daarom ongeveer uit als "155.78.23.4", zoals gebruikt in bovenstaand voorbeeld van een thuisnetwerk.

Statische en dynamische IP-adressen
Externe IP-adressen zie we in twee varianten: *statisch* (of *vast*) of *dynamisch*. Een statisch of vast IP-adres is een IP-adres dat in principe nooit verandert en permanent wordt toegekend aan een bepaald *device*. Webservers en mailservers zijn voorbeelden van *devices* die over een vast IP-adres moeten beschikken; ze zijn en blijven dan eenvoudig bereikbaar voor de buitenwereld. Om die redenen hebben zakelijke aansluitingen dan ook vrijwel altijd een vast (extern) IP-adres.

Omdat het IPv4-protocol "maar" ongeveer 4 miljard IP-adressen mogelijk maakt, zijn er niet meer genoeg IP-adressen om aan alle computers/*devices* die het internet op willen gaan een *vast* extern IP-adres toe te kennen.[200] Om die reden gebruiken ISP's vooral bij particuliere aansluitingen zogenaamde *dynamische* IP-adressen.

De systematiek daarachter is dat elke keer als (de wifi-router van) een klant zich aanmeldt bij de server van de provider aan die klant een IP-adres wordt toegewezen uit een bepaalde verzameling van bij die provider beschikbare IP-adressen. Meldt de klant zich weer af (bijvoorbeeld omdat hij zijn modem reset of uitzet) of maakt de klant bijvoorbeeld langere tijd geen actief gebruik van zijn internetverbinding, dan wordt dat toegekende IP-adres weer teruggezet in de adressenverzameling zodat het weer aan anderen kan worden uitgegeven. In dit systeem beschikt een klant (feitelijk: zijn wifi-router) dus niet per se constant over hetzelfde IP-adres en kan een bepaald IP-adres in een bepaalde periode dus voor meerdere klanten gebruikt worden. Het is echter belangrijk om zich te realiseren dat ook bij dynamische internetadressen *op elk bepaald tijdstip* een IP-adres maar uitgegeven aan *één* klant/router. De periode waarvoor een IP-adres wordt uitgegeven wordt de *leasetermijn* genoemd. Deze kan per router verschillen.

De provider bewaart in ieder geval enige tijd de gegevens waarmee ook bij dynamische IP-adressen kan worden nagegaan welk IP-adres op welk moment aan welke klant was uitgegeven. Zolang die informatie dus beschikbaar is kan derhalve ook bij een dynamisch IP-adres worden nagegaan met welk mobiel apparaat of via welke router op een bepaald moment via internet is gecommuniceerd, en aan welk(e) persoon of bedrijf dat IP-adres toebehoort.
Opmerking verdient ook dat het feit dat een "dynamisch" IP-adres is toegewezen niets zegt over de vraag of er een mobiele dan wel vaste computer/*device* bij de communicatie via dat IP-adres gebruikt is. Dat is namelijk allebei mogelijk.

Intern IP-adres
Een netwerk heeft echter niet alleen een extern IP-adres, maar ook interne IP-adressen. Zo'n intern IP-adres wordt uitgedeeld door de router van het netwerk. Door aan verschillende computers/*devices* in een netwerk interne IP-adressen toe te kennen kunnen deze uit elkaar gehouden worden. Binnen een bepaald netwerk zijn ook deze interne IP-adressen unieke adressen, maar daarbuiten zeker niet. Wifi-routers gebruiken als gevolg van internationale afspraken drie reeksen van interne IP-adressen, waarbij 192.168.[..] voornamelijk in thuisnetwerken wordt toegekend[201], zoals ook in bovenstaand voorbeeld.

De communicatie via internet verloopt dan als volgt. Op het moment dat vanaf een computer een website wordt bezocht, onthoudt de router het IP-adres van de computer waarvandaan deze website wordt opgevraagd. Als vervolgens op het internet de gevraagde website wordt gevonden, wordt de daarop aanwezige informatie naar het (unieke) IP-adres gestuurd dat de ISP aan de betreffende gebruiker heeft toegekend. Vervolgens

[199] Wilt u weten wat het IP-adres van uw internetverbinding is? Kijk dan op http://www.myip.nl/. Bovenaan ziet u uw IP-adres staan bij "IP Address (v4 of v6)".
[200] Om dit te ondervangen is een aantal serviceproviders al geheel of gedeeltelijk overgegaan op de IPv6-standaard dat veel meer IP-adressen mogelijk maakt, die overgang is echter technisch complex. Na volledige overgang zal waarschijnlijk weer aan elke gebruiker een vast IP-adres kunnen worden toegekend. Zie hierover verder het verderop bij par. 6.2.6. opgenomen: Technisch lemma: enige kanttekeningen bij de betrouwbaarheid van IP-adressen als grondslag voor rechterlijke beslissingen.
[201] Zie RFC 1918 (https://nl.wikipedia.org/wiki/RFC_1918). Interne IP-adressen beginnen met: 192.168.*.*, 172.16.*.* t/m 172.31.*.* en 10.*.*.* .

wordt via de bij dat externe IP-adres behorende wifi-router deze informatie weer doorgestuurd naar het interne IP-adres van de computer die de informatie oorspronkelijk had aangevraagd.

IP-adressen en domeinnamen
De cijfercombinaties van IP-adressen zijn voor gebruikers moeilijk te hanteren en te onthouden. Daarom wordt er – vooral bij websites – gebruik gemaakt van zogenaamde domeinnamen. Een domeinnaam is een unieke naam, zoals www.rechtspraak.nl. Dat loopt via het zogenaamde domeinnaamsysteem (DNS), dat het wereldwijd koppelt aan een bepaald IP-adres, vergelijkbaar op de wijze waarop in een telefoonboek namen worden gekoppeld aan telefoonnummers. Zo is rechtspraak.nl bijvoorbeeld thans[202] via het DNS gekoppeld aan het IP-adres *159.46.193.242*. Typt iemand derhalve www.rechtspraak.nl dan wordt via het DNS-"telefoonboek" razendsnel het bijbehorende IP-adres *159.46.193.242* opgezocht en wordt vervolgens met dat IP-adres (dat dus feitelijk hoort bij de server waarop de rechtspraak.nl website staat) verbinding gemaakt.

3.5.1. Achtergronden en afgrenzing ten opzichte van "bezit"

Deze gedraging is toegevoegd aan art. 240b Sr in het kader van de implementatie van het Verdrag van Lanzarote. Doordat deze strafbaarstelling pas in werking is getreden op 1 januari 2010, kan deze – vanwege het in art. 1 Sr neergelegde legaliteitsbeginsel – geen betrekking hebben op gedragingen die zich voor deze datum hebben voorgedaan. Dit impliceert dat de strafrechter bij de beoordeling of deze gedraging bewezen kan worden geacht, zal hebben te onderzoeken of met voldoende zekerheid kan worden vastgesteld dat de verdachte zich na 1-1-2010 de hier bedoelde toegang heeft verschaft. Die zekerheid zal vooral in die gevallen waarin het "zich toegang verschaffen" grotendeels moet worden afgeleid uit de aanwezigheid van voorheen gedownloade bestanden in zogenaamde *unallocated clusters* (waarvan de datering niet onproblematisch is[203]) niet altijd, en niet altijd eenvoudig, kunnen worden verkregen.

Technisch lemma: unallocated clusters / "deleted files"

In veel kinderpornozaken blijken op de computer van de verdachte (ook) bestanden te zijn aangetroffen in de zogenaamde unallocated clusters (in NFI-rapporten aangeduid als "niet toegewezen ruimte"[204]). Bij het schrijven van gegevens op een gegevensdrager worden deze gegevens geplaatst in zogenaamde clusters. Unallocated clusters zijn die stukjes van een gegevensdrager die compleet leeg zijn of zijn gevuld met gegevens waarvan de gebruiker heeft aangegeven dat deze verwijderd mogen worden – bijvoorbeeld nadat de gebruiker de prullenbak heeft geleegd. In beide gevallen ziet het bestandsbeheerssysteem deze clusters als ruimte die beschikbaar is om nieuwe bestanden te plaatsen. In die unallocated clusters aangetroffen bestanden worden ook wel aangeduid met de term "*deleted files*".

Van belang is te benadrukken dat de term "deleted files" niet verwijst naar door de gebruiker naar de prullenbak ("recycle bin") verplaatste bestanden, hoewel de term "deleted" naar algemeen spraakgebruik wel met dergelijke bestanden in verband wordt gebracht. Naar de prullenbak verplaatste bestanden zijn evenwel nog steeds toegankelijk (en dus niet definitief verwijderd/"deleted") voor de gebruiker: ze kunnen bijvoorbeeld met een simpele muisklik worden teruggezet naar de bestandsmap/bestandslocatie waarin ze zich voor verplaatsing naar de prullenbak bevonden.[205] In de jurisprudentie is zichtbaar dat door de politie in het (tot recent) gangbare proces-verbaal collectiescan wisselende aanduidingen voor definitief uit de prullenbak verwijderde bestanden zijn gebruikt. Processen-verbaal waarin onderscheid wordt gemaakt tussen "deleted

[202] Dat is 8 maart 2023.
[203] Zie hierna onder 3.5.3. en 6.2.4.1.
[204] Zie voor een volledigere overzicht van de thematiek uit dit technisch lemma het rapport "Terug naar de bestanden, technische toelichting over identificeren, verbergen en verwijderen van bestanden", Nederlands Forensisch Instituut 22 juni 2019.
[205] In enkele (oudere) uitspraken lijken bestanden die zich (nog) in de prullenbak bevinden en voor de gebruiker (nog) toegankelijk zijn, ten onrechte als "deleted files" te zijn beschouwd (zie o.m: Rb. Midden-Nederland 6-8-2019, ECLI:NL:RBMNE:2019:3655 en Rb. Noord-Holland 19-3-2015, ECLI:NL:RBNHO:2015:2853).

files" (aangeduid met 'D') en "recycle bin" (aangeduid met 'R'), bieden de rechtspraak het meest houvast[206], maar dat onderscheid wordt niet steeds gemaakt. Bovendien verdient opmerking dat de inrichting van het proces-verbaal collectiescan, dat inmiddels de naam "beschrijvend proces-verbaal art. 240b Sr" heeft gekregen, is gewijzigd. De categorie-aanduidingen "accessible", "deleted" en "other" worden niet langer gebezigd.

Evenals bij uit de prullenbak van een computer verwijderde bestanden, wordt de locatie waar "lost files" zich op een gegevensdrager bevinden aangeduid als "unallocated clusters". Een juridisch relevant verschil is dat "lost files" in beginsel min of meer per ongeluk ontstaan, terwijl het verwijderen van bestanden een actieve handeling veronderstelt (zij het wellicht door het activeren van een geautomatiseerd proces, zoals een schijfopruimingsprogramma). Het ligt voor de hand dat de gebruiker van een gegevensdrager daarover bevraagd wordt, omdat dergelijke handelingen relevant kunnen zijn voor de beoordeling van het opzet op het voorhanden hebben van dergelijke bestanden.

Het is hierbij belangrijk om zich te realiseren dat als een besturingssysteem als Windows een bestand wegschrijft naar een bepaald deel van een harde schijf, in de bestandstabel van het bestandssysteem (in Windows aangeduid met: NTFS) wordt geregistreerd dat dat deel van de harde schijf nu is gealloceerd ("allocated"), dat wil zeggen is toebedeeld aan een bestand, en dat (dus) geen andere gegevens meer naar dat deel van de harde schijf mogen worden weggeschreven.

Indien dat bestand vervolgens weer door een gebruiker van de harde schijf wordt verwijderd (dus niet alleen naar de prullenbak wordt verplaatst maar vervolgens ook daaruit wordt verwijderd) dan kan die ruimte echter weer de status 'niet-toegewezen/unallocated 'krijgen. Anders dan veel gebruikers denken is dan echter niet tevens het betreffende bestand fysiek van de harde schijf verdwenen. Integendeel, alle "verwijderde" gegevens zijn (in de vorm van "enen en nullen") precies op de oorspronkelijke locatie op de harde schijf blijven staan. Wat echter wel is veranderd is dat de naam of het label van het bestand (c.q. de map) in de bestandstabel (*file table*) van het bestandssysteem (dat onder meer bijhoudt op welke locatie welke bestanden op de harde schijf staan) wordt gewist. Dat heeft twee gevolgen. Allereerst verdwijnt daardoor de verwijzing in het bestandssysteem naar de locatie op de harde schijf waarop het verwijderde bestanden stond. Het bestandssysteem (en dus de computer) zal deze bestanden dus niet meer kunnen "vinden". Een tweede gevolg is dat de computer vervolgens de locaties waarop de verwijderde bestanden stonden weer als unallocated (dus: vrij) aanmerkt zodat op die locaties dus weer nieuwe gegevens mogen worden opgeslagen.

Vertaald naar de analoge wereld laat het voorgaande zich wellicht het beste vergelijken met een hele grote bibliotheek waar alle boeken op een op kast, plank en boeknummer bepaalde locatie staan, maar waarvan van een aantal boeken het kaartje met de naam van het boek en de overige gegevens uit de catalogus wordt gehaald. Het boek staat er dan dus nog wel, maar het cataloguskaartje waarmee je het kan vinden niet meer. Daarmee is het vervolgens onmogelijk geworden om snel en gericht vanuit de catalogus die boeken te vinden; hooguit kan je alle boekenrekken gaan aflopen in de hoop dat je die boeken ergens tegenkomt….

Het is wel van belang om vast te stellen dat het hier beschreven fenomeen zich (vrijwel) uitsluitend voordoet bij de traditionele mechanische harde schijven (HDD's). Bij puur elektronische opslag (met name bij SSD's, maar ook bij USB-sticks, geheugenkaarten etc.) worden verwijderde bestanden meestal daadwerkelijk verwijderd.[207]

Normaliter zal reeds eerder ingenomen schijfruimte echter alleen worden overschreven door de computer indien dat nodig is om nieuwe gegevens op te slaan en er geen geheel lege (in de zin van: nooit eerder benutte) schijfruimte meer beschikbaar is. Door de toenemende opslagcapaciteit van harddisks komt het tegenwoordig echter vaak voor dat deze nog veel lege schijfruimte over hebben. Zolang dat het geval is, zal een eerder "verwijderd" bestand meestal niet worden overschreven en zal dit dus op de harddisk aanwezig blijven. Is er echter geen "lege" opslagruimte meer dan zullen de enen en nullen van het verwijderde bestand worden overschreven door de enen en nullen van een nieuw bestand. Een eenmaal overschreven bestand is niet meer terug te halen. Wel zal, als het nieuwe bestand minder omvangrijk is dan het overschreven bestand, nog wel een gedeelte van het oorspronkelijke bestand op de harde schijf blijven staan; dit gedeelte kan dan mogelijk met speciale forensische software nog wel worden "teruggehaald".

[206] Zie o.m. Hof 's-Hertogenbosch 24-3-2021, ECLI:NL:GHSHE:2021:2969 en Rb. Rotterdam 2-6-2022, ECLI:NL:RBROT:2022:4297.
[207] Zie nader hierover Van den Hurk en De Vries, "Onderzoek aan digitale-gegevensdragers. Een technische en juridische verkenning", (PWS nr. 15) 2021, blz. 14.e.v.

Dat laatste geldt ook in meer algemene zin. Hoewel dus de computer een definitief uit de prullenbak "verwijderd" bestand niet meer zelfstandig kan vinden, is het wel mogelijk om met speciale software het bestand weer zichtbaar te maken. Er zijn vele varianten van dergelijke software vrijelijk via het internet te verkrijgen.[208] De krachtigste varianten van deze software, zoals het veelgebruikte programma *Encase* en het door het NFI ontwikkelde *Hansken,* zijn echter specifiek ontwikkeld voor (diepgaand) forensisch onderzoek en daardoor slechts tegen hoge kosten (of zelfs: niet) verkrijgbaar. Dergelijke krachtige software wordt daarom vooral door opsporingsdiensten gebruikt.

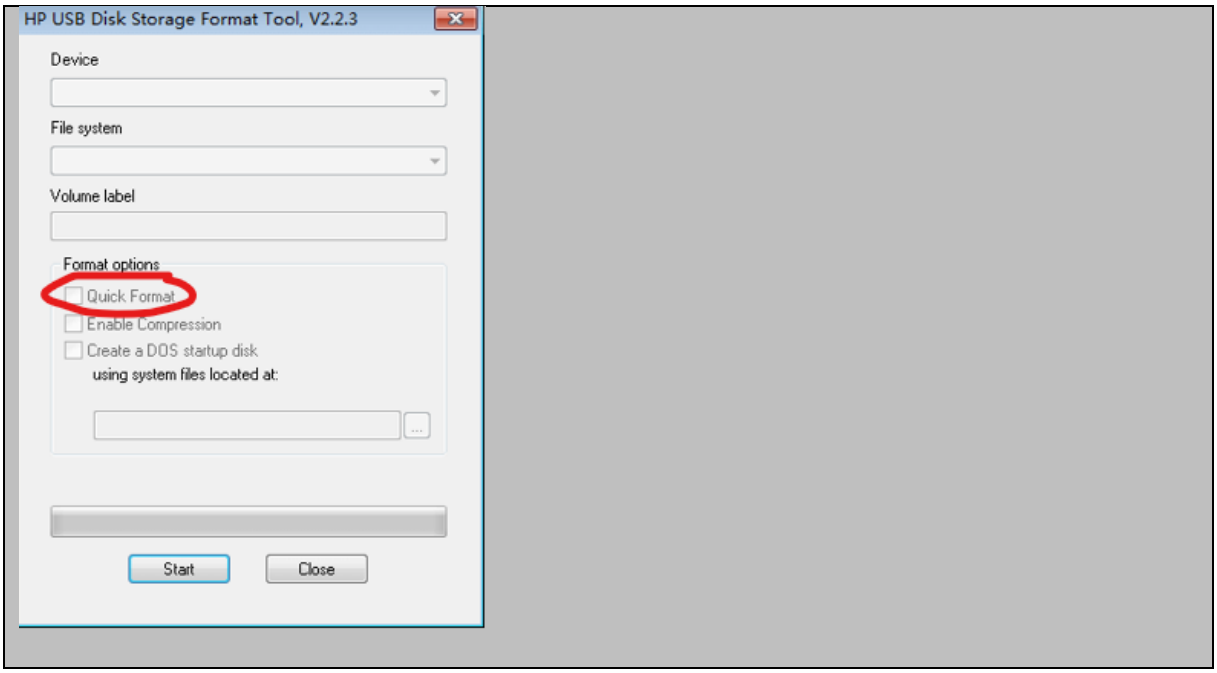
De werking van alle forensische software welke is ontwikkeld voor het doorzoeken van harddisks vertoont grote overeenkomsten. Die werking komt er feitelijk op neer dat de software systematisch een gehele hard disk afzoekt naar alle daarop fysiek aanwezige gegevens, ongeacht of deze nu in het bestandssysteem geregistreerd zijn (dus *allocated* zijn) of niet (en dus *unallocated* zijn). Vindt men dan gegevens die unallocated zijn, dan wordt bij de beschrijving van die gegevens/dat bestand in de forensische rapportage tevens aangegeven dat deze aangetroffen zijn/is "in de unallocated clusters". Het moge duidelijk zijn dat bij dergelijk forensisch onderzoek van een harde schijf regelmatig ook bestanden (of gedeelten daarvan) worden aangetroffen, waarvan de gebruiker dacht dat hij deze verwijderd had.

De beschreven methode wordt vaak aangeduid met de term 'carving'. Het kan worden gebruikt om naar een of meer specifieke bestanden te zoeken, of om een (deel van) een gewiste gegevensdrager te reconstrueren. Bestanden die aldus zijn teruggevonden of gereconstrueerd worden in processen-verbaal vaak opgenomen in een rubriek genaamd 'unallocated'. In uitspraken wordt vervolgens soms beschreven dat bestanden zich in 'de map 'unallocated' bevonden' of dat de bestanden 'carved' waren[209], daarmee de (verkeerde) indruk wekkend dat deze bestanden aldus zijn aangetroffen op de inbeslaggenomen gegevensdrager.

Wil men een bestand dus echt definitief van de harde schijf verwijderen, dan moet men overgaan tot het zogenaamde "wipen" van de harde schijf, of gebruik maken van zogenaamde (vaak gratis verkrijgbare) 'eraser software'. In feite komt dit neer op het overschrijven van de gehele harde schijf of specifieke delen daarvan met nieuwe gegevens. Over het algemeen wordt aangenomen dat het eenmalig overschrijven met nieuwe gegevens voldoende is om bestaande gegevens definitief te verwijderen. Herformatteren wordt regelmatig genoemd als methode waarmee dit resultaat ook verkregen kan worden, maar daarbij is wel voorzichtigheid geboden omdat het afhangt van de gekozen formatteringsmethode. Wordt gekozen voor "Quick Format" (zie onderstaande afbeelding), dan wordt alleen de verwijzingstabel van het bestandsbeheerssysteem gewist en ontstaan er slechts unallocated clusters.

[208] Zie voor een overzicht van voor (ook voor consumenten) beschikbare 'recovery tools' bijv. deze website: 15 Best Free Data Recovery Software in 2023 [Windows & Mac] (softwaretestinghelp.com).

[209] RB Limburg 23-6-2021, ECLI:NL:RBLIM:2021:4948 ("*De politie beschrijft dat de foto's en video's 'carved' waren. Dit houdt in dat de foto's en videos uit de index van de harde schijf verwijderd zijn*.)." Hiermee wordt vermoedelijk bedoeld te beschrijven dat de afbeeldingen door carving beschikbaar zijn gemaakt, niet dat ze in deze toestand waren aangetroffen. Een betere omschrijving van een dergelijke situatie is dat de afbeeldingen zich in unallocated clusters bevonden).



De uitbreiding van art. 240b Sr met het "zich toegang verschaffen" was ingegeven door de technologische ontwikkelingen. Kinderpornografisch materiaal wordt in toenemende mate *online* aangeboden (en bekeken) op besloten websites of binnen besloten netwerken. Toegang is veelal slechts mogelijk na betaling en/of indien men de juiste wachtwoorden en/of decryptiecodes en/of locatie kent. Er zijn echter ook "opslagplaatsen" van kinderporno (zoals Dropbox en andere cloudopslag), waarvoor geen betaling of wachtwoord nodig is en waar men kinderpornografisch materiaal vrijelijk met elkaar deelt. De URL's van deze "opslagplaatsen" worden – veelal via ook op dergelijk materiaal gerichte forums en chatgroepen gedeeld. Ook wordt steeds vaker aangeboden dat tegen betaling met de webcam (veelal in derde wereldlanden) gefilmd kindermisbruik in de vorm van streaming video *real time* (live) kan worden bekeken. Al deze modaliteiten hebben gemeen dat het voor het kunnen bekijken van kinderpornografische afbeeldingen niet langer nodig is om deze afbeeldingen te downloaden en evenmin dat het nodig is om deze op te slaan op een (eigen) gegevensdrager. Omdat zonder downloaden en opslag de gebruiker als regel ook niet een verdergaande beschikkingsmacht over de afbeeldingen zal hebben dan het enkele bekijken daarvan, zal dus het online *kijken* naar kinderpornografische afbeeldingen *de jure* niet als "in bezit hebben" kunnen worden aangemerkt. Zijn echter afbeeldingen van een bezochte internetsite gedownload, en nog toegankelijk aanwezig op een gegevensdrager van de downloadende persoon, dan zullen in de regel[210] zowel "zich toegang verschaffen tot" als "verwerven", als "in bezit hebben" met betrekking tot die afbeeldingen bewezen kunnen worden verklaard.[211]

---

[210] Tenzij sprake zou zijn van een vorm van downloaden vanaf de bezochte website naar (en/of opslag op) het systeem van betrokkene, die voor hem/haar als onvoorzienbaar moet worden beschouwd; zie hierover verder ook hierna onder 4.1.3.3.

[211] Aldus ook bijv. RB Oost-Brabant 14-4-2014, ECLI:NL:RBOBR:2014:1773 (bewust gezochte kinderpornografie gedownload van internet; gedownloade materiaal nog toegankelijk in temporary internet files; bewezenverklaring "zich toegang verschaffen" en "bezit"); RB Zwolle 13-10-2011, ECLI:NL:RBZLY:2011:BT7560 (downloaden, bewaren en weer uploaden; bewezenverklaard: een gewoonte maken van het in bezit hebben, verspreiden, aanbieden, verwerven en d.m.v. een geautomatiseerd werk de toegang daartoe verschaffen); RB Dordrecht 04-08-2011, ECLI:NL:RBDOR:2011:BS1434 (massaal en langdurig o.a. *tegen betaling* via internet downloaden van kinderporno; bewezenverklaard: gewoonte maken van het bezit van en het zich toegang verschaffen tot kinderporno).

3.5.2. Betekent "zich toegang verschaffen": "bekijken" of "actieve en gerichte handeling"?
De uitbreiding van art. 240b Sr met "zich toegang verschaffen" is dan ook bedoeld als vangnet voor die gevallen die (met name omdat geen sprake is van het opslaan van materiaal) niet onder de strafbaarstelling van "in bezit hebben" kunnen worden gebracht.[212]
Dit "vangnet" gaat blijkens de wetsgeschiedenis echter niet zover dat ook beoogd is het enkele "kijken" naar kinderpornografisch materiaal strafbaar te stellen. Integendeel, nadrukkelijk is niet beoogd om ook het enkele bekijken van kinderpornografisch materiaal zonder dat met betrekking tot het verkrijgen van toegang tot dat materiaal enige *actieve en/of gerichte* handeling is verricht, strafbaar te stellen. Als iemand dus onverwachts op het computerscherm van een ander kinderpornografische afbeeldingen ziet staan, dergelijke afbeeldingen plotsklaps door middel van een *pop-up*[213] op zijn eigen scherm ziet verschijnen, of daarmee na het nietsvermoedend aanklikken van een hyperlink wordt geconfronteerd, heeft hij deze afbeeldingen wel bekeken, maar is geen sprake van (strafbaar) handelen als bedoeld in art. 240b Sr.[214]

"Zich toegang verschaffen" impliceert derhalve een *actieve* handeling *gericht* op het verkrijgen van toegang tot kinderpornografische afbeeldingen.[215] De memorie van toelichting geeft als voorbeelden van dergelijke actieve en gerichte handelingen het aanklikken van een link[216], terwijl die link zelf al een indicatie geeft voor de (kinderpornografische) inhoud van de daarachter liggende website, het vaker bezoeken van een website met kinderpornografische

---

[212] Aldus Kamerstukken II, 31810, 2008/2009, nr. 3 (MvT) , p. 3-4; zie ook HR 7-2-2017, ECLI:NL:HR:2017:167 en RB Gelderland 30-10-2017, ECLI:NL:RBGEL:2017:5674.
[213] Een *pop-up* is een nieuw, vaak kleiner venster dat verschijnt bovenop een reeds op een *device* openstaand venster. Een pop-up verschijnt meestal als reactie op een actie van een gebruiker, zoals het aanklikken van een (onderdeel van een) website of (bijlage bij een) emailbericht. De gebruiker zal zich er vaak niet bewust van zijn dat zijn actie het verschijnen van een pop-up tot gevolg zal hebben en nog minder wat de inhoud daarvan zal zijn. Ongevraagde pop-ups worden vaak gebruikt door adverteerders die veel aandacht willen maar ook wel voor het plaatsen van malware. Pop-ups kunnen tot op zekere hoogte worden geblokkeerd door een zogenaamde *pop-up blocker* aan te zetten. Er zijn echter methoden (bijvoorbeeld door gebruikmaking van Flash en van zogenaamde *floaters* (delen van een webpagina die over de rest van een pagina verschijnen)) die de werking van pop-up blockers omzeilen.
[214] Kamerstukken II, 31810, 2008/2009, nr. 3 (MvT) , p. 4.
[215] Idem. Dit lijkt niet te zijn onderkend in RB Zeeland-West-Brabant 18-11-2022, ECLI:NL:RBZWB:2022:6878 ("(…) *waren de genoemde 6 afbeeldingen die op de Samsung S8 zijn aangetroffen vrij toegankelijk. (...) Deze afbeeldingen had hij dus in zijn bezit toen deze telefoon in beslag werd genomen. Dit betekent voorts dat hij zich op enig moment (...) de toegang tot deze afbeeldingen heeft verschaft* (…)."
[216] Het (via een internetzoekmachine) verrichten van een zoekslag naar kinderpornografische websites kan onzes inziens als zodanig niet worden aangemerkt als zich toegang verschaffen tot kinderpornografisch materiaal. In dat geval wordt immers niet voldaan aan de eis dat daadwerkelijk kennis is genomen van de inhoud van afbeeldingen op de betreffende website(s), bijvoorbeeld doordat wordt geklikt op (een van) de link(s) in de zoekresultaten.

afbeeldingen[217] en het betalen voor toegang tot een site.[218] Gezien deze voorbeelden lijkt aannemelijk dat van "zich toegang verschaffen" ook sprake is als men bijvoorbeeld via Twitter of Facebook of via accounts van derden kinderpornografische afbeeldingen bekijkt.[219] Hetzelfde lijkt te gelden als een ontvanger kinderpornografische afbeeldingen opent die als bijlage bij aan een hem (via een communicatiedienst) gestuurd bericht zijn gevoegd, mits eerdere en/of onderliggende communicatie en/of de naam van de bijlage de ontvanger reeds een indicatie gaven aangaande de mogelijke inhoud van die bijlage.[220] Problematischer ligt dit bij het openen van via Snapchat[221] toegezonden afbeeldingen, omdat de ontvanger lang niet altijd direct bij binnenkomst uit de omschrijving/benaming daarvan het karakter van de foto kan afleiden, zodat het openen daarvan hoogstwaarschijnlijk niet als een *op het verkrijgen van toegang tot kinderpornografisch materiaal gerichte* handeling kan worden aangemerkt. In voorkomende gevallen zal mogelijk wel uit onderliggende communicatie of andere bewijsmiddelen kunnen volgen dat de ontvanger ermee bekend was, of de aanmerkelijke kans aanvaardde dat hem via Snapchat een kinderpornografische afbeelding zou worden toegezonden. De daarop volgende handeling tot het openen daarvan kan dan wel worden aangemerkt als "het zich toegang verschaffen".[222]

---

[217] Kamerstukken II, 31810, 2008/2009, nr. 3 (MvT) , p. 4. Dan is immers als regel aannemelijk dat men tijdens het eerste bezoek al op de hoogte is geraakt van de kinderpornografisch aard van de daar zichtbare afbeeldingen op die site; het dan op een later moment weer bezoeken van die site zal dan bezwaarlijk anders kunnen worden geduid dan het zich – minst genomen voorwaardelijk opzettelijk – actief en gericht toegang verschaffen tot die afbeeldingen. In dezelfde zin ook: Hof Den Haag 6-10-2017, ECLI:NL:GHDHA:2017:2853 (e-archief) (toegang verschaffen tot kinderporno. "*Gelet op het aantal bezochte websites, de frequentie van het bezoek aan deze sites, de duur van het bezoek aan deze sites, het tijdstip waarop deze sites zijn bezocht, de voor verdachte als kinderporno kenbare inhoud van deze sites en het terugkerende karakter van de bezoeken aan veelal dezelfde sites is het hof van oordeel dat de verdachte deze websites opzettelijk bezocht heeft en tevens opzettelijk op deze sites heeft gebrowsd met het kennelijk doel kennis te nemen van kinderpornografische afbeeldingen van kennelijk minderjarige jongens. Derhalve komt het hof tot de conclusie dat de verdachte zich opzettelijk de toegang tot de sites waarop kinderpornografische afbeeldingen zijn afgebeeld heeft verschaft").*

[218] Idem. Dit laatste voorbeeld lijkt echter minder gelukkig, omdat uit de enkele betaling nog niet zonder meer kan worden afgeleid dat is beoogd toegang te verkrijgen tot *kinder*pornografische afbeeldingen. De gerichtheid daarop zal derhalve uit andere feiten en omstandigheden (zoals bijv. de naam van de website, informatie waaruit blijkt dat verdachte het karakter van de site kende of kon vermoeden etc.)

[219] In deze zin ook RB Den Haag 14-9-2017, ECLI:NL:RBDHA:2017:10941 (veelvuldig bekijken van kinderpornografische foto's via twitteraccounts van anderen; wordt gekwalificeerd als het "toegang tot dergelijke foto's verschaffen door middel van een geautomatiseerd netwerk en met gebruikmaking van een communicatiedienst).

[220] Zie ook Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (bewezenverklaring van "*zich de toegang verschaffen"*. Verdachte heeft vanaf een website meermalen links naar of groepsbestanden met digitale afbeeldingen toegezonden gekregen en/of gedownload. Vooraf wist hij niet wat er precies zou zitten in de bestandspakketten. Na ontvangst/het downloaden opende hij de pakketten. Als verdachte dan kinderporno zag, verwijderde hij dit meteen. Verdachte bleef echter ongezien soortgelijke pakketjes downloaden. Voorwaardelijk opzet op toegang verschaffen tot kinderpornografisch materiaal)

[221] *Snapchat* is een tot de sociale media gerekende gratis communicatiedienst/app die het (na installatie van de Snapchat-app) mogelijk maakt dat gebruikers van deze dienst elkaar afbeeldingen en video's kunnen sturen, eventueel met een bijschrift. Het bijzondere aan Snapchat is dat de toegezonden *snaps* – afhankelijk van de instelling – na lezing door de ontvanger automatisch worden verwijderd. De *snaps* zijn dan niet meer voor de ontvanger zichtbaar en ook niet aanwezig op het device van de ontvanger. Het is met de replay-functie mogelijk om een bekeken *snap* nogmaals te bekijken. Als het betreffende scherm wordt gesloten is de *snap* ook weg. Zie verder: https://support.snapchat.com/

[222] Aldus ook RB Gelderland 30-10-2017, ECLI:NL:RBGEL:2017:5674 **(**verdachte heeft om kinderpornografische foto's gevraagd, zich die via de applicatie Snapchat laten toezenden en vervolgens geopend. Verdachte heeft zich aldus met gebruikmaking van een geautomatiseerd werk en/of communicatiedienst de toegang tot de foto's verschaft). Enigszins mager gemotiveerd lijkt RB Limburg 8-5-2018, ECLI:NL:RBLIM:2018:4622 (verdachte heeft in het kader van algemene seks chats foto's ontvangen waarvan de inhoud pas kenbaar werd door deze aan te klikken. Deze werden vervolgens automatisch in een map op de computer van verdachte opgeslagen. Hij weet niet waarom hij ze vervolgens niet heeft verwijderd. Dit levert volgens de RB op dat verdachte zich daartoe de toegang heeft verschaft.).

Indicaties dat de handeling gericht was op het verkrijgen van kinderpornografische afbeeldingen (en dat er dus sprake was van opzet) kunnen ook zijn gelegen in de historische gegevens, die – al dan niet in samenhang met online betalingsverkeer – zijn te herleiden tot websites waarop kinderpornografie wordt aangeboden, of tot het beschikken over decryptiecodes, wachtwoorden, inloggegevens, hyperlinks of extensies, die kunnen worden gerelateerd aan websites, netwerken enz. waarop of waarbinnen zich kinderpornografische afbeeldingen bevinden.[223] Onzes inziens is ook goed verdedigbaar dat, indien uit het onderzoek ter terechtzitting anderszins (bijvoorbeeld uit een bewezenverklaring voor "bezit") is gebleken dat de verdachte een bijzondere belangstelling had voor kinderpornografische afbeeldingen, dat gegeven mede mag worden betrokken bij het oordeel of (al dan niet tevens) sprake was van een handeling gericht op het verkrijgen van toegang tot zulke afbeeldingen.[224]

3.5.3. Afbeeldingen in de unallocated clusters: onvoldoende bewijs voor "bezit", maar wel medebewijzend voor "zich toegang verschaffen"?

In dit kader is in het bijzonder van belang dat indien in de *unallocated clusters* van een gegevensdrager kinderpornografische afbeeldingen worden aangetroffen, dat in de rechtspraak over het algemeen niet worden aangemerkt als het "bezitten" van die afbeeldingen. Het aantreffen van dergelijke afbeeldingen vormt echter in de regel wel een (zeer) sterke aanwijzing dat de betreffende computergebruiker deze afbeeldingen eerder heeft gedownload van een internetsite[225], en dat hij zich dus eerder via een geautomatiseerd werk "toegang heeft verschaft" tot die afbeeldingen.[226] Verdere ondersteuning voor dit vermoeden

---

[223] Aldus ook bijv. Hof Den Haag 13-3-2012, ECLI:NL:GHSGR:2012:BV980. In dit verband is helder de CAG vóór HR 20-11-2018, ECLI:NL:HR:2018:2143: "*27. Het "zich toegang verschaffen" betekent in het onderhavige verband dat de verdachte een gedraging verricht die gericht is op het (via een geautomatiseerd werk) verkrijgen van toegang tot kinderpornografisch materiaal. Het opzet van de verdachte dient, al dan niet in voorwaardelijke vorm, gericht te zijn op het verkrijgen van die toegang. Er moet derhalve bewijs zijn van opzet op het moment dat de website wordt bezocht. Per toeval op een website belanden met daarop kinderpornografische afbeeldingen en deze afbeeldingen vervolgens opzettelijk bekijken, is niet strafbaar.*
28. Uit de bewijsmiddelen kan wat betreft het (voorwaardelijk) opzet op het verkrijgen van toegang het volgende worden afgeleid. De verdachte heeft heel vaak diverse bestanden gedownload, zonder precies te weten wat er in zat, en deze bestanden later uitgepakt en bekeken, terwijl (naar hij zelf heeft verklaard) dit een risico inhield, omdat op basis van de bestanden zelf niks valt te zeggen over de inhoud ervan (...) en je dan wel eens minder fraaie dingen tegenkomt die niet door de beugel kunnen (...). De verdachte heeft (naar hij heeft verklaard) bij het surfen op internet ook kinderporno gezien, dit weggegooid, maar niet alles (...). Voorts had de verdachte bijzondere belangstelling voor "naturisme foto's" van meisjes tussen de acht en vijftien jaar (...) en zocht hij in die sfeer op internet in omgevingen, zoals [C], de naam van een internetsite waar links naar downloads van bestanden met kinderporno worden aangeboden, in welke omgevingen de kans op het aantreffen van kinderpornografisch materiaal (dus) groot was (...). Tegen deze bewijsachtergrond is het oordeel van het hof dat, gezien het zoek- en downloadgedrag van de verdachte, zijn opzet, minst genomen in voorwaardelijke zin, ook in het kader van het zich toegang verschaffen was gericht op het kinderpornografisch karakter van de afbeeldingen, niet onbegrijpelijk en toereikend gemotiveerd."

[224] In die zin is mogelijk ook RB Breda 16-12-2011, ECLI:NL:RBBRE:2011:BU8399 te duiden, waarin overigens "het zich toegang verschaffen" nogal ruim lijkt te worden uitgelegd (verdachte wist dat hij telkens als hij een bepaalde digitale plaats bezocht hem vervolgens door anderen kinderpornografie zou worden toegezonden; was al diverse malen eerder gebeurd en diverse malen was al kinderpornografie onder hem in beslag genomen; verdachte is desondanks door gegaan met het bezoeken van deze plaats en werd hem ook kinderpornografie toegestuurd. De rechtbank merkt dit aan als actieve handeling met als doel het toegestuurd krijgen van kinderpornografie).

[225] Daaronder begrepen andere wijzen van online verkrijging, zoals uit een gedeelde cloudopslag of via P2P.

[226] Dit verband wordt nogal eens onvoldoende onderkend of begrepen, zoals bijvoorbeeld in RB Gelderland 16-2-2016, ECLI:NL:RBGEL:2016:856 ("niet wettig bewezen dat verdachte zich in de tenlastegelegde periode *de toegang heeft verschaft* tot 118 kinderpornografische foto's, nu deze foto's gewiste bestanden betroffen die zonder daarvoor bestemde software niet meer eenvoudig door verdachte te benaderen waren en niet is vast te stellen wanneer deze bestanden door verdachte zijn gewist. Voorts is niet gebleken dat voornoemde software op de gegevensdragers van verdachte is aangetroffen.").

kan bij verder onderzoek bijvoorbeeld worden gevonden in de internetgeschiedenis van de gebruiker (o.m. gebruikte zoektermen[227], de namen van bezochte websites en namen van gedownloade en/of bekeken torrents en/of afbeeldingsbestanden (o.m. opgeslagen in de *temporary internet files* en registers van (communicatie)applicaties)[228], (digitale) betaalgegevens[229] en aangetroffen digitale gegevens zoals decryptiecodes, wachtwoorden, inloggegevens en hyperlinks.

Aldus kan het aantreffen van kinderpornografische afbeeldingen in de *unallocated clusters* weliswaar niet altijd (voldoende) bewijs opleveren voor "bezit", maar kan het wel (mede) belangrijk bewijs vormen voor het "zich toegang verschaffen". Zoals hiervoor al gesteld[230] moet daarbij wel tevens worden beoordeeld of met voldoende zekerheid kan worden vastgesteld dat een eventueel "zich toegang verschaffen" heeft plaatsgevonden vóór dan wel na 1 januari 2010 (de datum van inwerkingtreding van het gewijzigde art. 240b Sr) en bovendien tevens in de in de tenlastelegging opgenomen pleegperiode.[231] Het is niet altijd

---

[227] Deze zoektermen moeten dan wel voldoende specifiek zijn. Zie bijv. RB Oost-Brabant 14-4-2014, ECLI:NL:RBOBR:2014:1773 (bewezenverklaring "zich toegang verschaffen tot"; kinderpornografische bestanden in *temporary internet files*; gezocht met zoekterm "naaktfoto's kinderen"); zie ook RB Gelderland 16-7-2013, ECLI:NL:RBGEL:2013:1665 (gewoonte maken van zich toegang verschaffen tot kinderporno bewezen op basis van temporary internetfiles, verklaring van verdachte over op internet kijken naar kinderpornografisch materiaal en kindermodellen en browsergeschiedenis op iPad); Zie voor een in dit opzicht opmerkelijke uitspraak RB Midden-Nederland 28-1-2014, ECLI:NL:RBMNE:2014:259 (vrijspraak zich toegang verschaffen tot kinderporno; "*geen andere handelingen verricht dan een op porno gerichte zoekterm in Google opgeven, waarna deze afbeeldingen kennelijk in beeld kwamen*"). Het opmerkelijke zit hem hier in het gegeven dat de RB de betreffende zoekterm, *"teenseks"* - kennelijk ook niet in relatie met het verder ten aanzien van andere afbeeldingen bewezen verklaren van het verwerven en het in bezit hebben van kinderpornografisch materiaal - niet aanmerkt als een op *kinder*porno *gerichte* zoekterm. Deze uitspraak is overigens in hoger beroep vernietigd; zie Hof Arnhem-Leeuwarden 18-3-2015, ECLI:NL:GHARL:2015:2016 ('*Verdachte heeft zich met behulp van een digitaal zoekprogramma toegang verschaft tot websites met porno. Hij trof daarop o.a. ook kinderpornografisch materiaal aan. Hij gebruikte daartoe specifieke zoektermen en wist en verwachtte dat dus ook en heeft dat ter terechtzitting nog eens bevestigd. Zijn opzet was dus mede gericht op het digitaal toegang verschaffen tot websites die ook kinderporno bevatten*.").

[228] Zie o.m. RB Limburg 1-8-2017, ECLI:NL:RBLIM:2017:7501 (Bezit kinderporno. Drie bestanden waren *accessible*, de overige bestanden stonden in de *temporary internet files* of tussen de gewiste bestanden afkomstig uit de *temporary files*. "*Van die bestanden kan dus niet gezegd worden dat er sprake was van een bewuste vastlegging van het materiaal, omdat de bestanden automatisch door het systeem zijn aangemaakt. Wel is de conclusie dat de verdachte zich opzettelijk de toegang tot deze bestanden heeft verschaft via een geautomatiseerd netwerk of met gebruikmaking van een communicatiedienst (namelijk: Ares). Getuige de gebruikte zoektermen, de bezochte internetsites en de hoeveelheid aangetroffen kinderporno is de verdachte actief op zoek geweest naar kinderporno.*").

[229] Zie bijv. RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (bestanden aangetroffen in niet zonder meer benaderbare verborgen mappen; bezit niet bewezen; aanwezigheid bestanden tezamen met verklaring verdachte dat hij op zoek is gegaan naar 3D-porno "*als zijnde dat er iets met kinderen gebeurt" en hij vervolgens is gestuit op echte kp, maar zich ook daarna nog meermalen langs dezelfde weg toegang heeft verschaft tot voornoemde 3D-porno voldoende bewijs voor bewezenverklaring "zich toegang verschaffen tot.*"); zie ook RB Gelderland 16-7-2013, ECLI:NL:RBGEL:2013:1665 (gewoonte maken van zich toegang verschaffen tot kinderporno op basis van *temporary internetfiles* en browsergeschiedenis op iPad); RB Breda 16-12-2011, ECLI:NL:RBBRE:2011:BU8399 ('toegang verschaffen tot' bewezen verklaard o.b.v. aantreffen kinderpornografie in temporary internet files en verklaring verdachte); RB Utrecht 6-10-2011, ECLI:NL:RBUTR:2011:BT8700 (gedownload van commerciële website, betaling met creditcard**).**

[230] Zie hiervoor onder 3.5.1.

[231] Zie bijv. Hof Den Haag 13-3-2012, ECLI:NL:GHSGR:2012:BV9803 ("Niet is komen vast te staan dat de verdachte *in de tenlastegelegde periode* een actieve handeling heeft verricht, gericht op het zich welbewust de toegang verschaffen tot kinderpornografisch materiaal, voor zover dit materiaal de in de tenlastelegging omschreven afbeeldingen/videofragmenten betreft." Vrijspraak). Opvallend is RB Amsterdam 21-10-2020, ECLI:NL:RBAMS:2020:5064 (dat verdachte gedurende 11 maanden van de tenlastegelegde periode (die drie jaar bedroeg) geen strafbare feiten heeft gepleegd, is geen beletsel om ten aanzien alle tenlastegelegde

even eenvoudig om tot die vaststelling te komen, bijvoorbeeld omdat gebruikers die zich inlaten met dit type materiaal veelal stelselmatig en grondig hun internetgeschiedenis en andere digitale en communicatiesporen wissen, en vanwege het gegeven dat de datering (metadata) van gegevens die in *unallocated clusters* staan, gecompliceerd kan zijn.

3.5.4 "door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst"

Dit onderdeel van art. 240b Sr is afgeleid van art. 20 van het Verdrag van Lanzarote, waarin is bepaald dat de verdragspartijen maatregelen zullen nemen om strafbaar te stellen "knowingly obtaining access, *through information and communication technologies*, to child pornography". De omschrijving "*through information and communication technologies"* lijkt een breder bereik te hebben dan "*door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst*". De verdragsdefinitie gaat namelijk uit van algemene technieken, onafhankelijk van eigenschappen van de daarbij gebruikte apparaten en ongeacht of daarbij ook een communicatiedienst is gebruikt. Art. 240b Sr is in dit opzicht beperkter, hoewel er gezien de huidige omschrijving van het begrip "geautomatiseerd werk" weinig licht meer lijkt te zitten tussen de Nederlandse wettekst en het Verdrag van Lanzarote. Voor zover vragen mochten rijzen omtrent de interpretatie van het begrip "geautomatiseerd werk" is het goed om zich te realiseren dat is beoogd met de gebruikte formulering "door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst" ook genoemd onderdeel uit het Verdrag van Lanzarote te dekken.[232]

De definitie van "geautomatiseerd werk" is neergelegd in art. 80sexies Sr en luidt thans: "*Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken*." Art. 80sexies Sr is laatstelijk gewijzigd met de op 1 maart 2019 in werking getreden Wet Computercriminaliteit III. Het bereik is – naar aanleiding van technologische ontwikkelingen – verder verruimd.

> Uit de Memorie van Toelichting bij de Wet Computercriminaliteit III[233] blijkt dat de wetgever door middel van deze gewijzigde definitie van het begrip "geautomatiseerd werk" nadere aansluiting zoekt bij de terminologie van het Cybercrime Verdrag (art. 1, onderdeel a). In deze nieuwe definitie vormt het op basis van een programma automatisch verwerken van computergegevens het meest essentiële bestanddeel. De Memorie van Toelichting stelt in dit verband dat de definitie computers, servers, modems, routers, smartphones en tablets omvat, maar ook technische apparaten die in verbinding staan met een netwerk, zoals de SCADA-systemen die worden gebruikt bij industriële productiesystemen, navigatiesystemen, televisies, een digitaal fototoestel met wifi-compatibiliteit of een pacemaker.[234]

De hiervoor reeds besproken redenen voor de specifieke strafbaarstelling van het "zich toegang verschaffen", alsook de formulering "met behulp van een geautomatiseerd werk" impliceren feitelijk tevens dat het geautomatiseerd werk (al dan niet in internet- of intranetverband) bij het zich toegang verschaffen verbinding met andere geautomatiseerde werken moet hebben gemaakt.[235]

---

gedragingen (verspreiden, invoeren, doorvoeren, verwerven en bezitten) tot een bewezenverklaring van de gehele ten laste gelegde periode te komen.

[232] Aldus Lestrade, *T&C Strafrecht*, art. 240b Sr, aant. 7, onder d.

[233] Kamerstukken II, 34372, nr. 3, p. 85/86 (pdf-versie).

[234] Idem.

[235] Ware het anders, dan zou ook het via een eigen PC toegang verschaffen tot een in hetzelfde privé-netwerk hangende externe hard disk of cloudomgeving met daarop kinderpornografische afbeeldingen naast "bezit" ook onder deze strafbaarstelling worden gebracht. Dat lijkt niet beoogd.

Niet noodzakelijk voor bewezenverklaring van "zich toegang verschaffen" is echter dat bij de toegangsverschaffing gebruik is gemaakt van technologische hulpmiddelen als ontsleuteling en/of dat daarbij beveiligingen moeten zijn doorbroken of anderszins een geautomatiseerd werk moet zijn *binnengedrongen* als bedoeld in art 138ab Sr.[236] Het gaat hier derhalve om *blootfeitelijk* toegang verschaffen, hetwelk veelal zal kunnen worden afgeleid uit de plaats waar de betreffende afbeeldingen zijn opgeslagen[237] en/of de uit *filepaths* en andere digitale gegevens blijkende (internet)herkomst van de bestanden.[238] Minder duidelijk is wat wordt bedoeld met het begrip gebruik maken van een *communicatiedienst*, nu dit begrip niet nader in het Wetboek van Strafrecht wordt gedefinieerd.

Wel is sinds 1 maart 2019 in art 138e Sv een definitie van "aanbieder van een communicatiedienst" opgenomen die luidt: "*Onder aanbieder van een communicatiedienst wordt verstaan de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst."*[239] Dit geeft wat ons betreft voldoende inzicht in de minimale eisen waaraan voldaan moet zijn wil van een communicatiedienst sprake zijn: communicatie met behulp van een geautomatiseerd werk is de kern, daaraan accessoire gegevensverwerking of -opslag wordt er tevens onder begrepen.

Hieruit volgt dat onder "gebruik maken van een communicatiedienst" in ieder geval het via een internetprovider als Vodafone, Ziggo en KPN gebruik maken van een internetverbinding valt. Aannemelijk is ook dat het communiceren via veelgebruikte communicatieapplicaties zoals Skype, WhatsApp[240], Twitter, Snapchat en Instagram als gebruik maken van een communicatiedienst kan worden aangemerkt.[241] Bezien vanuit de door art. 240b Sr beschermde belangen, alsook het naar het lijkt ruimere kader dat het Verdrag van Lanzarote in dezen biedt, lijkt namelijk een niet al te beperkte, of anders gezegd: verdragsconforme, interpretatie van het begrip communicatiedienst hier immers voor de hand te liggen.

In de praktijk zullen zich op dit punt naar verwachting weinig bewijsproblemen voordoen.[242]

---

[236] Aldus HR 7-2-2017, ECLI:NL:HR:2017:167 (cassatie van Hof Den Haag 30-12-2014, ECLI:NL:GHDHA:2014:4272; "*van "zich toegang verschaffen" is sprake als verdachte een gedraging verricht die is gericht op het verkrijgen van toegang tot kinderporno. Het opzet van verdachte dient, al dan niet in voorwaardelijke vorm, te zijn gericht op het verkrijgen van die toegang. In de overweging van het Hof ligt als zijn oordeel besloten dat voor bewezenverklaring van het bestanddeel "zich d.m.v. een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft" en dat uit de bewijsmiddelen moet blijken dat gebruik is gemaakt van technologische middelen zoals "versleuteling of een besloten computernetwerk". Dat oordeel getuigt van een te beperkte en dus onjuiste uitleg van art. 240b.1 Sr.*"

[237] Een internetbrowser zal bijvoorbeeld – tenzij door de gebruiker andere instructies zijn gegeven – gedownload materiaal normaliter in bepaalde vanuit dat browserprogramma standaard ingestelde downloadmappen opslaan.

[238] De meeste browsers bewaren bijvoorbeeld ook (tijdelijk) gegevens omtrent met welke internetsites vanaf de betreffende computer contact is geweest en/of welke bestanden zijn gedownload.

[239] Staatsblad 2018, 322 onder.

[240] Vgl. ook http://nos.nl/artikel/2168944-voor-het-eerst-kinderpornonetwerk-op-whatsapp-opgerold.html

[241] O.m. RB Gelderland 30-10-2017, ECLI:NL:RBGEL:2017:5674 (de verdachte heeft om kinderpornografische foto's gevraagd, die zich via de applicatie Snapchat laten toezenden en vervolgens geopend. De verdachte heeft zich aldus met gebruikmaking van een geautomatiseerd werk en/of communicatiedienst de toegang tot de foto's heeft verschaft); RB Den Haag 14-9-2017, ECLI:NL:RBDHA:2017:10941 (veelvuldig bekijken van kinderpornografische foto's via twitteraccounts van anderen; wordt gekwalificeerd als het "*toegang tot dergelijke foto's verschaffen door middel van een geautomatiseerd netwerk en met gebruikmaking van een communicatiedienst*").

[242] In deze zin ook Lestrade., *T&C Strafrecht*, art. 240b Sr, aant. 7, onder d., waar wordt gesteld: "*Feitelijk vallen alle technologieën waarmee verbinding kan worden gemaakt met het internet onder geautomatiseerd werk of*

3.6. "Een beroep of gewoonte maken" van misdrijven als bedoeld in art. 240b Sr

Het tweede lid van art 240b Sr verhoogt de maximale strafbedreiging op de hiervoor besproken in art 240b, eerste lid, Sr strafbaar gestelde gedragingen van vier naar acht jaar, indien van die gedragingen "een beroep of gewoonte" wordt gemaakt.
Het kwalificerend karakter van "een beroep of gewoonte maken" impliceert dat de strafrechter daarmee bij de straftoemeting alleen rekening mag houden, indien het "een beroep of gewoonte maken" ook mede in de tenlastelegging is opgenomen en in het vonnis/arrest ook in de bewezenverklaring en kwalificatie is opgenomen.[243]

Vooral als gevolg van de steeds toenemende snelheid van internetverbindingen en het toenemen en goedkoper worden van opslagcapaciteit worden bij verdachten steeds grotere hoeveelheden kinderpornografische afbeeldingen aangetroffen.[244] Waar in het analoge tijdperk het bezit van een groot aantal afbeeldingen over het algemeen alleen kon worden verkregen door middel van langdurig gericht verzamelen, kunnen in het digitale tijdperk in een tijdsperiode van enige uren vrijwel geautomatiseerd vele duizenden kinderpornografische afbeeldingen worden gedownload en opgeslagen.[245] Dit zou tot de gedachte kunnen leiden dat uit het enkele feit dat bij een verdachte een grote hoeveelheid afbeeldingen is aangetroffen, niet automatisch kan worden afgeleid dat ook sprake is geweest van "een beroep of gewoonte maken" als hier bedoeld.[246] Er wordt hier echter ook anders over gedacht.[247]

In de rechtspraak is nadere invulling gegeven aan het begrip "gewoonte". Een uitleg naar algemeen spraakgebruik, waarbij een "gewoonte" wordt omschreven als "telkenmale gedurende een langere periode iets te doen", verwijst niet naar voor de gewoonte redengevende omstandigheden en is weinig richtinggevend.[248]

---

communicatiedienst", hoewel dit lijkt te miskennen dat het internet zelf ook bestaat uit (een combinatie van) geautomatiseerde werken en communicatiediensten. Ondanks dat feitelijk ondenkbaar is dat iemand zich niet met een geautomatiseerde werk en/of door middel van een communicatiedienst op het internet aanmeldt, staat buiten kijf dat – indien eenmaal op het internet aangeland – vanaf dat moment aan het hier besproken vereiste is voldaan.
Aandacht verdient dat in voormeld citaat wordt gesproken over "technologieën", hetgeen mede zogenaamde protocollen lijkt te omvatten - zoals IPv4 en IPv6, maar ook TOR - die essentieel zijn voor toegang tot het internet. De begrippen geautomatiseerd werk noch communicatiedienst lijken dergelijke protocollen mede te omvatten; het gaat daarbij in wezen slechts om een verzameling van afspraken, technische normen, randvoorwaarden, etc.

[243] Het valt bij bestudering van de jurisprudentie op dat ook indien uit de feiten duidelijk blijkt dat sprake is van "een gewoonte maken", lang niet altijd bewezenverklaring van "een gewoonte maken" volgt. Verdere bestudering leert dat dit dan vermoedelijk vooral het gevolg was van het feit dat zulks niet (tevens) ten laste was gelegd; zie bijv. RB Oost-Brabant 26-4-2013, ECLI:NL:RBOBR:2013:CA3587 (vervaardigen, verspreiden en voorhanden hebben van een grote hoeveelheid kinderporno gedurende bijna 2 jaar; geen "gewoonte maken" tenlastegelegd); RB Den Bosch 29-10-2008, ECLI:NL:RBSHE:2008:BG3640 (downloaden, opslaan en 'verzamelen' van grote hoeveelheden kinderporno gedurende 5 weken).

[244] Zie bijv. Hof Den Haag 02-4-2012, ECLI:NL:GHSGR:2012:BW0675 (meerdere miljoenen afbeeldingen).

[245] Dit laatste zal vooral het geval zijn indien sprake is van een combinatie van een breedbandverbinding, (peer-to-peer)software die gebruik maakt van de Bittorrent-technologie en een door de gebruiker relatief breed geformuleerde zoekopdracht.

[246] In deze zin bijv. ook RB Oost-Brabant 12-4-2016, ECLI:NL:RBOBR:2016:1720 ("Dat het om veel *(auteurs: i.c. ruim 14.000 afbeeldingen)* materiaal gaat is onvoldoende om van een gewoonte te kunnen spreken").

[247] Uit de (door de Hoge Raad gevolgde) conclusie van AG Aben (ECLI:NL:PHR:2017:1227) bij HR 14-11-2017 en de hierna in de hoofdtekst te noemen conclusie van AG Vellinga bij HR 7-12-2010 zou men echter kunnen afleiden dat in hun optiek een gewoonte reeds kan bestaan bij het bezit van verscheidene kinderpornografische afbeeldingen of gegevensdragers met dergelijke afbeeldingen.

[248] Zie o.m. RB Gelderland 20-12-2022, ECLI:NL:RBGEL:2022:7207 ("*Van een gewoonte is bijvoorbeeld sprake als men gewend is telkenmale gedurende een langere periode iets te doen*."). RB Noord-Nederland 16-10-2018, ECLI:NL:RBNNE:2018:4117, nam in wezen louter op grond van de periode waarin de strafbare

De gewoonte kan ook worden afgeleid uit andere feiten en omstandigheden dan (louter) het aantal afbeeldingen dat iemand in zijn bezit had. In zijn conclusie[249] bij HR 7-12-2010 stelde AG Vellinga dat de gewoonte van art. 240b, lid 2, Sr kan worden afgeleid uit:
- de pluraliteit/hoeveelheid van afbeeldingen[250];
- de duur van het bezit[251];

---

activiteiten hadden plaatsgevonden aan dat sprake was van het maken van een gewoonte: "*De rechtbank stelt vast dat er over een periode van 14 maanden in meer of minder (sic!) mate sprake is geweest van het downloaden en verspreiden van kinderporno. Hoewel de rechtbank, gelet op het ontbreken van de door verdachte gehanteerde USB-stick en het opschonen van de computer door verdachte, niet kan vaststellen wat de precieze omvang is geweest van het bezit en het door verdachte verspreide materiaal, is de rechtbank op basis van de bewezenverklaarde periode van oordeel dat sprake is geweest van een gewoonte maken van het zich toegang verschaffen tot, het in bezit hebben en verspreiden van kinderpornografisch materiaal*." Wat ons betreft verdient dit geen navolging als niet tenminste de globale omvang van het bezit etc. kan worden vastgesteld.

[249] Conclusie AG Vellinga (ECLI:NL:PHR:2010:BN8215) bij HR 7-12-2010, ECLI:NL:HR:2010:BN8215 (gewoonte maken van het bezit van gegevensdragers met kinderporno, gedurende 3 jaar afbeeldingen en films downloaden, opslaan en bewaren in vele mappen, op 2 harde schijven en op honderden dvd's, verzameling tot ongeveer 41.213 kinderpornografische multimediafiles; cassatieberoep verworpen). In dezelfde zin ook o.m. RB Overijssel 19-10-2017, ECLI:NL:RBOVE:2017:3926 ("gewoonte gemaakt" bewezenverklaard op grond van de langdurige periode van bezit, het kijk- en zoekgedrag van verdachte in die periode en zijn handelswijze met betrekking tot het verspreiden, aanbieden en uitvoeren); RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735 ("gewoonte" gezien de hoeveelheid afbeeldingen, de lengte van de periode waarin verdachte deze afbeeldingen verzamelde en de frequentie waarmee hij zich met het verzamelen van deze afbeeldingen bezig hield); RB Den Haag 28-2-2017 ECLI:NL:RBDHA:2017:1837 (*"Ter beantwoording van de vraag of verdachte van het vervaardigen van (feit 2) en bezit van (feiten 2 en 3) kinderpornografisch materiaal een gewoonte heeft gemaakt neemt de rechtbank tot uitgangspunt het aantal afbeeldingen, het aantal feitelijke handelingen, de frequentie daarvan in de bewezenverklaarde periode alsmede de duur van deze periode*").

[250] Zie o.m. RB Zeeland-West-Brabant, 14-7-2022, ECLI:NL:RBZWB:2022:3852 (gelet op het aantal kinderpornografische afbeeldingen (ruim 18.000) dat verdachte in zijn bezit heeft gehad, vervaardigd, of waartoe verdachte zich de toegang heeft verschaft, en de lange periode waarin verdachte deze handelingen heeft verricht). RB Oost-Brabant 27-3-2018, ECLI:NL:RBOBR:2018:1428 (14.300 bestanden, verdeeld over diverse gegevensdragers, in een periode van twee maanden gedownload). RB Noord-Nederland 21-10-2017, ECLI:NL:RBNNE:2017:4460 (meermalen per week tientallen bestanden met kinderpornografisch materiaal downloaden); Hof Den Haag 06-6-2011, ECLI:NL:GHSGR:2011:BR5919 (5537 afbeeldingen gedurende een jaar gedownload); RB Arnhem 21-02-2011, ECLI:NL:RBARN:2011:BP5151 (kinderporno, 21.000 afbeeldingen/multimediafiles, lange periode bezit)
Zie echter ook: Hof Amsterdam 04-5-2016, ECLI:NL:GHAMS:2016:1891 (het verspreiden van zeven kinderpornografische afbeeldingen aan één ander persoon is onvoldoende om te kunnen spreken van een gewoonte als bedoeld in art. 240b, tweede lid, Sr. vrijspraak); RB Den Haag 28-2-2017 ECLI:NL:RBDHA:2017:1837 ("aantal aangetroffen kinderpornografische afbeeldingen van verdachtes pleegkind (19 foto's, waarvan 1 dubbel), de tijdstippen waarop deze afbeeldingen werden vervaardigd (op 20, 21 en 23 augustus 2014 en – in ieder geval - op 10 augustus 2015) alsmede de lengte van de periode van het bezit (15 maanden) niet dusdanig zijn dat geoordeeld kan worden dat verdachte *een gewoonte heeft gemaakt"*. Vrijspraak).

[251] Zie o.m. Hof Den Bosch 15-10-2017, ECLI:NL:GHSHE:2017:3719 ("gewoonte maken" bewezen want: vanaf december 2011 bewust kinderporno in bezit, in 2012 en 2013 via Bullchat kinderporno geruild en de grote hoeveelheid aangetroffen kinderpornografisch materiaal); Hof Amsterdam 21-04-2016, ECLI:NL:GHAMS:2016:1566 (3045 afbeeldingen op een gegevensdrager (externe harde schijf) en 2 geautomatiseerde werken (een computer en een laptop) die op 2 *december 2014* in de woning van de verdachte zijn aangetroffen. verklaring van de verdachte dat hij dit materiaal vanaf *augustus 2014* (via een chatbox) heeft ontvangen en opgeslagen. "Ook als het hof rekening houdt met de omstandigheid dat een klein deel van het materiaal niet (meer) eenvoudig benaderbaar was én met de door de verdediging gestelde mogelijkheid van dubbeltelling, dan valt naar het oordeel van het hof de aan de verdachte verweten gedraging, gelet op de hoeveelheid materiaal *en de duur van de periode waarin de verdachte dat heeft verzameld*, te kwalificeren als het maken van een gewoonte van het bezit van kinderporno");
Geen gewoonte: RB Noord-Nederland 11-8-2022, ECLI:NL:RBNNE:2022:2875 ("*Evenmin kan worden bewezen dat hij op 17 januari 2022 een gewoonte heeft gemaakt van het overtreden van art. 240b Sr.*"). De tenlastelegging van door bestandscarving weer zichtbaar gemaakte "deleted files" was opvallend genoeg beperkt tot 1 dag. RB Oost-Brabant 12-4-2016, ECLI:NL:RBOBR:2016:1720 ("niet bewezen dat verdachte een

- de wijze waarop het bezit is verworven (in één of meer keren)[252]; en
- uit de omstandigheid dat de verdachte de afbeeldingen niet alleen heeft verzameld, maar deze ook heeft geordend.[253]
- de wijze van verkrijging en het al dan niet verrichten van handelingen met de betreffende afbeeldingen en de eventuele frequentie daarvan.[254]

Hierop voortbouwend stelde AG Aben (onder meer onder verwijzing naar zijn ambtgenoot Machielse[255]) in zijn conclusie bij HR 14 november 2017 tevens dat een individu van het bezit van kinderpornografisch materiaal een gewoonte kan maken vanwege de *hoeveelheid* kinderpornografische afbeeldingen en de *tijd* die gemoeid is geweest met het aanleggen van de verzameling.[256]

Voor het aannemen van *een gewoonte maken* ex. art. 240b lid 2 Sr is geen commercieel oogmerk vereist.[257] Indien sprake is van een *beroep maken* zal dit motief echter veelal wel aanwezig moeten zijn. In recentere jurisprudentie zien we diverse gevallen waarin dit onvoldoende lijkt te worden onderkend.[258] Zonder dat aan dit aspect aandacht wordt besteed, is in die gevallen ”een beroep of gewoonte maken”, bewezen verklaard, terwijl volstaan had kunnen worden met “een gewoonte maken”. Onzes inziens verdient dat de voorkeur gezien de uiteenlopende betekenis van beide begrippen.[259]

---

gewoonte heeft gemaakt van het in bezit hebben van kinderpornografisch materiaal. Uit de bewijsmiddelen in het dossier kan niet worden opgemaakt hoeveel keer of *welke tijd* ermee gemoeid is geweest om het aangetroffen materiaal te downloaden of te kopiëren.”); RB Noord-Nederland 29-4-2016, ECLI:NL:RBNNE:2016:2105 (forse hoeveelheid afbeeldingen in bezit en verspreid. Vrijspraak *gewoonte maken van* omdat niet kan worden vastgesteld wat de specifieke data zijn waarop de afbeeldingen op de gegevensdragers terecht zijn gekomen).

[252] Zie o.m. Hof Arnhem-Leeuwarden 22-7-2021, ECLI:NL:GHARL:2021:7281 (verwerping bewijsverweer m.b.t. ‘een gewoonte maken’, nu een gewoonte maken tevens kan bestaan uit het binnen een relatief kort tijdbestek herhaaldelijk plaatsvinden van art. 240b Sr-gerelateerde gedragingen).
Van “een gewoonte maken” werd vrijgesproken in: Hof Arnhem-Leeuwarden 26-6-2019, ECLI:NL:GHARL:2019:5380 (vrijspraak; “*Gelet op het feit dat de aanmaakdatum van de afbeeldingen in de representatieve selectie bij alle afbeeldingen gelijk is (…) en gelet op de overige stukken in het dossier, kan het hof niet vaststellen wanneer binnen de ten laste gelegde periode de afbeeldingen op de computer van verdachte zijn terechtgekomen en hoe de wijze van verwerving was, hoeveel tijd daarmee gemoeid is geweest, of sprake is geweest van het aanleggen van een verzameling en of verdachte verder iets met de afbeeldingen heeft gedaan*.”).

[253] Zie o.m. RB Utrecht 9-2-2011, ECLI:NL:RBUTR:2011:BP3760 (gewoonte; veel kinderpornobestanden aangetroffen op verschillende gegevensdragers**,** verdachte geeft aan dat hij verzamelaar is); RB Utrecht 26-7-2010, ECLI:NL:RBUTR:2010:BN5867 (gewoonte, obsessief *verzamelen*); Vgl. echter ook: RB Arnhem 24-6-2011, ECLI:NL:RBARN:2011:BQ9825 (onvoldoende bewijs gewoonte maken van bezit kinderporno, geen regelmatige updates dan wel aanvulling van verzameling).

[254] Zie Hof Amsterdam 22-11-2018 (publicatiedatum: 26-8-2022), ECLI:NL:GHAMS:2018:5238.

[255] A.J. Machielse in: Noyon, Langemeijer & Remmelink, *Het Wetboek van Strafrecht* (losbl.), aant. 7 bij art. 240b.

[256] Conclusie van AG Aben (ECLI:NL:PHR:2017:1227) bij HR 14-11-2017 (hof kon oordelen dat het gedurende een periode van enkele maanden opbouwen van een verzameling van 201 kinderpornografische afbeeldingen is “een gewoonte maken van”).

[257] Aldus Hof Den Haag 17-4-2007, ECLI:NL:GHSGR:2007:BA3188 (het hof leidt dit af uit de relevante jurisprudentie en de strekking van art. 240b Sr (hoofdzakelijk het tegengaan van seksueel misbruik van jeugdigen)).

[258] Zie o.m. RB Amsterdam 30-9-2021, ECLI:NL:RBMNE:2021:4785; RB Midden-Nederland 30-6-2021, ECLI:NL:RBMNE:2021:2767 en RB Amsterdam 23-4-2021, ECLI:NL:RBAMS:2021:2011, waarin telkens “beroep of gewoonte maken” is bewezenverklaard, zonder dat duidelijk is waarop deze keuze berust.

[259] Zie voor een voorbeeld waarin mede is veroordeeld voor “een beroep maken”: RB Alkmaar 17-3-2011, ECLI:NL:RBALK:2011:BP8253 (beroepsmatig (in vof-verband) exploiteren van internetsites in welk verband grote hoeveelheden pornografisch materiaal van jonge modellen vanaf nieuwsgroepen op internet werden binnengehaald).

HOOFDSTUK 4: (VOORWAARDELIJK) OPZET OP HET MISDRIJF VAN ART. 240B SR

Technisch lemma: enige basisbeginselen van de werking van een computer

De taak van een computer (maar in wezen van ieder digitaal device, zodat het navolgende in grote lijnen niet alleen voor computers geldt) is in de kern het geautomatiseerd verwerken van daartoe ingevoerde gegevens (*input*), en de resultaten van die verwerking weer uit te voeren (*output*). Om deze taak te kunnen uitvoeren heeft een computer een aantal componenten, de zogenaamde hardware. Deze componenten kunnen slechts hun taak vervullen door met elkaar samen te werken. Om deze samenwerking mogelijk te maken wordt gebruik gemaakt van programma's, aangeduid als software. Feitelijk bestaat software uit lange reeksen van instructies in computercode.

Hardware: CPU en RAM(-cache) en ROM-geheugens
De hardware van een computer bestaat in de kern uit een CPU (Central Processing Unit, vaak aangeduid als de *processor*). Deze CPU communiceert aan de ene kant met het werkgeheugen en aan de andere kant met de randapparatuur zoals een printer, een monitor, een toetsenbord en muis, een wifi-router en meer permanente vormen van geheugenopslag zoals hard drives.

In iedere computer zit een CPU. Elke CPU heeft weer verbinding met meerdere elektronische modaliteiten (in de vorm van speciale chips) voor gegevensopslag, samen veelal het geheugen genoemd. Welke vorm die gegevensopslag heeft, is vooral afhankelijk van de vraag of die opslag voor langere of slechts voor korte tijd nodig is. Op iedere computer is in ieder geval een type geheugen (in de vorm van RAM-chips) aanwezig dat het RAM (*random-access memory*)-geheugen wordt genoemd. Dit RAM-geheugen vormt de basis voor het werkgeheugen van een computer. Kenmerkend aan het RAM-geheugen is dat elk stukje informatie in een dergelijk geheugen direct voor de CPU bereikbaar is. Er hoeft dus niet langs een van te voren bepaalde route naar gegevens gezocht te worden, zoals bijvoorbeeld bij een magnetische harde schijf (HDD, hard disk drive) wel het geval is. Daarom werkt RAM-geheugen veel sneller dan een HDD. Dat verschil wordt steeds kleiner door de toepassing van elektronische harde schijven (SSD, solid state drive). Deze laatste werken grosso modo hetzelfde als RAM-geheugen, zij het (iets) trager, maar de informatie erop blijft wel permanent bewaard. Nadeel van RAM-geheugen is dat de hoeveelheid data die daarop kan worden opgeslagen in verhouding tot bijvoorbeeld de opslagruimte op een hard disk aanmerkelijk beperkter is. Ook wordt de informatie in het RAM-geheugen normaliter niet permanent bewaard. Als de computer wordt uitgezet dan is de in het RAM-geheugen opgeslagen informatie veelal verdwenen, hoewel het kan voorkomen dat gedeelten van die informatie nog wel met speciale forensische software zijn terug te halen, of dat elders in de computer verwijzingen zijn opgeslagen naar de informatie die in het RAM-geheugen heeft gestaan. Vanwege de specifieke eigenschappen (en beperkingen) van het RAM-geheugen is de belangrijkste functie daarvan het opslaan van de op een bepaald moment in werking zijnde programma's en van eventuele andere gegevens die voor de werking van die programma's of van de computer voortdurend en snel nodig zijn.

Behalve met het RAM-geheugen heeft de CPU ook altijd verbinding met één of meer types ROM (read-only memory)-geheugen, meestal gesitueerd in speciale chips op het moederbord. Gegevens in een ROM-geheugen zijn in beginsel permanent, en in een niet veranderende vorm, opgeslagen. De CPU van de computer kan ze dus alleen maar lezen. Deze gegevens verdwijnen ook niet als de computer wordt uitgezet. Om die reden wordt in het ROM-geheugen veelal de voor de werking van elektronica in de computer benodigde software (*firmware*) opgeslagen. In forensisch opzicht zijn gegevens in het ROM-geheugen veelal niet interessant nu deze geen informatie omtrent het handelen van de gebruiker zullen bevatten.

Daarnaast beschikken veel *devices* ook over de mogelijkheid om gegevens op een zogenaamd extern geheugen zoals bijvoorbeeld een hard disk, een usb-stick, een dvd, een geheugenkaartje enz. op te slaan. Een grijs gebied vormt opslag op apparaten die min of meer permanent aan een device worden gekoppeld, zoals een geheugenkaartje of sommige externe harde schijven.

Software: BIOS/UEFI en het besturingssysteem
Om een computer te laten werken moet daarop altijd een zogenaamd besturingssysteem (operating system) zijn geïnstalleerd. Meestal is dit een variant van Microsoft Windows, zoals bijvoorbeeld Windows 10 en op

Apple computers een variant van OSX (meest recent Ventura[260]). Op smartphones en tablets wordt nagenoeg altijd als besturingssysteem een variant van Apple iOS, van Android of van Windows Mobile gebruikt.

Het besturingssysteem wordt – in ieder geval op PC's en laptops – opgeslagen op de harde schijf van de computer. Een van de functies van het besturingssysteem is het laten communiceren van de computer/CPU met de randapparatuur. Daarnaast staat er op de zogenaamde bootsector in een (al dan niet speciaal daarvoor aangebrachte chip met) ROM-geheugen van – wederom in ieder geval PC's en laptops – een gespecialiseerd programma, genaamd BIOS (inmiddels komt opvolger UEFI steeds vaker voor). Het zorgt er onder meer voor dat elke keer dat de computer wordt opgestart het besturingssysteem (gewoonlijk vanaf de hard drive) wordt geladen in het RAM-geheugen en de computer dus weet wat hij moet doen nadat hij is aangezet.
Daarbij worden ook de verbindingen met de randapparatuur getest en bepaalde standaardgegevens zoals de systeemtijd geregistreerd. Het hele proces van opstarten van een computer door middel van het laden van het besturingsprogramma en het verbinden met de randapparatuur wordt veelal het *booten* (of *booting up*) genoemd. Anders dan voor het besturingssysteem geldt dat voor de gebruiker van een computer het BIOS/UEFI doorgaans ongemerkt functioneert.

Wanneer een programma wordt gestart, dan wordt het eerst van de harde schijf (of een andere geheugenlocatie) gelezen en in het RAM-geheugen gezet. Pas daarna begint de CPU met het uitvoeren van het programma. Een programma bestaat uit een lange reeks instructies die één voor één naar de CPU worden gestuurd, die deze vervolgens precies in die volgorde uitvoert. Omdat bijvoorbeeld een besturingssysteem als Windows 11 (feitelijk ook een complex programma) zeer omvangrijk is[261], duurt het wel enige tijd voordat alle instructies doorlopen zijn en het systeem daadwerkelijk kan worden gebruikt.

Naast het besturingssysteem is op een computer ook nog andere, op het gebruik door die specifieke gebruiker gerichte, software in de vorm van programma's/applicaties aanwezig. Een gedeelte van die programma's wordt geleverd bij het desbetreffende besturingssysteem, zoals de browser Safari bij Mac OSX. De gebruiker kan uiteraard zelf andere programma's installeren, als de softwareleverancier een versie voor het betreffende besturingssysteem beschikbaar heeft gesteld.

Al deze programma's hebben hun eigen specifieke wijze hoe zij gegevens verwerken en al dan niet tijdelijk opslaan. De eigenaren van softwareprogramma's zijn niet altijd bereid om de gegevens daaromtrent te delen met bijvoorbeeld opsporingsdiensten. Naar Nederlands recht zijn zij ook niet verplicht die informatie vrij te geven, hoewel sommigen wel vrijwillig medewerking verlenen. Dat betekent dat niet zelden zelfs voor forensisch deskundigen de precieze werking van een programma niet geheel kan worden doorgrond, wat vooral bij de (juridisch veelal uiterst relevante) vraag of bij het gebruik van een bepaald programma bepaalde handelingen gericht door een gebruiker zijn uitgevoerd, dan wel geautomatiseerd of automatisch door het programma zelf, problematisch kan zijn. Een ander probleem dat zich met enige regelmaat voordoet is dat een deskundige een versie van bepaalde software dient te onderzoeken die ten tijde van het tenlastegelegde in gebruik was, maar dat die software niet meer beschikbaar is of eerst via een internetverbinding geüpdatet dient te worden naar de nieuwste versie voordat deze gebruikt kan worden.

4.0. Algemene aspecten van opzet in relatie tot art. 240b Sr

Tegen een verdenking van overtreding van art. 240b Sr, in het bijzonder tegen een verwijt dat men kinderporno *in bezit* heeft gehad, worden vaak verweren gevoerd. Veel van die verweren komen erop neer dat de verdachte niet betwist dat er kinderpornografisch materiaal op zijn computer staat, en dat hij dat materiaal dus feitelijk in zijn bezit had, maar dat hij stelt dat dit bezit niet opzettelijk was. Omdat voor het bewijs van een misdrijf altijd ook opzet moet worden bewezen, zal honorering van dit verweer tot vrijspraak (moeten) leiden.
Vanzelfsprekend omvat opzet hier ook het zogenaamde 'voorwaardelijk opzet', "*het willens en wetens de aanmerkelijke kans aanvaarden dat men het betreffende misdrijf zal plegen*".[262]

---

[260] Uitgebracht op 24 oktober 2022.
[261] Ter illustratie: om de omvang van software inzichtelijk te maken wordt wel gesproken in eenheden van een miljoen regels code, waarbij elke miljoen regels overeenkomt met ongeveer 18.000 A4-pagina's met programmeertaal. Zo beslaat Windows 11 (uit het jaar 2021) ongeveer 50 miljoen regels code en bevat een moderne luxe auto 100 miljoen regels code. Zie bijv.: https://informationisbeautiful.net/visualizations/million-lines-of-code/.
[262] Vaste rechtspraak; zie ook o.m. de conclusie van AG Knigge ECLI:NL:PHR:2006:AU9104 bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104.

Of sprake was van opzet wordt in het strafrecht veelal beoordeeld aan de hand van de uiterlijke verschijningsvorm van iemands gedragingen. Zo zal bij een verdachte die in een zoekmachine als Google de zoektermen "*sex pre-teens*" invoert, en vervolgens op een website met kinderpornografisch materiaal belandt, door de strafrechter zonder twijfel opzet worden aangenomen. Door zulke termen in te voeren, neemt de betrokkene immers op zijn minst de aanmerkelijke kans voor lief dat hij naar dergelijk materiaal zal worden geleid.[263] Toch zal het niet altijd zo eenvoudig liggen, bijvoorbeeld omdat niet altijd een verband kan worden gelegd tussen dergelijk zoekgedrag en aangetroffen bestanden.[264]

In de context van art. 240b Sr blijkt onder meer uit de jurisprudentieanalyse van Stevens en Koops[265] met betrekking tot deze bepaling, dat bij de vaststelling of sprake is van opzet op het bezit van kinderpornografische afbeeldingen drie elementen kunnen worden onderscheiden: *kennen* (in de zin van zich in meer of mindere mate bewust zijn van de aanwezigheid van dergelijke afbeeldingen op een of meer van zijn gegevensdragers), *kunnen* (in de zin van de beschikkingsmacht hebben over de betreffende afbeeldingen) en *willen* (in de zin van de bedoeling hebben deze afbeeldingen te bewaren, dan wel het nemen van onvoldoende maatregelen om na ontvangst van de afbeeldingen deze weer te verwijderen). Hierop voortbouwend geven Stevens en Koops ook een overkoepelend criterium: "*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*". Hoewel de publicatie van Koops c.s. waarin dit criterium is genoemd dateert uit 2009, geeft dit criterium onzes inziens ook thans nog de heersende rechtsopvatting weer.

Daarop aansluitend hebben verweren betreffende (het ontbreken van) opzet in art. 240b-zaken meestal betrekking op een of meer van de volgende aspecten:

a. men stelt geen *wetenschap* te hebben gehad van de aanwezigheid van het materiaal. Het gaat hierbij allereerst om verweren inhoudende dat een ander dan de verdachte de op de computer van de verdachte aangetroffen bestanden heeft gedownload (of met die computer websites met strafbaar materiaal heeft bezocht). Maar ook om verweren dat het aangetroffen kinderpornografisch materiaal buiten de verdachte om 'automatisch' (bijv. door gebruik van *P2P*- en/of torrent-software) op zijn computer terecht zou zijn gekomen;
b. men stelt geen *beschikkingsmacht* over het strafbare materiaal te hebben gehad. Hierbij gaat het vooral om verweren, inhoudende dat het (na gebruikmaking door de politie van forensische software) op de computer aangetroffen materiaal niet (meer) voor de verdachte zelf toegankelijk was;
c. men stelt de aanwezigheid (enz.) van het aanwezige materiaal niet *gewild* te hebben.

---

[263] Zie bijvoorbeeld Hof Arnhem-Leeuwarden 18-3-2015, ECLI:NL:GHARL:2015:2016 (zich toegang verschaffen tot kinderporno door het ingeven van op porno gerichte zoektermen in Google. Verdachte wist en verwachtte dat hij vervolgens ook kinderporno zou aantreffen).

[264] Zie o.m. RB Zeeland-West-Brabant 25-3-2021, ECLI:NL:RBZWB:2021:1421 ("*Onderzoek aan de gsm van verdachte heeft uitgewezen dat daarin zoektermen zijn gebruikt die zouden kunnen worden geïnterpreteerd als zoektermen die zien op kinderporno. De kans bestaat dat deze zoektermen treffers opleveren die bestaan uit 18+ -pornografisch materiaal. Op de gsm van verdachte zijn geen kinderpornografische bestanden aangetroffen. Deze onderzoeksgegevens zijn dan ook naar het oordeel van de rechtbank niet redengevend voor het bewijs. Hetzelfde geldt voor de aangetroffen chatgesprekken van ' [naam 2] ' met anderen, nu onvoldoende is komen vast te staan dat ' [naam 2] ' of één van de andere gespreksdeelnemers verdachte betreft."*).

[265] Stevens, L. & Koops, B.J., *'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno'*, Delikt en Delinkwent 2009, afl. 7/51, p. 669 e.v.; Grotendeels in dezelfde zin: AG Knigge in zijn conclusie (ECLI:NL:PHR:2006:AU9104) bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104.

> Onder deze categorie vallen onder meer verweren dat het aangetroffen materiaal als onbedoelde "bijvangst" met gedownload gewoon (= legaal volwassenen) pornografisch materiaal zou zijn meegekomen en/of dat men dacht het materiaal geheel verwijderd te hebben.

Deze verweren (die zich in meerdere varianten kunnen aandienen) worden in de volgende paragrafen 4.1 tot en met 4.3 nader besproken.

Daarnaast wordt ook langs een andere weg verweer gevoerd over (het ontbreken van) opzet. Daarbij gaat het in de regel om verweren die inhouden dat de verdachte er zich niet van bewust was dat het materiaal pornografisch was, dan wel dat de op het materiaal afgebeelde personen jonger dan 18 jaar waren. Deze aspecten worden hierna in paragraaf 4.4. besproken.

4.1. (Min of meer bewuste) wetenschap van het bezit

Uit de omvangrijke jurisprudentie ter zake kunnen diverse criteria c.q. aanwijzingen worden afgeleid die de rechter kan betrekken bij de beantwoording van de vraag of bij de verdachte sprake is geweest van "wetenschap" (in de zin van bewustheid) dat zich kinderpornografische afbeeldingen bevonden op geautomatiseerde werken en/of gegevensdragers waarover de verdachte beschikkingsmacht had, dan wel dat daarmee bepaalde handelingen (zoals verspreiding) zijn verricht.
Hierbij passen twee inleidende opmerkingen. Allereerst dat het hier niet om "wetenschap" in de meest strikte zin van het woord behoeft te gaan; ook uit het verrichten van handelingen waarvan redelijkerwijs kan worden verwacht dat deze zullen leiden tot het op een gegevensdrager vastleggen van kinderpornografische afbeeldingen, wordt, als deze vastlegging is gevolgd, maar die vastlegging verder niet is waargenomen of gecontroleerd door de betrokkene, *de jure* als wetenschap (mede in de zin van min of meer bewuste vastlegging) aangemerkt.
Ten tweede dat uit de vaststelling dat bepaalde kinderpornografische afbeeldingen bewust zijn vastgelegd op een geautomatiseerd werk of gegevensdrager, en dat de gebruiker van dat apparaat zich daarvan bewust was of moet zijn geweest, nog niet noodzakelijkerwijs behoeft te volgen dat *de verdachte* die betreffende gebruiker was.

4.1.1. Digitaal forensische aanwijzingen voor "wetenschap"/ "bewuste vastlegging"

Het verrichte digitaal forensische onderzoek geeft vaak belangrijke aanwijzingen voor de beoordeling of de verdachte wetenschap heeft gehad c.q. zich bewust is geweest van de hem ten laste gelegde gedragingen met het betreffende kinderpornografische materiaal. In het bijzonder gaat het daarbij om aanwijzingen, waaruit blijkt wie de afbeeldingen op het geautomatiseerde werk en/of de gegevensdrager heeft vastgelegd[266] (en hoe dat gebeurd is) en wie deze heeft geopend (dat impliceert immers kennisname)[267], gedeeld of verspreid.

---

[266] Vastlegging impliceert immers een bewuste handeling t.a.v. het betreffende bestand. Zie omtrent de opzet op het kinderpornografisch karakter van een vastgelegd bestand hierna onder 4.3. Vastlegging is echter niet zonder meer voldoende bewijs voor opzet indien een incidenteel kinderpornografisch bestand na vastlegging of kennisname vrijwel direct weer effectief is verwijderd; zie hierna verder onder 4.3.2.

[267] Bij digitaal forensisch onderzoek wordt in dit kader ook wel onderzoek ingesteld naar de inhoud van het logbestand/de cache van Windows Media Player. Indien namelijk afbeeldingen/video's worden afgespeeld in de Windows Media Player wordt in het logbestand van deze applicatie als regel de bestandsnaam van de door middel van deze player afgespeelde afbeeldings- en videobestanden geregistreerd. Deze registratie blijft normaliter staan, zelfs nadat de betreffende afbeelding/video zelf van de computer is verwijderd. Een dergelijke registratie impliceert derhalve dat de gebruiker de afbeelding/de video ook daadwerkelijk heeft *gezien*, en zal derhalve in de regel als bewijzend voor de wetenschap bij die gebruiker van het kinderpornografisch karakter van de afbeelding/video kunnen worden aangemerkt.

Bij dergelijke aanwijzingen kan onder meer gedacht worden aan:

- *de bestandsnaam van de afbeelding;*
  Een bestandsnaam geeft soms reeds een aanduiding van de aard en/of inhoud van een afbeelding, of daaruit kan blijken (of kan worden afgeleid) dat de bestandsnaam specifiek aan de afbeelding is toebedeeld door de gebruiker zelf.
- *de plaats, aard en naam van de map waarin de kinderpornografische afbeelding is aangetroffen;*
  Als de afbeeldingen zijn opgeslagen in een door de gebruiker zelf gecreëerde en/of van een eigen naam en/of wachtwoord voorziene en/of een tot de gebruiker te herleiden map of mappenstructuur is dat een zeer sterke aanwijzing dat de gebruiker wetenschap had van de aanwezigheid van de betreffende afbeeldingen[268]; als daarentegen de afbeeldingen zijn opgeslagen in mappen waarin materiaal automatisch wordt opgeslagen, of ook na verwijdering door de gebruiker aanwezig blijft (in *unallocated clusters*) hoeft dat niet zonder meer het geval te zijn.
- *de wijze waarop de kinderpornografische afbeelding op een gegevensdrager terecht is gekomen; in het bijzonder of dit automatisch is gebeurd, dan wel als gevolg van een bewuste handeling*[269]*;*
  Bij bewuste handeling kan allereerst worden gedacht aan handelingen die wijzen op een bijzondere belangstelling voor kinderpornografie, zoals het bezoeken van (al dan niet afgeschermde) websites, forums, nieuwgroepen en chatrooms waarop of via welke afbeeldingen op dat terrein beschikbaar zijn of kunnen worden verkregen; het betalen voor toegang tot een specifieke website; het gebruik van bepaalde op *kinder*pornografie gerichte zoektermen[270]; het zelf gemaakt of bewerkt hebben van afbeeldingen enz. Ook uit het feit dat de gebruiker bepaalde afbeeldingen heeft overgezet op of gekopieerd naar andere gegevensdragers of naar specifieke andere

---

[268] Zie o.m. RB Noord-Holland 29-6-2017 ECLI:NL:RBNHO:2017:5547 (verdachte heeft meerdere mappen aangemaakt met onder meer de namen 'girls9' 'girls11' en 'girls13'; minimaal voorwaardelijk opzet op bezit kinderpornografie); RB Oost-Brabant 27-5-2016, ECLI:NL:RBOBR:2016:2719 (rechtbank verwerpt de stelling dat de kinderpornografische afbeeldingen wellicht ongevraagd aan hem zijn toegezonden door personen waarmee hij (erotische) chats voerde nu de kinderpornografische afbeeldingen opgeslagen waren op de computer van verdachte in de hiervoor bedoelde *mappenstructuur;* RB Noord-Nederland 6-5-2021, ECLI:NL:RBNNE:2021:1748 ("*De omstandigheid dat het bestandspad "[naam]" op de computer van verdachte is aangetroffen duidt er naar het oordeel van de rechtbank op dat verdachte zich bezig hield met het verwerven van kinderpornografisch materiaal. Ook het bestandspad "[naam]" duidt daar op. In beide bestandspaden komt de naam '[verdachte]' voor en dat is de roepnaam van verdachte*.").

[269] Opgemerkt moet hier worden dat de enkele bewuste vastlegging van een naar uit onderzoek blijkt kinderpornografisch bestand door de verdachte nog niet zonder meer ook opzet constitueert. In het bijzonder kan dit kwestieus zijn indien een incidenteel kinderpornografisch bestand na vastlegging of kennisname vrijwel direct weer effectief is verwijderd; zie hierover verder hierna onder 4.3.2. Zie omtrent de vraag in hoeverre bij vastlegging de opzet ook gericht moet zijn geweest op het kinderpornografisch karakter van een vastgelegd bestand hierna onder 4.4.

[270] Zie bijvoorbeeld HR 8-5-2001, ECLI:NL:HR:2001:AB1517 (bewuste vastlegging kinderporno, voorwaardelijk opzet, zoeken naar en vastleggen porno via nieuwsgroepen als 'alt.sex.pre-teens'); Hof Arnhem 12-4-2012, ECLI:NL:GHARN:2012:1131 (verdachte zocht bewust met o.m. de term "teens" naar porno en haalde grote aantallen bestanden tegelijk binnen); RB Noord-Holland 29-6-2017, ECLI:NL:RBNHO:2017:5547 (verdachte heeft op een bepaalde internetsite gezocht op de termen 'teen' en 'under 13'); RB Arnhem 26-10-2010, ECLI:NL:RBARN:2010:BO1711 (bewuste vastlegging in mappen met zelf gekozen namen op D-schijf). Aandacht hierbij verdient wel dat het dan wel moet gaan om op *kinder*porno gerichte zoektermen, hetwelk bepaald niet zonder meer kan worden gelijkgesteld met op gewone porno gerichte zoektermen; aldus ook o.m. RB Midden-Nederland 28-1-2014, ECLI:NL:RBMNE:2014:259 (o.a. vrijspraak van zich toegang verschaffen tot kinderporno omdat de verdachte geen andere handelingen heeft verricht dan een op porno gerichte zoekterm in Google opgeven) en HR 26-10-2010, ECLI:NL:HR:2010:BO1713 (uit gebezigde bewijsmiddelen (w.o. die met betrekking tot downloaden van veel porno) kan niet worden afgeleid dat het (voorwaardelijk) opzet van de verdachte was gericht op het in het bezit hebben van de bewezenverklaarde *kinder*pornografische afbeelding).

mappen op een gegevensdrager, of deze afbeeldingen heeft verspreid, volgt minimaal het sterke vermoeden dat de gebruiker zich bewust was van de aanwezigheid van deze afbeeldingen. Voor de beoordeling of kinderpornografische afbeeldingen automatisch of door middel van een bewuste handeling op de gegevensdrager is terechtgekomen, kunnen de (standaard)instellingen van gebruikte software of applicaties relevant zijn.[271]

- *het door de verdachte één of meermalen openen van de betreffende kinderpornografische bestanden (en het/de tijdstip(pen) waarop dat gebeurd is);*
  Het openen van een bestand is een bewuste handeling waarna van de inhoud van het bestand wordt kennisgenomen; daarna moet diegene die het bestand heeft geopend zich dus van de aanwezigheid bewust zijn.
- *de bevinding dat kinderpornografische afbeeldingen op verschillende tijdstippen op de gegevensdrager zijn opgeslagen;*
  De bevinding dat kinderpornografische afbeeldingen op meerdere momenten zijn opgeslagen kan een aanwijzing zijn dat er sprake is geweest van een bijzondere en/of gerichte belangstelling voor dergelijk materiaal. Dat kan anders zijn, indien gebruik is gemaakt van "geautomatiseerde zoeksoftware" (zoals Gigatribe) waarmee zonder tussenkomst van de gebruiker voortdurend op bepaalde vooraf ingegeven zoektermen wordt gezocht, en waarvan de resultaten vervolgens ook geautomatiseerd worden gedownload naar de computer van de gebruiker. Indien een zoekterm is ingegeven die kinderpornogerelateerd is zal zulks echter weer wel een belangrijke aanwijzing zijn dat sprake is geweest van bewust, op het verkrijgen van kinderpornografisch materiaal gericht, handelen.
- *de hoeveelheid kinderpornografisch materiaal die is aangetroffen en de plaatsen waar dat materiaal is opgeslagen;*
  Een grote hoeveelheid materiaal vormt een aanwijzing voor bijzondere belangstelling voor kinderpornografie. In het bijzonder geldt dit als het materiaal op meerdere gegevensdragers is opgeslagen, omdat zulks impliceert dat er meermalen handelingen moeten zijn verricht om het materiaal aldus opgeslagen te krijgen. Voorzichtigheid is echter geboden indien gebruik is gemaakt van geautomatiseerde zoeksoftware. Bij gebruik van dergelijke software kunnen na een eenmalige invoer van een of meer zoektermen soms in zeer korte tijd zeer grote hoeveelheden digitaal materiaal geautomatiseerd worden gedownload. In een dergelijk geval kan dus niet reeds op basis van de aangetroffen *hoeveelheid* materiaal worden geconcludeerd dat ook sprake was van opzet op de aanwezigheid daarvan.[272]
  Omgekeerd kan geconstateerd worden dat een klein aantal kinderpornografische afbeeldingen is gedownload/aangetroffen, maar zulks naast een groot aantal volwassenen pornografische afbeeldingen of andere bestanden. Zeker indien gebruik is gemaakt van p2p-software als Gigatribe of vele archiefbestanden (zip, rar e.d.) zijn gedownload dient dit tot voorzichtigheid te leiden omtrent de aanwezigheid van opzet met betrekking tot de aanwezigheid van opzet op het bezit van *kinder*porno. De

---

[271] RB Den Haag 28-11-2022, ECLI:NL:RBDHA:2022:12655 ("*Het opslaan van een sticker is een bewuste handeling*."). De rechtbank stelt vast dat 1 kinderpornografische afbeelding als 'sticker' (kort gezegd: bewerkte afbeeldingen (uitsneden) die via een chatapplicatie, zoals WhatsApp, kunnen worden verstuurd) is opgeslagen, waarbij in het midden wordt gelaten welke applicatie daarvoor is gebruikt. Nu het gaat om een telefoon, zou het om de applicatie WhatsApp kunnen gaan. De overweging dat het opslaan van een sticker een bewuste handeling (van de gebruiker) is, lijkt ons in het geval van WhatsApp correct nu via WhatsApp ontvangen stickers pas worden geopend als de gebruiker daartoe een handeling verricht. Voor andere applicaties kan dit anders zijn, bijvoorbeeld indien stickers automatisch worden opgeslagen.

[272] Dat ligt vanzelfsprekend anders als de zoektermen duidelijk kinderporno gerelateerd zijn en/of blijkt dat (een deel van) de bestanden ook zijn geopend en daarna niet zijn verwijderd.

> kinderpornografische afbeeldingen zouden dan namelijk door de gebruiker niet beoogde en onvoorziene "bijvangst" kunnen zijn.[273]

Indien sprake is van "*het zich via een geautomatiseerd werk toegang verschaffen tot kinderpornografische afbeeldingen*" zal de aanwezigheid van de wetenschap/bewustheid moeten worden beoordeeld aan de hand van hetgeen bekend[274] is omtrent het zoekgedrag van de verdachte, waarbij onder meer acht kan worden geslagen op elementen als de gebruikte zoektermen, namen van de bezochte websites, de frequentie waarmee websites en andere internetlocaties met kinderpornografisch materiaal zijn gezocht en bezocht, of daarvoor betaald is en of er communicatie met derden is geweest waarbij is gesproken over het karakter van de betreffende websites of afbeeldingen.[275]

4.1.2. "De afbeeldingen zijn door een ander of anderszins zonder mijn weten (geautomatiseerd) op mijn computer/gegevensdrager geplaatst"

Door de ontwikkeling van de digitaal-forensische opsporingstechnieken zal in veel gevallen waarin art. 240b-zaken aan de rechter worden voorgelegd weinig discussie bestaan over de vraag of op een bepaalde computer kinderpornografisch materiaal aanwezig was, en hoe dit technisch gezien op de betreffende computer(s) of gegevensdrager(s) is vastgelegd.
Deze ontwikkeling vertaalt zich ook in een verschuiving van de aard van de door verdachten in deze zaken gevoerde verweren. Steeds vaker betreffen deze niet zozeer de vraag of er kinderpornografische afbeeldingen op een bepaalde computer/gegevensdrager zijn aangetroffen, maar de vraag of deze daarop terecht zijn gekomen door handelingen van *de verdachte* c.q. als gevolg van aan *de verdachte* toe te rekenen handelingen.
Vooraleerst gaat het dan veelal om verweren in de sfeer van: "mijn computer was gehackt" of "een ander heeft mijn computer gebruikt". Ook wordt wel aangevoerd dat het materiaal al aanwezig was op door de verdachte van anderen verkregen computers en/of gegevensdragers. In essentie is dan het verweer dat (een) ander(e) *perso(o)n(en)* dan verdachte de gewraakte afbeeldingen heeft/hebben vastgelegd/verspreid (enz.).
Daarnaast gaat het om verweren welke inhouden dat bepaalde *software* buiten de wil en wetenschap van de verdachte "automatisch" bepaalde kinderpornografische bestanden op zijn computer(s) en/of gegevensdragers zou hebben vastgelegd. Gezien de oplopende frequentie waarmee dergelijke verweren worden gevoerd wordt hierop in de navolgende paragrafen uitvoeriger ingegaan.

---

[273] Zie o.m. HR 26-10-2010, ECLI:NL:HR:2010:BO1713 (1 kinderpornografische film; volgens verdachte nooit bewust gedownload en/of door hem gezien, kennelijk "meegekomen" met downloaden van veel porno; HR casseert omdat uit bewijsmiddelen geen (voorwaardelijk) opzet kan blijken op downloaden *kinder*porno); RB Den Haag 29-2-2008, ECLI:NL:RBSGR:2008:BC5528 (geen bewuste vastlegging, automatische opslag door downloadprogramma LimeWire, automatisch aangemaakte map 'Music Incomplete', vijf bestanden, geen opzet op bezit); zie met betrekking tot de "bijvangst"-problematiek verder hierna onder 4.1.3.1.
[274] Die informatie kan zijn verkregen uit digitale sporen en/of uit verklaringen van de verdachte of getuigen.
[275] Zie in deze zin ook: Hof Den Haag 6-10-2017, ECLI:NL:GHDHA:2017:2853 (e-archief) ("*Gelet op het aantal bezochte websites, de frequentie van het bezoek aan deze sites, de duur van het bezoek aan deze sites, het tijdstip waarop deze sites zijn bezocht, de voor verdachte als kinderporno kenbare inhoud van deze sites en het terugkerende karakter van de bezoeken aan veelal dezelfde sites is het hof van oordeel dat de verdachte deze websites opzettelijk bezocht heeft en tevens opzettelijk op deze sites heeft gebrowsed met het kennelijke doel kennis te nemen van kinderpornografische afbeeldingen van kennelijk minderjarige jongens. Derhalve komt het hof tot de conclusie dat de verdachte zich opzettelijk de toegang tot de sites waarop kinderpornografische afbeeldingen zijn afgebeeld heeft verschaft.*") en RB Noord-Holland 29-6-2017, ECLI:NL:RBNHO:2017:5547 (Uit de internetgeschiedenis van de tablet blijkt dat verdachte op een bepaalde internetsite heeft gezocht op de termen 'teen' en 'under 13'. Voorts heeft verdachte meerdere mappen aangemaakt met onder meer de namen 'girls9' 'girls11' en 'girls13'. Verdachte wist dan ook, of heeft tenminste bewust de aanmerkelijke kans aanvaard, dat de tablet kinderpornografisch materiaal bevatte. Verdachte heeft daarmee opzettelijk, al dan niet in voorwaardelijke vorm, kinderporno in zijn bezit gehad.).

4.1.2.1. Beoordelingsmaatstaf voor dergelijke verweren

In de hedendaagse digitale wereld kan zo goed als niets met 100% zekerheid worden uitgesloten. Het binnendringen van een computer (een "*hack"*) kan hebben plaatsgevonden zonder dat daarna nog digitale sporen daarvan worden aangetroffen. Evenzo kunnen derden iemands computer hebben gebruikt (bijvoorbeeld door zijn stiekem afgelezen wachtwoord te gebruiken), zonder dat zulks nog achteraf valt vast te stellen.

Bij de beoordeling van een dergelijk verweer behoort derhalve niet als maatstaf te worden aangelegd of kan worden "*uitgesloten"*[276]*,* "*de mogelijkheid aanwezig is*"[277] of "*onvoldoende kan worden weerlegd*"[278] dat een bepaalde computer gehackt is, maar of – alle feiten en omstandigheden in ogenschouw nemende – dit verweer al dan niet in meer of mindere mate aannemelijk is geworden.[279] Evenzo dient de rechter zich hierbij niet al te zeer te laten leiden (dan wel in verwarring te laten brengen) door hetgeen allemaal wel niet op ICT-terrein mogelijk zou zijn en/of door rapporten van deskundigen van de verdediging die *in zijn algemeenheid* schetsen wat zich bijvoorbeeld op het gebied van "hacken" zou kunnen hebben voorgedaan.[280] Met advocaat-generaal Machielse zouden wij menen dat de strafrechter, behoudens sterke aanwijzingen voor het tegendeel, ervan mag uitgaan dat op een computer (of met een wachtwoord beveiligde cloudopslag[281]) aangetroffen gedownloade of gekopieerde bestanden zijn gedownload c.q. gekopieerd door de eigenaar/vaste gebruiker van die computer. Evenzo mag de rechter er – wederom behoudens sterke aanwijzingen voor het tegendeel – van uitgaan dat wanneer uit nadere (meta)data blijkt dat bepaalde sites zijn benaderd en/of bestanden zijn gedownload, geopend, gekopieerd en/of afgespeeld die handelingen zijn uitgevoerd door degene die van die laptop de gebruiker of eigenaar is.[282]

---

[276] In dit licht minder juist lijken derhalve de motiveringen van o.m. RB Midden-Nederland 21-10-2013, ECLI:NL:RBMNE:2013:5232 (vrijspraak bezit kinder- en dierenporno nu *niet valt uit te sluiten* dat een andere gebruiker van de computer dan de verdachte de afbeeldingen heeft gedownload) en RB Zutphen 12-1-2011, ECLI:NL:RBZUT:2011:BP0616 (vrijspraak bezit kinderporno; het valt *niet uit te sluiten* dat de verdachte niet op de hoogte was van de aanwezigheid van de afbeeldingen, verweer dat mogelijk anderen dan verdachte onder zijn account naar kinderpornografisch materiaal hebben gezocht, gedownload en opgeslagen of dat deze versluierd en versleuteld zijn meegekomen met ander pornografisch materiaal kan onvoldoende worden weerlegd.).

[277] RB Oost-Brabant 22-12-2015, ECLI:NL:RBOBR:2015:7415.

[278] Minder gelukkig is bijvoorbeeld RB Midden-Nederland 1-7-2013, ECLI:NL:RBMNE:2013:2609 (vrijspraak bezit kinderporno, het alternatieve scenario *wordt niet weerlegd* door de stukken in het dossier. Evenmin volgt uit het dossier dat verdachte de laptop in zijn bezit heeft gehad op het moment dat de kinderporno op de laptop terecht is gekomen. Immers, niet kan worden vastgesteld dat de juiste dag, datum en tijdstip waren ingesteld op de laptop.).

[279] Vgl. o.m. Hof Arnhem 12-4-2012, ECLI:NL:GHARN:2012:1131, appel inzake ECLI:NL:RBARN:2010:BN3053 (stelling dat anderen toegang hadden tot de computer op geen enkele wijze aannemelijk geworden, zulks mede gelet op verklaring van de verdachte dat hij bewust zocht naar porno en grote aantallen bestanden tegelijk binnenhaalden.). Vgl. ook RB Zeeland-West-Brabant 14-7-2022, ECLI:NL:RBZWB:2022:3852 (betreft de aannemelijkheid van het scenario dat 130.000 kinderpornografische afbeeldingen als bijvangst zijn meegekomen bij het downloaden van volwassenenporno (hetgeen dan een aanzienlijke veelvoud van 130.000 afbeeldingen zou moeten betreffen).).

[280] Hof Arnhem-Leeuwarden 1-4-2016, ECLI:NL:GHARL:2016:2600 (mede gezien bevindingen politie hackverweer niet aannemelijk geworden; deze bevindingen worden niet weerlegd door het door de verdediging overgelegde rapport van computerdeskundige X. "*In voornoemd rapport worden weliswaar diverse mogelijkheden beschreven van de wijzen waarop door onbekend gebleven derden ongemerkt kan zijn ingelogd op de privé-server van verdachte, echter dat één van die mogelijkheden zich hier ook daadwerkelijk heeft voorgedaan is op basis van het technisch onderzoek van de politie op geen enkele wijze gebleken."*)

[281] Zie RB Noord-Holland 19-3-2018, ECLI:NL:RBNHO:2018:2286 ("*Naar het oordeel van de rechtbank mag in beginsel ervan worden uitgegaan, tenzij het tegendeel aannemelijk is geworden, dat de eigenaar van een met een wachtwoord beveiligd Skype- en Dropbox-account degene is die de daarmee verstuurde en daarin aangetroffen chatgesprekken, foto's en video's heeft verzonden en ontvangen."*).

[282] Zie Machielse in zijn conclusie ECLI:NL:PHR:2008:BD4872 (onder 6.5.) bij HR 30-9-2008, ECLI:NL:HR:2008:BD4872.

4.1.2.2. "Mijn computer is gehackt"

Gezien hetgeen thans bekend is over de ontwikkelingen op het gebied van de computercriminaliteit en vooral over de omvang en groei van het fenomeen "hacken"[283] komt het ons voor dat een dergelijk verweer door de rechter niet reeds aanstonds zonder nadere motivering mag worden verworpen. Onzes inziens kan voor het activeren van een nadere inhoudelijke rechterlijke motiveringsplicht, dan wel het entameren van nader onderzoek, echter wel verlangd worden dat de verdachte in ieder geval tot op zekere hoogte zijn verweer feitelijk onderbouwt[284], waarbij de enkele overlegging van nieuwsberichten of rapporten, waarin *in algemene zin* wordt gesproken over de mogelijkheid van "*hacking*" (of het geven van een demonstratie waaruit een dergelijke *mogelijkheid in zijn algemeenheid blijkt*[285]) niet reeds volstaat.[286]

Soms blijkt ook uit het digitaal-forensische basisonderzoek (en dus zonder dat nader deskundigenonderzoek wordt opgedragen en uitgevoerd) dat het (uiterst) onwaarschijnlijk moet worden geacht dat van "*hacking*" sprake is geweest. De jurisprudentie laat voorbeelden

---

[283] "*Hacken*" dient hier te worden gelezen als het zich met behulp van *technische hulpmiddelen* of door middel van een *technische ingreep* (zoals het installeren van een computervirus) toegang verschaffen tot iemand anders computer(netwerk); het heeft hier derhalve een engere betekenis dan de in art. 138ab Sr geformuleerde definitie van "computervredebreuk". Die omvat namelijk ook bijv. het onbevoegd gebruiken van een gebruikersnaam en wachtwoord om zich toegang te verschaffen tot een geautomatiseerd werk. Deze laatste vormen van gebruik van computers door anderen dan de primair gerechtigde gebruiker worden besproken in de hierna volgende paragraaf 4.1.2.3.

[284] Aldus bijv. Hof Amsterdam 9-9-2021, ECLI:NL:GHAMS:2021:2718 ("*Dat het e-mailadres van de verdachte is gehackt en dat die omstandigheid ertoe heeft geleid dat de betreffende bestanden zijn binnengehaald en vervolgens zijn terechtgekomen in een submap van een door de verdachte aangebrachte map, is evenmin aannemelijk geworden.*"). RB Overijssel 9-2-2018, ECLI:NL:RBOVE:2018:401 (verdachte heeft verweer dat zijn computer gehackt zou zijn niet aannemelijk kunnen maken en in het dossier is voor dit scenario geen enkel aanknopingspunt te vinden.); RB Noord-Nederland 7-10-2017, ECLI:NL:RBNNE:2017:4683 (het verweer dat een ander dan verdachte dierenporno op zijn computer heeft geplaatst is niet aannemelijk geworden. De verklaring is onvoldoende feitelijk onderbouwd.); RB Gelderland 21-8-2015, ECLI:NL:RBGEL:2015:5425 (voor zover verdachte heeft willen betogen dat niet zij, maar degene die haar e-mailaccount destijds heeft gehackt, (verreweg de meeste van voormelde) e-mailberichten naar aangevers heeft gestuurd met gebruikmaking van haar gegevens, wordt dit verweer verworpen. Immers, bij gebrek aan iedere feitelijke onderbouwing is niet aannemelijk geworden dat verdachtes e-mailaccount is gehackt.); RB Overijssel 31-5-2016, ECLI:NL:RBOVE:2016:1852 (verweer (dat iemand anders gebruik maakte van de computer) niet concreet onderbouwd en daarmee onvoldoende aannemelijk gemaakt.); RB Oost-Brabant 19-8-2015 ECLI:NL:RBOBR:2015:4938 ("*De door de verdediging geopperde mogelijkheid dat het kinderpornografisch materiaal door derden op de laptop is geplaatst, acht de rechtbank in het licht van de gebezigde bewijsmiddelen en bij gebreke van een nadere, concrete en verifieerbare onderbouwing niet aannemelijk. De rechtbank ziet in het procesdossier en het verhandelde ter terechtzitting ook geen aanknopingspunten in die richting.*").

[285] In deze zin minder gelukkig achten wij dan ook: RB Oost-Brabant 22-12-2015, ECLI:NL:RBOBR:2015:7415 (Vrijspraak bezit kinderporno. De verdachte heeft laten zien hoe de afbeeldingen buiten zijn medeweten op zijn gegevensdragers terecht hebben kunnen komen).

[286] Vgl. ook Hof Arnhem-Leeuwarden 1-4-2016, ECLI:NL:GHARL:2016:2600 (mede gezien bevindingen politie hackverweer niet aannemelijk geworden; deze bevindingen worden niet weerlegd door het door de verdediging overgelegde rapport computerdeskundige X. "*In voornoemd rapport worden weliswaar diverse mogelijkheden beschreven van de wijzen waarop door onbekend gebleven derden ongemerkt kan zijn ingelogd op de privé-server van verdachte, echter dat één van die mogelijkheden zich hier ook daadwerkelijk heeft voorgedaan is op basis van het technisch onderzoek van de politie op geen enkele wijze gebleken"*) en Hof Amsterdam 30-1-2018, ECLI:NL:GHAMS:2018:240 ("Blijkens de motivering van de verzoeken gaat de raadsman er klaarblijkelijk van uit dat het "kraken" van het wachtwoord en de pincode van de telefoon in kwestie door het NFI gevolgen kan hebben gehad voor de integriteit van de data op die telefoon. Het hof stelt vast dat *in de gegeven toelichting is volstaan met het enkele opwerpen van die theoretische voorstelling dat mutaties in de data kunnen zijn opgetreden* als gevolg van de ontsleuteling van wachtwoord en pincode. Dat vormt evenwel een onvoldoende onderbouwing voor deze verzoeken. Het hof wijst beide verzoeken dan ook af. Voor het verzochte verhoor van de deskundige en onderzoek in de vorm van contra-expertise is de noodzaak niet gebleken.").

zien, waarin het materiaal was geplaatst in specifieke mappen, die qua naam en overige inhoud door de verdachte zelf zijn gecreëerd en gevuld of die door de verdachte waren voorzien van specifieke aanvullende beveiliging door middel van wachtwoorden of codering[287], dan wel dat sprake was van communicatie via met wachtwoorden afgeschermde e-mailaccounts[288] of van gebruikmaking van aan de verdachte toebehorende e-mailadressen, telefoons en usb-sticks.[289] Soms levert ook een analyse van bijvoorbeeld loggegevens van gebruikte software of de inhoud van communicatie (sterke) aanwijzingen op dat van "hacken" geen sprake is geweest.[290] Actieve overige bemoeienis van de verdachte met kinderpornografie (bijvoorbeeld in de vorm van deelnemen aan chatrooms, gebleken verzamelwoede, gericht zoeken) wordt in de jurisprudentie eveneens als aanwijzing gezien dat het *hacking*-verweer onaannemelijk moet worden geacht.[291]

Kan het verweer echter niet aanstonds langs deze weg worden verworpen, dan zal veelal nader digitaal-technisch deskundigenonderzoek moeten plaatsvinden. De juiste vraagstelling is daarbij bepaald niet van ondergeschikt belang. Bedacht moet daarbij worden dat zelfs indien sprake is geweest van "hacking" daarvan niet altijd ook (traceerbare) digitale sporen

---

[287] Zie o.m. RB Gelderland 7-10-2017, ECLI:NL:RBGEL:2017:6305 (verweer dat anderen kinderporno op de computers van verdachte hebben geplaatst wordt als niet aannemelijk geworden verworpen. Uit de bestandslocaties, waarin telkens de naam van verdachte stond en de verklaring van de hoofdbewoner dat een van de twee computers van verdachte was, leidt de rechtbank af dat de afbeeldingen op de dag van aanhouding in zijn bezit waren.); RB Den Haag 31-7-2006, ECLI:NL:RBSGR:2006:AY5348 (verweer verworpen dat hackers kinderporno hadden geplaatst binnen het op de harde schijf aangetroffen programma Privacy Master dat beveiligd is met een wachtwoord bestaande uit het favoriete sigarettenmerk, leeftijd en geboortejaar van de verdachte.).

[288] Zie bijv. RB Rotterdam 5-4-2016, ECLI:NLRBROT:2016:2538 (verweer verworpen dat zijn e-mailaccounts zijn gehackt en dat de verdachte niet degene is die kinderporno per mail heeft verzonden en ontvangen.).

[289] RB Noord-Nederland 20-10-2017, ECLI:NL:RBNNE:2017:4022 (verweer van de raadsman dat verdachte niet degene was achter de Facebook en Instagram accounts wordt verworpen, nu niet aannemelijk is geworden dat een ander dan verdachte achter deze accounts zat. De rechtbank wijst er op dat niet alleen vrijwel alle betrokken accounts naar verdachtes internetverbinding zijn te herleiden, maar dat ook gebruik is gemaakt van verdachtes e-mailadres, telefoon en USB-stick.).

[290] Vgl. ook RB Noord-Holland 19-3-2018, ECLI:NL:RBNHO:2018:2286 (hack-verweer verworpen; o.m. omdat in communicatie met slachtoffer het door anderen dan verdachte weinig gebruikte woord "mooierd" regelmatig wordt gebezigd; ook sprake van met wachtwoord beveiligde Dropbox en afwezigheid van indicaties voor "hacking".); Hof Arnhem-Leeuwarden 1-4-2016, ECLI:NL:GHARL:2016:2600 (uit het proces-verbaal Digitaal onderzoek kinderpornografie blijkt dat het programma Teamviewer elke geslaagde verbinding met de server van een gehackte computer en elke poging daartoe vastlegt en dat het Teamviewer ID van de computer waarmee verbinding wordt gemaakt wordt geregistreerd. Tijdens het technisch onderzoek door de politie is geen spoor van dit soort verbindingen is aangetroffen, anders dan sporen afkomstig van bij verdachte in beslag genomen computermateriaal.).

[291] Zie o.m. de conclusie (onder 6.3. en 6.4) van AG Machielse bij HR 3-9-2008, ECLI:NL:HR:2008:BD4872 (filmpje aangetroffen in C:\Documents and Settings\[naam verdachte]\My Documents\My Music\; is bovendien afgespeeld met verdachtes media-programma); RB Noord-Nederland 27-7-2017, ECLI:NL:RBNNE:2017:2882 ("gehackt"-verweer. Raadsman voert aan dat de digitaal rechercheur deze mogelijkheid niet heeft kunnen uitsluiten en dat dit aanleiding zou moeten zijn om het NFI opdracht te geven over te gaan tot tegenonderzoek. Dit verweer wordt verworpen, op basis van de bevindingen van de digitaal rechercheur (geen malware, firewall ingeschakeld, kinderporno op makkelijk toegankelijke locatie en één bestand als meest recent geopend in een programma, chatgesprekken over kinderen en kinderpornografisch materiaal.)). Hof Arnhem 12-4-2012, ECLI:NL:GHARN:2012:1131 (stelling dat anderen toegang hadden tot de computer op geen enkele wijze aannemelijk geworden, zulks mede gelet op verklaring van de verdachte dat hij bewust zocht naar porno en grote aantallen bestanden tegelijk binnenhaalden.); RB Zwolle 11-7-2006, ECLI:NL:RBZLY:2006:AY5104 (verdachte met voornaam Hans heeft gezocht naar termen als 'alt.sex.stories.incest' en 'little' en de plaatjes zijn aangetroffen in de map D:\users\laptop\C\Hans); Hof 's-Gravenhage 15-11-2002, ECLI:NL:GHSGR:2002:AF0684 ((obsessieve) verzamelwoede voor kinderporno; verdachte heeft met een daartoe ingestelde zoekrobot automatisch kinderporno uit nieuwsgroepen gehaald; geen aanwijzingen voor bemoeienis van derden.); RB Middelburg, 12-2-2003, ECLI:NL:RBMID:2003:AF4981 (inbraakverweer o.m. verworpen op grond van de vaststelling dat verdachte dagelijks berichten ontving m.b.t. kinderporno)

achterblijven.[292] Deskundigen zullen desgevraagd dan ook zelden tot nooit kunnen en willen verklaren dat kan worden *uitgesloten* dat in een bepaald geval sprake is geweest van "hacking". Het NFI kan dan ook weinig tot niets aanvangen met vragen als: "was deze computer gehackt" of "kan worden uitgesloten dat deze computer was gehackt".[293]

Het verdient daarom aanbeveling om naar aanleiding van een *hacking*-verweer allereerst aan de deskundige de vraag te stellen of op de betreffende computer/gegevensdrager digitale sporen (in de zin van *malware* of anderszins) aanwezig zijn, welke er op zouden kunnen wijzen dat de computer (in de tenlastegelegde periode) is gehackt. Terzijde: indien dergelijke sporen vervolgens niet worden aangetroffen, wordt zulks wel als aanwijzing gezien voor de onaannemelijkheid van het *hacking*-verweer.[294]
Idealiter zou de vraagstelling zich echter niet hiertoe moeten beperken. In het bijzonder niet, omdat een zeer groot aantal computers in aanraking komt met malware en daarom ook sporen van malware bevat.[295] Het enkele feit dat op een computer sporen zijn aangetroffen van malware betekent daarom nog niet noodzakelijkerwijs dat daarmee of daardoor ook de aanwezigheid van geheel andere sporen (zoals opgeslagen kinderpornografische afbeeldingen of browseractiviteit) is verklaard. Anders gezegd: of "hacking" een mogelijke verklaring is voor de aanwezigheid van bepaalde delictssporen hangt niet zo zeer af van de sporen van "hacking", maar veeleer van de (specifieke) sporen van het delict.[296]

Wat de strafrechter derhalve in deze gevallen eigenlijk zou moeten willen weten is dus niet alleen of de computer gehackt is geweest, maar veeleer of er aanwijzingen zijn of de aangetroffen kinderpornografische afbeeldingen door de verdachte dan wel (buiten diens controle) door een ander op zijn computer/gegevensdrager zijn vastgelegd.[297] Onderzoek daarnaar is mogelijk en vindt plaats door analyse met speciale forensische zoeksoftware van alle zich op de computer/gegevensdrager bevindende gegevens, waaronder bijvoorbeeld ook zoek- en opslaggeschiedenissen en mail- en chatberichten.[298] Aldus kunnen mogelijk de afbeeldingen worden gekoppeld aan (de tijdstippen en inhoud van) bepaalde gesprekken, chats, zoekacties en websitebezoeken van de verdachte dan wel van andere personen die van de computer gebruik hebben gemaakt. Goed denkbaar is derhalve dat naast de hiervoor genoemde vraag naar de aanwezigheid van op "hacken" wijzende digitale sporen in dit

---

[292] Bron: NFI (ir. R. Schramp) in het deskundigenrapport d.d. 20 januari 2015 inzake de strafzaak met parketnummer 09-720877-12.
[293] Informatie van NFI-deskundigen aan de eerste auteur. Zoals hiervoor reeds gesteld behoeft een "hack" niet noodzakelijkerwijs digitale sporen achter te laten, zodat uit het ontbreken van dergelijke sporen niet zonder meer kan worden afgeleid dat er "dus" *geen* "hack" zal zijn geweest. In zo'n geval kan echter wel de conclusie worden getrokken dat de bevindingen van het digitaal forensisch onderzoek de stelling van de verdachte dat zijn computer zou zijn gehackt niet ondersteunen.
[294] RB Rotterdam 21-1-2016, ECLI:NL:RBROT:2016:547 (verwerping hack-verweer na NFI-onderzoek; "geen sporen aangetroffen die erop wijzen dat computer *daadwerkelijk* gehackt is"); RB Utrecht 1-12-2008, ECLI:NL:RBUTR:2008:BG5730; Vgl. ook RB Den Bosch 30-7-2012, ECLI:NL:RBSHE:2012:BX2902 (bezit kinderporno, verdachte ontkent wetenschap te hebben gehad van de aanwezigheid van de kinderpornografie op de in beslag genomen gegevensdragers, onderzoek wijst uit dat er geen malware op de gegevensdragers aanwezig is geweest; wij wijzen er op dat in dit vonnis ook in beslag genomen computers als gegevensdragers worden aangeduid, dit is relevant omdat in het kader van onderzoek naar malware moet worden gekeken naar het geautomatiseerde werk waaraan de gegevensdrager was gekoppeld toen de kinderpornografie daarop terecht kwam nu malware zich doorgaans in of nabij een besturingssysteem zal bevinden).
[295] Microsofts "Global threat activity"-overzicht vermeldt dat op het moment van schrijven in de laatste 30 dagen in Nederland 372.574 apparaten in aanraking kwamen met malware. Bron: Cyberthreats, viruses, and malware - Microsoft Security Intelligence (geraadpleegd op: 20 maart 2023).
[296] Aldus ook NFI (ir. R. Schramp) in het deskundigenrapport d.d. 20 januari 2015 inzake de strafzaak met parketnummer 09-720877-12.
[297] Vgl. in deze zin ook de (door de HR gevolgde) conclusie van AG Aben.
[298] Het NFI en de politie gebruiken daarvoor nu het door het NFI ontwikkelde programma Hansken.

verband aan de deskundige tevens de vraag wordt gesteld of "*er nader digitaal onderzoek kan worden gedaan of, en zo ja in hoeverre, de aanwezigheid van de aangetroffen kinderpornografische afbeeldingen op computer/gegevensdrager X kan worden gerelateerd aan handelingen van de verdachte met betrekking tot die computer/gegevensdrager*", dan wel dat de iets neutralere vraag wordt gesteld of "*er aanwijzingen zijn dat de bestanden X,Y.Z (waarbij dan met name (een selectie uit) de in het kader van de tenlastelegging relevante bestandsnamen moeten worden genoemd) (na installatie van een ….) vanuit een ander geautomatiseerd werk van afstand op de computer van de verdachte zijn geplaatst en/of gecreëerd"*.

Komt het vervolgens tot een inhoudelijke beoordeling van een "hack-verweer" dan kunnen de algemene beschouwingen daaromtrent uit het arrest van het Hof Den Haag van 19 december 2018[299], opgesteld langs de lijn van het bovenstaande een nuttig handvat c.q. beoordelingskader bieden:

> *"3.2.1.*
> *In onderhavige strafzaak wordt derhalve de inhoud van de feitelijke bevindingen ten aanzien van het digitaal bewijs niet betwist, noch de kwalificatie daarvan als strafbare feit, maar wordt een zogenaamd "hackverweer" gevoerd dat er kort samengevat op neerkomt dat die strafbare handelingen niet door verdachte zelf of met zijn medeweten zijn verricht, maar door een (veelal onbekende) derde die zich toegang tot zijn computer had verschaft. Het hof stelt voorop dat bij de beoordeling van een dergelijk verweer als maatstaf dient te worden aangelegd of – alle feiten en omstandigheden in ogenschouw nemende – dit verweer al dan niet in meer of mindere mate aannemelijk is geworden (vergelijk HR 16 maart 2010, ECLI:NL:HR:2010:BK3359). Het is aan de verdachte om die feiten en omstandigheden aan te voeren. Volgens vaste jurisprudentie mag de rechter, naast de weerlegging in de bewijsmotivering, ook de onwaarschijnlijkheid, onaannemelijkheid en/of de ongeloofwaardigheid van alternatieve scenario's in zijn oordeelsvorming betrekken.*
> *3.2.2.*
> *Voorts mag de rechter er, behoudens sterke aanwijzingen voor het tegendeel, van uitgaan dat op een computer (of in een beveiligde online omgeving) aangetroffen gedownloade of gekopieerde bestanden daarop zijn geplaatst door de gebruiker van die computer. Evenzo mag de rechter er, behoudens sterke aanwijzingen voor het tegendeel, van uitgaan dat wanneer uit nadere (meta)data blijkt dat bepaalde websites of bepaalde bestanden zijn geopend, die handelingen zijn verricht door de gebruiker van die computer.*
>
> *3.2.3.*
> *In relatie tot het fenomeen "hacking" dient voorts te worden bedacht dat zelfs indien sprake is geweest van "hacking" daarvan niet altijd ook (traceerbare) digitale sporen achterblijven. Dit maakt dat ook bij vergaand en deskundig onderzoek nimmer zal kunnen worden uitgesloten dat in een bepaald geval sprake is geweest van "hacking". Daarnaast is het een feit van algemene bekendheid dat een zeer groot aantal computers in aanraking komt met malware en daarom ook (veelal door beveiligingssoftware geneutraliseerde) sporen van malware bevat. Het enkele feit dat op een computer sporen zijn aangetroffen van malware betekent derhalve nog niet noodzakelijkerwijs dat zulks ook een aannemelijke verklaring vormt voor de aanwezigheid van bepaalde (digitale) delictsporen, zoals opgeslagen browser- of communicatieactiviteiten en kinderpornografische afbeeldingen.*
>
> *3.2.4.*
> *Naar het oordeel van het hof zijn derhalve bij de beoordeling of "hacking" een aannemelijke verklaring vormt voor de bevindingen van het digitaal-forensisch onderzoek niet zozeer de aan- dan wel afwezigheid van sporen van "hacking" van belang, maar veeleer de (specifieke) sporen van het delict. En meer specifiek: of er aanwijzingen zijn of de aangetroffen digitale gegevens door de verdachte dan wel (buiten diens controle) door een ander op de computer van de verdachte zijn vastgelegd.*

[299] Hof Den Haag 19-12-2018, ECLI:NL:GHDHA:2018:3528.

3.2.5.
Uit het voorgaande volgt allereerst dat, indien een "hackverweer" als hiervoor bedoeld wordt gevoerd, het voor bewezenverklaring niet vereist is dat – al dan niet via wettige bewijsmiddelen – is aangetoond dat kan worden uitgesloten dat een bepaalde computer is "gehackt".

3.2.6.
Voorts volgt uit het voorgaande dat eventuele (deskundigen)verklaringen inhoudende of beschrijvende de algemene en/of theoretische mogelijkheid dat de betreffende computer is gehackt, zonder dat daarbij tevens een specifieke relatie wordt gelegd met de feiten uit de betreffende zaak en het daarin verrichtte (digitaal-forensische) onderzoek, in de regel op zichzelf onvoldoende redengevend zullen (kunnen) zijn voor de conclusie dat min of meer aannemelijk is geworden dat ook in het voorliggende geval de computer is gehackt.

3.2.7.
Bij de beoordeling of een "hackingverweer" in meer of mindere mate aannemelijk is geworden kunnen diverse factoren worden betrokken, waaronder onder meer:
- de aan- dan wel afwezigheid van digitale sporen met betrekking tot het daadwerkelijk (kunnen) binnendringen door derden in de betreffende computer.

Hierbij kan onder meer gedacht worden aan het al dan niet aantreffen van (sporen van) hackingsoftware of zogenaamde remote access tools, en van het ongeautoriseerde gebruik door derden daarvan, op de betreffende computer;
- het niveau van fysieke en digitale bescherming van de computer tegen gebruik door derden/(digitaal) binnendringen. Te denken valt daarbij aan feiten zoals de feitelijke locatie en de feitelijke toegankelijkheid voor derden van de betreffende computer, alsook de aanwezigheid en het niveau van de op de computer aanwezige toegangsbeveiliging en verdere beveiligingssoftware;
- de aan- dan wel afwezigheid van digitale sporen (en/of andere feiten en omstandigheden) waaruit, bijvoorbeeld vanwege de inhoud, kan worden afgeleid wie (ook) op of omstreeks het moment van plegen van de strafbare gedragingen de gebruiker van de computer was.

Bij onderzoek kan bijvoorbeeld blijken dat vanaf de computer zeer kort voor of na de strafbare handelingen ook communicatie (email, chats) is gevoerd, waarvan de inhoud een relatie heeft met de verdachte (dan wel een bepaalde derde) of dat gegevens zich op bestandslocaties bevinden die redelijkerwijs alleen bekend of toegankelijk waren voor de verdachte;
- de mate waarin, en het moment waarop, de verdachte medewerking heeft verleend aan eventueel nader onderzoek naar zijn verweer.
Hierbij kan gedacht wordt aan het al dan niet (tijdig) verstrekken door de verdachte van bijvoorbeeld wachtwoorden en toegangscodes, welke nodig zijn voor het verrichten van (nader) digitaal- forensisch onderzoek;
- andere feiten en omstandigheden die wijzen op een bijzondere (inhoudelijke) betrokkenheid van de verdachte of een derde bij de op of via de betreffende computer gepleegde gedragingen.
Hierbij valt onder meer te denken aan fysieke sporen (bijv. afbeeldingen of valse credit cards) die bij de verdachte of derden zijn aangetroffen en die een relatie hebben met de op de computer aangetroffen digitaal-forensische sporen (bijv. digitale kinderpornografie; gephishte credit card gegevens);
- getuigenverklaringen omtrent het gebruik van de betreffende computer door verdachte dan wel door derden;
- de aan- dan wel afwezigheid van een motief voor derden om in de computer van de verdachte binnen te dringen."

4.1.2.3. "Een derde heeft gebruik gemaakt van mijn computer/gegevensdrager etc."

In de huidige steeds verder digitaliserende wereld zijn computers overal aanwezig. In kantoren staan vaak tientallen computers, die niet zelden slecht (een plakkertje met het wachtwoord erop of beveiligd met algemene wachtwoorden bekend onder meerdere werkenden) tegen gebruik door anderen dan de legitieme gebruiker. Evenzo zijn in steeds meer huishoudens meerdere computers aanwezig (veelal aangesloten op een wifi-netwerk), waarvan de wachtwoorden bij alle gezinsleden bekend zijn, zo zij überhaupt al beveiligd zijn.

Onbeveiligde of onvoldoende[300] beveiligde wifirouters kunnen bovendien veelal ook van buiten de woning of het kantoor waar de wifirouter is geplaatst door onbevoegden gebruikt worden.[301] Laptops, maar ook tablets en smartphones, zijn ook al lang niet meer aan een vaste plaats gebonden, en worden niet zelden meegenomen naar en/of uitgeleend aan anderen dan de eigenlijke hoofdgebruiker.

Kortom, het is bepaald geen uitzondering meer dat (delen van) netwerken, computers en gegevensdragers door meerdere personen kunnen worden gebruikt, dan wel dat meerdere personen daartoe toegang hebben. Ook komt het voor dat mensen ongevraagd afbeeldingen krijgen toegezonden. Dit maakt dat het verweer "een ander heeft de afbeeldingen op mijn computer/smartphone geplaatst" (en/of "een ander heeft van mijn wifiverbinding gebruikt gemaakt") voor de strafrechter niet altijd even makkelijk op zijn merites is te beoordelen.[302] Het verweer blijkt dan ook zeker de laatste jaren relatief kansrijk te zijn.[303]
Een aantal aandachtspunten is echter wel aan te geven. Allereerst lijkt het toch geen al te wilde veronderstelling dat de verdachte die een dergelijk verweer voert toch op enigerlei wijze zal moeten stellen, en waar mogelijk: concreet zal moeten onderbouwen, dat en hoe anderen toegang konden krijgen tot "zijn" computer (en zijn *wachtwoord(en)*)[304], en ook zoveel mogelijk welke personen dat waren. Veelal zal dit kunnen worden gerealiseerd door middel van verklaringen van getuigen. Bij de verificatie daarvan wordt de rechter overigens nogal eens gehinderd door het feit dat in het proces-verbaal maar zelden in detail wordt beschreven hoe en waar *precies* de betreffende computer of gegevensdrager was aangetroffen

---

[300] Hierbij kan bijvoorbeeld worden gedacht aan het plaatsen van de wifirouter naast het buitenraam, waarbij de sticker met cruciale gegevens (de "naam" van het wifinetwerk en het nimmer gewijzigde password) zichtbaar is.
[301] Opmerking hierbij verdient wel dat gegeven het beperkte bereik van wifisignalen de - gestelde - betreffende onbevoegde gebruiker dan wel binnen een afstand van hooguit enige tientallen meters (veelal zelfs aanmerkelijk minder) in de buurt van de wifirouter heeft moeten kunnen komen. Onder omstandigheden (grote ommuurde en bewaakte tuin o.i.d.) kan blijken dat dit onwaarschijnlijk geacht moet worden.
[302] Zie over de werking en kwetsbaarheid van wifi ook hierna in deze paragraaf opgenomen technisch lemma "wifi".
[303] Zie o.m. m.b.t. tot "uitlenen": RB Den Haag 4-12-2008, ECLI:NL:RBSGR:2008:BG6090 (vrijspraak; computers meerdere weken uit de macht van verdachte geweest, terwijl bovendien niet kan worden vastgesteld wanneer de afbeeldingen precies zijn geplaatst.); *zie voor andere zaken waarin dit verweer werd gehonoreerd* o.m. Hof Den Bosch 25-4-2017, ECLI:NL:GHSHE:2017:1786 (afbeeldingen stonden op een laptop die regelmatig in een restaurant werd gebruikt door personeel, en daarnaast ook door de partner van verdachte. Niet met zekerheid vast te stellen dat het verdachte is geweest die verantwoordelijk is voor de aanwezigheid van deze afbeelding op de laptop. Vrijspraak.); RB Gelderland 7-7-2016, ECLI:NL:RBGEL:2016:3677 (vrijspraak bezit en verspreiden van kinderpornografie omdat niet buiten gerede twijfel kan worden vastgesteld dat de verdachte degene is geweest die het heeft gedaan. Verdachte heeft twee zoons.); RB Gelderland 28-8-2015, ECLI:NL:RBGEL:2015:5477 (computer (systeemkast) stond in de woonkamer en behoorde toe aan medeverdachte X , die verklaard heeft dat van zijn PC gemeenschappelijk gebruik werd gemaakt. Voorts kan op grond van de aanwezige dossierstukken niet worden vastgesteld dat *verdachte* de bedoelde 36 afbeeldingen heeft binnengehaald op de computer van medeverdachte X. Vrijspraak.);
[304] In deze zin kennelijk ook: Hof Amsterdam 9-9-2021, ECLI:NL:GHAMS:2021:2718 (de stelling van verdachte dat iemand anders zich geruime tijd op het kinderpornoforum heeft kunnen bevinden zonder dat verdachte dit heeft gezien, wordt ongeloofwaardig bevonden en is niet verenigbaar met zijn verklaring dat hij in die periode altijd zicht had op het gebruik van zijn computer, de omstandigheid dat er na de verhuizing van verdachte nog 'laatste wijzigingen' aan de bestanden hebben plaatsgevonden en er nog een verbinding is gemaakt met het TOR-netwerk); RB Noord-Nederland 15-4-2021, ECLI:NL:RBNNE:2021:1925 (Mede gelet op de verklaring van de ex-partner van verdachte dat anderen alleen in het bijzijn van verdachte gebruik maakten van zijn laptop, acht de rechtbank niet aannemelijk dat een ander gedurende een langere periode gebruik zou hebben gemaakt van zowel de laptop als de telefoon van verdachte); RB Noord-Nederland 29-6-2017, ECLI:NL:RBNNE:2017:2352 (Bewijsverweer dat verdachte niet de ontvanger is geweest van de per WhatsApp naar zijn telefoon gezonden kinderpornografische afbeeldingen van de driejarige dochter van de medeverdachte wordt verworpen. Mede gezien latere skypegesprekken via de laptop van verdachte over deze foto's wordt onaannemelijk geacht dat verdachte ten tijde van de ontvangst van de afbeeldingen zijn telefoon zou zijn kwijt geraakt).

(stond de computer aan of uit, zat er een sticker met het password op de computer/het toetsenbord, was de kamer waar de computer stond afgesloten; waar lag de betreffende usb-stick of DVD exact[305] etc.) en gedetailleerde informatie omtrent het moment waarop bepaalde incrimerende bestanden op de computer zouden zijn geplaatst niet zelden ook in het proces-verbaal ontbreekt.[306]

Ook nader digitaal forensisch onderzoek kan aanwijzingen opleveren omtrent de aannemelijkheid van het verweer. Analoog aan hetgeen hiervoor onder 4.1.2.2. is beschreven met betrekking tot het "hackverweer" zal het onderzoek zich daarbij primair moeten richten op sporen en andere aanwijzingen waaruit – vooral door koppeling voor wat betreft tijd en inhoud van de overige computerinhoud aan de gegevens omtrent (het moment van vastlegging/verspreiding etc. van) de afbeeldingen – zou kunnen worden afgeleid of de aangetroffen kinderpornografische afbeeldingen door de verdachte dan wel door een ander zijn vastgelegd.[307] Vanzelfsprekend zal ook de wijze waarop en de mate waarin er sprake is van beveiliging van de computer/gegevensdrager in dit onderzoek moeten worden betrokken.[308]

Tenslotte moet men natuurlijk ook het gezond verstand blijven gebruiken en acht blijven slaan op hetgeen ook uit ervaringsregels kan voortvloeien. Zo lijkt het ook niet erg waarschijnlijk dat een 14-jarige zoon van een verdachte, die ook de computer gebruikt, grote hoeveelheden

---

[305] Zie bijv. RB Gelderland 28-8-2015, ECLI:NL:RBGEL:2015:5477 (Aangetroffen losse harde schijf met daarop afbeelding Y. "*Nu er geen proces-verbaal van doorzoeking ter inbeslagneming in het dossier aanwezig is, verdachte heeft verklaard dat hij alleen verantwoordelijk is voor de computer aanwezig op zijn slaapkamer en medeverdachte X heeft verklaard dat de computer in de woonkamer door meerdere personen wordt gebruikt, is onduidelijk of de in de tenlastelegging opgenomen foto Y wel afkomstig is van de computer van verdachte*")
[306] Zie o.m. RB Zeeland-West-Brabant 8-9-2020, ECLI:NL:RBZWB:2020:4199 (o.a. vrijspraak van bezit van kinderpornografisch materiaal, nu het dossier geen aanwijzingen bevatte dat verdachte beschikkingsmacht had over deze afbeeldingen en van die afbeeldingen evenmin kan worden vastgesteld hoe lang deze op de gegevensdragers stonden); RB Overijssel 13-8-2020, ECLI:NL:RBOBR:2020:4012 (o.a. vrijspraak van bezit van kinderpornografisch materiaal (uitsluitend bestaande uit "deleted files"), nu op basis van het dossier niet kan worden vastgesteld of verdachte op enig (eerder) moment hierover de beschikkingsmacht heeft gehad.
[307] Zie o.m. Hof Arnhem-Leeuwarden 3-5-2017, ECLI:NL:GHARL:2017:3682 (Verweer dat een ander dan verdachte achter de chatsessie (Torchat) zit wordt verworpen, onder opneming van bewijsoverweging rb en inhoud van aanvullend onderzoek naar de buddylijst van Torchat); RB Oost-Brabant 19-8-2015, ECLI:NL:RBOBR:2015:4938 (kinderpornografie is weggeschreven in account van verdachte, metadata van de betrokken afbeeldingen (datum plaatsing en opening) geven bovendien aan dat afbeeldingen waren geplaatst voor meenemen laptop door derde(n); Verklaring van de verdachte dat derden de kinderpornografie op de laptop hebben geplaatst niet aannemelijk geacht.); Hof Arnhem 12-4-2012, ECLI:NL:GHARN:2012:1131, appel inzake ECLI:NL:RBARN:2010:BN3053 (verspreiden en bezit kinderporno. Stelling dat anderen toegang hadden tot de computer op geen enkele wijze aannemelijk geworden. Mede gelet op verklaring van de verdachte dat hij bewust zocht naar porno en grote aantallen bestanden tegelijk binnenhaalde. NB: blijkens het vonnis gezocht met de term 'teens'); RB Arnhem 24-6-2011, ECLI:NL:RBARN:2011:BQ9825 (bezit kinderporno, *geen sprake van handelingen door derden*, nu de kinderpornografische media zijn aangetroffen op externe harddisk en cd's/dvd's en in diverse specifieke mappen was opgeborgen, en de externe harddisk op de piano lag en de cd's/dvd's in de slaapkamerkast waren opgeborgen); RB Zutphen 18-10-2011, ECLI:NL:RBZUT:2011:BU1269 (verweer 'ex-echtgenote heeft de kinderporno gedownload' verworpen, gezien plaatsing in specifieke mappen, erkenning door verdachte dat één film door hemzelf is opgeslagen en ontkenning door ex-echtgenote van downloaden).
[308] Vgl. voor de relevantie daarvan o.m. RB Arnhem 24-9-2012, ECLI:NL:RBARN:2012:BX8141 (verwerping verweer dat een ander de kinderporno op verschillende gegevensdragers heeft geplaatst; computer was beveiligd door alleen bij verdachte bekend wachtwoord; getuigen spreken tegen dat verdachte zijn laptop ook wel uitleende); zo zal het ook onwaarschijnlijk zijn dat een willekeurige derde zo maar een goed beveiligde wifirouter zal kunnen hacken, ten aanzien van huisgenoten zal dat dan echter minder snel kunnen worden uitgesloten, en zal beoordeeld moeten worden hoe aannemelijk het is dat de betreffende huisgenoten de betreffende gewraakte communicatie hebben gevoerd, waarbij factoren als leeftijd, tijdstippen, motieven, technische kennis etc. een rol zullen kunnen spelen.

kinderporno en extreme dierenporno zou opslaan in een map met een ‘sigarettenwachtwoord’ dat wijst in de richting van zijn – als verdachte aangemerkte – vader.[309]

Technisch lemma: wifi

Wat is wifi?
Wifi is de term die gebruikt wordt om een draadloos netwerk (een zogenaamd Wireless Local Area Network, of WLAN) aan te duiden. Het netwerk kan worden gebruikt om draadloos verbinding te leggen met een router/modem (in dit lemma verder aangeduid als router)[310], die via een vaste verbinding toegang tot internet biedt. Dat kan thuis, op een bedrijf of op een openbare locatie zoals een vliegveld zijn. De routers die in het laatste geval worden gebruikt om toegang te geven tot internet worden veelal “wifi-hotspots” genoemd. Iets nauwkeuriger beschouwd valt wifi te onderscheiden in een aantal verschillende in internationaal (commercieel) verband overeengekomen standaarden, zoals in onderstaand overzicht weergegeven (bron: Wikipedia):

Generation	IEEE Standard	Adopted	Radio Frequency (GHz)
Wi-Fi 7	802.11be	(2024)	2.4/5/6
Wi-Fi 6E	802.11ax	2020	6[2]
Wi-Fi 6		2019	2.4/5
Wi-Fi 5	802.11ac	2014	5[3]
Wi-Fi 4	802.11n	2008	2.4/5
*(Wi-Fi 3)**	802.11g	2003	2.4
*(Wi-Fi 2)**	802.11a	1999	5
*(Wi-Fi 1)**	802.11b	1999	2.4
*(Wi-Fi 0)**	802.11	1997	2.4

Hoe werkt wifi?
Wifi werkt met radiogolven. Om gebruik te maken van het draadloos netwerk via de router, en zodoende het internet te bereiken, moet een device zijn voorzien van een zender en ontvanger voor radiogolven. In computers en laptops wordt deze zend en ontvangstinrichting doorgaans aangeduid als wifi-netwerkkaart. In smartphones en andere kleinere (IoT-)devices gaat het feitelijk om een (gedeelte van een) chip. De hiervoor bedoelde inrichtingen communiceren via radiogolven met het zogenaamde *access point* van een router.

Aandacht verdient hier wel dat een access point *niet* hetzelfde is als een router. Het verbindt immers geen devices met elkaar en heeft ook op zichzelf geen verbinding met het internet. Een access point deelt ook geen IP-adressen uit. De werking van een access point lijkt derhalve op die van een ouderwetse radiozendinstallatie: geschikt om radiogolven te ontvangen en te verzenden, maar verder niets.
Een device met een wifi-netwerkkaart (of chip) kan actief op zoek gaan naar een bepaald access point en zelfs (als het al eerder bij een dergelijk access point aangemeld is geweest) daarmee direct verbinding maken, zodat niet telkens opnieuw het wachtwoord behoeft te worden ingevoerd. Op deze wijze kan dus als regel ook een ieder die een bepaald device met een wifi-voorziening in handen heeft, gebruik maken van de wifi-access points waartoe dat device al reeds eerder toegang heeft gekregen.

Wat is het bereik van wifi?
Bij wifi worden gegevens draadloos verzonden en ontvangen via de antenne van het access point en de devices van de ontvangers. Daarbij kan gebruik worden gemaakt van verschillende frequenties, zie het schema hierboven. Elke frequentie kent een aantal kanalen, waardoor mogelijkheden ontstaan om te voorkomen dat signalen in elkaars vaarwater zitten (denk aan het draadloos netwerk van de buren). De lagere frequentie van 2,4 GHz kent een groter haalbaar bereik. Het haalbare bereik wordt in eerste instantie bepaald door de onderlinge afstand en hoogte van de antenne, de kwaliteit van apparatuur en de omgeving (muren,

[309] RB Den Haag 31-7-2006, ECLI:NL:RBSGR:2006:AY5348.
[310] Zie technisch lemma: hoe communiceren computers met internet.

aanwezigheid van elektronische apparaten die voor verstoring van het signaal zorgen, etc.). Recentelijk is door een NFI-deskundige in een strafzaak (ter terechtzitting) aangegeven dat 125 meter in zijn algemeenheid bij wifi-netwerken als grens kan worden beschouwd van het bereik waarbinnen het maken van een verbinding technisch mogelijk is (zie: Rb. Noord-Holland, 28-6-2022, ECLI:NL:RBNHO:2022:5536). In de praktijk is deze afstand sterk afhankelijk van de concrete omstandigheden en de gebruikte apparatuur. In een woning met dikke gewapend betonnen muren of vloeren kan het soms maar 10 meter of zelfs nog minder zijn.

Indien dit voor de beoordeling van een bepaalde strafzaak van belang is, en de oorspronkelijke apparatuur nog beschikbaar is, kan de sterkte (en daarmee het bereik) van een wifi-signaal vanaf een bepaald device, en of de bereikbaarheid van een bepaalde "draadloze" router soms ook achteraf nog worden onderzocht.
Het beperkte bereik van wifi impliceert ook dat indien is vastgesteld dat via een bepaald device verbinding is gemaakt met een bepaald access point (of met een draadloze router of modem waarin dit access point is ingebouwd) daaraan als regel de conclusie kan worden verbonden dat het betreffende device (en de gebruiker daarvan) zich op een (zeer) korte afstand van dat access point moet hebben bevonden.

Inmiddels zijn verschillende producten op de markt om het bereik van het wifi-netwerk te vergroten. Naast de zogenaamde repeaters, die vaak bekabeld zijn verbonden met de router en in feite een tweede access point vormen, zijn sinds enkele jaren zogenaamde mesh-systemen te koop. Deze mesh-systemen (zoals Google Nest Wifi) kunnen het wifi-netwerk als het ware spreiden. Over het algemeen bestaan mesh-systemen uit meerdere apparaten (ook wel nodes). Een van de apparaten wordt dichtbij de router gezet en daarop aangesloten. Dit apparaat stuurt het signaal (evt. draadloos) door aan de overige apparaten, die elders neergezet kunnen worden en zo overal op korte afstand een snelle verbinding kunnen aanbieden.

Beveiliging en "hacken" van routers
De toegang tot het draadloos netwerk en de gegevens die via het draadloos netwerk worden gedeeld moeten goed worden beschermd. Tegenwoordig wordt daarvoor veelal het WPA (Wifi Protected Access) protocol gebruikt. De huidige versie van het protocol is WPA3, geïntroduceerd in 2018, maar veel routers gebruiken nog het in 2006 geïntroduceerde WPA2. Dit protocol beveiligt de over het draadloos netwerk verstuurde gegevens door deze te versleutelen (encryptie) en beschermt de toegang tot het draadloos netwerk.

WPA2 gebruikt voor de toegangscontrole een encryptiesleutel van 256-bits. Gebruikers kiezen een wachtwoord van minimaal 8 karakters en vervolgens wordt - samen met de netwerknaam (SSID) een unieke sleutel gegenereerd voor elk draadloos apparaat. Deze sleutels worden continue opnieuw gegenereerd. Het zijn die sleutels die worden gebruikt voor een veilige verbinding. De gegevens die vervolgens worden uitgewisseld zijn versleuteld met het encryptiealgoritme AES, dat eveneens een 256-bit encryptiesleutel gebruikt.

Hoewel ook deze vorm van beveiliging niet 100% veilig[311] is – zoiets kan uiteraard nooit gegarandeerd worden – wordt WPA2 nog altijd beschouwd als een zeer veilige vorm van beveiliging van het draadloos netwerk.

In het kader van de beoordeling van mogelijke "hacking" verweren wordt hier tevens opgemerkt dat steeds meer routers – althans voor enige tijd - in hun geheugen ook de gegevens opslaan van de devices die via de betreffende router toegang hebben gekregen tot internet. Het kan daarom verstandig zijn om –zeker indien er aanwijzingen zijn dat sprake is van het onrechtmatig gebruik van een router en/of identificatie van een daarbij gebruikt device vermoedelijk wenselijk is – (ook) een dergelijke router in beslag te (laten) nemen en/of het geheugen/de loggegevens van die router door een deskundige te laten uitlezen.

Openbare wifi-hotspots, zoals die op luchthavens en in de trein, zijn als regel niet beveiligd. Dat wil zeggen: iedereen kan zonder wachtwoord daarvan gebruik maken om met hun device dat met zo'n hotspot verbinding

[311] In oktober 2017 was er veel publiciteit over diverse kwetsbaarheden in WPA2. Vooral Android en Linux bleken kwetsbaar, maar ook macOs en iOS waren niet helemaal veilig. Apple heeft de kwetsbaarheden ondertussen al d.m.v. updates opgelost. Ook veel routerfabrikanten hebben al updates/patches gemaakt om de kwetsbaarheden weg te nemen. Een aanval via deze kwetsbaarheden kan alleen gegevens ontsleutelen die onbeveiligd via de wifi-verbinding werden gestuurd. Zie verder: https://www.security.nl/posting/535333/Wifi-netwerken+kwetsbaar+door+ernstige+lekken+in+WPA2-beveiliging.
Men kan zich overigens in dit verband de vraag stellen waarom iemand al die moeite zou doen bij een willekeurige gebruiker, terwijl men op eenvoudige wijze en zo goed als anoniem ook op zeer vele plaatsen ook via wifi-hot spots toegang kan krijgen tot het internet.

maakt op internet te komen. Er zijn risico's dat een ander op hetzelfde openbare netwerk gegevens afluistert – als die gegevens worden gedeeld via een onbeveiligde verbinding met een website.

4.1.2.4. "De afbeeldingen stonden (al) op een 2e hands/eerder gebruikte computer/gegevensdrager"

Met enige regelmaat wordt ook het verweer gevoerd dat de strafbare afbeeldingen zich al op een computer en/of gegevensdrager bevonden voordat deze (weer) in het bezit van de verdachte kwam.[312] Ook hier kan worden verlangd dat zo'n verweer, in ieder geval ten aanzien van de gestelde verkrijging van een derde, minimaal enigszins aannemelijk moet zijn gemaakt.[313] Slaagt de verdachte daarin, dan zal – naast eventueel het horen van degene waarvan de computer/de gegevensdrager afkomstig zou zijn – nader digitaal forensisch onderzoek in de rede liggen. Logischerwijs dient het digitale onderzoek daarbij primair gericht te zijn op sporen en andere aanwijzingen waaruit – mede door koppeling voor wat betreft tijd en inhoud van de overige computerinhoud aan de gegevens omtrent (het moment van vastlegging/verspreiding etc. van) de afbeeldingen – zou kunnen worden afgeleid op welk tijdstip, en zo mogelijk door wie, de aangetroffen kinderpornografische afbeeldingen zijn vastgelegd.

Ook hierbij dient de rechter zich echter te realiseren dat het digitaal forensisch onderzoek zijn beperkingen kent, en bepaalde gestelde alternatieve handelingsscenario's slechts zelden zal kunnen *uitsluiten*.[314] De uitkomst van dergelijk onderzoek zal zo goed als altijd een waarschijnlijkheidsinschatting inhouden, die moet worden bezien in de context van hetgeen overigens aan bewijs beschikbaar is.

---

[312] Zie o.m. RB Zeeland-West-Brabant 7-9-2020, ECLI:NL:RBZWB:2020:4197 (verweer dat de computer destijds nieuw is gekocht verworpen en dat verdachte niet actief op zoek is geweest naar kinderporno verworpen; gelet op de aangetroffen zoektermen in combinatie met de aangetroffen sporen van websites en bestandsnamen en de 667 aangetroffen (verwijderde) kinderpornografische bestanden); RB Zeeland-West-Brabant 12-3-2014, ECLI:NL:RBZWB:2014:1628 (verweer dat de afbeeldingen het gevolg zijn van het overnemen van de files door een geïnfecteerde harddisk bij de reparatie van de computer in China verworpen);.

[313] Vgl. in dit opzicht RB Midden-Nederland 1-7-2013, ECLI:NL:RBMNE:2013:2609, waarin verdachte stelde dat zijn laptop een periode gestolen was geweest, hetwelk o.m. door een getuigenverklaring werd onderbouwd; omdat niet kon worden vastgesteld dat de juiste dag, datum en tijdstip waren ingesteld op de laptop volgde naar het oordeel van de rechtbank niet uit het dossier dat verdachte de laptop in zijn bezit heeft gehad op het moment dat de kinderporno op de laptop terecht is gekomen. Volgde vrijspraak.

[314] Bij vastlegging van bestanden op een gegevensdrager wordt via het besturingssysteem (bijv. Windows of Apple IOS) aan het bestand een datum van vastlegging op die gegevensdrager gekoppeld. Die datum wordt ontleend aan de datum/tijd-instellingen van dat besturingssysteem. Iedere gebruiker kan die datum/tijd instellingen echter zelf (eenvoudig tijdelijk in Windows en lastiger maar (meer) permanent in de BIOS van zijn systeem) veranderen. Zo kan het zijn dat bestanden op een computer bijvoorbeeld een opslagdatum in de toekomst hebben gekregen. Het is van belang te onderkennen dat naast de zogenaamde BIOS-klok in computers ook sprake zal zijn van een (en mogelijk meerdere) softwareklok(ken). Nu ook computers tegenwoordig vaak met het internet verbonden zijn, zal de tijd van deze softwareklokken steeds worden gesynchroniseerd met de UTC-tijdstandaard. Dit kan tot zeer complexe situaties leiden die om hoogwaardig forensisch onderzoek vragen. Bij smartphones is het veelal aanmerkelijk lastiger voor gebruikers om de instelling van data en tijdstippen te wijzigen omdat deze devices deze gegevens meestal synchroniseren met die van het netwerk waarmee zij verbinding hebben en/of maken.
In voorkomend geval dient voldoende aandacht te worden geschonken aan de vraag of de op het moment van vastlegging ingestelde datum ook de toen geldende werkelijke datum/tijd was (zie hierover ook verder hierna onder 6.2.4.1). In dit licht wel wat kort door de bocht geformuleerd lijkt dan ook de motivering van de in de voorgaande noot opgenomen uitspraak RB Midden-Nederland 1-7-2013, ECLI:NL:RBMNE:2013:2609) ("*niet kan worden vastgesteld dat op moment van vastlegging de juiste datum was ingesteld*", vrijspraak).

4.1.3. "De kinderporno is automatisch op mijn computer gezet"
Een eveneens regelmatig gevoerd verweer houdt in dat de betreffende kinderpornografische afbeeldingen als gevolg van een door de verdachte onvoorziene werking van bepaalde software "automatisch" op verdachtes computer of een aan hem toebehorende gegevensdrager terecht is gekomen. Niet zelden wordt dan betoogd dat de aangetroffen kinderporno al dan niet als onbedoelde "bijvangst" is meegekomen met het – al dan niet omvangrijke – resultaat van een (geautomatiseerde) zoekopdracht naar "gewone" porno. Daarbij is wel enig nader onderscheid te maken naar gelang het karakter van de gebruikte software. Hierop wordt hierna ingegaan.

4.1.3.1. "De kinderporno kwam als "bijvangst" mee met een omvangrijke hoeveelheid gewone porno"
Het is al enige jaren mogelijk om met behulp van bepaalde software een computer via internet en zonder verdere tussenkomst van de gebruiker voortdurend aan de hand van bepaalde ingegeven zoektermen te laten zoeken naar bepaalde op het internet aanwezige gegevens en de resultaten vervolgens zonder verdere tussenkomst van de gebruiker op te slaan op diens computer c.q. op een door die gebruiker of die computer aangewezen gegevensdrager of *cloud*opslag. Met behulp van zo'n geautomatiseerd zoekprogramma kunnen, zeker indien gebruik wordt gemaakt van snelle verbindingen, in korte tijd (zeer) grote hoeveelheden data en dus ook grote hoeveelheden (beeld)bestanden worden binnengehaald.

Het moge dan ook duidelijk zijn dat het ingeven van zoektermen zoals bijvoorbeeld "seks", "jong" en "porno" bij gebruik van dergelijke programma's kan leiden tot het downloaden van grote hoeveelheden pornografisch materiaal, waaronder mogelijk ook materiaal dat *de jure* als kinderpornografisch materiaal kan worden aangemerkt. Zelfs indien niet wordt gezocht op porno, maar bijvoorbeeld op muziek, kan het voorkomen dat de ingevoerde zoektermen[315] leiden tot het downloaden van kinderpornografisch materiaal.[316]
Dit impliceert dat uit het enkele feit dat op een gegevensdrager (al dan niet naast "gewone") pornografische afbeeldingen ook (kennelijk gedownloade) *kinder*pornografische afbeeldingen zijn aangetroffen, niet zonder meer kan worden afgeleid dat de gebruiker zich ook "willens en wetens heeft blootgesteld aan de aanmerkelijke kans" *kinder*pornografisch materiaal in bezit te krijgen.[317]

---

[315] Denk hierbij bijvoorbeeld aan het als zoekterm invoeren van bepaalde -soms seksueel zeer expliciete- titels of tekstgedeelten uit rap- en hiphopnummers.
[316] Zie bijvoorbeeld RB Noord-Nederland 21-2-2017, ECLI:NL:RBNNE:2017:648 (gering aantal kinderpornografische afbeeldingen. Verdachte downloadde met behulp van een zogenoemd *peer-to-peer*programma porno. RB: "Hij gebruikte hierbij, onder andere, de zoekterm "*young*". Verdachte heeft ter terechtzitting aangegeven slechts de intentie te hebben gehad om pornobestanden te downloaden van jonge vrouwen. Na het bekijken van de gedownloade pornografische bestanden, zo verklaarde verdachte, verwijderde hij deze direct. Uit het dossier blijkt dat de kinderporno is aangetroffen op een toegankelijke – *accessible* – plaats op de computer van verdachte. Dit houdt in dat deze afbeeldingen niet door verdachte zijn gewist, terwijl hij dit kennelijk wel doet met pornografisch materiaal dat hij heeft gedownload. *Nu verdachte de kinderporno niet heeft verwijderd moet hij hebben geweten dat die bestanden vanaf dat moment op de gegevensdrager werden bewaard*." Bewezenverklaring van bezit). Wij merken hierbij wel op dat bij het wissen van bestanden op een computer deze doorgaans in een prullenbak terechtkomen. Dat is nog steeds een (in de woorden van de rechtbank) toegankelijke, accessible plaats. Pas na het verwijderen van bestanden uit de prullenbak zijn deze niet meer toegankelijk.
[317] In deze zin ook o.m. HR 26-10-2010, ECLI:NL:HR:2010:BO1713 (uit gebezigde bewijsmiddelen kan niet worden afgeleid dat het opzet van de verdachte al dan niet in voorwaardelijke vorm was gericht op het in het bezit hebben van de bewezenverklaarde *kinder*pornografische afbeelding, downloaden van veel porno); idem o.m. AG Knigge in zijn conclusie (ECLI:NL:PHR:2006:AU9104, r.o. 13) bij HR 28-2- 2006, ECLI:NL:HR:2006:AU9104.

Het antwoord op de vraag of in deze gevallen wel (voorwaardelijk) opzet zal kunnen worden aangenomen, zal afhangen van de omstandigheden van het geval. Voor wat betreft beoordelingscriteria kan daarbij overwegend worden aangesloten bij de aanwijzingen als die hiervoor reeds genoemd zijn onder 4.1.1., zoals onder meer de gebruikte zoektermen en de naam van de bestanden en de websites (of andere internetlocaties) waarvandaan deze zijn gedownload.[318] Daarnaast kan hier ook de hoeveelheid kinderpornografisch materiaal een rol spelen, en de wijze waarop een verdachte daarmee na het ontvangen daarvan is omgegaan[319], de wijze waarop het materiaal is opgeslagen daaronder begrepen.[320]

Indien slechts enkele kinderpornografische afbeeldingen worden aangetroffen naast een grote hoeveelheid "gewone" porno of ander gedownload materiaal, kan dat een aanwijzing zijn dat sprake is van onbedoelde "bijvangst".[321] Indien het echter gaat om in absolute zin grotere hoeveelheden kinderpornografisch materiaal, en zeker als dit ook op verschillende momenten is gedownload, zal aan het feit dat er tevens grote(re) hoeveelheden "gewone" porno zijn

---

[318] Zie o.m. Hof Amsterdam 22-3-2018, ECLI:NL:GHAMS:2018:970 (geen zoektermen gericht op kinderpornografie aangetroffen, kan niet worden vastgesteld dat bewust is gezocht, verhoudingsgewijs zeer klein aantal kinderpornografische bestanden op zeer grote hoeveelheid andere afbeeldingen; vrijspraak); RB Gelderland 23-11-2017, ECLI:NL:RBGEL:2017:6030 (Bijvangstverweer van verdachte wordt verworpen, op grond van de gebruikte zoektermen (o.m. nackte madchen en nude young qirls), gericht op expliciet (jonge) kinderen; RB Noord-Holland 29-6-2017, ECLI:NL:RBNHO:2017:5547 (Onaannemelijk dat enkele afbeeldingen op automatische wijze op de tablet terecht zijn gekomen en verdachte deze onbewust heeft opgeslagen. Verdachte heeft verklaard dat hij zoek ging naar plaatjes van tienermeisjes. Uit de internetgeschiedenis van de tablet blijkt dat verdachte op een bepaalde internetsite heeft gezocht op de termen 'teen' en 'under 13'. Voorts heeft verdachte meerdere mappen aangemaakt met onder meer de namen 'girls9' 'girls11' en 'girls13'. Verdachte wist dan ook, of heeft tenminste bewust de aanmerkelijke kans aanvaard, dat de tablet kinderpornografisch materiaal bevatte. Verdachte heeft daarmee opzettelijk, al dan niet in voorwaardelijke vorm, kinderporno in zijn bezit gehad); RB Midden-Nederland 4-7-2018, ECLI:NL:RBMNE:2018:3096 (Acht kinderpornografische afbeeldingen aangetroffen op telefoon verdachte. Verdachte zou deze niet bewust hebben verworven en/of opgeslagen. "*De rechtbank is van oordeel dat verdachte door zijn deelname aan voornoemde Whatsappgroepen bewust de aanmerkelijke kans heeft aanvaard dat daarin ook foto's werden gedeeld van meisjes die jonger zijn dan achttien jaar. Bovendien volgt uit het dossier dat verdachte interesse had in, en contact had met minderjarige meisjes en hen ook vroeg om hem naaktfoto's te sturen. Dit maakt de verklaring van verdachte dat de aangetroffen kinderporno 'bijvangst' was onaannemelijk*."). In dezelfde zin ook bijv. Stevens, L. & Koops, B.J., '*Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno*', Delikt en Delinkwent 2009, afl. 7/51, p. 669, onder 2.2.2.

[319] Zie bijvoorbeeld over (niet-)handelen na ontvangst: RB Rotterdam 11-11-2020, ECLI:NL:RBROT:2020:10171 (bijvangstverweer: 51 kinderpornografische afbeeldingen zouden als thumbnails zijn meegekomen van een bulkdownload van een server in Leipzig. Verwerping van dit verweer, o.a. omdat de thumbnails niet op de betreffende server stonden en als de bulkdownload (zoals door de verdediging gesteld) zonder enige vorm van selectie is overgezet, zou dat wel verwacht mogen worden); RB Noord-Nederland 21-2-2017, ECLI:NL:RBNNE:2017:648 (gering aantal kinderpornografische afbeeldingen, bewezenverklaring van bezit. Verdachte downloadde met behulp van een zogenoemd *peer-to-peer*-programma porno; reeds aangehaald in voetnoot 306). Opvallend is dat de rechtbank de overweging dat de verdachte moet hebben gewezen dat de betreffende bestanden werden bewaard, steunt op de door verdachte algemeen omschreven werkwijze van downloaden van porno. Tegen de achtergrond dat er kennelijk geen bewijs voorhanden is dat de verdachte de betreffende kinderpornografische afbeeldingen daadwerkelijk heeft gezien en daarmee kennis heeft genomen van de inhoud – en die afbeeldingen toch heeft laten staan – is die redenering niet solide.

[320] Vgl. in deze zin ook RB Gelderland (militaire kamer) 19-3-2018, ECLI:NL:RBGEL:2018:1204 ("bijvangst"-verweer verworpen; verdachte wist dat er bij het verzamelen van porno ook regelmatig kinderpornografie meekwam en heeft deze bestanden ook in mappen opgeslagen); RB Limburg 4-4-2017, ECLI:NL:RBLIM:2017:3006 (afbeeldingen niet op een willekeurige plek op de laptop opgeslagen, maar gerubriceerd en ondergebracht in mappen, waarbij gestructureerd te werk is gegaan. Bewezenverklaring bezit).

[321] Aldus bijv. Hof Amsterdam 22-3-2018, ECLI:NL:GHAMS:2018:970; Vgl. ook RB Den Haag 29-2-2008, ECLI:NL:RBSGR:2008:BC5528 (geen bewuste vastlegging, automatische opslag door downloadprogramma Limewire, automatisch aangemaakte map 'Music Incomplete', vijf bestanden, geen opzet op bezit)

aangetroffen waarschijnlijk minder gewicht worden toegekend.[322] Als reeds is bemerkt dat eerder kinderporno is gedownload als gevolg van het uitvoeren van bepaalde zoekopdrachten, dan legt dat een zeer vergaande onderzoeksplicht op de gebruiker om na volgende zoeksessies het gedownloade materiaal te controleren op de aanwezigheid van kinderpornografisch materiaal. Komt hij deze niet voldoende na, dan zal als regel voorwaardelijk opzet kunnen worden aangenomen.[323]

4.1.3.2. Opzet en up/downloaden via peer-to-peer (P2P) software

Lange tijd maakten veel computergebruikers voor het zoeken naar bestanden gebruik van zogenaamde peer-to-peer (P2P-)software.[324] Thans is dit gebruik op zijn retour, hoewel het in bepaalde vormen (zoals in besloten *friend-to-friend* (F2F)-netwerken) nog wordt gebruikt in relatie tot de verkrijging en verspreiding van kinderpornografisch materiaal.[325] Hoe P2P-software technisch werkt is reeds hiervoor beschreven, zodat hier wordt volstaan met een verwijzing daarnaar.[326] Er zijn ook enkele juridische aspecten aan verbonden die nadere bespreking verdienen.

Een P2P-programma is over het algemeen feitelijk ook een soort zoekmachine. Indien een gebruiker van een P2P-programma via zo'n programma zoektermen invoert en andere acties onderneemt die vervolgens leiden tot het via het P2P-netwerk downloaden van kinderpornografisch materiaal naar zijn computer, wordt vrijwel altijd (opzet op) bezit van dit materiaal aangenomen.[327] Er is in deze gevallen namelijk sprake van opzet, beschikkingsmacht en van bewuste vastlegging van kinderpornografisch materiaal.

---

[322] Hof Amsterdam 30-9-2020, ECLI:NL:GHAMS:2020:2542 (bijvangstverweer: op de computer van verdachte zijn meer dan 81.000 afbeeldingen aangetroffen, waarvan 357 kinderpornografische afbeeldingen, een percentage van 0.4%. Nu verdachte deze bestanden vervolgens niet heeft verwijderd, is daarmee de opzet op het in bezit hebben gegeven. Of verdachte deze bestanden heeft aangetroffen als bijvangst, dan wel daar bewust naar heeft gezocht, is daarbij niet relevant); RB Oost-Brabant 27-5-2016, ECLI:NL:RBOBR:2016:2719 (geen sprake van bijvangst, gelet op verhouding tussen pornografisch en kinderpornografisch materiaal en verklaring van verbalisant ter terechtzitting dat bij een percentage van 11 geen sprake kan zijn van toevallige bijvangst. Indien er sprake is van bijvangst, ligt dit onder de 10 procent). Men kan zich bij deze uitspraak wel de vraag stellen wat de wetenschappelijke basis is van het genoemde percentage.

[323] Zie HR 28-10-2003, ECLI:NL:HR:2003:AL4314 (en de voorafgaande conclusie van AG Vellinga van 28 oktober 2003, ECLI:NL:PHR:2003:AL4314 en RB Noord-Nederland 29-5-2017, ECLI:NL:RBNNE:2017:1929 (veroordeling voor bezit en verspreiding van kinderporno. Verweer "bijvangst" wordt verworpen, op zichzelf niet onaannemelijk dat er sprake was van bijvangst gezien de verhouding tussen volwassenenporno en kinderporno, maar hoewel verdachte wetenschap had van de aanwezigheid van meegekomen kinderporno heeft hij deze niet verwijderd). Een voorbeeld van een onzes inziens niet adequate reactie op een dergelijk verweer is te zien in RB Midden-Nederland 15-10-2019, ECLI:NL:RBMNE:2019:4766 ("*Het aangetroffen dierenpornografisch materiaal stond op een dvd. Verdachte was de enige gebruiker van zijn computer en heeft de afbeeldingen zelf op de dvd gebrand. Bij deze stand van zaken moet het ervoor worden gehouden dat verdachte de betreffende afbeeldingen bij het opslaan op een dvd heeft gezien en dus wist dat deze op de gegevensdrager stonden*.") De veronderstelling dat verdachte het dierenpornografisch materiaal moet hebben gezien is - afgezet tegen de feitelijke handelingen die in zijn algemeenheid nodig zijn om bestanden op een dvd te branden - zonder nadere feitelijke onderbouwing op zijn minst gedurfd te noemen.

[324] Veelgebruikte P2P-programma's zijn onder meer,;, , Gigatribe, Napster, , ,, uTorrent, BitTorrent, qBittorrent, Seedr en Frostwire. eMule, eDonkey2000, Limewire, Kazaa, Morpheus, Ares(-Galaxy) en Vuze zijn uit het verleden bekend maar niet meer beschikbaar of verouderd.

[325] Zie bijv. https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/child-sexual-exploitation (2017).

[326] Zie voor de technische kant van P2P-software het hiervoor bij 3.4.1.1. opgenomen 'Technisch lemma: peer-to-peer (P2P)-programma's.

[327] Hoge Raad 11-9-2007, ECLI:NL:HR:2007:BA6316 (zoeken en downloaden kinderpornografie via P2P-programma Kazaa, wetenschap van opslag in map shared files van eigen computer); RB Groningen 28-1-2008, LJN BC3529 (downloaden via P2P-programma Limewire van aan de naam reeds als kinderpornografie te herkennen films; opslag in shared map; verdachte had blijkens aanschaf wissoftware ook wetenschap van deze

Zeker in de begintijd van de P2P-software waren lang niet alle gebruikers op de hoogte van de werking van dergelijke programma's, zodat zij konden worden "verrast" door het feit dat door hen gedownload materiaal (waaronder kinderpornografisch materiaal) via hun computer/harde schijf ook direct toegankelijk was (en ook direct kon worden gedownload) door anderen. Door hen werd dan ook vooral in de context van de hen tenlastegelegde bestanddelen "verspreiden", "aanbieden" en/of "openlijk tentoonstellen" aangevoerd dat zij op deze gedragingen geen voorwaardelijk opzet hadden gehad.

Hoewel dergelijke verweren in eerste instantie nog wel eens werden gehonoreerd[328], lijkt dat de laatste jaren steeds minder het geval.[329] Dit wekt ook geen verbazing, nu de werking van P2P-software, en in het bijzonder het mechanisme van het automatisch delen met andere gebruikers, breed bekend is geworden en die werking – mede op internet – ook op velerlei plaatsen wordt beschreven. Het lijkt zeker heden ten dage dan ook bepaald onwaarschijnlijk dat een gebruiker van P2P-software niet op de hoogte zou zijn van de werking daarvan.[330] In het licht van deze toch wel zo langzamerhand als feit van algemene bekendheid te duiden werking van P2P-software lijkt het geen grote stap om tevens te verlangen dat degene die dergelijke software in gebruik neemt, vooraf controleert wat in zijn geval de basisinstellingen zijn; laat hij zulks na dan valt moeilijk in te zien waarom de verdachte ten aanzien van de dan voorzienbare basiswerking van de P2P-software (kort gezegd: het automatisch delen/tentoonstellen van op de *shared drive* aanwezig materiaal) geen strafrechtelijk verwijt zou kunnen worden gemaakt. Of anders gezegd: er lijkt dan toch sprake te zijn van een situatie waarin de verdachte willens en wetens de aanmerkelijke kans heeft aanvaard dat door hem op zijn *shared drive* gedownloade of opgeslagen afbeeldingen vanaf diezelfde shared drive (verder) zouden worden verspreid.[331] De in een uitspraak van de rechtbank Midden-Nederland gestelde eis dat uit de bewijsmiddelen moet blijken dat de keuze om te delen vanuit

---

opslag) HR 30-9-2008, ECLI:NL:HR:2008:BD4872 (kinderpornografisch videobestand aangetroffen in My Musicmap, maar heeft ook gestaan in shared folder van P2P-programma Kazaa; blijkt ook te zijn afgespeeld; verweer dat bestanden "automatisch zouden zijn geladen" verworpen).

[328] Zie bijv. RB Amsterdam 3-7-2009, ECLI:NL:RBAMS:2009:BJ8160 (bezit kinderporno, peer-to-peer-netwerk**,** geen feit van algemene bekendheid dat d.m.v. bepaalde software gedownloade bestanden ook ter beschikking worden gesteld van derden; deskundigenverklaring dat bij installatie van de betreffende software niet behoeft te worden ingestemd met openstelling voor derden); RB Den Haag 29-2-2008, ECLI:NL:RBSGR:2008:BC5528 (geen bewuste vastlegging, automatische opslag door P2P-downloadprogramma Limewire, automatisch aangemaakte map 'Music Incomplete', vijf bestanden, nog niet bekeken; geen opzet).

[329] Zie bijv. RB Noord-Nederland 21-11-2017, ECLI:NL:RBNNE:2017:4460 (veroordeling voor verspreiden kinderpornografie door delen via P2P "hoewel verdachte zich hier wellicht niet (altijd) van bewust was"). Zie echter voor een recente "uitzondering": RB Midden-Nederland 10-10-2017, ECLI:NL:RBMNE:2017:5057 (De rechtbank oordeelt dat het enkel automatisch toegankelijk stellen van kinderpornografisch materiaal via een zogeheten shared drive niet voldoende is om te komen tot bewezenverklaring van het aanbieden van kinderporno, nu het dossier onvoldoende aanknopingspunten biedt voor de conclusie dat dit een actieve keuze is geweest van de verdachte. Vrijspraak).

[330] Zie o.m. ook RB Arnhem 5-3-2013, ECLI:NL:RBONE:2013:BZ3290 (Verweer dat er geen sprake is van opzet is verworpen**,** gelet op wetenschap van de verdachte ten aanzien van de werking van het peer-to-peerprogramma); RB Gelderland 10-3-2014, ECLI:NL:RBGEL:2014:1541 (o.a. veroordeling voor aanbieden kinderpornografie via P2P-programma Shareaza; blijkens eigen verklaring wetenschap bij de verdachte omtrent werking programma).

[331] Wellicht is in deze zin ook de vanuit het opzetperspectief nogal cryptisch geformuleerde uitspraak RB Noord-Nederland 21-11-2017, ECLI:NL:RBNNE:2017:4460 ("Bij het downloaden van dit materiaal maakte verdachte onder meer gebruik van Peer2Peer programma's en bij het gebruik van dergelijke downloadprogramma's worden tegelijkertijd met het downloaden van bestanden ook bestanden geüpload en zo met anderen gedeeld. *Hoewel verdachte zich hier wellicht niet (altijd) van bewust was* (curs. auteurs) heeft hij daarnaast ook bewust kinderpornografisch materiaal met een ander gedeeld en zich aldus meerdere malen schuldig gemaakt aan het verspreiden van kinderpornografisch materiaal.").

een shared drive een actieve keuze is geweest van de verdachte[332] lijkt dan ook in zijn algemeenheid een te zware beoordelingsmaatstaf.

Mocht daaromtrent toch twijfel bestaan, dan kan digitaal-forensisch onderzoek soms nadere informatie verschaffen. Zo kan bijvoorbeeld worden nagegaan of de verdachte zelf instellingen in het programma heeft gewijzigd (of bepaalde gegevens al bij installatie moest instellen of wijzigen), dan wel of het programma bij installatie zichzelf geheel automatisch instelde. Daarnaast kan vanzelfsprekend ook overigens alleszins aannemelijk zijn dat de verdachte wetenschap draagt van de werking van de gebruikte P2P-software, bijvoorbeeld op basis van zijn opleiding, zijn eigen verklaringen of hetgeen anderszins blijkt over zijn computer(programma)gebruik.

4.1.3.3. "Als bijlage meegezonden afbeelding is zonder mijn wetenschap opgeslagen"

Een wat recenter verweer betreft afbeeldingen die over het algemeen in de *cache*[333] of in niet direct voor een gebruiker toegankelijke submappen van een social media-applicatie zoals Windows Live Messenger zijn aangetroffen. Betoogd wordt dan dat dergelijke afbeeldingen aan de verdachte (ongevraagd) zijn toegezonden, hij deze niet heeft geopend/bekeken of opgeslagen, maar dat deze afbeelding(en) door het programma zelf direct na binnenkomst in de map zijn geplaatst waar zij zijn aangetroffen. Anders dan wel in de rechtspraak is geoordeeld[334], kan een dergelijk scenario bij bepaalde applicaties technisch gezien bepaald niet op voorhand worden uitgesloten.[335] Tenzij er reeds andere redenen zijn om het verweer te verwerpen (bijvoorbeeld indien mocht blijken dat de afbeeldingen op verzoek zijn toegezonden, en/of deze wel zijn geopend of bekeken, of dat reeds uit het proces-verbaal blijkt dat het betreffende programma niet op deze wijze bijlagen opslaat e.d.) ligt het derhalve in de rede om in een dergelijk geval nader deskundigenonderzoek op te dragen naar de waarschijnlijkheid van dat scenario *in het concrete geval,* bij welk onderzoek zowel de inhoud van de betreffende computer(gegevens) als hetgeen bekend is over de werking van de specifieke applicatie zal moeten worden betrokken.

4.1.3.4. Verzwaarde onderzoeksplicht na eerder aantreffen van kinderpornografisch materiaal

De Hoge Raad[336] heeft voorts geoordeeld dat wanneer een verdachte bij het downloaden van pornografisch materiaal eenmaal kinderpornografie is tegengekomen, hij zich (bij het voortzetten van het downloaden van pornografisch materiaal) ervan moet vergewissen dat er

---

[332] RB Midden-Nederland 10-10-2017, ECLI:NL:RBMNE:2017:5057 (de rechtbank oordeelt dat het enkel automatisch toegankelijk stellen van kinderpornografisch materiaal via een zogeheten *shared drive* niet voldoende is om te komen tot bewezenverklaring van het aanbieden van kinderporno, nu het dossier onvoldoende aanknopingspunten biedt voor de conclusie dat dit *een actieve keuze* is geweest van de verdachte. Vrijspraak voor aanbieden van kinderpornografie).

[333] Zie omtrent de *cache* verder hierna onder 4.2.1.4.

[334] In zijn algemeenheid onjuist lijkt derhalve RB Gelderland 29-2-2016, ECLI:NL:RBGEL:2016:1109 (verweer: "*ongevraagd toegezonden, niet geopend, en niet bekend met filmpjes*". "*De militaire kamer acht het een feit van algemene bekendheid dat alleen gedownloade en geopende filmpjes in het geheugen van een smartphone worden opgeslagen.*").

[335] Zo verklaarde een NFI-deskundige in zijn rapport in een zaak met parketnummer 09/757756-12: "*Microsoft heeft per email uitgelegd hoe en wanneer bestanden in de MessengerCache terecht komen. De email legt uit dat afbeeldingen automatisch, zonder tussenkomst van de gebruiker, in de MessengerCache worden geplaatst wanneer deze worden uitgewisseld via Windows Live Messenger*" In de onderliggende email (d.d. 16 april 2015) stelt Microsoft: "*When a photo is shared during a conversation, although the user does not download the photo, the photo can still be found within a temporary folder on the users hard drive*".

[336] In dezelfde zin ook: Knigge in zijn conclusie (ECLI:NL:PHR:2006:AU9104, onder 13.) bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104, waarbij hij ook verwijst naar HR 28-10-2003, ECLI:NL:HR:2003:AL4314 (en de voorafgaande conclusie van AG Vellinga van 28 oktober 2003, ECLI:NL:PHR:2003:AL4314. .

niet nog meer c.q. opnieuw kinderpornografie op zijn computer aanwezig is c.q. is meegekomen. Wordt dit nagelaten dan zal dus voorwaardelijk opzet op het in bezit hebben[337] van de betreffende kinderpornografische afbeeldingen kunnen worden aangenomen.[338] Soms kan ook hier (nader) digitaal forensisch onderzoek goede diensten bewijzen, omdat daardoor bijvoorbeeld nadere informatie kan worden verkregen of, en zo ja: wanneer, bepaalde kinderpornografische bestanden zijn *geopend* en op welke datum of data bepaalde bestanden zijn gedownload.[339]

Aannemelijk is dat eenzelfde verzwaarde onderzoeksplicht (c.q. verlaagde drempel ten aanzien van voorwaardelijk opzet) zal gelden ten aanzien van personen die bij een bezoek aan bepaalde sites op andere locaties geconfronteerd worden met kinderpornografisch materiaal en desondanks daarna ook doorgaan met het bezoeken van diezelfde site.

4.2. Opzet en beschikkingsmacht

Zoals hiervoor aangegeven wordt in de jurisprudentie voor de bewezenverklaring van bezit van kinderpornografisch materiaal tevens vereist dat de verdachte over het (normaliter in bestandsvorm) opgeslagen digitale kinderpornografische materiaal kon *beschikken*. Dit laatste is te verstaan als: er toegang toe hebben, het kunnen openen om het te bekijken en/of er handelingen mee kunnen verrichten en het te kunnen verwijderen.[340]
In de rechtspraktijk blijkt het begrip beschikkingsmacht in belangrijke mate te worden geobjectiveerd. Zoals uit het volgende zal blijken, wordt bijvoorbeeld niet aangenomen dat er slechts dan geen beschikkingsmacht is, als het volstrekt onmogelijk is om toegang te krijgen tot de bestanden. Het ontbreken van beschikkingsmacht wordt namelijk ook aangenomen als slechts via speciale forensische software toegang kan worden verkregen tot de incriminerende bestanden (of daarvoor zeer specialistische kennis nodig is), terwijl niet aannemelijk is geworden dat de verdachte over dergelijke specifieke software of kennis kon beschikken. Anderzijds is het enkele (gestelde) niet weten van een gebruiker dat hij nog kon beschikken over de betreffende bestanden niet zonder meer voldoende (en soms zelfs onvoldoende) om in rechte ook aan te nemen dat die beschikkingsmacht ontbrak of niet moet worden verondersteld. Zulks geldt te meer als op basis van het onderzoek ter terechtzitting, dan wel op basis van algemene ervaringsregels of als feit van algemene bekendheid moet worden aangenomen *dat een gemiddelde gebruiker* die wetenschap wel had (en/of het onaannemelijk

---

[337] De verzwaarde onderzoeksplicht geldt ten aanzien van het bestanddeel in bezit hebben, en dus niet ten aanzien van verwerven (hoewel aan laatstgenoemd bestanddeel ten opzichte van in bezit hebben nauwelijks onderscheidend betekenis toekomt). Zie enigszins curieus: RB Zeeland-West-Brabant, 18 november 2022, ECLI:NL:RBZWB:2022:6878 ("*Voor het verwerven van dergelijke afbeeldingen is daarbij is (sic!) wel vereist dat verdachte (voorwaardelijk) opzet heeft gehad op de inhoud van het verworvene. Naar het oordeel van de rechtbank is hiervan sprake. (...). Hij heeft bewust het aanmerkelijke risico aanvaard dat bij het zoeken van afbeeldingen van jonge meisjes en het downloaden van pakketten met dergelijke afbeeldingen, hij zich ook de toegang zou verschaffen tot kinderpornografische afbeeldingen en deze afbeeldingen zou verwerven.*")
[338] In deze zin ook o.m. Hof Den Bosch 14-10-2011, ECLI:NL:GHSHE:2011:BV2397 (o.a. bezit kinderporno, downloaden met behulp van *eMule* en verplaatsing bestanden naar andere mappen, ondanks wetenschap dat bij downloaden kinderpornografisch materiaal binnen kon komen verder geen controles uitgevoerd; verweer verworpen)
[339] Zie ook verder hierna onder 6.2.4.1.
[340] Zie in dit verband ook: Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (Bewezenverklaring bezit van thumbnail afbeelding, die door verdachte op zijn niet openbare Twitter account is geüpload, een handeling die enkel kan worden verricht als verdachte beschikkingsmacht heeft over de afbeelding en zich van de aanwezigheid op de computer bewust is).

wordt geacht dat deze verdachte die kennis niet had). Bij dit laatste kan hetgeen blijkt omtrent het ICT-kennisniveau van de verdachte een rol spelen.[341]

4.2.1. Beschikkingsmacht toegespitst op enkele specifieke bestands- en opslagkenmerken
Zoals hiervoor aangegeven is essentieel voor beschikkingsmacht dat men een bepaald bestand kan benaderen om het te openen, dan wel daarmee handelingen kan verrichten als verzenden, kopiëren etc.. Of en in hoeverre dat kan hangt vooral af van de vraag om wat voor bestanden het gaat en/of waar die bestanden in de computer c.q. een gegevensdrager zijn aangetroffen. In de jurisprudentie zijn dan ook vele uitspraken te vinden die mede op deze vraag een antwoord geven. Hoewel daaruit niet altijd een even consistente lijn valt te halen, geeft deze jurisprudentie wel een redelijk inzicht hoe althans een aantal veelvoorkomende bestands- en opslagkenmerken *de jure* moeten worden beoordeeld.
Voorts blijkt daaruit dat als het dossier onvoldoende informatie bevat omtrent de locatie e.d. van de in de tenlastelegging genoemde[342] bestanden met kinderpornografische afbeeldingen als regel vrijspraak volgt, omdat de opzet op het bezit daarvan veelal niet kan worden vastgesteld.[343]

4.2.1.1. Toegankelijke bestanden (accessible files)
Toegankelijke bestanden zijn die bestanden die door de gebruiker van de computer eenvoudig, (bijvoorbeeld) door aanklikken, kunnen worden geopend, en/of die duidelijk herkenbaar zijn in de bestandsstructuur, en derhalve ook kunnen worden verzonden, gekopieerd etc.. Ten aanzien van dergelijke bestanden wordt in de rechtspraak als regel aangenomen dat de gebruiker/verdachte daarover de beschikkingsmacht in de hiervoor bedoelde zin had.[344] Of een bepaald (afbeeldings)bestand direct toegankelijk is behoort ook te worden vermeld in het politie-proces-verbaal of deskundigenrapport.[345] Een wat grijs gebied

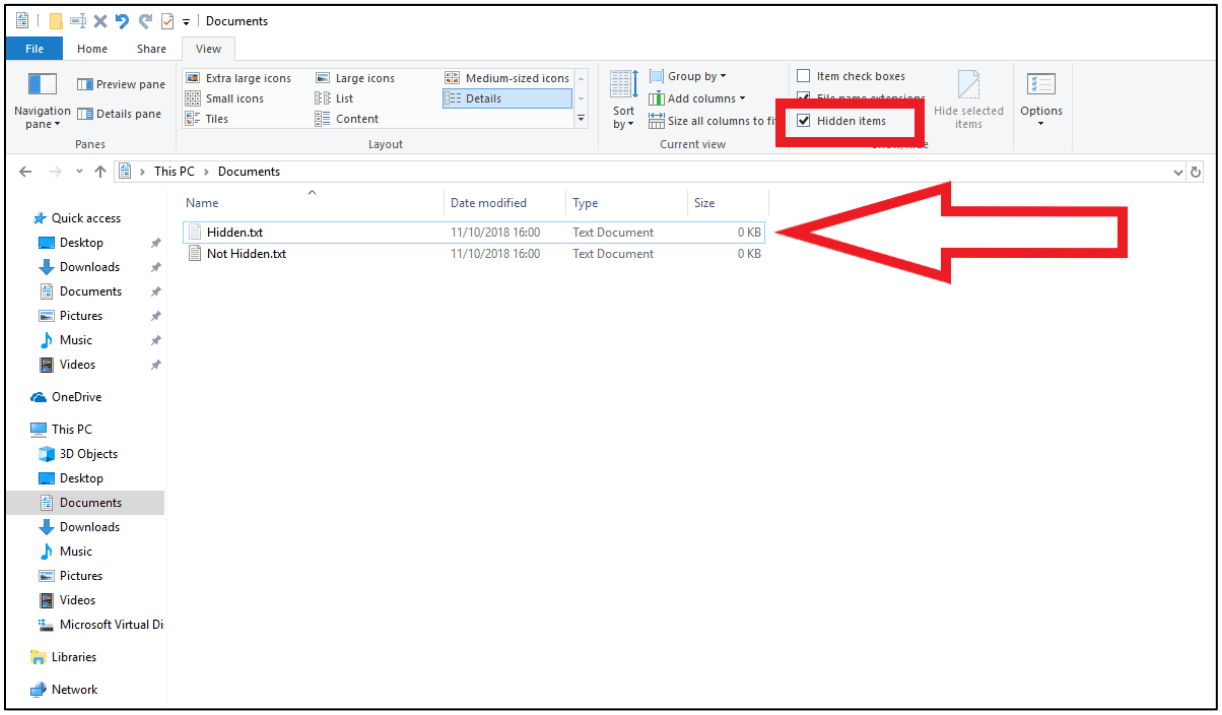
---

[341] Zie over dit en andere aspecten van beschikkingsmacht ook de conclusie van AG Knigge (ECLI:NL:PHR:2006:AU9104) bij HR 28-2-2006 (ECLI:NL:HR:2006:AU9104).
[342] Er moet dus ook om deze reden uit de tenlastelegging voldoende blijken om welke bestanden het gaat; zie hieromtrent o.m. RB Noord-Nederland 20-10-2017, ECLI:NL:RBNNE:2017:4022 (kinderpornografisch materiaal aangetroffen in *accessible* files, zijnde 5 afbeeldingen. Het is niet vast te stellen of deze afbeeldingen op de tenlastelegging zijn gekomen. Vrijspraak).
[343] Zie onder meer: RB Den Haag 25-9-2017, ECLI:NL:RBDHA:2017:11341 (op de gegevensdragers van verdachte zijn kinderpornografische filmpjes aangetroffen. "*Echter, er is geen informatie over zoekopdrachten, wijze van downloaden, waar het is opgeslagen, wijze van overzetten van computer naar externe harde schijf. Daarom kan de rechtbank geen oordeel vormen over de vraag of het ging om bijvangst, over de wetenschap van de inhoud van de bestanden, de vraag of verdachte deze bewust van computer naar externe gegevensdragers heeft overgeschreven en of hij wetenschap had van de bewaring van die bestanden op de externe schijf*.". Onvoldoende bewijs van opzet. Vrijspraak); RB Rotterdam 2-8-2017, ECLI:NL:RBROT:2017:6023 (vrijspraak voor het bezit/verwerven/ het zich toegang verschaffen tot kinderporno wegens het ontbreken van opzet (al dan niet in voorwaardelijke zin) daarop. T.a.v. vijf kinderpornografische filmpjes op de mobiele telefoon van verdachte is onduidelijk waar, wanneer en hoe de filmpjes op de mobiele telefoon zijn opgeslagen en of deze benaderbaar waren voor de verdachte en zo ja of hij zich daarvan bewust was).
[344] Zie o.m. conclusie van AG Machielse bij HR 3-9-2008, ECLI:NL:HR:2008:BD4872 (kinderpornobestanden in 'my documents'); Hof Amsterdam 21-9-2017, ECLI:NL:GHAMS:2017:4045 (De bestanden kunnen aangemerkt worden als kinderpornografische afbeeldingen. Gelet op de vindplaats (deels in de map 'verzonden items') minst genomen voorwaardelijk opzet op bezit daarvan); RB Zutphen 27-4-2011, ECLI:NL:RBZUT:2011:BQ2758 (afbeeldingen aangetroffen in normaal bereikbare en toegankelijke mappen, en niet in een plaats voor automatische opslag van onbewust gedownloade bestanden); RB Alkmaar 7-12-2010, ECLI:NL:RBALK:2010:BO6526 (kinderporno in zelfde map aanwezig als waar verdachte volwassenen porno in opsloeg); RB Assen 15-10-2010, ECLI:NL:RBASS:2010:BO0534 (veroordeling voor o.m. fotobestanden aangetroffen in Windows Photo Gallery).
[345] Hierbij kan niet worden volstaan – hetgeen in een niet te onderschatte aantal zaken toch gebeurt – met een enkele tabel waarin het totaal aantal als kinderpornografische aangemerkte afbeeldingen dat toegankelijk is wordt vermeld. In ieder geval per afbeelding die is opgenomen in de tenlastelegging zal het dossier moeten

betreft bestanden die in de zogenaamde prullenbak staan, zie nader par. 4.2.1.2.. Gezien de eigenschappen van de prullenbak rekenen wij ook daarin aanwezige bestanden tot de *accessible files*.

4.2.1.1.1. Hidden files / verborgen bestanden

Bijzondere aandacht verdient hier echter het feit dat er in ieder geval één categorie toegankelijke bestanden (*accessible files*) moet worden onderscheiden die niet zonder meer voor een gebruiker in de bestands(mappen)structuur herkenbaar is. Dat zijn de zogenaamde "*hidden files*" (verborgen bestanden).[346] Dergelijke bestanden kan een gebruiker normaliter alleen op zijn computer zien (en openen) wanneer de (standaard)instellingen zodanig zijn aangepast dat deze verborgen bestanden en mappen zichtbaar worden weergegeven. Dit laatste vereist overigens geen bijzondere technische kennis of vaardigheden. Op het internet zijn talloze handleidingen, ook van bijvoorbeeld Microsoft zelf, beschikbaar waarmee eigenlijk elke gebruiker op heel eenvoudige wijze "*hidden files*" kan laten weergegeven.[347] Dan ziet het er ongeveer uit als op deze afbeelding, waarbij het plaatsen van het vinkje in het rode kader heeft geleid tot het zichtbaar worden van het met de pijl aangegeven bestand:



vermelden of de afbeelding toegankelijk is, anders zal de rechter niet kunnen vaststellen dat ten aanzien van *die kinderpornografische afbeeldingen* sprake is van beschikkingsmacht.

[346] *Hidden files* (verborgen bestanden) zijn computerbestanden waarvan de naam niet op het scherm verschijnt in de lijst als men (de inhoud van) een map opvraagt. Ze worden enkel zichtbaar als men er expliciet om vraagt. Men kan naast bestanden ook mappen verbergen. Dat zijn namelijk ook bestanden. Die worden dan meestal aangeduid als *hidden folders* (verborgen mappen).
Een verborgen bestand is op de meeste computers meestal een configuratiebestand en is enkel van belang voor het systeembeheer (voor installatie van software en dergelijke). Een gewone gebruiker hoeft ze niet of zelden te zien en veelal is het zelfs beter dat de gewone gebruikers er afblijven, omdat een wijziging in een configuratiebestand de werking van een programma ernstig kan verstoren. Om die reden worden door softwarefabrikanten veel van dergelijke bestanden als *hidden files* (en steeds vaker ook in hidden folders) opgeslagen.

[347] Zie bijvoorbeeld https://support.microsoft.com/nl-nl/help/14201/windows-show-hidden-files en https://helpdeskgeek.com/windows-10/how-to-show-hidden-files-in-windows-10/.

Na aldus *de hidden files* zichtbaar te hebben gemaakt kan een gebruiker ook eenvoudig bestanden in de *hidden files*-(mappen)structuur opslaan en daarna ook weer benaderen.[348] Indien kinderpornografisch bestanden in de "*hidden files*" zijn aangetroffen, zal in beginsel uit het proces-verbaal c.q. het verhandelde ter terechtzitting moeten blijken dat hetzij van een dergelijke aanpassing van de instellingen op een inbeslaggenomen computer en/of gegevensdrager sprake was, hetzij dat deze mogelijkheid en/of de mogelijkheid van bestandsopslag onder de "*hidden files*" bij de verdachte bekend was. Een (sterke) aanwijzing voor dit laatste kan overigens zijn dat bestanden die normaliter niet in de *hidden files* thuishoren, zoals digitale kinderpornografische afbeeldingen, wel in een *hidden* files map zijn geplaatst.[349] Blijkt zulks niet, dan kan ten aanzien van materiaal in dergelijke *hidden files* niet zonder meer worden aangenomen dat dit materiaal toegankelijk was voor de verdachte.[350] Daarbij moet wel worden opgemerkt dat dit steeds minder een '*insider-tip*'lijkt te zijn. Onder de wat jongere alsook meer ervaren computergebruikers is dit steeds vaker geen geheim meer. Een kritische ondervraging en beoordeling op dit punt kan dan op zijn plaats zijn. Ronduit onjuist zijn overwegingen dat dergelijke *hidden files* alleen met hiervoor bestemde software te benaderen zijn.[351]

4.2.1.2. Bestanden in de "prullenbak" ("recycle bin")

Nagenoeg alle besturingssystemen bevatten een zogenaamde "prullenbak" (In het Engels ook wel "*trash*" (Mac OSX) of "*Recycle Bin*" (Windows) genoemd). Feitelijk is dit een map waarin bestanden terecht komen, waarvan de gebruiker heeft aangegeven dat deze verwijderd moeten worden. Door de plaatsing in de prullenbak zijn de betreffende bestanden echter niet van de computer verdwenen[352] en evenmin zijn zij daardoor niet meer toegankelijk voor de gebruiker. Integendeel, feitelijk zijn deze bestanden dan alleen maar verplaatst van de oorspronkelijke locatie op de computer naar de map "prullenbak". Bestanden behouden na plaatsing in de "prullenbak" ook hun oorspronkelijke bestandsnaam en kunnen direct en zonder gebruikmaking van andere en/of bijzondere software weer worden geopend en/of elders op de computer of een (externe) gegevensdrager worden (terug)geplaatst. De aanwezigheid van bestanden in de "prullenbak" impliceert derhalve dat de gebruiker ook na plaatsing van een bestanden in de prullenbak de *beschikkingsmacht* over dat bestand heeft behouden.[353] In de huidige rechtspraak wordt voorts aangenomen dat een gemiddelde

---

[348] De reden om bepaalde bestanden (bijvoorbeeld die met kinderpornografische afbeeldingen) in de "*hidden files*" op te slaan kan zijn dat een bepaalde gebruiker de aanwezigheid van die bestanden op een bepaalde computer "onzichtbaar" wenst te maken voor andere gebruikers (zoals gezinsleden) van diezelfde computer.

[349] Ook hier is echter voorzichtigheid bij het trekken van conclusies gewenst; in bepaalde gevallen kunnen ook bestanden, bijvoorbeeld *thumbnails* die in de *temporary files* waren opgeslagen, als gevolg van bijvoorbeeld een backup in de *hidden files* terechtkomen zonder dat de gebruiker zich daarvan bewust is geweest.

[350] Vgl. ook RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441, onder 4.3.2.

[351] RB Rotterdam 14-4-2021, ECLI:NL:RBROT:2021:3525 (45 kinderpornografische afbeeldingen betroffen thumbnails in een (verborgen) thumbnail-databasebestand. Het verborgen databasebestand waar de thumbnails in zijn opgeslagen, is alleen met hiervoor bestemde software te benaderen. Voor de aangetroffen video's, die zich bevinden in de categorie 'deleted', geldt dat ook deze niet zijn te benaderen zonder speciale software.) Hier lijken *hidden files* en *deleted files* (waarmee vermoedelijk niet wordt gedoeld op bestanden die zich in de prullenbak bevonden (zie hierover par. 4.2.1.2.) maar daaruit waren verwijderd en zich aldus in unallocated clusters bevonden) ten onrechte over een kam geschoren te worden.

[352] Sterker nog, de bestanden worden fysiek niet verplaatst, alleen de verwijzing in de index van de gegevensdrager wordt aangepast.

[353] Deze opvatting wordt thans zeer breed in de rechtspraak gedeeld. Zie o.m. RB Assen 15-3-2013, ECLI:NL:RBNNE:2013:BZ3851 (veroordeling bezit kinderporno, aantreffen bestanden in prullenbak); RB Arnhem 26-11-2012, ECLI:NL:RBARN:2012:BY4100 (veroordeling bezit kinderporno, verwerping verweer dat 17.000 bestanden in de prullenbak zijn geplaatst door herstelsoftware na een crash van de computer); RB Utrecht 9-2-2011, ECLI:NL:RBUTR:2011:BP3760 (veroordeling o.m. vanwege digitale kinderporno in prullenbak); RB Assen 15-10-2010, ECLI:NL:RBASS:2010:BO0534 (veroordeling voor bestanden in prullenbak);.

computergebruiker zich bewust behoort te zijn van de werking van de prullenbak[354] en derhalve ook kan worden aangenomen dat de gemiddelde gebruiker ermee bekend is dat hij feitelijk beschikkingsmacht heeft over de inhoud van de prullenbak. Deze beschikkingsmacht levert derhalve in beginsel ook voorwaardelijk opzet op.[355]

Onder omstandigheden kan plaatsing in de prullenbak echter wel een aanwijzing zijn dat de verdachte het bezit van het betreffende materiaal niet *gewild* heeft. Hierop wordt hierna onder 4.3.2. nader ingegaan, waarbij echter reeds nu wordt opgemerkt dat volgens vaste jurisprudentie plaatsing van (afbeeldings)bestanden in de prullenbak niet als een effectieve wijze van verwijdering wordt beschouwd.

4.2.1.3. Bestanden in map "Recovered folders" / "recovered files" / "lost files"

Technisch lemma: *recovered files, lost files* en *heap dumps*

De map "*recovered folders*" (soms ook "*recovered files*" genoemd) bevat normaliter (tijdelijke) bestanden zoals mails, tekstverwerkingsdocumenten, afbeeldingen e.d. die werden gebruikt door applicaties (zoals programma's) en systeemprocessen, op een moment dat die software of dat proces niet op een juiste manier werd afgesloten. Dit laatste kan diverse oorzaken hebben, zoals een stroomstoring, een crash van de harddisk, een software probleem door bijvoorbeeld een virusscanner, enz. De eerstvolgende keer na het incident dat het systeem wordt opgestart, verzamelt het systeem automatisch deze tijdelijke bestanden en plaatst ze in een map genaamd "*recovered folders* (of bijv. *recovered files*).

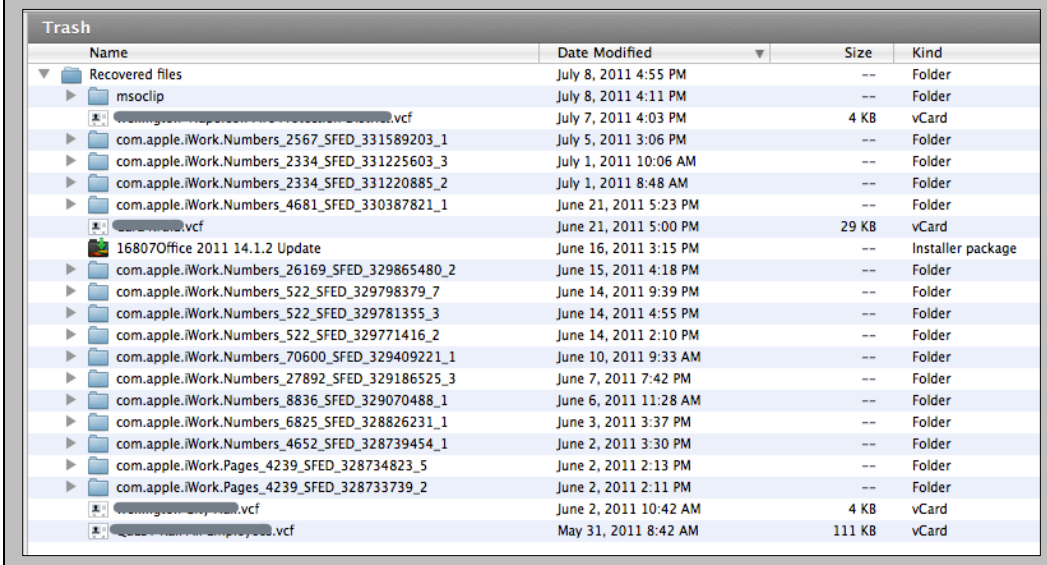
Op een computer die draait op Windows en waarop Outlook wordt gebruikt wordt deze map *recovered folders* ook wel geplaatst in de map "*prullenbak*" (of: "*thrash can"*). Dit laatste kan verwarrend zijn. Een "prullenbak" heeft namelijk op zich niets met *recovered folders* te maken. Voor het bestandsysteem is een prullenbak namelijk een "gewone" map. Het besturingssysteem behandelt deze map echter op een uitzonderlijke manier, waardoor daarin bijvoorbeeld ook zonder gerichte handeling van de gebruiker gegevens (zoals die in de *recovered folders*) terecht kunnen komen. De creatie en plaatsing van *recovered folders* en *files* maakt het in beginsel mogelijk voor de gebruiker om eventueel belangrijk geachte gegevens, die anders als gevolg van de storing of het onjuist afsluiten verloren zouden zijn gegaan weer terug te krijgen.

Dit "terugkrijgen" vereist echter wel enige computerkennis, onder meer omdat "*recovered files*" als regel geen bestandsnaam en datumaanduiding hebben (maar een niet tot de inhoud te herleiden rij van letters en cijfers) en hun aanwezigheid in de map waar zij zijn geplaatst niet altijd op het scherm zichtbaar is, omdat ze (zoals bijvoorbeeld bij Microsoft Word) als zogenaamde "*hidden" files* zijn opgeslagen. Bij Apple software is het wel iets eenvoudiger omdat de *recovered files* normaliter met die (map)naam in de prullenbak worden opgeslagen; ook dan zijn echter de individuele bestandsnamen niet direct te lezen (zie de afbeelding hierna). Met gespecialiseerde software, zoals de forensische software die de politie en het NFI gebruikt, is echter tamelijk eenvoudig de inhoud van *Recovered Folders* of *Files* te benaderen en weer zichtbaar te maken. *Hidden files* zijn op zichzelf ook voor eenieder met minimale inspanning zichtbaar te maken.[356]

---

[354] Aldus o.m. RB Utrecht 9-2-2011, ECLI:NL:RBUTR:2011:BP3760.
[355] In dezelfde zin: Stevens, L. & Koops, B.J., '*Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno*', Delikt en Delinkwent 2009, afl. 7/51, p. 669 e.v.
[356] Zie hiervoor onder 4.2.1.1.1.

Print van *recovered files folder* en *–files* in prullenbak van Apple macBook (OS X 10.6.8.)



Lost files
Lost files zijn bestanden die nog op een computer aanwezig zijn, maar niet meer direct vanuit de normale mappenstructuur zichtbaar zijn. Een veel voorkomende oorzaak voor het ontstaan van *lost files* is het verwijderen van een map (en alle daarin aanwezige bestanden) en het daarna aanmaken van een nieuwe mapnaam. De oude mapnaam wordt dan overschreven (en is niet meer te vinden), maar de daarin voorheen aanwezige bestanden niet. Deze bestanden blijven dus - tot zij ook zelf weer worden overschreven – aanwezig op de computer en in de Windows (MFT)verwijzingstabel, maar zijn voor een normale gebruiker niet meer zichtbaar. Met forensische software, zoals het ook door de Nederlandse politie veel gebruikte EnCase-programma, zijn deze wel zeer eenvoudig terug te halen.

Heap dumps
De *heap* is de naam voor een deel van het RAM (werk)geheugen dat wordt gebruikt door een actieve toepassing. *Heap dumps* bevatten een kopie van de inhoud van dit geheugen. Dit type bestanden wordt geschreven door het Windows besturingssysteem als een toepassing onverwacht stopt, bijvoorbeeld door een crash van de computer of de actieve toepassing. Het wordt over het algemeen aangetroffen in een tijdelijke map op de computer. De inhoud van dergelijke *heap dumps* kan relevante informatie bevatten. Zo kan een *heap dump* van een P2P-uitwisselingsprogramma bestandsnamen bevatten die duiden op kinderpornografische inhoud, wat grond kan zijn voor een vermoeden van interesse in dergelijk materiaal.

Naar mag worden aangenomen zal een gemiddelde gebruiker niet weten dat elders niet meer op zijn computer aanwezig materiaal zich nog wel in *recovered folders* of *files* kan bevinden. Het is ook niet vanzelfsprekend dat hij in staat zal zijn om die mappen en/of bestanden (weer) te benaderen en/of te openen. Daarom wordt in de jurisprudentie vrijwel unaniem aangenomen dat het enkele aantreffen van kinderpornografisch materiaal in de map *recovered folders* (c.q. de map *recovered file*s c.q. de map *lost files*) onvoldoende bewijs vormt voor het hebben van (voorwaardelijk) opzet op het “in bezit hebben” van het in die map bevindende kinderpornografische materiaal.[357]

[357] Zie o.m. RB Rotterdam 29-6-2021, ECLI:NL:RBROT:2021:6110 (partiële vrijspraak t.a.v. 2 bestanden op de laptop van verdachte, waarvan één bestand was aangetroffen in de map ‘*lost files*’. Uit een getuigenverklaring volgt dat dit filmpje abusievelijk verkeerd in de collectiescan was opgenomen omdat het niet (meer) toegankelijk was zonder gebruikmaking van (speciale) software); RB Limburg 17-12-2014, ECLI:NL:RBLIM:2014:11386 (vrijspraak kinderpornografisch materiaal in *lost files* en *temporary internet files*; niet kan worden aangenomen dat gemiddelde computergebruiker over voldoende kennis van tijdelijke mappen beschikt om aan te nemen dat het aantreffen van bepaalde bestanden in de tijdelijke mappen het bezit daarvan impliceert; RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (kinderpornografie in *lost files*; vrijspraak).

Blijkt echter dat de verdachte over een meer dan gemiddelde kennis van computers en/of van de werking van de opslag en benadering van tijdelijke bestanden beschikt, dan kan dit anders komen te liggen. Hetzelfde geldt, indien uit digitaal forensisch onderzoek blijkt dat de in de map *recovered folders* (etc.) opgeslagen kinderpornografische afbeeldingen feitelijk wel gedurende een zekere vast te stellen periode voor de verdachte beschikbaar waren voor benadering en/of opening, of dat de verdachte die afbeeldingen bewust in die map opsloeg. Dan zal waarschijnlijk wel opzet op het "in bezit hebben" van die afbeeldingen kunnen worden aangenomen.[358]

Betreft het materiaal in de map "*Lost Files*" dan kan dergelijk onderzoek onder omstandigheden overigens ook tot de conclusie leiden dat voorafgaand aan de plaatsing (bewuste) verwijderingshandelingen zijn verricht, hetgeen een aanwijzing kan zijn dat de verdachte juist geen opzet had op het bezit van die afbeeldingen[359], maar ook van het feit dat hij zich op enig moment bewust is geweest van de aanwezigheid daarvan.

Tenslotte dient ook hier te worden onderkend dat het aantreffen van kinderpornografisch materiaal in de map *Recovered Folders* of *Lost files* (etc.) wel een aanwijzing kan vormen dat de verdachte zich op enig moment via een geautomatiseerd werk "toegang heeft verschaft" tot kinderporno, zodat een eventuele vrijspraak voor "het in bezit hebben" niet automatisch ook een vrijspraak voor dit bestanddeel van de delictsomschrijving van art. 240b Sr impliceert.

4.2.1.4. Bestanden in mappen met tijdelijke internetgegevens

Technisch lemma: Tijdelijke internetgegevens

Internetbrowsers (zoals Google Chrome, Mozilla Firefox en Microsoft Edge) slaan automatisch website-gegevens op in daartoe bestemde bestanden of mappen op een device. Deze website-gegevens, welke kunnen bestaan uit cookies, scripts en ook afbeeldingen, worden opgeslagen zodat deze beschikbaar zijn wanneer de gebruiker dezelfde website opnieuw bezoekt. Een internetpagina laadt immers sneller als gegevens die tussentijds niet veranderd zijn vanaf het device worden geladen, in plaats van via de internetverbinding opnieuw moeten binnenkomen. Bovendien dragen bepaalde opgeslagen website-gegevens bij aan het gemak, bijvoorbeeld doordat de sessie bewaard wordt en de gebruiker daardoor niet opnieuw hoeft in te loggen.

Een generieke naam voor al deze website-gegevens zou tijdelijke internetgegevens kunnen zijn. In het Engels wordt veelal gesproken over '*internet browser cache'*.[360] Er wordt nog wel eens gesproken over '*Temporary Internet Files'*, de term die Microsoft gebruikte bij de inmiddels niet meer ondersteunde browser Internet Explorer. De aanduiding "tijdelijk" of "*temporary*" is hierbij overigens in zekere zin misleidend. De tijdelijke gegevens kunnen langere tijd en in theorie zelfs eindeloos op het device van een gebruiker blijven staan,

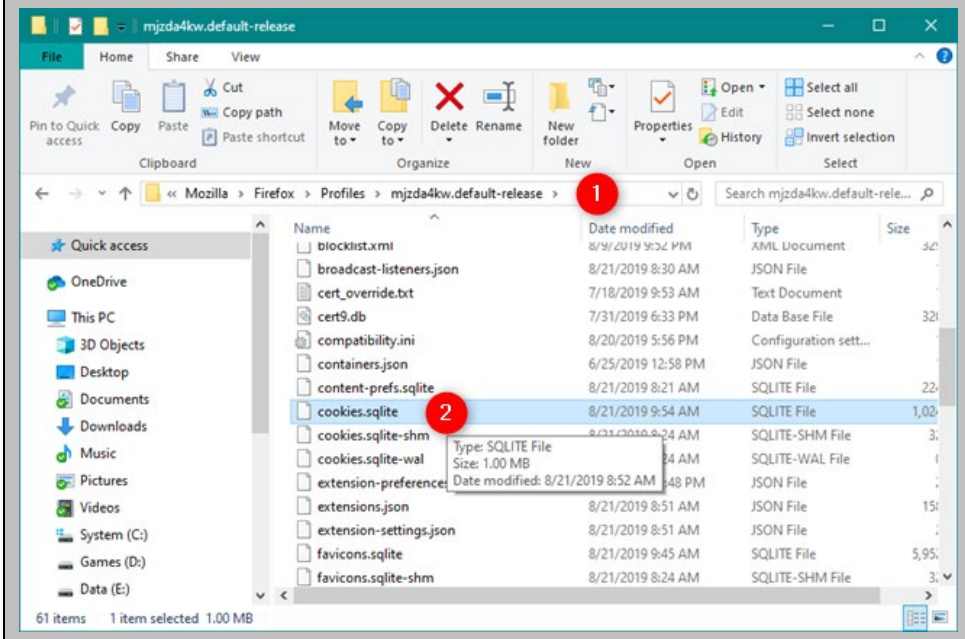
[358] Hof Den Bosch 19-6-2018, ECLI:NL:GHSHE:2018:2643 (verdachte had op zijn telefoon 47 kinderpornografische afbeeldingen van benadeelde partij 3, die niet zichtbaar waren voor de gebruiker. Bezit kon daarom niet bewezen worden geacht. Leerzaam is wat het hof hier vervolgens aan heeft toegevoegd: "*De redenering van het openbaar ministerie dat de verdachte bedoelde afbeeldingen 'ooit' in bezit moet hebben gekregen omdat hij een relatie heeft gehad met [benadeelde partij 3] zou op zichzelf wellicht nog wel te volgen zijn indien een bepaalde tijdsperiode ten laste was gelegd (bijvoorbeeld een periode gerekend vanaf de aanvang van die relatie), maar de redenering kan niet leiden tot een bewezenverklaring van het in bezit hebben van die afbeeldingen op 26 maart 2014 zoals i.c. ten laste is gelegd. Op die datum (de datum van inbeslagname van de gsm) waren de afbeeldingen immers niet (meer) zichtbaar voor de gebruiker van de gsm*."

[359] Vgl. RB Noord-Holland 23-4-2014, ECLI:NL:RBNHO:2014:3705 (afbeeldingen in *lost files*; raadsman betoogt dat plaatsing in lost files volgens deskundige aangehaald in uitspraak RB Amsterdam 24-12-2008 (n.g.) impliceert dat voorafgaand verwijderingshandelingen zijn verricht; RB constateert dat afbeeldingen voor verdachte niet benaderbaar waren; vrijspraak van *bezit* kinderpornografie).

[360] Zie ook "I didn't see that! An examination of internet browser cache behavior following website visits", G. Horsman, Digital Investigation, 2 maart 2018.

totdat de tijdelijke internetgegevens door de gebruiker – handmatig, via een schijfopruimingsprogramma zoals CCleaner of na deïnstallatie van de betreffende browser – worden gewist.

De tijdelijke internetgegevens zijn voor een gebruiker slechts beperkt inzichtelijk. Waar voorheen alle tijdelijke internetgegevens in een daartoe bestemde, verborgen map werden opgeslagen en na enige handelingen van de gebruiker konden worden ingezien, worden tijdelijke internetgegevens tegenwoordig vooral in daartoe bestemde databases opgeslagen. In het hieronder opgenomen voorbeeld is te zien dat Microsoft Firefox, geïnstalleerd op besturingssysteem Windows 10, de tijdelijke internetgegevens heeft opgeslagen op de volgende locatie (1): "`C:\Users\[USERNAME]\AppData\Roaming\Mozilla\Firefox\Profiles`". Te zien zijn verschillende database-bestanden, zoals het databasebestand "cookies.sqlite" (2) waarin alle cookies zijn ondergebracht. Deze database is, zij het niet zo eenvoudig, te openen via een optie in de browser zelf.[361]



Over het algemeen worden afbeeldingen en andere mediabestanden opgeslagen in een cachebestand in dezelfde map. Het is voor de gebruiker bepaald niet eenvoudig deze gegevens te bekijken, doordat er feitelijk sprake is van een gecomprimeerde database die niet te openen is met reguliere programma's. Er bestaan freeware toepassingen die een gebruiker in staat stellen om een cachebestand van zijn browser en daarin opgeslagen afbeeldingen in te kunnen zien, en een aantal browsers biedt ook zelf toepassingen met die functie aan, maar over het algemeen kan gesteld worden dat dergelijk onderzoek van de gebruiker trekken vertoont van "echt" forensisch digitaal onderzoek.

Privacy mode

Veel internetbrowsers bieden de mogelijkheid tot browsen in een *privacy mode*. Bekende namen voor deze toepassing zijn Incognito Modus (Google Chrome) en InPrivate (Microsoft Edge). De functie van de toepassing is de gebruiker van de browser in staat te stellen om te browsen zonder dat de browser tijdelijke internetbestanden opslaat op het device. In feite komt het hierop neer dat de browser een apart venster hanteert, geschiedenis wordt niet opgeslagen en cookies worden apart opgeslagen. Wordt het venster gesloten, dan verwijdert de browser deze cookies. Het staat daarmee volledig los van andere toepassingen die een mate van anonimiteit op het internet verschaffen, zoals het gebruik van een proxy, de TOR-browser en dergelijke. Bovendien blijven bij sommige browsers bepaalde gegevens toch bewaard.[362]

Hoewel de *tijdelijke internetbestanden* voor gebruikers over het algemeen niet direct toegankelijk zijn, bestaan er mogelijkheden om de tijdelijke internetbestanden in te zien. Het

[361] Zie voor een uitleg: https://www.digitalcitizen.life/how-view-remove-cookies-mozilla-firefox
[362] Zie o.a. Hughes et al., "Browsers private mode: is it what we were promised?", *Computers* 2021(10), 165. Horsman et al., "A forensic examination of web browser privacy-modes", *Forensic Science International* 2019(1).

is echter de vraag hoe veel van hen zich in de eerste plaats daadwerkelijk bewust zijn van de geautomatiseerde opslag van tijdelijke internetgegevens.[363] Evenzo is het de vraag of een gemiddelde computergebruiker kennis heeft van de precieze werking van de door hem gebruikte internetbrowser en de mogelijkheden om tijdelijke internetgegevens te benaderen of effectief te verwijderen.

De rechtspraak laat tot op heden in overwegende mate het beeld zien dat het enkele aantreffen van kinderpornografisch materiaal in tijdelijke internetgegevens niet als voldoende bewijs voor het hebben van opzet op het "in bezit hebben" van dat materiaal wordt beschouwd.[364] Er zijn echter ook uitspraken, waarin – zo begrijpen wij deze althans – de aanwezigheid van bestanden in de tijdelijke internetgegevens als een voor de gebruiker kenbaar en voorzienbaar gevolg van zijn zoeken op internet naar kinderpornografisch materiaal wordt geduid, en waarin dus ook ten aanzien van in die map opgeslagen afbeeldingen tot een bewezenverklaring van "in bezit hebben" wordt gekomen.[365]

---

[363] In dit verband toch wel opvallend: RB Gelderland (militaire kamer) 19-3-2018, ECLI:NL:RBGEL:2018:1204 ("*In de rij "Temporary files" staan de bestanden die zijn aangetroffen op de locatie waar de tijdelijke internetbestanden worden opgeslagen. Deze bestanden zijn zonder speciale software door de gebruiker te benaderen. Derhalve kan ook bewezen worden dat verdachte deze film in zijn bezit heeft gehad").* Dat iets in zuiver technische zin mogelijk is, wil immers nog niet zonder meer zeggen dat een verdachte daarvan ook op de hoogte was en/of in staat was c.q. moest worden geacht die technische operatie zelf ook uit te voeren.

[364] Zie o.m. Hof Amsterdam 21-9-2017, ECLI:NL:GHAMS:2017:4045 (de bestanden kunnen aangemerkt worden als kinderpornografische afbeeldingen; Voor een deel van de afbeeldingen volgt vrijspraak, nu deze onvoldoende blijk geven van een seksuele gedraging en/of deze zijn aangetroffen in *cache*-mappen of in de *Temporary Internet Files*, terwijl niet uitgesloten kan worden dat verdachte omtrent die afbeeldingen onwetend is geweest van een mogelijke aanwezigheid daarvan op die locaties van zijn laptop); Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (vrijspraak t.a.v. diverse kinderpornografische afbeeldingen in de vorm van thumbnails in *cache* nu deze zich op een voor een gemiddelde computergebruiker niet zonder meer toegankelijke of zichtbare opslaglocatie bevonden en mitsdien het opzet op bezit van die afbeeldingen niet is vast te stellen); RB Noord-Nederland 20-10-2017, ECLI:NL:RBNNE:2017:4022 (voor zover het gaat om bestanden die in de *temporary internet files* en *deleted items* stonden opgeslagen is niet gebleken dat verdachte over specifieke kennis of software beschikte om deze bestanden in te zien. Vrijspraak); RB Limburg 1-10-2017, ECLI:NL:RBLIM:2017:7501 (bezit kinderporno. Drie bestanden waren *accessible*, de overige bestanden stonden in de *temporary internet files* of tussen de gewiste bestanden afkomstig uit de *temporary files*. Van die bestanden kan dus niet gezegd worden dat er sprake was van een bewuste vastlegging van het materiaal, omdat de bestanden automatisch door het systeem zijn aangemaakt); RB Gelderland 31-12-2015, ECLI:NL:RBGEL:2015:8242 (vrijspraak van bezit van afbeeldingen in de *temporary internet files,* in een map die als *'hidden'* is aangemerkt. Deze bestanden waren voor de gebruiker van de computer niet zichtbaar. Ook is uit onderzoek van de digitale rechercheurs naar voren gekomen dat niet actief is gezocht naar kinderporno en evenmin is speciale software aangetroffen waardoor de bestanden alsnog zichtbaar zijn geworden).

[365] Zie bijv. RB Oost-Brabant 19-10-2021, ECLI:NL:RBOBR:2021:5487 ("*ook de grote hoeveelheid thumbnails (kleine fotobestanden) en cachebestanden (tijdelijke bestanden) duiden naar het oordeel van de rechtbank op actief zoeken naar kinderporno, nu dit soort bestanden automatisch wordt opgeslagen wanneer men een zoekopdracht uitvoert*"); RB Zeeland-West-Brabant 7-9-2020, ECLI:NL:RBZWB:2020:4197 ("dat verdachte niet gericht op zoek is geweest naar kinderporno brengt naar het oordeel van de rechtbank echter niet mee dat het verweer van de verdediging, dat geen sprake is geweest van opzet *(KCC: op het in bezit hebben van kinderporno)* opgaat"). RB Rotterdam 22-3-2016, ECLI:NL:RBROT:2016:2166 (films zijn aangetroffen in de *temporary internet files*, "Volgens de huidige jurisprudentie hoeft de gemiddelde computergebruiker niet op de hoogte te zijn van het verschijnsel "tijdelijke internetbestanden", zodat ook dit niet als zodanig opzettelijk bezit oplevert. Dat ligt anders wanneer uit omstandigheden kan worden afgeleid dat de verdachte actief is bezig geweest met dergelijk materiaal. Verdachter heeft actief gezocht en vervolgens het gevondene bekeken. De wil van de verdachte was derhalve gericht op het verkrijgen van (i.c.) dierenporno. Daarmee is, zowel ten aanzien van de verwijderde films, als de films die aangetroffen zijn in de *tijdelijke internetbestanden*, aan het (voorwaardelijk) opzetvereiste voldaan.".

Hoewel in deze uitspraken wellicht wat snel over de vereisten van "beschikkingsmacht" en "wetenschap" (van de *aanwezigheid* van de betrokken afbeeldingen) lijkt te worden heengestapt, passen deze uitspraken wel in een trend dat een simpel "wist ik niet"-verweer bij herhaalde en gerichte internetzoekacties blijkend uit tijdelijke internetgegevens steeds minder wordt aanvaard.[366] Het lijkt dan ook niet al te gewaagd zijn om te veronderstellen dat – met de toename van de kennis van de gemiddelde computergebruikers – een verweer dat inhoudt dat men niet wist/vermoedde dat de resultaten van internetzoekacties ook op de computer/in de tijdelijke internetgegevens werden opgeslagen, de komende jaren minder zal worden aanvaard.

Overigens dient ook hier te worden opgemerkt dat het aannemen van opzet in deze gevallen in ieder geval meer in de rede ligt, indien – al dan niet na daarop gerichte bevraging – blijkt dat de verdachte over een meer dan gemiddelde kennis van computers en/of het fenomeen "tijdelijke internetgegevens" beschikt.[367] Hetzelfde geldt indien uit forensisch digitaal onderzoek blijkt dat de verdachte zich feitelijk wel toegang verschafte tot het in de tijdelijke internetgegevens opgeslagen materiaal.[368] Een indicatie[369] voor wetenschap van het bestaan en de werking van tijdelijke internetgegevens kan ook zijn een door de gebruiker geïnstalleerde *browserplugin* of *add-on* in de betreffende browser die automatisch de tijdelijke internetgegevens verwijdert bij het afsluiten van de browser.

Tenslotte dient ook hier te worden onderkend dat het aantreffen van kinderpornografisch materiaal in de tijdelijke internetgegevens of in een andere cachemap in de regel wel een (sterke) aanwijzing zal vormen dat de verdachte zich via een geautomatiseerd werk toegang heeft verschaft tot kinderporno (het betreft hier immers per definitie materiaal dat op een eerder moment via het internet is benaderd), zodat een eventuele vrijspraak van "in bezit hebben" bepaald niet automatisch ook een vrijspraak van dit bestanddeel van de delictsomschrijving van art. 240b Sr impliceert.

4.2.1.5. Bestanden in "unallocated clusters" / "deleted files"

In zeer veel art. 240b-zaken blijkt uit het proces-verbaal dat (soms: grote aantallen) afbeeldingen, of gedeelten daarvan, zijn aangetroffen in de *unallocated clusters* van een onderzochte gegevensdrager (meestal een harde schijf). De afbeeldingen zijn daarop meestal

---

[366] Er zijn echter ook gevallen bekend waarin een dergelijk verweer juist weinig kritisch werd aanvaard; zie o.m. RB Den Haag 1-12-2020, ECLI:NL:RBDHA:2020:12227 ("*Hoewel het aantreffen van dergelijke 'thumbnail' en 'cache' bestanden wel een (sterke) aanwijzing vormt dat de verdachte de ten laste gelegde gedragingen met het betreffende kinderpornografische materiaal heeft gepleegd, bevat het dossier daarvoor onvoldoende bewijs. Zo ontbreken onder andere gegevens waaruit blijkt dat de verwachte (sic!) bewust naar dergelijke afbeeldingen heeft gezocht en hoe vaak dat zou zijn gebeurd en wanneer de afbeeldingen op de mobiele telefoon zijn bekeken dan wel op de gegevensdragers hebben gestaan en in het laatste geval op welke wijze zij daarop terecht zijn gekomen.*").

[367] Een belangrijke *aanwijzing* daarvoor kan bijvoorbeeld zijn dat op de betreffende computer software is geïnstalleerd die de gebruiker in staat stelt om verborgen cache-bestanden zichtbaar te maken.

[368] Zie bijv.: RB Oost-Brabant 14-4-2014, ECLI:NL:RBOBR:2014:1773 (bestanden in *temporary internet files*; op grond van het verrichte onderzoek kan worden vastgesteld dat verdachte bewust naar deze afbeeldingen heeft gezocht en dat verdachte ook bewust een handeling heeft verricht waardoor deze op de computer zijn opgeslagen, hetgeen ook blijkt uit de verklaring die verdachte hierover heeft afgelegd en de door hem op internet ingevoerde zoektermen).

[369] Voor het ontlenen van een indicatie lijkt het gewenst om nader vast te stellen in hoeverre de gebruiker op de hoogte is van de werking van een dergelijk programma en wat zijn precieze bedoeling is geweest bij het installeren van de *plugin* of *add-on*. Voorzichtigheid is ook hier geboden, nu het bepaald niet ondenkbaar is dat de gebruiker uit andere, legitieme overwegingen ("het scheelt schijfruimte") een dergelijk programma heeft geïnstalleerd.

terecht gekomen, doordat de gebruiker met betrekking tot de betreffende afbeeldingen een verwijderingsinstructie (zoals de opdracht tot het legen van de prullenbak) heeft gegeven. Daarin kan een aanwijzing besloten liggen dat de verdachte de afbeeldingen niet in zijn bezit wilde hebben en dacht deze effectief verwijderd te hebben. Dit geldt vooral bij geringe aantallen afbeeldingen, waarbij bovendien niet onaannemelijk is dat deze op één moment zijn verwijderd. Als op verschillende momenten afbeeldingen zijn "gewist" lijkt goed verdedigbaar dat zulks als een aanwijzing worden gezien dat verdachte kennelijk ook op verschillende momenten kinderpornografisch materiaal heeft ontvangen, en die vervolgens weer (al dan niet na enige tijd) heeft verwijderd. Het is verdedigbaar dat indien een dergelijke omstandigheid is geconstateerd, van de verdachte daaromtrent een nadere uitleg kan worden gevraagd, bij gebreke waarvan eventueel zou kunnen worden aangenomen dat de verdachte in de periode tussen binnenkrijgen van de afbeeldingen en het "wissen" daarvan, die afbeeldingen in bezit heeft gehad.[370]

Zoals uit de technische uitleg blijkt, zijn bestanden in de *unallocated clusters* bovendien normaliter niet (meer) toegankelijk voor een normale gebruiker. Omdat dan ook de beschikkingsmacht over die afbeeldingen ontbreekt, is naar vaste rechtspraak de enkele bevinding dat kinderpornografische afbeeldingen zijn aangetroffen in de *unallocated clusters* van een gegevensdrager onvoldoende voor het aannemen van "*bezit*" in de zin van art. 240b Sr.[371]

Dit kan echter anders zijn, indien er sprake is van bijkomende omstandigheden, waaruit bijvoorbeeld blijkt de verdachte kon beschikken over specialistische, forensische software voor het "terughalen" van verwijderde bestanden.[372] Een tweede relevante omstandigheid kan in dit verband zijn de bevinding dat de *unallocated* bestanden gedurende een zekere periode beschikbaar voor opening zijn geweest. Dit laatste kan bijvoorbeeld blijken uit metadata[373] of browserinformatie, waaruit blijkt wanneer de betreffende bestanden gedownload zijn en wanneer zij weer zijn verwijderd.[374] Bij dit laatste kan eventueel ook worden betrokken de

---

[370] Zie in deze zin ook Hof Den Haag 29-10-2015, ECLI:NL:GHDHA:2015:2992 en hierna onder 4.3.2.

[371] Aldus ook o.m. Koops e.a., a.w., p. 6; In deze zin ook o.m. RB Limburg 23-6-2021, ECLI:NL:RBLIM:2021:4948; RB Noord-Nederland 6-5-2021, ECLI:NL:RBNNE:2021:1748; RB Noord-Nederland 15-4-2021, ECLI:NL:RBNNE:2021:1925; RB Amsterdam 26-1-2017, ECLI:NL:RBAMS:2017:537; RB Gelderland 28-8-2015, ECLI:NL:RBGEL:2015:5477; RB Noord-Nederland 19-3-2015, ECLI:NL:RBNNE:2015:1302; RB Noord-Holland 2-9-2014, ECLI:NL:RBNHO:2014:8421. *In dit licht opmerkelijk is*: RB Rotterdam 15-11-2017, ECLI:NL:RBROT:2017:8965 (t.a.v. bezit *deleted files* oordeelt de rechtbank dat 4 van de 44 bestanden op de USB stick weliswaar *deleted* waren, maar dat verdachte heeft verklaard dat de USB stick van hem is en niemand anders die gebruikte. Verdachte moet deze derhalve op enig moment in de tenlastegelegde periode in het bezit hebben gehad. Bewezenverklaring bezit kinderporno).

[372] Hof Den Haag 4-6-2015, ECLI:NL:GHDHA:2015:1381 (uit verklaringen van de verdachte blijkt dat hij beschikte over de kennis en software om de bestanden op zijn vastgelopen harde schijf weer toegankelijk te maken; bewezenverklaring bezit); RB Zeeland-West-Brabant 6-6-2013, ECLI:NL:RBZWB:2013:CA2290 (speciale software aangetroffen waarmee bestanden in de *unallocated clusters* te benaderen zijn; bewezenverklaring bezit); vgl. ook: RB Gelderland 28-8-2015, ECLI:NL:RBGEL:2015:5477 (volgens de in het proces-verbaal opgenomen toelichting zijn bestanden die '*deleted* zijn' zonder daarvoor bestemde software niet meer eenvoudig te benaderen door de gebruiker. Gesteld noch gebleken is dat verdachte beschikte over deze speciale software).

[373] Zie over dergelijke metadata, waaronder de datum- en tijdgegevens betreffende (handelingen met) bestanden hierna onder 6.2.4.

[374] Vgl. Hof Den Haag 29-10-2015, ECLI:NL:GHDHA:2015:2992 (kinderpornografie aanwezig op *unallocated clusters* op usb-stick en externe hard disk; uitzondering op regel dat zulks niet leidt tot bewijs van "bezit"; verdachte heeft erkend te hebben gedownload en deze ook op externe gegevensdragers te hebben vastgelegd; dit laatste vereist een actieve, bewuste handeling gericht op vastlegging; in de tijd tussen het vastleggen van de afbeeldingen op de externe gegevensdragers en het op enig moment weer "wissen" daarvan, had verdachte de

aanwezigheid op het systeem van betrokkene van speciale verwijderingssoftware die periodiek eerder gedownloade bestanden verwijdert. Dan kan immers worden gesteld dat in ieder geval in de periode tussen het downloaden en het moment waarop deze software (blijkens de instellingen) de bestanden weer verwijderde, betrokkene beschikkingsmacht over deze bestanden had.[375]

Het aantreffen van kinderpornografisch materiaal in de *unallocated clusters* zal – ook indien "*bezit*" niet kan worden bewezen – in de regel ook een (sterke) aanwijzing vormen dat de verdachte zich op enig moment voordat het materiaal in de *unallocated clusters* terecht kwam "via een geautomatiseerd werk toegang heeft verschaft" tot het betreffende materiaal. Een eventuele vrijspraak voor "in bezit hebben" impliceert dan ook geenszins dat ook vrijspraak voor dit bestanddeel van de delictsomschrijving van art. 240b Sr dient te volgen.[376]
Naast het aantreffen van de afbeeldingen in de *unallocated clusters* zal dan echter ook nog ander (steun)bewijs moeten voorliggen, waaruit in ieder geval moet kunnen worden afgeleid dat de verdachte actieve bemoeienis had met kinderpornografisch materiaal op internet. Daarbij kan onder meer worden gedacht aan de zoekopdrachten die de verdachte in zijn browser heeft ingegeven, de sites die hij heeft bezocht, aanwijzingen omtrent de internetlocatie waarvandaan de afbeeldingen afkomstig zijn, de inhoud van chatsessies of een (deels) bekennende verklaring van de verdachte. In dergelijke gevallen zal dus het gegeven dat kinderpornografische bestanden zijn aangetroffen in de *unallocated clusters* wel kunnen

---

afbeeldingen in zijn "bezit"). Uit deze uitspraak blijkt echter niet hoe is vastgesteld dat de afbeeldingen gedurende een zeker tijd ook beschikbaar waren voor de verdachte. Dit was wel het geval in RB Midden-Nederland 14-5-2018, ECLI:NL:RBMNE:2018:2060 ("*Echter, onder de deleted kinderpornografische bestanden bevinden zich ook foto's en films van [slachtoffer]. Ten aanzien van deze foto's en films heeft verdachte zowel bij de politie als ter terechtzitting erkend dat hij deze bestanden heeft gemaakt. Van deze bestanden staat aldus vast dat verdachte daarover de beschikking heeft gehad en van een aantal van deze bestanden ook wanneer hij die heeft gehad.*").

[375] Zo begrijpen de auteurs ook RB Overijssel 26-2-2016, ECLI:NL:RBOVE:2016:671 (afbeeldingen op *unallocated clusters* meegenomen bij bewezenverklaring vanwege surf -en uitwisselingsgedrag en aanwezigheid programma *CCleaner,* dat periodiek wiste) (opm. auteurs: CCleaner is een zeer populaire 'utility' voor onder meer het verwijderen van bepaalde bestanden) en mogelijk (want geen expliciete overweging m.b.t. beschikkingsmacht) RB Gelderland 2-5-2016, ECLI:NL:RBGEL:2016:2502 (zoektermen en zoekslagen via torrent websites herleidbaar naar verschillende aangetroffen kinderpornografische afbeeldingen en/of filmbestanden. Computers waar afbeeldingen op stonden waren bovendien nieuw aangeschaft na inbeslagname van eerdere computers in mei 2012. Ook gelet op verklaringen dat computers nieuw waren. Gelet op deze feiten en omstandigheden is de rechtbank van oordeel dat verdachte naast de bestanden die op 23 april 2014 in een '*accessible'* cluster stonden ook de bestanden die '*deleted*' waren en bestanden die in '*unallocated' clusters* stonden op enig moment in de periode van 11 mei 2012 tot en met 23 april 2014 heeft verworven en in zijn bezit heeft gehad). Een variant hierop deed zich voor in RB Midden-Nederland 20-6-2018, ECLI:NL:RBMNE:2018:2779 (er was sprake van verwijderde en niet door de gebruiker te benaderen en zichtbare bestanden, met uitzondering van een bestand waarvan de bestandnaam de tussenvoeging 'VERPLAATSEN NAAR EXTERNE SCHIJF' bevatte. Hieruit maakte de rechtbank op dat het bestand, na gedownload te zijn, door de gebruiker van de gegevensdrager hernoemd is. De rechtbank stelt vast dat de verdachte zich hiervan bewust is geweest.).

[376] Het onderscheid tussen in bezit hebben en zich via een geautomatiseerd werk de toegang verschaffen lijkt onvoldoende te zijn gemaakt in RB Gelderland 16-2-2016, ECLI:NL:RBGEL:2016:856 ("De rechtbank acht niet wettig bewezen dat verdachte zich in de tenlastegelegde periode *de toegang heeft verschaft* tot 118 kinderpornografische foto's, nu deze foto's gewiste bestanden betroffen die zonder daarvoor bestemde software niet meer eenvoudig door verdachte te benaderen waren en niet is vast te stellen wanneer deze bestanden door verdachte zijn gewist. Voorts is niet gebleken dat voornoemde software op de gegevensdragers van verdachte is aangetroffen").

bijdragen tot het bewijs dat de verdachte zich "via een geautomatiseerd werk toegang heeft verschaft tot kinderpornografische afbeeldingen".[377]

Een bijzonder aandachtspunt bij het onderzoek en de beoordeling van materiaal dat in de *unallocated clusters* is aangetroffen, is dat veelal de datering van (delen van) bestanden in de *unallocated clusters* ontbreekt. Soms omdat deze informatie ontbreekt, of niet voldoende betrouwbaar is vast te stellen, maar soms (helaas) ook omdat daaraan bij het opmaken van het proces-verbaal eenvoudig geen aandacht is besteed.[378] Zulks kan – zeker als de tenlastelegging een relatief beperkte periode omschrijft, en het onderzoek niet mede gericht is geweest op deze datering – tot problemen leiden bij de beantwoording van de vraag of de gestelde gedraging ook in de tenlastegelegde periode is begaan.[379]

Denkbaar is echter wel dat in voorkomende gevallen in de tenlastelegging dan als ondergrens de productie- dan wel aanschafdatum van de gegevensdrager (of de productie- of verkoopdatum van het geautomatiseerde werk waarin de gegevensdrager zich bevond) wordt genomen waarop het incriminerende materiaal is aangetroffen.[380] Deze datum zal dan vanzelfsprekend wel uit het dossier c.q. uit het onderzoek ter terechtzitting moeten blijken.

4.3. Opzet en de wil om het materiaal te bezitten, ontvangen enz.

Het komt in de rechtspraktijk regelmatig voor dat verdachten van overtreding van art. 240b Sr niet ontkennen dat het kinderpornografisch materiaal op hun computer aanwezig is (of is geweest), of dat zij daartoe feitelijk (via internet) toegang hebben gehad, maar aanvoeren dat die aanwezigheid of die toegang niet door hen beoogd c.q. gewild was.
Hier is oplettendheid geboden, want een dergelijk verweer houdt indirect een beroep in op het ontbreken van opzet, en vergt, indien het verworpen wordt, derhalve een expliciete motivering van de rechter.

Het verweer doet zich hoofdzakelijk in twee verschijningsvormen voor. De eerste vorm is dat de verdachte stelt dat het betreffende kinderpornografische materiaal is "meegekomen" met ander (meestal "gewoon" pornografisch materiaal) en dat men dat niet of niet direct heeft onderkend. De tweede modaliteit is dat men stelt het materiaal wel ontvangen en/of gezien te

---

[377] Vgl. m.b.t. "*hidden files*" bijv.: RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (bij bezoeken aan 3D websites waarvandaan ook werd gedownload meermalen ook echte kinderporno aangetroffen; grote aantallen kinderpornografische afbeeldingen in verborgen mappen aangetroffen, niet aannemelijk dat verdachte deze bij toeval samen met een 3D film heeft bekeken; (voorwaardelijk) opzet aangenomen t.a.v. "*toegang verschaffen tot*..."); RB Zeeland-West-Brabant 6-6-2013, ECLI:NL:RBZWB:2013:CA2290.

[378] Daarbij kan het echter wel zijn dat in de inhoud van de aangetroffen bestanden ook aanwijzingen te vinden zijn in welke periode zij (vermoedelijk) zijn ontvangen c.q. "verwijderd".

[379] RB Amsterdam 18-3-2016, ECLI:NL:RBAMS:2016:1474, r.o. 4.2.3.; RB Noord-Nederland 19-3-2015, ECLI:NL:RBNNE:2015:1302 (vrijspraak bezit kinderporno, aangetroffen in *unallocated clusters* en/of *deleted items*, periode kan niet worden vastgesteld).

[380] Zie bijv. ook RB Gelderland 2-5-2016, ECLI:NL:RBGEL:2016:2502 (bij datering mede betrokken dat computers op aanschafdatum nieuw waren). Aan de hand van de serienummers op gegevensdragers kan een fabrikant veelal de productiedatum verstrekken. De afbeeldingen moeten namelijk noodzakelijkerwijs na die datum op de gegevensdrager zijn geplaatst. Voor geautomatiseerde werken als PC's of laptops in zijn geheel hoeft dat niet altijd op te gaan, omdat men de daarin geplaatste gegevensdragers kan hebben vervangen. Indien echter de verdachte verklaart, dat dit niet gebeurd is of dat anderszins blijkt, kan eventueel ook de verkoopdatum waarop het geautomatiseerde werk aan de verdachte is verkocht als onderste begrenzing dienen ten aanzien van het tijdstip waarop de afbeeldingen op de gegevensdrager zijn geplaatst. Indien de tenlastelegging inhoudt "het zich via een geautomatiseerd werk toegang verschaffen tot ..." zal dan wel deze productie (of verkoop)datum moeten zijn gelegen na 1-1-2010, omdat voor deze datum deze gedraging nog niet strafbaar was gesteld.

hebben, maar het vervolgens (direct) te hebben verwijderd. Vanzelfsprekend kunnen beide verschijningsvormen zich ook tezamen voordoen.

4.3.1. "De kinderporno was 'bijvangst' bij het downloaden van 'gewone' porno"
Zoals onder 4.1.3.1. al is beschreven in het kader van het vereiste van wetenschap ten aanzien van de aanwezigheid van het materiaal, impliceert het enkele feit dat (al dan niet naast "gewone" pornografische afbeeldingen) *kinder*pornografische afbeeldingen zijn aangetroffen niet zonder meer tevens dat de gebruiker zich ook "willens en wetens heeft blootgesteld aan de aanmerkelijke kans" dat *kinder*pornografisch materiaal in bezit te krijgen.[381]

Of in deze gevallen wel voorwaardelijk opzet zal kunnen worden aangenomen, zal afhangen van de omstandigheden van het geval. Voor wat betreft beoordelingscriteria kan daarbij allereerst worden aangesloten bij de aanwijzingen voor de wetenschap omtrent de aanwezigheid van het materiaal als die hiervoor reeds genoemd zijn onder 4.1.1., zoals onder meer de gebruikte zoektermen, de naam van de bestanden[382] of websites en de mappen waarin de afbeeldingen zijn geplaatst.[383]

Daarnaast kan hier ook de hoeveelheid kinderpornografisch materiaal een rol spelen. Indien slechts enkele kinderpornografische afbeeldingen worden aangetroffen naast een grote hoeveelheid gewone porno of ander gedownload materiaal, kan dat een aanwijzing zijn dat sprake is van door de verdachte niet beoogde "bijvangst".[384] Indien het echter gaat om in

---

[381] In deze zin ook o.m. HR 26-10-2010, ECLI:NL:HR:2010:BO1713 (bewijsmiddelen inhoudende dat één filmbestand is aangetroffen, dat mogelijk is meegekomen met het *downloaden* van veel gewone porno, zijn ook in samenhang met de verklaring van verdachte dat hij wel eens kinderpornosites had *bekeken*, onvoldoende voor aannemen voorwaardelijk opzet op *bezit*. Zie ook de conclusie van AG Aben (ECLI:NL:PHR:2010:BO1713) bij dit arrest; idem o.m. AG Knigge in zijn conclusie (r.o. 13) bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104.

[382] Vgl. RB Limburg, 9-2-2021, ECLI:NL:RBLIM:2021:1070 (bezit kinderporno, verwerping bijvangstverweer in verband met de locatie op de usb-stick waar de afbeeldingen zijn aangetroffen: "*het verweer van de verdachte dat de foto's per ongeluk mee zijn gedownload, slaagt niet, gelet op de locatie waar de afbeeldingen zijn aangetroffen (op een losse usb-stick in een vrij toegankelijke map)*.")

[383] In dezelfde zin o.m. RB Noord-Nederland 12-12-2014, ECLI:NL:RBNNE:2014:6406 (bezit kinderporno, bijvangstverweer verworpen mede gelet op zoektermen in internetgeschiedenis); RB Rotterdam 18-4-2013, ECLI:NL:RBROT:2013:BZ7889 (meermalen bezoek internetsite met direct zichtbare kinderporno; verweer toevallig met surfen op computer gekomen verworpen, voorwaardelijk opzet); RB Haarlem 11-8-2011, ECLI:NL:RBHAA:2011:BR4793 (bezit kinderporno, verweer bijvangst 'm.b.t. bezit afbeeldingen t.a.v. kinderen in leeftijdscategorie 0-6 jaar' verworpen, omdat via LimeWire werd gezocht naar kinderporno van oudere minderjarigen en deze vervolgens ook werd gedownload naar "mijn documenten"; een van de bestanden droeg de bestandsnaam "Toddler Rape"; aanmerkelijke kans aanvaard dat ook kinderporno van een jongere leeftijdscategorie zou meekomen; voorwaardelijk opzet aangenomen); ***Deels anders:*** Hof Amsterdam 18-8-2016, ECLI:NL:GHAMS:2016:3698 (*zoektermen als 'Young', 'Fresh' en 'Teen' hebben in deze specifieke zaak onvoldoende zeggingskracht*, mede gezien feit dat ook op 18+ is gezocht; zeer geringe hoeveelheid kinderpornografische afbeeldingen in relatie tot "gewone" porno aangetroffen; kinderpornografie afbeeldingen zijn blijkens tijdstempels van de bestanden bovendien niet geopend. Vrijspraak)

[384] Vgl. bijv. Rb. Amsterdam 29-12-2021, ECLI:NL:RBAMS:2021:7706 ("*Het in verhouding zeer beperkte aantal kinderpornografische beelden dat is aangetroffen duidt op mogelijke bijvangst die onbedoeld door verdachte is gedownload. De politie schrijft hierover dat de hoeveelheid foto's van kinderporno niet meer dan een drietal foto's bedraagt – ter vergelijking: in andere zaken ziet de rechtbank veelvuldig tienduizenden of honderdduizenden foto's – en dat kinderporno geen onderwerp lijkt waar verdachte op gefocust is*."); Hof Amsterdam 18-8-2016, ECLI:NL:GHAMS:2016:3698; RB Limburg 27-7-2014, ECLI:NL:RBLIM:2014:6733 (vrijspraak bezit 21 afbeeldingen dierenporno, aannemelijk dat dit bijvangst was bij het downloaden van ruim 1500 afbeeldingen/video's van kinderporno); RB Den Haag 29-2-2008, ECLI:NL:RBSGR:2008:BC5528 (geen bewuste vastlegging, automatische opslag door downloadprogramma LimeWire, automatisch aangemaakte map 'Music Incomplete', vijf bestanden, geen opzet op bezit); Opmerkelijk in dit opzicht: Hof Den Haag 13-5-2015, ECLI:NL:GHDHA:2015:1193 waar opzet op het bezit en zich toegang verschaffen tot kinderporno werd aangenomen, hoewel in de strafoverwegingen werd overwogen dat minder dan één procent van de 400.000

absolute zin grotere aantallen kinderpornografisch materiaal, en zeker als dit op verschillende momenten is gedownload of qua inhoud overeenkomsten vertoont (qua sekse, qua leeftijdscategorie, qua afgebeelde gedragingen, qua kleding enz.) zal aan het feit dat er tevens een grote(re) hoeveelheid gewone porno is aangetroffen waarschijnlijk minder gewicht worden toegekend.[385] In dat geval is het immers weinig waarschijnlijk dat dergelijke qua inhoud overeenkomende afbeeldingen het resultaat zullen zijn van het *random* meekomen met "gewone" porno. Veeleer zal dan aannemelijk zijn dat de aanwezigheid het resultaat is geweest van gericht zoeken naar, of selecteren van, dergelijke afbeeldingen. Hetzelfde geldt in het geval dat uit het digitale onderzoek blijkt dat op bepaalde momenten de "gewone" porno wel is verwijderd, maar de kinderporno niet.[386]

Als de verdachte reeds heeft bemerkt dat al eerder kinderporno naar zijn computer is gedownload als gevolg van het uitvoeren van bepaalde zoekopdrachten, dan legt dat een zeer vergaande onderzoeksplicht op hem om na volgende zoeksessies het gedownloade materiaal te controleren op de aanwezigheid van kinderpornografisch materiaal.[387] Komt hij deze onderzoeksplicht niet voldoende na dan zal als regel voorwaardelijk opzet kunnen worden aangenomen. Een verweer dat men het kinderpornografisch deel van het materiaal niet gewild heeft, zal in een dergelijk geval dan ook zeer waarschijnlijk worden verworpen.[388] Hetzelfde zal naar verwachting gelden als een verdachte op een bezochte website reeds eerder kinderpornografisch materiaal heeft aangetroffen, en desondanks voortgaat met het bezoeken van die website.[389]

---

afbeeldingen bij verdachte was van kinderpornografische aard was, alsook dat de verdachte ter terechtzitting in hoger beroep aannemelijk had gemaakt dat hij in het geheel niet uit was op het bekijken of verzamelen van afbeeldingen van kinderpornografische afbeeldingen.

[385] Vgl. Hof Amsterdam 30-9-2020, ECLI:NL:GHAMS:2020:2542 (verwerping bijvangstverweer; gelet op de verklaring van verdachte dat hij moet hebben geweten dat hij de bestanden in bezit had, omdat hij de bestanden heeft geopend. Nu verdachte deze bestanden vervolgens niet heeft verwijderd, is daarmee de opzet op het in bezit hebben gegeven. Of verdachte deze bestanden heeft aangetroffen als bijvangst, dan wel daar bewust naar heeft gezocht, is daarbij niet relevant); RB Overijssel 24-6-2013, ECLI:NL:RBOVE:2013:1506 (bijvangst-verweer verworpen gezien het feit dat het om afbeeldingen gaat van jongens in dezelfde leeftijdsgroep, terwijl verdachte ook in deze leeftijdsgroep jongens was geïnteresseerd); Zie ook RB Oost-Brabant 27-5-2016, ECLI:NL:RBOBR:2016:2719 (geen sprake van bijvangst, gelet op verhouding tussen pornografisch en kinderpornografisch materiaal. Gebruik gemaakt van verklaring van verbalisant ter terechtzitting dat bij een percentage van 11 geen sprake kan zijn van bijvangst. Indien er sprake is van bijvangst, ligt dit onder de 10 procent.) *Opmerking:* men kan zich echter de vraag stellen in hoeverre deze stelling in zijn algemeenheid juist is, en zo dit al het geval zou zijn, wat dat dan zegt over de toepassing in het specifieke geval.

[386] RB Noord-Nederland 21-2-2017 ECLI:NL:RBNNE:2017:648 (downloaden van porno met peer-to-peerprogramma met onder meer zoekterm "young". Verdachte stelt na bekijken bestanden direct te hebben vernietigd.

[387] In deze zin o.m. RB Noord-Holland 7-9-2017, ECLI:NL:RBNHO:2017:7507 (na het telkens ontvangen van kinderpornografisch materiaal, waar hij naar vroeg in het kader van chats op websites en Skype, klikte verdachte dit weliswaar weg, maar heeft vervolgens niet heeft gecontroleerd of deze daadwerkelijk waren verwijderd van zijn computer. Voorwaardelijk opzet op bezit.).

[388] In dezelfde zin ook: AG Knigge in zijn conclusie (ECLI:NL:PHR:2006:AU9104, r.o. 13.) bij HR 28-2-2006, ECLI:NL:HR:2006:AU9104 en Hof Arnhem-Leeuwarden 18-3-2015, ECLI:NL:GHARL:2015:2016 (zich toegang verschaffen tot kinderporno door het ingeven van op porno gerichte zoektermen in Google. Verdachte wist en verwachtte dat hij ook kinderporno zou aantreffen, opzet op "zich toegang verschaffen"); RB Groningen 12-4-2010, ECLI:NL:RBGRO:2010:BM1069 (doorgegaan met downloaden van "gewone" pornosites waarvan hij wist dat van die site ook kinderpornografisch materiaal meekwam; verwerping bijvangstverweer); RB Utrecht 18-10-2010, ECLI:NL:RBUTR:2010:BO1225 (bezit kinderporno, verdachte was er mee bekend dat met "voetfetish-afbeeldingen" ook kinderporno meekwam, materiaal was voorts ook opgeslagen op specifieke map met persoonlijke informatie van verdachte; bijvangstverweer verworpen, voorwaardelijk opzet aangenomen).

[389] Vgl. ook RB Midden-Nederland 23-12-2013, ECLI:NL:RBMNE:2013:7441 (bij bezoeken aan 3D websites meermalen ook echte kinderporno aangetroffen; grote aantallen kinderpornografische afbeeldingen in verborgen

Indien uit onderzoeksbevindingen blijkt dat de verdachte andere handelingen met betrekking tot de betreffende afbeeldingen heeft verricht dan louter verwijderen/deleten, zoals bijvoorbeeld het meermalen openen of het kopiëren/overbrengen (bijvoorbeeld door "branden" of back-uppen) daarvan naar een andere locatie op de computer of naar een andere gegevensdrager, dan zal een "bijvangst"-verweer zeer waarschijnlijk eveneens worden verworpen. Alsdan zal immers in de regel reeds uit deze gedragingen kunnen worden afgeleid dat verdachte bekend was met de aanwezigheid van deze afbeeldingen en daarover kennelijk ook wilde (blijven) beschikken.[390] De rechtspraak is echter verdeeld over hoe in dit opzicht materiaal moet worden beoordeeld dat na het maken van een (integrale) back-up op een (andere) gegevensdrager terecht is gekomen.[391] Zeker indien er ook aanwijzingen zijn dat de verdachte zich bezighield met het bezoeken van websites met mogelijk kinderpornografisch materiaal (dan wel het downloaden, zich laten toezenden (enz.) van kinderpornografisch materiaal), lijkt het echter aannemelijk dat de strafrechter dan een zeer vergaande onderzoeksplicht aan de zijde van de verdachte aan zal nemen. Anders gezegd: van de verdachte zal dan worden gevergd dat hij, indien hij bij gelegenheid van een back-up materiaal kopieert naar een ander systeem of naar een andere gegevensdrager, ten aanzien van alle gekopieerde bestanden nagaat of deze al dan niet een kinderpornografische inhoud hebben.

---

mappen aangetroffen, niet aannemelijk dat verdachte deze bij toeval samen met een 3D film heeft bekeken; rechtbank gaat niet uit van mogelijkheid van eenmalige bijvangst; (voorwaardelijk) opzet aangenomen t.a.v. "toegang verschaffen tot...); RB Rotterdam 18-4-2013, ECLI:NL:RBROT:2013:BZ7889 (meermalen bezoek internetsite met direct zichtbare kinderporno; verweer "toevallig met surfen op computer gekomen" verworpen, voorwaardelijk opzet); Vgl. voor wat betreft het element herhaald downloaden na kennisname kinderpornografisch materiaal ook: RB Den Haag 18-11-2016, ECLI:NL:RBDHA:2016:14018 (weliswaar is van de bestanden alleen de "*file created date*" weergegeven, (maar) uit die data is wel af te leiden dat de bestanden op verschillende tijdstippen op de telefoon terecht zijn gekomen, zodat een eenmalige zogenoemde "*bijvangst*" bij het downloaden van andere bestanden niet aannemelijk is. Van de HTC telefoon waren voorts ook kinderpornografische bestanden verwijderd. Daaruit kan worden afgeleid dat verdachte er kennelijk bewust voor heeft gekozen om de aangetroffen foto's níet te verwijderen.)

[390] O.m. Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (Bewezenverklaring bezit van in cache aangetroffen thumbnailafbeelding, die door verdachte echter ook op zijn niet openbare Twitter-account is geüpload, een handeling die enkel kan worden verricht als verdachte beschikkingsmacht heeft over de afbeelding *en zich van de aanwezigheid op de computer* bewust is); Hof Den Haag 29-10-2015, ECLI:NL:GHDHA:2015:2992 (kinderpornografie aanwezig op *unallocated clusters* op usb-stick en externe hard disk; uitzondering op regel dat zulks niet leidt tot bewijs van "bezit"; verdachte heeft erkend te hebben gedownload en deze ook op externe gegevensdragers te hebben vastgelegd; dit laatste vereist een actieve, bewuste handeling gericht op vastlegging; in de tijd tussen het vastleggen van de afbeeldingen op de externe gegevensdragers en het op enig moment weer "wissen" daarvan, had verdachte de afbeeldingen in zijn "bezit"); Hof Den Haag 25-9-2014, ECLI:NL:GHDHA:2014:3279 (bezit cd-rom met kinderpornografische afbeeldingen en een filmfragment, afbeeldingen blijkens proces-verbaal kennelijk bewust geselecteerd en overgezet op cd-rom; verweer bijvangst verworpen).

[391] Hof Den Haag 25-9-2014, ECLI:NL:GHDHA:2014:3279 (back-up bevat andere beelden dan bronsysteem, kennelijk sprake geweest van selectie; (voorwaardelijk) opzet aangenomen); RB Zeeland-West-Brabant, 25-3-2021, ECLI:NL:RBZWB:2021:1421 (verdachte is eerder veroordeeld wegens het bezit van kinderpornografische bestanden op zijn computer. Deze computer is destijds in beslag genomen. Van de foto's op die computer, waaronder ook privé-foto's, is door verdachte een back-up gemaakt en verdachte heeft verklaard dat die back-up door zijn stiefvader op de nieuwe computer van verdachte is gezet; niet uitgesloten kan worden dat de verklaring van verdachte dat de kinderpornografische bestanden afkomstig zijn van de back-up van zijn vorige computer klopt. Vrijspraak van bezit van kinderporno).
RB Midden-Nederland 23-12-2013 ECLI:NL:RBMNE:2013:7441 (rechtbank sluit niet uit dat afbeeldingen (voornamelijk *thumbnails*) zonder dat verdachte zich daarvan bewust is geweest bij het maken van een algemene back-up op een externe harde schijf terecht zijn gekomen; geen (voorwaardelijk) opzet aangenomen.).

Technisch lemma: back-up bestanden.

Zoals in dit boek beschreven staat in het kader van de beoordeling van bijvangstverweren in kinderpornografiezaken regelmatig ter discussie of kinderpornografische bestanden die in een back-up-bestand op een gegevensdrager worden aangetroffen voor de verdachte benaderbaar waren. Bij de beoordeling van dergelijke verweren verdient onder meer aandacht welk type back-up bestand aan de orde is, en of de verdachte ook redelijkerwijs in staat moet worden geacht om de inhoud van het back-up bestand te benaderen. Tegen die achtergrond is het zinvol op de hoogte te zijn van de techniek achter het maken en gebruiken van back-up bestanden.

Back-up-bestanden en archiefbestanden
Naar algemeen spraakgebruik wordt de term 'back-up' omschreven als een (al dan niet van beveiligingsmaatregelen voorziene) kopie van gegevens. Het aanmaken van een back-up-bestand is een wezenlijk andere vorm van gegevensbeheer dan archiveren. Back-up-bestanden dienen om vorige versies van gegevens terug te zetten nadat de oorspronkelijke bestanden (onbedoeld) zijn gewist, beschadigd of overschreven. Archiefbestanden dienen om gegevens terug te halen die - doorgaans bewust - zijn verwijderd van de oorspronkelijke locatie (bijvoorbeeld om ruimte vrij te maken) en niet zijn gewijzigd nadat ze in het archiefbestand zijn opgeslagen. De termen 'back-up-bestand' en 'archiefbestand' zijn aldus niet inwisselbaar.

Lokale back-ups en in de cloud opgeslagen back-ups
Een back-up kan een integrale kopie van een volledige gegevensverzameling (zoals: alle bestanden op een gegevensdrager) betreffen, maar ook een kopie van een deel van een gegevensverzameling (zoals: de instellingen van een gebruikersaccount van een besturingssysteem op een computer of een mobiel apparaat). Tevens relevant is het onderscheid tussen lokaal opgeslagen back-up bestanden en in de cloud opgeslagen back-up bestanden. Bij lokale back-ups wordt het back-up bestand op een gegevensdrager opgeslagen die bij de gebruiker zelf aanwezig of tenminste in beheer is. Het handmatig overzetten van bestanden op een computer naar een USB-stick of een externe harde schijf, maar ook het opslaan van een lokale back-up op hetzelfde apparaat waarop de door de gebruiker geselecteerde bestanden aanwezig zijn, zijn hiervan voorbeelden. Een van de voordelen van lokale back-ups is dat er geen internetverbinding nodig is om de back-up te benaderen. Een van de nadelen van lokale back-ups is dat de gebruiker zelf beveiligingsmaatregelen moet treffen om toegang door derden te bemoeilijken, bijvoorbeeld door het back-up bestand te versleutelen, maar ook om het teloorgaan door diefstal, branden technisch probleem etc. te voorkomen. Bij in de cloud opgeslagen back-ups worden op het apparaat opgeslagen gegevens (voor zover de gebruiker dat in de backup- en synchronisatie-instellingen van het apparaat heeft aangegeven automatisch) opgeslagen op een cloudserver. Applicatiegegevens kunnen bijvoorbeeld automatisch worden opgeslagen in een cloudaccount (zoals: iCloud, Google, Dropbox).

Naast het door een apart back-up-programma of -applicatie laten verzorgen van een back-up van (delen van) een gegevensdrager, zijn er ook computerprogramma's of applicaties die zelfstandig, alleen voor door hen gebruikte of gegenereerde gegevens, een back-up maken. Welke gegevens hierbij lokaal en/of in de cloud als back-up worden opgeslagen, is afhankelijk van de instellingen van de betreffende (chat)applicatie. Voor WhatsApp geldt dat van de chatgeschiedenis standaard een lokale back-up van de chatgeschiedenis van de laatste 7 dagen wordt opgeslagen. Via bestandsbeheer kan deze lokale back-up worden teruggezet. WhatsApp biedt tevens de mogelijkheid om een back-up van de chatgeschiedenis in Google Drive of iCloud op te slaan. Bij opslag van de back-up in Google Drive bestaat sinds september 2021 de mogelijkheid om end-to-end versleuteling toe te passen. Nog iets gecompliceerder is de situatie waarin een algemene back up-toepassing bijvoorbeeld de chatgeschiedenis van WhatsApp opslaat. Hiervoor bestaan verschillende mogelijkheden. Deze hoeft u niet allemaal te kennen, maar het is wel goed om zich te beseffen dat indien gesproken wordt over 'de back-up' van bijvoorbeeld WhatsApp, die niet altijd over hetzelfde hoeft te gaan.

Drie hoofdvarianten van back-ups: *full, incremental, differential*.
Ongeacht de wijze van opslag (lokaal of in de cloud) kunnen 3 hoofdvarianten van back-ups worden onderscheiden. Tussenvarianten van de hierna beschreven hoofdvarianten zijn mogelijk. Een '*full back-up'* betreft een (doorgaans op vaste momenten uitgevoerde) volledige kopie van een gegevensverzameling (inhoudsgegevens en metadata daarvan). Een van de voordelen van een '*full back-up*' is dat het relatief eenvoudig is om de gegevensverzameling in de oorspronkelijke toestand te herstellen, nu er maar vanuit 1 back-up bestand wordt gewerkt. Een van de nadelen is dat het maken van '*full back-ups'* tijdrovend is en relatief veel opslagruimte kost.

Een '*incremental back-up'* betreft een combinatie van een '*full back-up*' (die daarna eventueel regelmatig wordt uitgevoerd) en tussentijdse kopieën van gegevens die voor of na de laatste *full back-up* zijn gewijzigd. Deze back-up techniek veronderstelt dat in het verleden tenminste 1 *full back-up* is gemaakt. Een van de voordelen van een '*incremental back-up'* is dat tijdswinst kan worden geboekt doordat het niet nodig is om telkens een volledige kopie van de gegevensverzameling te maken. Een van de nadelen is dat het bewerkelijker is om de gegevensverzameling in de oorspronkelijke toestand te herstellen, nu de gebruiker dient te beschikken over de laatste, '*full back-up'* en *alle* tussentijdse kopieën van gegevens die nadien zijn gewijzigd.

Een '*differential back-up'* vereist, anders dan een '*incremental back-up'*, slechts de meest recente '*full back-up'* en de meest recente tussentijdse kopie van gegevens die nadien zijn gewijzigd. Een van de voordelen is dat het minder bewerkelijk is om de gegevensverzameling in de oorspronkelijke toestand te herstellen dan bij een '*incremental back-up'*, nu de gebruiker niet behoeft te beschikken over alle tussentijdse kopieën. Een van de nadelen is dat het maken van '*differential back-ups'* meer tijd kost (immers, alle veranderingen sinds de laatste 'full back-up' moeten worden opgeslagen) en dat meer opslagruimte nodig is dan bij '*incremental back-ups'*.

4.3.2. "Ik heb de kinderporno (direct) na binnenkomst/waarneming gedeletet"
Zoals hiervoor al aangegeven levert de enkele aanwezigheid van kinderpornografisch materiaal op een computer en/of een gegevensdrager nog niet voldoende bewijs voor bezit als bedoeld in art. 240b Sr op. Is er echter tevens sprake van (veronderstelde) beschikkingsmacht en wetenschap met betrekking tot de aanwezigheid van dergelijk materiaal, dan zal daaruit in beginsel wel de opzet, al dan niet in voorwaardelijke zin, op het bezit van voormeld materiaal kunnen worden afgeleid. Een uitzondering op dit uitgangspunt wordt echter aangenomen, indien de verdachte aannemelijk maakt dat hij het materiaal ongewild heeft verkregen en vervolgens ook effectief en voortvarend heeft verwijderd.[392]
In een dergelijk geval heeft de verdachte immers wel op enig moment de feitelijke beschikkingsmacht over voormeld materiaal gehad, en was hij ook met de aard van het materiaal bekend, maar kan worden aangenomen dat hij het bezit daarvan niet *gewild* heeft.

In de rechtspraak is in dit kader het criterium van de "effectieve verwijdering" ontwikkeld. De toepassing van dit criterium is redelijk complex, mede omdat hetgeen menige verdachte verstaat onder verwijderen van bestanden niet noodzakelijkerwijs samenvalt met hetgeen *de jure* wordt verstaan onder "effectieve verwijdering". Uit de jurisprudentie kan allereerst worden afgeleid dat van effectieve verwijdering geen sprake is, indien de verdachte na de "verwijdering" toch de beschikkingsmacht over de afbeeldingen heeft behouden of op enig

[392] Vgl. RB Amsterdam 23-4-2021, ECLI:NL:RBAMS:2021:2011 ("*uit de verklaring van verdachte kan worden afgeleid dat hij ook wel eens bestanden verwijderde als hij spijt kreeg en wilde stoppen met het kijken naar kinderporno, maar hij heeft niet verklaard dat hij ooit een bestand direct na ontvangst via WhatsApp heeft verwijderd.*").

moment na de verwijdering weer heeft verkregen. Dit betekent dat bijvoorbeeld *niet* als "effectieve verwijdering" wordt beschouwd het plaatsen van afbeeldingen in de "prullenbak" (of: *trash / recycle bin*). Deze afbeeldingen blijven immers, zoals thans van algemene bekendheid wordt geacht, ook na plaatsing in de "prullenbak" nog eenvoudig toegankelijk voor de gebruiker.[393]

Daarnaast is ook het tijdsaspect van belang. Als een verdachte na het bij hem bekend worden van de aanwezigheid van het materiaal (c.q. na het moment waarop hij redelijkerwijs kon vermoeden dat dergelijk materiaal aanwezig was) dit niet (vrijwel) direct verwijderd heeft, kan dat als een aanwijzing worden gezien dat de verdachte ook over dat materiaal *wilde* beschikken.[394] Dat geldt te meer als er in de tussentijd door de verdachte ook gedragingen (zoals meermalen openen[395], kopiëren, bewerken, plaatsen in mappen etc.) met betrekking tot de betreffende afbeeldingen zijn verricht.[396] Daarbij vallen voor wat betreft het tijdsaspect geen echt harde grenzen te geven, zij het dat de Hoge Raad in een voorkomend geval, waarin sprake was van een tijdvak van vier dagen tussen het via het P2P-programma Kazaa zoeken naar kinderpornobestanden (en het vervolgens downloaden van bestanden met "spannende namen" naar een *shared files*-map[397]) en het vervolgens gaan kijken naar het gedownloade materiaal, als een voldoende lange tijdsduur aanmerkte om opzet op het bezit van die kinderporno aan te nemen.[398] In de lagere rechtspraak is echter ook bij een aanmerkelijk korter tijdsverloop tussen binnenkomst en verwijdering al opzet aangenomen, al ging het daarbij om gevallen waarbij de verdachte als gevolg van zijn gedragingen (zoals herhaald zoeken op website met trefwoorden die eerder al kinderporno opleverden of vragen om toezending van kinderporno) redelijkerwijs kon vermoeden dat dergelijk materiaal ook gedownload was c.q. zou worden ontvangen.[399] Men zou echter in dergelijke gevallen ook kunnen betogen dat in die voorafgaande gedragingen reeds de wil op het bezitten besloten lag, zodat het tijdsverloop tussen het downloaden en het verwijderen niet meer relevant is.[400] Onwenselijk zou immers zijn dat het opzettelijk downloaden van kinderpornografie niet als strafbare handeling zou worden aangemerkt als deze binnen zekere tijd weer wordt verwijderd. Dat zou een onbedoelde omkering van de gedachte achter het leerstuk van de effectieve verwijdering zijn.

In voorkomende gevallen zal niet meer precies kunnen worden vastgesteld wanneer de verdachte kennis heeft genomen van de aanwezigheid van de betreffende afbeeldingen.[401] Dan is, tenzij de verdachte daarover zelf nader verklaart, ook de tijd die is verlopen tussen die kennisname en de verwijdering onbekend. Dit is wel in het voordeel van de verdachte

---

[393] Zie HR 16-1-2007, ECLI:NL:HR:2007:AZ0221 (vrijspraak van bezit digitale kinderporno, verwijderen uit de prullenbak, *criterium 'effectieve verwijdering'*) en verder hiervoor onder 4.2.1.2.
[394] Zie RB Gelderland 7-4-2017, ECLI:NL:RBGEL:2017:2117 (bewust kinderpornografie gedownload; het heeft volgens de verklaring van verdachte vervolgens lang geduurd voordat hij naar de downloads ging kijken; opzet op bezit van kinderpornografie).
[395] Zie RB Groningen 12-4-2010, ECLI:NL:RBGRO:2010:BM1069 (meerdere bestanden met ook duidelijke kinderpornografie gerelateerde namen voor verwijdering tot 2 maal toe geraadpleegd; opzet).
[396] Hof 's-Hertogenbosch 25-1-2007, ECLI:NL:GHSHE:2007:AZ8027.
[397] Dit is een voor een computergebruiker benaderbare en niet-tijdelijke map, waarvandaan ook door andere gebruikers van het betreffende programma afbeeldingen kunnen worden gedownload.
[398] HR 11-9-2007, ECLI:NL:HR:2007:BA6316.
[399] RB Assen 25-11-2008, ECLI:NL:RBASS:2008:BG9649. Vgl. ook RB Midden-Nederland, 30-8-2016, ECLI:NL:RBMNE:2016:4869 (kortstondig op telefoon hebben a.g.v. toezending met Snapchat is *bezit* in de zin van art. 240b Sr).
[400] In deze zin begrijpen wij (naast de in de vorige noot genoemde uitspraak) ook AG Knigge in zijn conclusie bij HR 11-9-2007, ECLI:NL:PHR:2007:BA6316, r.o. 13.
[401] Niet zelden kan echter door deskundigen wel worden nagegaan wanneer een afbeelding voor het laatste door een gebruiker is geopend (*accessed*). Zie over de datering d.m.v. zogenaamde tijdstempels onder 6.2.4.1.

uitgelegd.[402] Onder omstandigheden is evenwel denkbaar dat het tijdsverloop in het nadeel van de verdachte wordt uitgelegd, in het bijzonder indien blijkt dat verdachte met betrekking tot de betreffende afbeeldingen ook andere gedragingen dan het louter downloaden en openen heeft verricht.

4.4. Opzet op leeftijd afgebeelde persoon c.q. (kinder)pornografisch karakter afbeelding

Regelmatig wordt ook het verweer gevoerd dat uit de bewijsmiddelen niet kan blijken dat de verdachte opzet had op het bezit van *kinder*pornografische afbeeldingen. In dat kader is het allereerst van belang zich te realiseren dat, zoals hiervoor onder 3.3.1. beschreven, de in art. 240b Sr opgenomen leeftijdsgrens van 18 jaar van de afgebeelde en bij de seksuele handeling(en) betrokken perso(o)n(en) is geobjectiveerd. Het opzet behoeft daarop dus geen betrekking te hebben.[403] Daaruit volgt tevens dat het voor de *bewezenverklaring* irrelevant is of de verdachte wist van de minderjarigheid van de afgebeelde perso(o)n(en).[404] Zoals hiervoor reeds onder 3.3.1. besproken, is evenmin van belang of de betreffende minderjarige in werkelijkheid nu wel of niet de 18-jarige leeftijd heeft bereikt, indien deze althans naar het oordeel van de rechter jonger oogt. Dit heeft tot gevolg dat er in de praktijk ook weinig tot geen aanleiding zal bestaan om onderzoekswensen en verweren met betrekking tot de (vermoede) leeftijd van de afgebeelde persoon te honoreren.[405]

Aangenomen kan worden dat bij werkelijke onwetendheid op dit punt eventueel – dus los van de bewezenverklaring – wel een beroep op afwezigheid van alle schuld kan worden gedaan. Die dwaling zal dan wel als verontschuldigbaar moeten kunnen worden aangemerkt. Gezien de strekking van de strafbepaling (het bieden van bescherming aan minderjarigen) zal een dergelijk avas-beroep overigens naar verwachting niet snel worden gehonoreerd.[406]

Ingewikkelder wordt het als het gaat over de vraag of de verdachte ook opzet moet hebben gehad op het verboden karakter van de afbeeldingen. Daarover was na een arrest van de Hoge Raad[407] (en de daaraan voorafgaande conclusie van AG Aben[408]) uit 2010 onduidelijkheid ontstaan. AG Harteveld heeft in dit kader echter in zijn – door de Hoge Raad in zijn arrest van 18 november 2014[409] gevolgde – conclusie gesteld dat een zodanige opzet niet vereist is.[410] Zijn inziens volgt uit de formulering van art. 240b Sr in samenhang bezien met de geobjectiveerde leeftijdsgrens en met de met art. 240b Sr beoogde bescherming van minderjarigen dat het opzet in zoverre niet méér behoeft te omvatten dan dat verdachte zich in meerdere of mindere mate bewust is geweest van de "aard of het karakter" van die

---

[402] Hof 's-Gravenhage 23-2-2006, ECLI:NL:GHSGR:2006:AV2588; RB Zeeland-West-Brabant, 8 september 2020, ECLI:NL:RBZWB:2020:4199 ("*het dossier verschaft geen duidelijkheid over het tijdsverloop tussen de binnenkomst en verwijdering van de betreffende bestanden, niet uitgesloten kan worden dat verdachte de bestanden onmiddellijk na binnenkomst als ongewenst heeft verwijderd*.").
[403] Dit is ten aanzien van leeftijd gerelateerde zedendelicten al zeer lang vaste jurisprudentie; zie o.m. HR 20-1-1959, *NJ* 1959, 102 en HR 20-1-1959, *NJ* 1959, 103 (de zogenaamde "leeftijdsarresten").
[404] Aldus AG Harteveld in zijn conclusie (ECLI:NL:PHR:2014:2095), onder 6.2. bij HR 18-11-2014 ECLI:NL:HR:2014:3304; Aldus ook al HR 21-4-1998, *NJ* 1998/782 m.nt. t Hart.
[405] Zie in dit verband met name HR 18-11-2008, ECLI:NL:HR:2008:BF0170.
[406] Zie hierover verder hierna onder 5.4.
[407] HR 26-10-2010, ECLI:NL:HR:2010:BO1713.
[408] Conclusie AG Aben bij het in de vorige noot vermelde arrest, ECLI:NL:PHR:2010:BO1713.
[409] HR 18-11-2014 ECLI:NL:HR:2014:3304; Idem: RB Overijssel 15-9-2015, ECLI:NL:RBOVE:2015:4299.
[410] Conclusie AG Harteveld (ECLI:NL:PHR:2014:2095) bij HR 18-11-2014 ECLI:NL:HR:2014:3304 (cassatie verworpen m.b.t het verweer dat verdachte geen opzet (want geen wetenschap) had gehad van kinderpornografisch karakter van materiaal; ook verwerping cassatiemiddel tegen strafmaatoverweging ("proceshouding").

afbeelding(en). Het vereiste opzet van de verdachte behoeft dus geen betrekking te hebben op de *strafbare aard* van de afbeelding, maar slechts op de inhoud, in die zin dat de verdachte zich er min of meer van bewust was dat er op de afbeelding sprake was van een als seksueel te duiden gedraging met of door een jong persoon.

In de woorden van Harteveld: "*De vraag naar de juridische kwalificatie*[411] *van de afbeelding ("is hetgeen is afgebeeld aan te merken als de afbeelding van een seksuele gedraging zoals bedoeld in de delictsomschrijving, of toch niet") is dus ter vaststelling door de rechter en op de uitkomst van die vaststelling wordt geen opzet van de dader vereist. Dit onderdeel van de delictsomschrijving zou men dus ook als een geobjectiveerd bestanddeel kunnen betitelen, immers onttrokken aan de opzet-eis*."

Uit het voorgaande volgt derhalve tevens dat een eventueel gestelde dwaling omtrent de strafbare aard van de afbeelding (bijvoorbeeld ten aanzien van de vraag of daarop een seksuele gedraging zichtbaar is en/of de leeftijd van de bij die gedraging betrokken persoon) dus niet relevant is voor de bewezenverklaring (van opzet). Wel kan het een rol spelen bij de beantwoording van de vraag of wellicht sprake is van afwezigheid van alle schuld en of verdachte om die reden niet strafbaar is.[412] Zie hierover verder hierna onder 5.4.

[411] Harteveld spreekt hier onder 6.2. van de in de vorige noot vermelde conclusie over "het karakter" van de afbeelding, hetgeen wellicht wederom verwarring kan oproepen. Onzes inziens gaat het hier in de kern om de juridische duiding van de afbeelding. Of anders gezegd: om de juridische kwalificatie hiervan.
[412] Aldus ook Harteveld in de in de voorgaande noten vermelde conclusie, onder 6.2.

HOOFDSTUK 5. BEROEP OP SCHULD- EN STRAFUITSLUITINGSGRONDEN (OVAR)

5.1. Bewezenverklaarde ex art. 240b Sr is (toch) niet kwalificeerbaar als zedenmisdrijf

5.1.1. Het arrest van de Hoge Raad van 9 februari 2016

In een voor velen toch wel enigszins verrassend arrest heeft de Hoge Raad op 9 februari 2016[413] geoordeeld dat ook als is voldaan aan alle bestanddelen van art. 240b Sr, en mitsdien de overtreding van die bepaling terecht bewezen is verklaard, er gevallen denkbaar zijn waarin de bewezenverklaarde gedraging desondanks niet als het in art. 240b Sr strafbaar gestelde misdrijf tegen de zeden moet worden gekwalificeerd. De Hoge Raad lijkt daarbij, gezien de verwijzing naar specifieke passages uit de wetsgeschiedenis, vooral te doelen op situaties waarin met instemming van betrokken 16- of 17-jarigen, en in de privésfeer (en dus zonder oogmerk van verspreiding), afbeeldingen zijn gemaakt van seksuele handelingen door of met een leeftijdgenoot.

De Hoge Raad motiveert deze beslissing als volgt:

> *"Aangenomen moet worden dat art. 240b Sr te ruim is geredigeerd, in die zin dat deze bepaling ook gevallen bestrijkt waarin volgens de wetsgeschiedenis strafrechtelijke aansprakelijkstelling achterwege kan of dient te blijven. Relevante factoren voor het bepalen van dergelijke gevallen zouden daarbij in het bijzonder zijn de concrete gedraging van de verdachte, de leeftijd van de betrokkenen, de instemming van de betrokkenen en het ontbreken van enige aanwijzing voor een risico van verspreiding van de afbeelding(en) onder anderen dan de betrokkenen. Deze gevallen zouden in de – bij de verdere behandeling van het wetsvoorstel niet weersproken – visie van de Minister nader moeten worden omschreven in de Aanwijzing kinderpornografie. Geen van de elkaar opvolgende Aanwijzingen kinderpornografie bevat evenwel enige omschrijving in die zin. Een verdachte die wordt vervolgd ter zake van het misdrijf van art. 240b Sr, kan zich derhalve niet met vrucht beroepen op die Aanwijzing. Daardoor laat zich nog sterker het gemis voelen dat de wetgever niet zelf art. 240b Sr zo heeft geformuleerd dat het zich niet uitstrekt over gevallen waarin naar zijn opvatting strafrechtelijke aansprakelijkstelling achterwege behoort te blijven."*

Vervolgens formuleert de Hoge Raad een instructienorm voor de strafrechter:

> *"Bij deze stand van zaken is het aan de strafrechter om – ook al is voldaan aan alle bestanddelen van art. 240b Sr – in het soort gevallen dat is genoemd in de wetsgeschiedenis, aan de hand van factoren als hiervoor genoemd de vraag onder ogen te zien of het gedrag van de verdachte, alle omstandigheden in aanmerking genomen, van dien aard is dat het moet worden gekwalificeerd als het in die bepaling als misdrijf tegen de zeden strafbaar gestelde feit, en ingeval die vraag ontkennend wordt beantwoord, de verdachte te ontslaan van alle rechtsvervolging op de grond dat het bewezenverklaarde niet een strafbaar feit oplevert."*

De keuze van de Hoge Raad om in de bedoelde situaties een kwalificatieuitsluitingsgrond aan te nemen is opmerkelijk te noemen. De ook door de Hoge Raad aangehaalde wetsgeschiedenis lijkt er namelijk veeleer op te wijzen dat het de bedoeling van de wetgever was dat handelingen met "sexting-materiaal" dat op zichzelf aan alle vereisten van art. 240b Sr voldoet, wel als een strafbaar feit moeten worden gezien, maar dat de strafrechtelijke aansprakelijkstelling daarvoor achterwege dient te blijven. Dat lijkt er veeleer op te wijzen dat de wetgever voor ogen stond dat het ontbreken van strafwaardigheid in het specifieke geval via de opportuniteit van de vervolgingsbeslissing of een strafuitsluitingsgrond zou worden opgelost en niet via een kwalificatieuitsluitingsgrond.

---

[413] HR 9-2-2016, ECLI:NL:HR:2016:213.

Men kan bovendien de vraag stellen of in dit arrest de Hoge Raad hier niet te veel betekenis heeft toegekend aan bepaalde passages in de wetsgeschiedenis uit 2001-2002 en te weinig aan de letter en geest van bijvoorbeeld het (latere) Verdrag van Lanzarote, waarin het belang van de bescherming van de afgebeelde minderjarige (nog) meer centraal is komen te staan.[414] Zeker in een tijd waarin het risico altijd aanwezig is dat via sociale media afbeeldingen van minderjarige (seks)partners op enig moment ook onder derden zullen worden verspreid, en waarin gelijkheid in leeftijd zeker niet altijd ook gelijkwaardigheid en vrijheid op het niveau van beslissingen omtrent de wijze waarop uiting en vorm wordt gegeven aan seksualiteit impliceert, lijkt er een zekere spanning te bestaan tussen dit arrest en voormelde beschermingsgedachte. Ook lijkt wat onderbelicht te zijn gebleven dat mede met het oog op voormeld risico van verspreiding de (aanvankelijke) instemming van een 16- of 17-jarige met de vervaardiging van kinderporno de schadelijke effecten ervan niet wegneemt.[415]

5.1.2. Beoordeling van de kwalificatie

Hoe het ook zij, het lijkt in ieder geval niet gewaagd te veronderstellen dat dit arrest in art. 240b-zaken regelmatig aanleiding zal geven tot discussie. Dit geldt te meer, nu de strafrechter in de visie van de Hoge Raad ook *ambtshalve* genoemde aspecten bij de kwalificatievraag zal dienen te betrekken. Bepaalde raadslieden zullen het arrest vermoedelijk ook aangrijpen om ten behoeve van hun cliënten te betogen dat en waarom ondanks bewezenverklaring van alle bestanddelen van art. 240b Sr, de betreffende gedraging niet als zedenmisdrijf moet worden gekwalificeerd.[416]

Het lijkt aangewezen dat de strafrechter de zaken daarbij vooral scherp blijft zien. Zorgvuldige lezing van het arrest leert dat het slechts ziet op een beperkte categorie van situaties, namelijk die waarin sprake is van :

- 16- of 17-jarige verdachten[417],
- die met instemming van betrokkene,
- in de privésfeer (dus zonder verspreidingsoogmerk),

---

[414] Daarbij kan echter aan de Hoge Raad worden toegegeven dat zowel Richtlijn 2011/92/EU als het Verdrag van Lanzarote op zich wel de juridische ruimte bieden voor voormelde benadering.

[415] Aldus ook de Nota naar aanleiding van het verslag bij de wijziging van art. 240b in 2002 (Kamerstukken II 2001-2002, 27 745, nr. 6, blz. 15-16); In dezelfde zin: Hof Den Haag 7-6-2016, ECLI:NL:GHDHA:2016:1703 (Het bezit van of het aanzetten tot het vervaardigen van seksueel getinte "bloot foto's of filmpjes/video's" van een 14-jarige leeftijdgenote en het versturen van deze foto's of filmpjes/video's naar de verdachte of een medeverdachte, heeft in casu niets met pedofilie te maken, maar valt ter bescherming van de minderjarige afgebeelde niettemin onder de strafbepaling. Het bezit van deze foto's en filmpjes/video's verschaft de verdachte een zekere macht over het afgebeelde slachtoffer; immers de macht om de afbeeldingen al of niet te verspreiden. Daardoor komt de afgebeelde onder druk te staan en wordt haar privacy bedreigd. Zij geniet de bescherming van de wet, ook al heeft zij zelf door de foto's en filmpjes te versturen hieraan meegewerkt.)

[416] Zie bijv. Hof Arnhem-Leeuwarden 9-9-2016, ECLI:NL:GHARL:2016:10785.

[417] Vgl. ook HR 18-11-2014, ECLI:NL:HR:2014:3291 (verspreiden door 18-jarige van seksueel getinte afbeeldingen van 16/17-jarige vriendin; terecht gekwalificeerd als verspreiden van kinderporno in de zin van 240b Sr) en Hof Arnhem-Leeuwarden 7-4-2017, ECLI:NL:HR:2017:3108 (afbeeldingen gemaakt door deels ruim 18-jarige verdachte van 3,5 jaar jongere vriendin; "*uit wetsgeschiedenis blijkt dat ovar is uitgesloten voor periode dat aangeefster jonger dan 16 jaar was.*" V.w.b. periode daarna: leeftijdsverschil aanmerkelijk mede gelet op de persoonlijkheid van aangeefster; ook dreigementen betreffende openbaarmaking; beroep op ovar ook voor periode na bereiken 16-jarige leeftijd verworpen). Zie echter ook voor kennelijk ruimer aanvaardbaar geacht leeftijdsverschil: RB Rotterdam 18-5-2017, ECLI:NL:RBROT:2017:4260 (22-jarige verdachte had een relatie met een 17-jarig meisje. Geen sprake van een zodanig groot leeftijdsverschil (verdachte 22 jaar, aangeefster 17 jaar), dat dit in het nadeel van verdachte moet worden meegewogen. Toch geen geslaagd beroep op ovar, nu tevens sprake was van verspreiding).

- bij afwezigheid van enige aanwijzing voor een risico van verspreiding,[418]
- afbeeldingen hebben gemaakt van een leeftijdgenoot.[419]

Een dergelijke beperkte uitleg is waarschijnlijk ook de enige die kan worden gebracht binnen het kader van het Verdrag van Lanzarote en Richtlijn 2011/92/EU (ter bestrijding van seksueel misbruik en seksuele uitbuiting en kinderpornografie).[420] Ingevolge die internationale regels is het namelijk toegelaten uitzonderingen te maken op de daarin opgenomen verplichtingen ten aanzien van strafbaarstelling en vervolging met betrekking tot kinderpornografie indien het betreft "*materiaal waarbij kinderen zijn betrokken die seksueel meerderjarig zijn*[421]*, wanneer dit materiaal is vervaardigd en in bezit wordt gehouden met de toestemming van die kinderen en uitsluitend voor persoonlijk gebruik van de betrokkenen, voor zover het niet met misbruik gepaard ging*"[422] respectievelijk "*afbeeldingen die met de toestemming van seksueel meerderjarige kinderen zijn gemaakt voor uitsluitend privégebruik*".[423]

Indien derhalve zowel de verdachte, als de gedraging(en), als de betrokkene voldoen aan de door de Hoge Raad gestelde criteria zal ontslag van rechtsvervolging voor de hand liggen. Aangenomen mag worden dat als de strafrechter tot een ander oordeel komt, hij dat - ook als ter zake geen verweer is gevoerd - nader zal dienen te motiveren.
In andere gevallen zal zeer waarschijnlijk niet sprake zijn van een wezenlijke verandering ten opzichte van de huidige situatie, waarin als regel bij bewezenverklaring de bewezenverklaarde gedraging ook als overtreding van art. 240b Sr wordt gekwalificeerd.[424]

5.2. De "kunst"- c.q. "wetenschaps"exceptie

In voorkomende gevallen wordt wel aangevoerd dat weliswaar sprake is van bezit of vervaardiging (etc.) van een afbeelding van een seksuele gedraging met een minderjarige, maar dat die gedraging niet strafbaar is omdat het kunst zou betreffen of de wetenschap zou

---

[418] A fortiori kan worden aangenomen, dat waar sprake is geweest van feitelijke verspreiding en hierbedoeld risico van verspreiding zich derhalve feitelijk heeft gematerialiseerd, het verweer op ovar dient te worden verworpen. Aldus ook RB Rotterdam 18-5-2017, ECLI:NL:RBROT:2017:4260.
[419] Hoewel dit niet expliciet in het arrest is verwoord, volgt onzes inziens uit de samenhang met de wetsgeschiedenis (o.m. Kamerstukken II 2001-2002, 27 745, nr. 6, blz. 15-16) en de in de volgende alinea genoemde internationale overeenkomsten, dat die leeftijdgenoten/afgebeelde personen zelf ook minimaal 16 jaar of ouder moeten zijn. Anders echter: RB Zutphen 24-1-2008, ECLI:NL:RBZUT:2008:BC2954 (16-jarige verdachte die pornografische foto's maakt van 15-jarige vriendin; ovar).
[420] Publicatieblad EU, 2011, L 335/1.
[421] Ingevolge de definities (onder c.) van Richtlijn 2011/92/EU is "seksuele meerderjarigheid": de leeftijd beneden die waarbij het overeenkomstig het nationale recht verboden is met een kind seksuele handelingen aan te gaan. Voor Nederland volgt uit art. 245 Sr dat deze leeftijd 16 jaar bedraagt.
[422] Art. 8, lid 3 van Richtlijn 2011/92/EU.
[423] Art. 20, lid 3, tweede gedachtestreepje, Verdrag van Lanzarote.
[424] Illustratief is dit geval dat in hetzelfde arrest (HR 9-2-2016, ECLI:NL:HR:2016:213), waarin sprake was van een 16-jarige jongen die (met medeweten van sommige meisjes en ten aanzien van andere meisjes heimelijk) video's van zijn seksuele omgang met 4 meisjes van 13-15 jaar had gemaakt en bewaard, de Hoge Raad met het hof oordeelde dat de in de bewezenverklaring omschreven gedragingen van de verdachte ten aanzien van alle meisjes konden worden gekwalificeerd als - kort gezegd - het vervaardigen en in bezit hebben van kinderporno in de zin van art. 240b Sr. Soortgelijk: HR 18-11-2014 ECLI:NL:HR:2014:3291 (Mede gelet op de wetsgeschiedenis heeft het Hof het bewezenverklaarde handelen van verdachte (i.c. naaktfoto's van minderjarige vriendin verzonden) terecht gekwalificeerd als - kort gezegd - het verspreiden van kinderporno in de zin van art. 240b Sr).

dienen. Men spreekt dan (ten aanzien van de kunst) wel van de kunstexceptie (*"exceptio artis"*).[425]

Een absoluut wetenschaps- of kunstverweer is tot op heden nimmer door het EHRM of door de nationale strafrechter aanvaard.[426] Het enkele feit dat een afbeelding die de jure voldoet aan de maatstaven voor kinderpornografie (ook) als object voor wetenschappelijk onderzoek of als kunst moet worden beschouwd, sluit derhalve strafbaarheid niet uit.[427] Hierbij is tevens van betekenis dat uit de wetsgeschiedenis kan worden afgeleid dat de wetgever zowel de kunst- als de wetenschapsexceptie in deze context niet heeft gewild.[428]

Daarmee is echter toch nog niet alles gezegd. Zowel in de rechtsliteratuur[429] als in de context van de rechtspraak[430] is onzes inziens met kracht van argumenten naar voren gebracht dat in dergelijke gevallen zowel bij de vervolgingsbeslissing door de officier van justitie, als bij de beoordeling door de strafrechter, het belang van strafvervolging (waaronder begrepen de met het desbetreffende delict beschermde rechtsbelangen) moeten worden afgewogen tegen het belang van het zo vrij mogelijk kunnen verrichten van wetenschappelijk onderzoek c.q. van de 'kunstvrijheid' in de zin van een artistiek belang. Jurisprudentie is er echter weinig, met name ook omdat de wetenschapsexceptie meestal niet nader feitelijk wordt onderbouwd[431] en

---

[425] Over dit onderwerp is recent relatief weinig gepubliceerd. Als het meest actueel en relevant zou het artikel van C.P.M. Cleiren en S.R. Bakker, *De kunstexceptie; Gemiste kansen voor de artistieke vrijheid?* in: Strafblad, december 2011, p. 33-49 kunnen worden genoemd. Het navolgende is ook voor een belangrijk deel aan de inhoud van dit artikel ontleend. Meer recent, maar wat minder *on topic*: Bakker, S. e.a, *Bedreigende rap en de kunstexceptie* , PROCES 2015, aflevering 3, p. 175 e.v..

[426] Aldus ook: Cleiren en Bakker, *a.w.,* p. 40; S. Bakker e.a., a.w., onder 2.1.; AG Machielse in r.o. 8.2 van zijn conclusie (ECLI:NL:PHR:2001:ZD2776) bij HR 9-10-2001 ECLI:NL:HR:2001:ZD2776 (Danslessen-arrest); Zie verder ook HR 8-12-2015, ECLI:NL:HR:2015:3483, (r.o. 4.3.1.) *NJ* 2016/95 m.nt N. Keijzer, NBSTRAF 2016/18 m.nt. Van der Kruijs; JIN 2016/18 m.n.t de Bruijn-Lückers ("*'s Hofs oordeel dat schilderijen niet reeds naar hun aard buiten het bereik van art. 240b Sr vallen, is juist. Uit de wetsgeschiedenis volgt daarbij bovendien dat het in dit verband niet nodig is geacht om een uitzondering te maken voor artistieke virtuele kinderporno omdat virtuele uitingen die artistiek zijn, doorgaans geen realistische uitstraling hebben. Die uitzondering is ook niet wenselijk geacht, omdat artisticiteit die zou kleven aan een realistische virtuele pornografische afbeelding daaraan niet het strafwaardige karakter ontneemt*.").

[427] Aldus ook Cleiren en Bakker, *a.w.,* p. 36-37 en bijv. EHRM 24-5-1988, *NJ* 1991, 685 (*Müller/Zwitserland*): "*Artists are certainly not immune for the possibilities of limitations as provided for in par. 2 of Article 10*".

[428] Een motie van die strekking (Kamerstukken II 1994/95, 23 682, nr. 6) om een kunstexceptie bij art. 240b Sr op te nemen is namelijk al voor de stemming daarover ingetrokken, terwijl wel een motie en amendement (in de vorm van tweede lid bij art. 240b Sr) werden aangenomen waarin een uitzondering op 240b was opgenomen met betrekking tot therapeutische, educatieve en wetenschappelijke doeleinden (Kamerstukken II 1994/95, 23 682, nrs. 9 en 14). Art. 240b, tweede lid, Sr is echter vervolgens in 2002 weer geschrapt, omdat deze exceptie naar het oordeel van de Tweede Kamer te veel mogelijkheden voor misbruik bood. Zie hierover ook: W. Sorgdrager, *Geen exceptio artis, maar wel bescherming van kunst*, In: AA 2009, nr. 5, p. 294 en AG Knigge in r.o. 56 e.v. van zijn conclusie (ECLI:NL:PHR:2010:BO6446) bij HR 7-12-2010, ECLI:NL:HR:2010:BO6446.

[429] O.m. Cleiren en Bakker, *a.w.* , p. 38; F. Janssens, 'Eén hand en één voet aan de exceptio artis; de kunstexceptie nader bekeken', Mediaforum 1995-02, p. 21-22 en r.o. 56 van de conclusie van AG Knigge (ECLI:NL:PHR:2010:BO6446) bij HR 7-12-2010, ECLI:NL:HR:2010:BO6446.

[430] Zie bijv. AG Knigge in r.o. 84-85 van zijn conclusie (ECLI:NL:PHR:2010:BO6446) bij HR 7-12-2010, ECLI:NL:HR:2010:BO6446, *NJ* 2011, 81.

[431] Vgl. bijv. Hof Arnhem-Leeuwarden 25-3-2019, ECLI:NL:GHARL:2019:2852 (Verdachte, een afgestudeerd en gepromoveerd criminoloog, stelt dat hij er in alle redelijkheid vanuit is gegaan dat het in voorraad hebben van kinderpornografisch materiaal in zijn geval is toegestaan omdat het materiaal voor een wetenschappelijk doel – de archivering t.b.v. wetenschappelijk onderzoek – wordt gebruikt. Het verweer wordt verworpen. *"...(Niet) blijkt van het bestaan van (een begin van) een onderzoek op wetenschappelijke basis (...) die in een potentieel rechtvaardigend verband te brengen zou zijn met hetgeen op de gegevensdragers van verdachte is aangetroffen aan kinderpornografisch en/of dierenpornografisch materiaal. Evenmin is gebleken dat enig onderzoek van verdachte op dit vlak was of zou worden ingebed in, bijvoorbeeld, een onderzoeksprogramma, of*

het kunstverweer als zodanig slechts zeer zelden door verdachten is gevoerd, ook niet waar dat wellicht wel in de rede had gelegen.[432]

Aangezien een formele geschreven of ongeschreven wetenschaps- of kunstexceptie als straf- of schulduitsluitingsgrond in het Nederlandse strafrecht ontbreekt, zal een beroep op een dergelijke belangenafweging juridisch dienen te worden geplaatst in:

- de vorm van een bewijsexceptie ("de afbeeldingen zijn vanwege hun wetenschappelijk/artistieke karakter niet als kinderpornografisch aan te merken")[433]; of
- de vorm van een kwalificatieverweer (de afbeeldingen voldoen weliswaar aan de omschrijving van art. 240b Sr, maar de gedragingen van de verdachte zijn, alle omstandigheden in aanmerking genomen, niet van dien aard dat deze moeten worden gekwalificeerd als het in art. 240b Sr als misdrijf tegen de zeden strafbaar gestelde feit)[434]; of
- de vorm van een beroep op het ontbreken van de materiële wederrechtelijkheid.

---

dat er concrete belangstelling was voor uitgave van enig door verdachte te produceren wetenschappelijk werk. Uit het onderzoek (...) blijkt ook nergens dat op verdachtes computers is gebleken van enige vorm van evaluatie, analyse en/of ordening van het verworven en bekeken beeldmateriaal. In tegenspraak met verdachtes stelling – dat het noodzakelijk was eerst een archief van deze afbeeldingen ten behoeve van wetenschappelijk onderzoek aan te leggen – is niet gebleken nu verreweg het meeste materiaal blijkt te zijn gewist.
Het op deze wijze jarenlang op zeer grote schaal downloaden van kinderpornografisch materiaal kan naar het oordeel van het hof redelijkerwijs geen wetenschappelijk doel dienen. Het gegeven dat op de gegevensdragers van verdachte (delen van) chats zijn aangetroffen waaraan hij zelf onder diverse pseudoniemen deelnam en waarin – ook door verdachte – op zeer grove wijze werd gesproken over het seksueel misbruiken van (zeer) jonge kinderen, sterkt het hof in zijn oordeel dat het beweerde wetenschappelijk doel ontbrak."). Vgl. ook RB Midden-Nederland, 15-5-2019, ECLI:NL:RBMNE:2019:2161 (verweer: tussen 2015-2017 ruim 20.000 foto's en 3.000 filmpjes van kinderpornografische aard verzameld naar aanleiding van een tv-programma over kindermisbruik, omdat verdachte wilde aantonen hoe makkelijk kinderporno online te vinden is. De verdachte is echter nooit naar het politiebureau gegaan, zelfs niet toen hij werd verdacht van het bezit van kinderporno. Het verweer wordt als ongeloofwaardig verworpen); RB Rotterdam, 13-11-2020, ECLI:NL:RBROT:2020:10242, *NJFS* 2021/145 (verweer (beroep op het ontbreken van de materiële wederrechtelijkheid): verdachte zou het kinderpornografisch materiaal voor wetenschappelijke doeleinden hebben verzameld. RB verwerpt dit verweer, nu dit op geen enkele wijze aannemelijk is geworden); RB Rotterdam, 7 februari 2023, ECLI:NL:RBROT:2023:2471 (verweer (beroep op art. 9a Sr: verdachte wilde met zijn handelen juist aandacht vragen voor het op televisie tonen van kinderporno tijdens het kinderprogramma Shaun het Schaap verworpen als ongeloofwaardig).

[432] Zo werd in de bekende Holland Festival-zaak (waarbij een foto van een bekende fotograaf in beslag werd genomen, waarop een naakt kind zichtbaar was zittend op de arm van een volwassen man met een erectie) die leidde tot HR 26-9-2000, ECLI:NL:HR:2000:AA7230, *NJ* 2001, 61 (m.nt. de Hullu) bij de Hoge Raad niet met zoveel woorden een kunstexceptie-verweer gevoerd; hetzelfde geldt met betrekking tot de zaak die leidde tot HR 7-12-2010, ECLI:NL:HR:2010:BO6446 (foto's en fotocollages van professionele fotograaf van seksuele gedragingen van jongens van 7-17 jaar).

[433] In deze zin begrijpen wij ook Cleiren en Bakker, a.w., p. 40, en AG Knigge in r.o. 84 en 85 van zijn conclusie (ECLI:NL:PHR:2010:BO6446) bij HR 7-12-2010, ECLI:NL:HR:2010:BO6446. Vgl. ook HR 8-12-2015, ECLI:NL:HR:2015:3483, (r.o. 4.3.1.), *NJ* 2016/95 m. nt N. Keijzer, NBSTRAF 2016/18 m. nt. Van der Kruijs; JIN 2016/18 m.nt. De Bruijn-Lückers.

[434] Vgl. HR 12-3-2013, ECLI:NL:HR:2013:BZ2653 (Tongzoenarrest-II) en HR 9-2-2016, ECLI:NL:HR:2016:213.

De beoordeling van een dergelijk beroep, in welke sleutel dan ook geplaatst, is met name in geval van de kunstexceptie niet eenvoudig, vooral omdat het daarbij nagenoeg onontkoombaar is dat de strafrechter zich althans enig oordeel vormt over de artistieke strekking van de afbeelding c.q. het artistieke karakter van de verweten gedraging.[435] Omdat er weinig persoonlijker is dan het oordeel over wat kunst is, wordt hier de strafrechter gevraagd uiterst glad ijs te betreden. Met Cleiren en Bakker komt het ons voor dat het oordeel van de rechter over het artistiek karakter van een zekere afbeelding (of reeks afbeeldingen) dan ook niet slechts op een subjectieve waardering van die rechter zal mogen berusten, maar tot op zekere hoogte ook aan objectieve maatstaven zal moeten voldoen.[436] Bij de concretisering van dit laatste kan men onder meer denken aan aspecten als: heeft de vervaardiger een opleiding als kunstenaar genoten, heeft hij bekendheid als kunstenaar, is hij en/of zijn werk ook in bredere zin binnen de kunstgemeenschap geaccepteerd enzovoorts. Ook zal bij deze toetsing de context waarbinnen de afbeelding is vervaardigd, verspreid, getoond of verkregen een rol spelen. Zo is het denkbaar dat bij de afweging mede een rol speelt of bij de afbeelding zelf al duidelijk werd (gemaakt) dat het ging om een artistieke uiting (waardoor overigens ook de vraag kan rijzen of de afbeelding is vervaardigd voor *primary sexual purposes,* en dus de afbeelding reeds daarom kan worden gekwalificeerd als kinderpornografisch), of de plaats of het medium waar(op) het is getoond (bijvoorbeeld een museum dan wel op een schimmige *darkweb*-site).[437]

Ten aanzien van de vraag of een afbeelding een artistiek karakter heeft, zal de strafrechter marginaal moeten toetsen. Anders dan Cleiren en Bakker[438] zouden wij echter menen dat daarbij niet als maatstaf zou moeten worden gehanteerd of de gedraging c.q. de afbeelding "een kennelijk artistiek karakter heeft". Daardoor zou onvoldoende recht worden gedaan aan het specifieke karakter van de kunstexceptie en zou de lat in strafrechtelijke zin voor verdachten waarschijnlijk te hoog worden gelegd. Anderzijds ligt wel een aanzienlijke mate van objectivering in de rede, omdat anders de persoonlijke opvatting van de betrokkene omtrent het artistieke gehalte van de afbeelding reeds al grotendeels beslissend zou zijn. In dit licht zou een toetsingscriterium als "*Is de gedraging van dien aard en onder zodanige omstandigheden geschied dat zij in het algemeen, en naar algemene maatstaven, kan worden aangemerkt als een artistieke kunstuiting*" wellicht werkbaar zijn.

Als de gedraging c.q. de afbeelding voormelde marginale rechterlijke toetsing omtrent het artistieke karakter daarvan heeft doorstaan, zal de strafrechter moeten afwegen of in het concrete geval de 'kunstvrijheid' zwaarder weegt dan het geschonden rechtsbelang, in casu het belang van de bescherming van minderjarigen (het bestrijden van het tegengaan van een subcultuur die het vervaardigen (etc.) van kinderpornografisch materiaal bevordert daaronder begrepen). Die beoordeling zal moeten plaatsvinden in het licht van de context waarin de betreffende gedraging of uiting heeft plaatsgevonden, waarbij de rechter ook (wellicht veranderde[439]) maatschappelijke opvattingen, traditie, gevoeligheden en nationale culturele

---

[435] Onzes inziens is - ook bezien in het licht van latere jurisprudentie van de HR (waaronder HR 9-1-2001, *NJ* 2002, 76, m.nt. De Hullu) HR 11-12-1990, *NJ* 1991, 313, m.nt. 't Hart (Theo van Gogh-arrest), voor zover daarin wordt overwogen: "*Met name hoefde het hof zich niet uit te laten over de vraag of het artikel als geheel moet gelden als een kunstwerk*" naar huidig recht bezien daarom te absoluut in zijn formulering.
[436] Cleiren en Bakker, *a.w.*, p. 38.
[437] Vgl. ook S. Bakker e.a, *Bedreigende rap en de kunstexceptie* , PROCES 2015, aflevering 3, p. 175 e.v., onder 2.5 en 2.6.
[438] Cleiren en Bakker, *a.w,* p. 39.
[439] Zo zullen bepaalde afbeeldingen van – soms ook met naam genoemde minderjarigen – in bepaalde "artistieke" fotoboeken of van "beroemde" fotografen uit de jaren '70 en '80 van de vorige eeuw naar huidige maatstaven als kinderpornografisch kunnen worden beschouwd. Het gegeven dat die afbeeldingen in de jaren '70

eigenheden zal moeten meewegen. Meer concreet brengt dit mee dat bij de afweging ook kan worden betrokken of, en zo ja: op welke wijze, de afbeelding kenbaar was voor derden: het is – ook vanuit de beschermingsgedachte van art. 240b Sr – waarschijnlijk toch wat anders of een "artistiek" werk in het privé-atelier van een kunstenaar hangt of door deze laatste breed op internet wordt verspreid. Evenzo zal de strafrechter vanuit diezelfde beschermingsgedachte bij de belangenafweging waarschijnlijk gewicht toekennen aan aspecten als het op de afbeeldingen herkenbaar afgebeeld zijn van bepaalde minderjarigen en de aard en het karakter van de op de afbeelding getoonde seksuele gedragingen.

Honoreert de strafrechter het beroep, dan zal afhankelijk van de grondslag daarvan de strafrechter tot een vrijspraak dan wel ontslag van rechtsvervolging van de verdachte komen.

5.3. Vrijwillige medewerking van en/of geen schade bij betrokken minderjarige

Met enige regelmaat wordt – veelal in het kader van een beroep op het ontbreken van de materiële wederrechtelijkheid – in art. 240b-zaken aangevoerd dat de afgebeelde minderjarige persoon heeft ingestemd met de vervaardiging of dat niet gebleken is dat deze daardoor schade heeft geleden. Met uitzondering van de situaties welke hiervoor onder 5.1. zijn omschreven (i.e. consensuele privé-afbeeldingen van en door adolescenten zonder risico op verspreiding), volgt uit de rechtspraak[440] dat dergelijke omstandigheden niet kunnen afdoen aan het kinderpornografische karakter van een afbeelding en/of de strafbaarheid van de betreffende gedraging met betrekking tot die afbeelding.

Het is derhalve voor de beoordeling van het kinderpornografisch karakter van een afbeelding *irrelevant* of een minderjarige instemde of meewerkte aan de totstandkoming van de betreffende afbeeldingen. De gedachte hierachter is dat jeugdigen in voorkomende gevallen ook tegen zichzelf in bescherming genomen moeten kunnen worden.[441] Zulks te meer omdat er ook nogal eens vraagtekens kunnen worden geplaatst bij de vrijwilligheid van de betreffende instemming.[442] Evenzo ontneemt de omstandigheid dat niet gebleken is dat de

---

als kunst werden gezien zal echter gezien de gewijzigde opvattingen van de (internationale) wetgever (en wellicht breder: de samenleving) niet zonder meer de doorslag hoeven te geven indien de hier bedoelde belangenafweging onder de huidige regelgeving moet plaatsvinden. Vgl. in die zin ook AG Knigge in r.o. 83 e.v. van zijn conclusie (ECLI:NL:PHR:2010:BO6446) bij HR 7-12-2010 ECLI:NL:HR:2010:BO6446. Daarbij kan worden opgemerkt dat niet kan worden uitgesloten dat de ook in dergelijke fotoboeken afgebeelde toenmalig minderjarigen ook thans nog schade zouden kunnen ondervinden als gevolg van (verdere) publicatie van foto's waarop zij zijn afgebeeld.

[440] O.m. HR 18-11-2014, ECLI:NL:HR:2014:3291 (16/17-jarig meisje sms't naaktfoto's van zichzelf aan 18/19-jarige jongen, die ze vervolgens verder verspreidt; cassatie tegen veroordeling voor art. 240b Sr verworpen) en Hof Den Haag 2-4-2012, ECLI:NL:GHSGR:2012:BW0675.

[441] Zie bijv. RB Rotterdam 22-11-2017, ECLI:NL:RBROT:2017:9328 ("*door de verdachte is het geslachtsdeel van het slachtoffer meermalen op beeld vastgelegd. Gelet op het grote verschil in leeftijd tussen het slachtoffer en de verdachte (een jongen van (bijna) 16 jaar en een man van 49 jaar) is daarmee gehandeld in strijd met een sociaal-ethische norm. Kinderen, ook kinderen van (bijna) 16 jaar, dienen beschermd te worden tegen de schade die door het maken van dit soort opnamen kan ontstaan. De eventuele instemming van het (bijna) 16-jarige slachtoffer met de vervaardiging van de pornografische opnamen neemt in dit geval de schadelijke effecten ervan niet weg*").

[442] Hierbij kan ook gedacht worden aan situaties waarin loverboys met "instemming" van het betrokken meisje seksueel getinte afbeeldingen maken om deze als "wervingsmateriaal" op internet te plaatsen; zie hierover ook Mr. C.E. Dettmeijer-Vermeulen (toen Nationaal Rapporteur Mensenhandel) en mr. dr. M. Boot-Matthijssen, *Minderjarige slachtoffers in mensenhandelzaken: Ze wilde het zelf. Toch?,* Tijdschrift Praktijkwijzer Strafrecht (TPWS), 2014/30, par. 5. Vgl. ook RB Midden-Nederland 24-4-2015, ECLI:NL:RBMNE:2015:2846 (veroordeling mensenhandel (minderjarig meisje in prostitutie te brengen) en vervaardigen en bezit kinderporno mbt foto's bij seksadvertentie); RB Rotterdam 4-6-2015, ECLI:NL:RBROT:2015:4080 (mensenhandel jegens

afgebeelde minderjarige concrete schade heeft opgelopen, niet het kinderpornografisch karakter aan de betreffende afbeelding.[443]

Zoals elders aangegeven kunnen genoemde omstandigheden er onder omstandigheden echter wel toe leiden dat wordt afgezien van vervolging[444], dan wel dat de gedragingen met de betreffende afbeeldingen niet worden gekwalificeerd als overtreding van art. 240b Sr.[445]

5.4. Geen (vermoeden van) wetenschap van minderjarigheid

Het komt wel voor dat verdachten aanvoeren zich totaal niet bewust te zijn geweest van het feit dat een afbeelding (vanwege de daarop zichtbare seksuele gedraging en/of de kennelijke leeftijd van de daarop afgebeelde persoon) als kinderpornografisch wordt beschouwd. Raadslieden zijn echter nogal eens vaag over de juridische sleutel waarin dit verweer dan dient te worden geplaatst.[446] Dit is van belang omdat – zoals hiervoor al onder 4.4. aangegeven – die bewustheid voor het aannemen van opzet en dus voor de bewezenverklaring niet is vereist.

Het ontbreken van die bewustheid kan echter ook worden geduid als dwaling omtrent de strafbare aard van de afbeelding en houdt dan een beroep in op de (ongeschreven) schulduitsluitingsgrond "afwezigheid van alle schuld" (hierna: 'avas').[447] Dit is een verweer waarop de rechter gemotiveerd dient te responderen en dat bij aanvaarding leidt tot ontslag van rechtsvervolging.

Gezien de strekking van de strafbepaling (het bieden van bescherming aan minderjarigen en het tegengaan van een ongewenste subcultuur) zal een dergelijk avas-verweer overigens naar verwachting niet snel worden gehonoreerd.[448] In dit kader zal waarschijnlijk ook meewegen

---

een minderjarige, o.a. plaatsen van seksadvertenties op internet; RB Noord-Nederland, 13-5-2015, ECLI:NL:RBNNE:2015:2306 **(**mensenhandel jegens 16-jarige; vervaardigen/verspreiden en voorhanden hebben van kinderpornografische afbeeldingen (t.b.v. seksadvertenties).

[443] HR 10-6-2014, ECLI:NL:HR:2014:1359, r.o. 3.5; HR 7-12-2010, ECLI:NL:HR:2010:BO6446, r.o. 3.4.

[444] Zie hierna onder 7.1.1.

[445] Zie hiervoor onder 5.1.

[446] Ook gerechten lijken hierbij de weg wel eens kwijt te raken; zie bijv. RB Oost-Brabant 18-11-2016, ECLI:NL:RBOBR:2016:6439 (Vrijspraak, weliswaar sprake van "zich toegang verschaffen tot"**,** maar RB kan niet vaststellen dat verdachte op dat moment wist of redelijkerwijs diende te vermoeden dat het afbeeldingen betrof van een persoon onder de 18 jaar), waarbij over het hoofd wordt gezien dat in art. 240b Sr de (kennelijke) leeftijd is geobjectiveerd, en derhalve de wetenschap van de verdachte daaromtrent voor de bewezenverklaring niet relevant is. Dit laat onverlet dat de omstandigheden in deze zaak wellicht wel aanleiding hadden kunnen geven voor een ontslag van rechtsvervolging vanwege *avas*.

[447] Aldus ook de Conclusie van AG Harteveld (ECLI:NL:PHR:2014:2095), r.o. 6.2, bij HR 18-11-2014 ECLI:NL:HR:2014:3304). Zie voor het beoordelingskader van een beroep op *avas* ook de conclusie van AG Harteveld (ECLI:NL:PHR:2017:62), r.o. 3.9 bij HR 14-2-2017, ECLI:NL:HR:2017:231.

[448] Zie o.m. HR 20-1-1959, *NJ* 1959, 102 en HR 20-1-1959, *NJ* 1959, 103 (de zogenaamde "leeftijdarresten"), waarbij de Hoge Raad overwoog: "*De vraag, of bij den dader van een strafbaar feit alle schuld in strafrechtelijken zin afwezig is, moet evenwel worden beantwoord in verband met den aard en de strekking van de strafbepaling, welker overtreding den verdachte verweten wordt. Voor wat art. 247 Sr. betreft blijkt uit de wettelijke omschrijving van die bepaling, dat daarmede is beoogd personen beneden den leeftijd van zestien jaren t.a.v. misdrijven tegen de zeden een zo doeltreffend mogelijke strafrechtelijke bescherming te doen geworden. Hieruit volgt dat art. 247 Sr. ook de strekking heeft deze jeugdige personen te beschermen tegen verleiding, die mede van hen zelf kan uitgaan. Gelet op de bescherming welke als voormeld bepaaldelijk art. 247 Sr. beoogt te geven aan een persoon, die den leeftijd van zestien jaren nog niet heeft bereikt, zou het doel van deze strafbepaling worden gemist, indien een verweer als hoger weergegeven (dat de getuige d. J. er uitziet als een vrouw, die den leeftijd van zestien jaren is gepasseerd, en dat deze getuige, voordat hij (req.) het bewezenverklaarde feit pleegde, desgevraagd een hogere leeftijd dan vijftien jaar heeft opgegeven) haar toepassing zou vermogen uit te sluiten*".

dat reeds in het gecombineerde gebruik van bepaalde op jeugdigheid/jonge leeftijd en seksualiteit/naaktheid gerichte zoektermen een zeker risico gelegen is dat men ook kinderporno aantreft. In zo'n geval lijkt het derhalve niet erg waarschijnlijk dat zal worden aanvaard dat sprake is van het ontbreken van *alle* schuld. Aannemelijk is ook dat zulks niet anders wordt door de enkele vermelding op een website dat alle afgebeelde personen achttien jaar of ouder zijn[449] of door een mededeling van die strekking, of andere gedraging van de afgebeelde zelf.[450] Evenzo lijkt aannemelijk dat aanwijzingen op een site zelf dat men niet kan instaan voor de meerderjarigheid van de afgebeelde personen, in de weg zullen staan aan de aanvaarding van een avas-verweer.

5.5. "louter bezit van *virtuele* kinderpornografie is niet strafbaar"

Incidenteel wordt onder verwijzing naar incidentele passages uit de wetsgeschiedenis en naar het recht van privéleven, zoals vastgelegd in art. 8 van het Verdrag tot bescherming van de Rechten van de mens en de fundamentele Vrijheden (EVRM) en/of art. 3 van het Kaderbesluit ter bestrijding van seksuele uitbuiting[451] wel betoogd dat privébezit van virtuele kinderporno geen strafbaar handelen zou zijn. Dit verweer is tot op heden echter verworpen.[452]

---

[449] Aldus RB Oost-Brabant 7-6-2013, ECLI:NL:RBOBR:2013:CA2370 (verwerping verweer dat sprake is van een verontschuldigbare dwaling ten aanzien van de leeftijd van de gefotografeerde modellen, op de website stond een disclaimer inhoudende dat alle modellen die zijn weergegeven op de betreffende website de leeftijd van 18 jaar of ouder hebben, uiteraard ten tijde van het vervaardigen van de beeldopname).

[450] Zie o.m. ook de hiervoor weergegeven overwegingen in HR 20-1-1959, *NJ* 1959, 102 en HR 20-1-1959, *NJ* 1959, 103. Vgl. ook Hof Den Haag 7-6-2016, ECLI:NL:GHDHA:2016:1703 (O.m. aanwezig hebben van seksueel getinte "bloot foto's of filmpjes/video's" van een 14-jarige leeftijdgenote; Het aanwezig hebben van deze foto's en filmpjes/video's verschaft de verdachte een zekere macht over het afgebeelde slachtoffer; immers de macht om de afbeeldingen al of niet te verspreiden. Daardoor komt de afgebeelde onder druk te staan en wordt haar privacy bedreigd. Zij geniet de bescherming van de wet, ook al heeft zij zelf door de foto's en filmpjes te versturen hieraan meegewerkt).

[451] Welke bepaling de aangesloten lidstaten de mogelijkheid biedt bezit en vervaardiging van virtuele kinderporno voor persoonlijk gebruik vrij te laten.

[452] RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (Na behandeling van het wetsvoorstel voor art. 240b Sr heeft de wetgever er voor gekozen om het bezit en vervaardigen van virtuele kinderporno strafbaar te stellen. Dat bij de behandeling van het wetsvoorstel de mogelijkheid is besproken om het bezit van virtuele kinderporno niet strafbaar te stellen, brengt daar geen verandering in. Van een vrijwaring tegen strafrechtelijke aansprakelijkheid als neergelegd in art. 3 van het Kaderbesluit heeft de Nederlandse wetgever kennelijk geen gebruik willen maken. Verweer verworpen).

HOOFDSTUK 6: ONDERZOEKS- EN BEWIJSASPECTEN

6.1. Opsporing en opsporingsmiddelen

6.1.1.1. Politieorganisatie en –werkwijze

De opsporing van gedragingen met betrekking tot kinderpornografie is feitelijk grotendeels neergelegd bij de Nationale Politie, hoewel de Koninklijke Marechaussee incidenteel ook op dit gebied actief is. Binnen de Nationale Politie is het taakveld kinderpornografie primair neergelegd bij de Teams Bestrijding Kinderporno en Kindersekstoerisme (TBKK). Deze teams bestaan uit een Landelijke Eenheid (gevestigd in Zoetermeer), die naast eigen landelijke onderzoeken ook projectvoorbereiding voor door lokale teams uit te voeren onderzoeken uitvoert, en 10 lokale teams TBKK. De totale formatie (landelijk en lokaal) van het TBKK bedroeg in 2018 ongeveer 150 fte.[453] Met name het TBKK bij de Landelijke Eenheid beschikt over hoogwaardige inhoudelijke kennis en – ook vanwege de directe werkrelatie met het Team High Tech Crime van dezelfde Landelijke Eenheid – over geavanceerde (ICT-)technische kennis en faciliteiten.

Bij het Openbaar Ministerie is één landelijk Officier van Justitie Kinderporno/Transnationaal Seksueel Misbruik, met daarnaast 4 OvJ's bij het Landelijk Parket met de portefeuille kinderpornografie en kindersekstoerisme werkzaam.[454] Zij leiden de onderzoeken van de Landelijke Eenheid en hebben ook een onderverdeling in portefeuilles/expertises (zoals kindersekstoerisme, Indigo-beleid, computercontroles, sexting, etc). Deze OvJ's zijn werkzaam bij het Landelijk Parket. Daarnaast zijn er bij de Arrondissementsparketten ook nog zeden-OvJ's die onderzoeken met betrekking tot art. 240b Sr draaien.

Door vertegenwoordigers van de internetindustrie is eind jaren negentig ook het Meldpunt Kinderporno op Internet (MKP) opgericht[455], waar burgers en bedrijven online ook laagdrempelig vermoedens omtrent gedragingen met kinderpornografie kunnen melden. Het MKP werkt op basis van een met het Openbaar Ministerie gesloten overeenkomst. Omdat het MKP zich niet bezig mag houden met opsporing, behandelt het slechts meldingen van kinderpornografie op openbaar internet, zoals die betreffende websites en openbare fora. Het MKP verzendt ook Notice and Take Down (NTD)-berichten[456] aan Nederlandse ISP/ESP's en doormelding van meldingen bestemd voor buitenlandse ISP/ESP's via het INHOPE-netwerk.[457] Overige voor Nederland van belang zijnde opsporingsindicaties meldt het MKP bij de Landelijke Eenheid TBKK.

---

[453] Informatie ontleend aan de bijlage Resultaten kinderporno en kindersekstoerisme 2018 bij Kamerbrief aanpak online seksueel misbruik en bestuurlijke handhaving van Minister van Justitie en Veiligheid Grapperhaus van 3 juli 2019.

[454] Idem.

[455] Dit Meldpunt is onderdeel van het publiek/privaat gefinancierde Expertisebureau Online Kindermisbruik (EOKM).

[456] Deze taaktoedeling roept wel enige vragen op aangezien het verzenden van NTD-berichten ex art. 125p Sv is voorbehouden aan de OvJ, na machtiging door de RC. Waarschijnlijk stuurt het MKP dus een NTD-bericht op eigen titel, en wordt eerst indien daaraan geen gevolg wordt gegeven, op verzoek van het MKP ook een formeel bevel ex art. 125p Sv door de OvJ afgegeven. Zie over de NTD-bevoegdheid in relatie tot WCC-III ook het webblog van J.J. Oerlemans, Van-een-take-down-bevel-naar-internetfilters-voor-politiedoeleinden.

[457] INHOPE is de internationale organisatie van internet hotlines voor illegale online content, waarin 43 landen zijn vertegenwoordigd in een netwerk, door lidmaatschap van in totaal 47 (niet-politionele) organisaties die de taken van burgerlijke meldpunten uitvoeren.

De politie en het Meldpunt Kinderporno op Internet hebben internationaal goede operationele contacten met o.m. Facebook en Twitter. Deze techbedrijven en vele andere aanbieders van communicatiediensten hebben ook een zelfstandig beleid om kinderpornografisch materiaal te signaleren en te verwijderen. Steeds vaker wordt daarbij gebruik gemaakt van PhotoDNAsoftware[458], waarmee afbeeldingen die worden geüpload automatisch worden gecontroleerd op, onder andere, kinderpornografische content. Veelal hebben deze dienstenaanbieders ook een beleid om de accounts via welke kinderpornografisch materiaal is ontvangen of verspreid permanent te verwijderen.

Vermeldenswaard is in verband met het voorgaande het antwoord op Kamervragen van de Staatssecretaris van Economische Zaken en Klimaat van 29 januari 2019[459] waarin zij zich op het standpunt stelt dat zodra beeldmateriaal op de server van een hostingpartij is aangekomen niet langer de e-privacyregels (welke inhouden dat aanbieders van telecommunicatiediensten in beginsel geen kennis mogen nemen van de inhoud van het verkeer dat zij verzorgen) van toepassing zijn, maar de regels van de Algemene verordening gegevensbescherming, waardoor het de hostingpartij is toegestaan met behulp van de zogenoemde hashdatabase strafbare kinderpornografische content van zijn server te verwijderen. Voorts wordt in dit antwoord aangekondigd dat, indien het aantal meldingen van kinderporno niet daalt, de optie zal worden verkend om in de wet te voorzien in het maken van een uitzondering op het communicatiegeheim ten behoeve van het voorkomen van strafbare feiten. Wij merken in verband hiermee op dat de kwaliteit van het via hashvergelijking of met gebruik van PhotoDNAsoftware opsporen van kinderpornografische afbeeldingen zodanig is dat de kans op vals-positieve ontdekkingen te verwaarlozen is.

Dienstenaanbieders, zoals Facebook, Instagram, Whatsapp, YouTube en Twitter - die in de Verenigde Staten gevestigd zijn - moeten ingevolge de Amerikaanse wetgeving het gegeven dat kinderporno is aangetroffen ook melden aan The National Center for Missing & Exploited Children (NCMEC). Indien uit door het NCMEC verkregen gegevens, zoals IP-adressen waarmee een gebruikersaccount op het betreffende platform is aangemaakt, blijkt dat er mogelijk in Nederland te lokaliseren personen bij betrokken zijn, wordt de betreffende informatie gemeld en overgedragen aan het TBKK bij de Landelijke Eenheid. Canada kent een vergelijkbaar instituut: het National Child Exploitation Crime Centre (NCECC), dat eveneens de verkregen informatie meldt en overdraagt aan het TBKK bij de Landelijke Eenheid.

---

[458] PhotoDNA is wereldwijd de meest gebruikte technologie om al bekend beeldmateriaal op het internet te detecteren. Zie m.n. Lee et al., "Detecting child sexual abuse material: A comprehensive survey", Forensic Science International: Digital Investigation 2020, vol. 34, p. 7: "PhotoDNA is used by many organizations world-wide for detecting and reporting images of CSA and is available for free to law enforcement and tool providers." Ten opzichte van de hierna in par. 6.2.1. te bespreken hashwaardevergelijking betrekt deze software de inhoud van de afbeeldingen in de beoordeling, en is daarom in zekere zin 'slimmer' te noemen.

[459] Brief d.d. 29 januari 2019 aan de Voorzitter van de Tweede Kamer der Staten-Generaal.

In de praktijk blijkt dat veruit de meeste kinderpornozaken in Nederland worden geïnitieerd vanuit meldingen via het NCMEC, NCECC, het MKP en via buitenlandse opsporingsautoriteiten.[460] Het grote aantal meldingen[461] (en de soms gebrekkige inhoudelijke kwaliteit daarvan) in combinatie met de beschikbare opsporingscapaciteit, maakt echter dat slechts een klein percentage (ongeveer 6%) van deze meldingen daadwerkelijk leidt tot een concreet politieonderzoek. Bij de selectie van de zaken die worden opgepakt worden bepaalde criteria gehanteerd, zoals: meerdere meldingen met vermoedelijk dezelfde betrokkenen, recidive, aard van het materiaal, aard van de gedraging (productie, verspreiding dan wel bezit), fysiek misbruik, context van een gevoelig beroep, mogelijkheid tot identificatie van een slachtoffer, enzovoorts. Behalve via voormelde meldingen worden aanwijzingen van overtreding van art. 240b Sr veelal ook gevonden in de context van andere zedenzaken (zoals ontucht met minderjarigen) en mensenhandel. Steeds vaker worden dan naast die specifieke andere feiten ook de kinderpornofeiten zelfstandig onderzocht en ten laste gelegd.[462]

6.1.1.2 Ontoegankelijkmaking van gegevens

In de artt. 54a Sr en 125p Sv is de ontoegankelijkmaking van gegevens opgenomen.[463] Vóór 1 maart 2019 was de gehele regeling in art. 54a Sr opgenomen en was enkel sprake van een 'notice and takedown-procedure'. Omdat deze regeling voor de uitvoeringspraktijk diverse onzekerheden opriep, werd deze bevoegdheid weinig toegepast. Recentelijk lijkt de regeling in het kader van de aanpak van malafide hostingbedrijven en/of wederverkopers van hostingdiensten (resellers) op meer belangstelling te kunnen rekenen.[464] Thans bevat art. 125p Sv de eigenlijke bevoegdheid voor de officier van justitie om (na verkregen machtiging van de rechter-commissaris) aan een aanbieder van een communicatiedienst een bevel te geven om "terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten." Praktisch gezien vertoont de procedure overeenkomsten met die van het leggen van beslag in die zin dat sprake is van een voorlopige maatregel die gevolgd moet worden door een definitieve rechterlijke beslissing, in beginsel in het kader van een einduitspraak in een strafzaak.[465] Ook is het voor belanghebbenden mogelijk om te klagen tegen de toepassing van deze maatregel.[466]

---

[460] Zie bijv. RB Midden-Nederland 6-8- 2019, ECLI:NL:RBMNE:2019:3655 (door TBKK ontvangen meldingsrapport NCECC n.a.v. via een berichtendienst uitgewisseld kinderpornografisch materiaal); RB Midden-Nederland 8-8-2018, ECLI:NL:RBMNE:2018:4057 (door TBKK ontvangen meldingsrapport NCMEC n.a.v. op Twitter geplaatst kinderpornografisch materiaal); Hof Den Haag 25-9-2018, ECLI:NL:GHDHA:2018:2489 (idem, n.a.v. in Microsoft Skydrive geüpload kinderpornografisch materiaal);

[461] Uit de bijlage Resultaten kinderporno en kindersekstoerisme 2018 bij Kamerbrief aanpak online seksueel misbruik en bestuurlijke handhaving van Minister van Justitie en Veiligheid Grapperhaus van 3 juli 2019 blijkt dat het aantal meldingen van online seksueel misbruik en kinderpornografie is gestegen van ongeveer 5.000 in het jaar 2015 tot maar liefst ruim 30.000 in het jaar 2018. Daarvan worden slechts enkele honderden zaken opgepakt. De meldingen die uiteindelijk vanuit het NCMEC in Nederland aankomen, vormen overigens maar ongeveer 25% van de meldingen over strafbare feiten die via Nederlandse IP-adressen zijn gepleegd; ongeveer 75% wordt niet doorgezet op basis van afspraken over de inhoud van die meldingen (Bron: Landelijk Parket Rotterdam 2017).

[462] Dit lijkt mede het gevolg van de inspanningen van mr. C.E. Dettmeijer-Vermeulen en mr. dr. M. Boot-Matthijssen, zoals neergelegd in hun artikel: *Minderjarige slachtoffers in mensenhandelzaken: Ze wilde het zelf. Toch?*, Tijdschrift Praktijkwijzer Strafrecht (TPWS), 2014/30, par. 5.

[463] Voor de volledigheid verwijzen wij hier naar de 'vrijwillige' notice and takedown-procedure zoals omschreven in de "Gedragscode Notice-and-Take-Down", die in par. 6.1.1.1 wordt genoemd.

[464] Zie o.m. de Kamerbrief "Terugkoppeling reseller-actie" d.d. 8 maart 2023 van de Minister van Justitie en Veiligheid.

[465] Dit vloeit voort uit art. 354 lid 3 Sv.

[466] Dit vloeit voort uit art. 552a, eerste lid, tweede volzin, Sv.

Art. 54a Sr bevat thans (louter) een vervolgingsuitsluitingsgrond voor “een tussenpersoon die een communicatiedienst verleent”.[467] Deze wordt niet vervolgd indien hij voldoet aan een bevel tot ontoegankelijkmaking van gegevens als bedoeld in art. 125p Sv. In een arrest van het Gerechtshof Den Haag is op basis van interpretatie van de wetsgeschiedenis van art. 54a Sr/art. 125p Sv, beslist dat ingeval een telecommunicatiedienstverlener wordt verdacht van medeplichtigheid aan verboden handelingen van zijn klanten, onder bepaalde omstandigheden (ook zonder dat het OM een bevel ex art. 125p Sv heeft afgegeven) direct tot vervolging kan worden overgegaan.[468]

6.1.2. (Bijzondere) opsporings- en dwangmiddelen

6.1.2.1. Algemeen
De maximale straf op het een gewoonte of beroep maken van de in art. 240b Sr omschreven gedragingen met betrekking tot kinderpornografie is acht jaar.[469]
Dit betekent dat in beginsel bij verdenking van overtreding van art. 240b Sr naast de normale opsporingsbevoegdheden zoals bijvoorbeeld inbeslagname, ook alle bijzondere opsporingsbevoegdheden mogen worden ingezet.

In dit type zaken blijken echter vooral de volgende bijzondere opsporingsmiddelen te worden ingezet[470]:
- de mogelijkheid om ex artt. 126na, 126nc en 126uc Sv gegevens (bijvoorbeeld de tenaamstelling van een IP-adres) van ISP’s of dienstenaanbieders als Google, Microsoft, Facebook en WhatsApp op te vragen;
- de mogelijkheid om ex artt. 126m Sv of 126t Sv met behulp van een internettap de communicatie van en naar de computer(s) van een verdachte te volgen;
- de mogelijkheid om ex artt. 126nd Sv en 126ud Sv 'overige gegevens' zoals gegevens omtrent (creditcard)betalingen te vorderen.

Nu de Wet Computercriminaliteit-III in werking is getreden, is bij verdenking van bepaalde gedragingen met betrekking tot kinderpornografie ook het heimelijk (en op afstand) binnendringen in een geautomatiseerd werk dat in gebruik is bij een verdachte toegestaan. Het betreffende art. 126nba Sv kan worden toegepast met het oog op bepaalde onderzoekshandelingen.[471] Deze onderzoekshandelingen zijn opgenomen in het eerste lid van het artikel in sub a tot en met e. De eerste drie onderzoekshandelingen (a. de vaststelling en vastlegging van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker daarvan, b. de uitvoering van een bevel tot opnemen van vertrouwelijke communicatie of het opnemen van communicatie door middel van een technisch hulpmiddel en c. de uitvoering van een

---

[467] Opvallend is dat in de hier besproken bepaling de geadresseerde verschillend wordt omschreven. In art. 125p wordt de term “aanbieder van een communicatiedienst” zoals omschreven in art. 138g Sv gebruikt. Dat in art. 54a Sr een ander begrip wordt gehanteerd vloeit blijkens de Memorie van Toelichting (TK 2015-2016, 34372, nr. 3, blz. 84) voort uit de omstandigheid dat het oude art. 54a Sr een implementatie van de Richtlijn inzake elektronische handel vormde. Wat hier ook van zij, wat ons betreft is een en ander geen aanleiding om aan te nemen dat in art. 54a Sr inhoudelijk iets anders wordt bedoeld dan in art. 125p Sv. Dat zou wetssystematisch ook niet te rijmen zijn.
[468] Hof Den Haag, 23-8-2022, ECLI:NL:GHDHA:2022:1550.
[469] Art. 240b, tweede lid, Sr.
[470] Zie hierover verder ook: Oerlemans, J.J. , *Een verborgen wereld: kinderpornografie op internet*, Tijdschrift voor Familie- en Jeugdrecht (FJR), 2010, afl. 10, p. 81 e.v..
[471] Het voert te ver om alle eisen die worden gesteld aan de inzet van de zogenaamde hackbevoegdheid hier uitvoerig te benoemen, maar belangrijk om op te merken is dat de officier van justitie onder meer toestemming moet hebben van de Centrale Toetsingscommissie alvorens een bevel te kunnen uitvaardigen en de rechter-commissaris daarvoor een machtiging moet verlenen.

bevel tot observatie) kunnen worden toegepast als het gaat om strafbare feiten waarvoor op grond van art. 67, eerste lid, Sv voorlopige hechtenis is toegelaten en die een ernstige inbreuk op de rechtsorde opleveren. De vierde en vijfde onderzoekshandeling (d. het vastleggen van gegevens die in het geautomatiseerde werk zijn opgeslagen en e. de ontoegankelijkmaking van gegevens) kunnen worden toegepast als het gaat om een misdrijf waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen.

Concreet betekent dit dat alle onderzoekshandelingen zouden kunnen worden verricht ten aanzien van art. 240b, eerste en tweede lid, Sr. Gelet op het strafmaximum in lid 1 (4 jaar) voldoet het aan de op dat punt gestelde eis van art. 126nba lid 1 onder a tot en met c. Art. 240b, eerste lid, Sr is in art. 2 van het Besluit onderzoek in een geautomatiseerd werk aangewezen als een misdrijf waarbij ook de onderzoekshandelingen genoemd in art. 126nba, lid 1, onder d en e, Sv kunnen worden verricht. Het strafmaximum van art. 240b, tweede lid, Sr is maximaal 8 jaar gevangenisstraf, waardoor alle in art. 126nba, eerste lid, Sv genoemde onderzoekshandelingen kunnen worden verricht. Vermoedelijk zal de aanvullende eis dat het moet gaan om een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert, geen beletsel vormen.

Dat de mogelijkheid thans bestaat wil evenwel niet zeggen dat gerekend kan worden op de inzet van de hackbevoegdheid in de context van de opsporing van kinderpornografie. Andere strafbare feiten, zoals (grootschalige) computervredebreuk en andere cyberdelicten, maar ook zware georganiseerde misdaad, zullen vermoedelijk de komende tijd meer prioriteit krijgen.

In veel gevallen zal de opsporing zich in eerste instantie richten op de gegevens die bekend zijn naar aanleiding van een melding, zoals hierboven onder 6.1.1.1. omschreven. Kan op basis van voormeld onderzoek een verdachte of computerlocatie voldoende geïdentificeerd worden, dan wordt vervolgens in lichtere gevallen[472] die persoon of locatie bezocht en wordt uitlevering ex art. 551 Sv van (de computers en gegevensdragers met) kinderpornografisch materiaal verzocht.[473] Bij toepassing van art. 551 Sv kunnen, *bij verkregen toestemming daartoe van de (hoofd)bewoner*, dezelfde opsporingshandelingen in de woning worden toepast als gebruikelijk tijdens een doorzoeking onder leiding van een rechter-commissaris. Te denken valt hierbij aan het maken van foto's van de woning, het opmeten van vertrekken, het openen van kasten etc.

---

[472] Het gaat dan om de verdenking van een relatief eenvoudig delict, zoals het enkele bezit, verspreiden of zich toegang verschaffen tot. Bij een zwaardere verdenking (vervaardigen, grootschalig verspreiden of misbruik) wordt (met de RC) doorzocht op grond van art. 110 Sv (Bron: Landelijk Parket Rotterdam).

[473] In het kader van het zogenaamde INDIGO-beleid (zie hierna onder 7.1.1.) is een dergelijk bezoek als volgt nader uitgewerkt: "*Alle verdachten worden onaangekondigd thuis bezocht waarbij gekozen wordt voor een low-profile benadering die zo min mogelijk aandacht oproept. Hierbij wordt door de ter plaatse aanwezige politiemedewerkers, waarvan ten minste 1 bevoegd zedenrechercheur voor de beoordeling van eventueel aangetroffen materiaal, een inschatting gemaakt omtrent de aard van de verdenking in relatie tot de situatie die wordt aangetroffen. Aan de (hoofd)bewoner wordt toestemming gevraagd tot binnentreding en onderzoek in de woning. Door de politiemedewerkers wordt de verdachte geïnformeerd over de aard van het onderzoek, de verdenkingen en indien daarvoor na afweging van de aangetroffen situatie, het Indigo traject. Dreiging met maatregelen bij niet medewerking dient te worden voorkomen.*
Indien eenmaal in de woning van de verdachte, de ter plaatse aanwezige verbalisanten van mening zijn dat er sprake is van een ernstiger verdenking dan aanvankelijk leek en/of contra indicaties voor Indigo afdoening blijken, kan er altijd ter plekke worden gekozen voor koerswijziging. Dat wil zeggen bevriezen van de operatie en direct contact opnemen met de teamleider en officier van justitie om te overleggen over hoe verder. Ook kan worden afgeschaald naar bijvoorbeeld de Indigo brief".

Ook vindt regelmatig direct, dan wel nadat aan een vordering tot uitlevering geen gehoor is gegeven en/of de verdachte geen toestemming geeft de woning te doorzoeken, onder leiding van de rechter-commissaris[474] of officier van justitie een doorzoeking ter inbeslagname plaats.[475] Dit betreft alleen computerapparatuur en gegevensdragers, voor gekopieerde gegevens geldt een ander juridisch kader (zie artt. 126nc e.v. Sv) nu deze niet in beslag kunnen worden genomen. De uitgeleverde gegevens en/of in beslag genomen computers en gegevensdragers worden daarna voor inhoudelijk onderzoek overgedragen aan gespecialiseerde medewerkers van de politie. Indien bijzondere deskundigheid vereist is worden vervolgens ook wel forensische onderzoeksinstellingen zoals het NFI ingeschakeld.

6.1.2.2. Onderzoek van gegevensdragers

Er is langere tijd discussie geweest over de vraag of de zelfstandige[476] inbeslagname en het daarop volgende digitaal forensisch onderzoek door de politie van *smartphones*, zonder dat de verdachte daarvoor toestemming had gegeven en zonder dat zij daarvoor een machtiging van de officier van justitie en/of de rechter-commissaris hebben gekregen, in overeenstemming is met het recht op privéleven ingevolge het EVRM. De rechtspraak was daarover verdeeld.[477]

---

[474] Zie art. 110 Sv. Zie voor een (uitzonderlijk) geval waarin de rechtbank aan een onrechtmatige binnentreding de consequentie van uitsluiting van het bewijs van een aangetroffen gegevensdrager met kinderpornografische afbeeldingen verbond: RB Gelderland 21-2-2017, ECLI:NL:RBGEL:2017:889.

[475] Zie voor de wijze van handelen door de rechter(-commissaris) indien de bestanden (al dan niet onder een geheimhouder) in beslag worden genomen en daartegen bezwaar wordt gemaakt: HR 9-2- 2021, ECLI:NL:HR:2021:193 (Conclusie AG: ECLI:NL:PHR:2021:18); het oordeel van de rechtbank dat het onderzoek is verricht door zodanige functionarissen en op zodanige wijze dat is gewaarborgd dat het verschoningsrecht niet in het gedrang komt, getuige niet van een onjuiste rechtsopvatting en is niet onbegrijpelijk; HR 25-10-2016, ECLI:NL:HR:2016:2418 (Conclusie AG: ECLI:NL:PHR:2016:1029): "*Ingevolge art. 98.4 Sv kan de verschoningsgerechtigde tegen de beschikking van de R-C ex art. 552a Sv een klaagschrift indienen bij de Rb. Nu de Rb. heeft vastgesteld dat de klager m.b.t. de bedoelde bestanden zich op zijn verschoningsrecht heeft beroepen en de R-C daaromtrent (nog) niet heeft beslist, had de Rb. de behandeling van het klaagschrift dienen aan te houden en de stukken in handen van de R-C moeten stellen teneinde een beschikking te geven a.b.i. art. 98.1 Sv. Het oordeel van de Rb. dat het klaagschrift in afwachting van de beschikking van de R-C ongegrond moet worden verklaard, is onjuist*"; Zie mbt art. 552a Sv ook: HR 24-1-2017, ECLI:NL:HR:2017:71 (Art. 552a.1 Sv voorziet evenwel in het doen van beklag over de kennisneming of het gebruik van gegevens, opgeslagen, verwerkt of overgedragen door middel van een geautomatiseerd werk en vastgelegd bij een onderzoek in zodanig werk. Anders dan de RB heeft overwogen leidt ECLI:NL:HR:2012:BX5510 niet tot een ander oordeel aangezien het in die zaak ging om de inbeslagneming van externe harde schijven en het klaagschrift strekte tot vernietiging van de gegevens die op die harde schijven waren opgeslagen) en RB Overijssel 1-2-2017, ECLI:NL:RBOVE:2017:417 (beklag over de kennisneming en het gebruik van gegevens die op vordering ex art. 126ng Sv zijn verstrekt. Openbaar ministerie mag gebruik maken van fiscale gegevens *uit de cloud* die het OM (in het kader van een strafzaak tegen een verdachte) heeft gevorderd bij een aanbieder van een fiscaal softwarepakket).

[476] Het gaat hierbij om (onderzoek aan) voorwerpen die door opsporingsambtenaren zelfstandig in beslag kunnen worden genomen en dus *niet* om voorwerpen die in het kader van een doorzoeking onder leiding van de OvJ of RC in beslag zijn genomen. Overigens kunnen deze functionarissen wel tevens opdracht aan de politie geven om inbeslaggenomen *devices* te onderzoeken op grond van artt. 104 jo. 110 Sv. Tevens kan de vastlegging van gegevens opgeslagen op een in de woning aanwezig device plaatshebben, zie artt. 110 jo. 125i Sv.

[477] Zie voor een overzicht van de juridische argumenten pro en contra: E. Gritter, *Opsporing in de digitale wereld: het onderzoek van in beslag genomen gegevensdragers*, Delikt en Delinquent, (2016/43) 2016, afl 7, p. 493 e.v., en R. van den Bosch, *Privacy in het digitale tijdperk: over de rechtmatigheid van het onderzoek aan een in beslag genomen smartphone*, Tijdschrift Praktijkwijzer Strafrecht (TPWS), 2016, aflevering 17, 2016/48; Voor een meer algemeen beeld van de uitvoeringspraktijk mbt de inbeslagneming van gegevens: zie P.A.M. Mevis, J.H.J. Verbaan en B.A. Salverda, *Onderzoek aan in beslag genomen elektronische gegevensdragers en geautomatiseerde werken ten behoeve van de opsporing en vervolging van strafbare feiten*, 2016, p. 6.

In een aantal gelijksoortige arresten oordeelde de Hoge Raad in april 2017 echter:

> "*2.6. Voor het doen van onderzoek door een opsporingsambtenaar aan inbeslaggenomen elektronische gegevensdragers en geautomatiseerde werken teneinde de beschikking te krijgen over daarin opgeslagen of beschikbare gegevens vereist de wet geen voorafgaande rechterlijke toetsing of tussenkomst van de officier van justitie. Indien de met het onderzoek samenhangende inbreuk op de persoonlijke levenssfeer als beperkt kan worden beschouwd, biedt de algemene bevoegdheid van opsporingsambtenaren, neergelegd in art. 94 Sv, in verbinding met art. 95 en 96 Sv, daarvoor voldoende legitimatie. Dit zal het geval kunnen zijn indien het onderzoek slechts bestaat uit het raadplegen van een gering aantal bepaalde op de elektronische gegevensdrager of in het geautomatiseerde werk opgeslagen of beschikbare gegevens. Indien dat onderzoek zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijk leven van de gebruiker van de gegevensdrager of het geautomatiseerde werk, kan dat onderzoek jegens hem onrechtmatig zijn. Daarvan zal in het bijzonder sprake kunnen zijn wanneer het gaat om onderzoek van alle in de elektronische gegevensdrager of het geautomatiseerde werk opgeslagen of beschikbare gegevens met gebruikmaking van technische hulpmiddelen*."[478]

Daarbij overwoog de Hoge Raad tevens:

> "*2.8. Mede gelet op het vooralsnog ontbreken van een daarop toegesneden wettelijke regeling verdient het volgende opmerking. De bevoegdheid tot inbeslagneming van voorwerpen en de daarin besloten liggende bevoegdheid tot het verrichten van onderzoek aan die voorwerpen kunnen op grond van art. 95 en 96 Sv ook worden uitgeoefend door de op grond van art. 148 Sv met het gezag over de opsporing belaste officier van justitie, nu deze blijkens art. 141, aanhef en onder a, Sv met opsporing is belast. Voorts kunnen die bevoegdheden op grond van art. 104, eerste lid, Sv worden uitgeoefend door de rechter-commissaris. De hier genoemde wettelijke bepalingen bieden tevens de grondslag voor het verrichten van onderzoek aan inbeslaggenomen voorwerpen door de officier van justitie respectievelijk de rechter-commissaris, indien de inbeslagneming is geschied door een opsporingsambtenaar.*
> *In zo een geval vormen de genoemde wettelijke bepalingen een toereikende grondslag voor onderzoek aan inbeslaggenomen voorwerpen - waaronder elektronische gegevensdragers en geautomatiseerde werken - dat een meer dan beperkte inbreuk op de persoonlijke levenssfeer meebrengt. Daarbij valt - in het licht van art. 8 EVRM - aan onderzoek door de rechter-commissaris in het bijzonder te denken in gevallen waarin op voorhand is te voorzien dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn*."

Met deze zogenaamde 'Smartphone-arresten' is meer duidelijkheid gekomen over het beoordelingskader dat voor het onderzoek aan in beslag genomen gegevensdragers door de rechter moet worden gehanteerd. Uit de voorgaande overwegingen van de Hoge Raad kan worden afgeleid dat de zelfstandige bevoegdheid van een verbalisant tot inbeslagname van een *devices* zoals een smartphone[479] een toereikende grondslag biedt voor een onderzoek naar de zich daarop bevindende gegevens, indien de met het onderzoek samenhangende inbreuk op de persoonlijke levenssfeer als beperkt kan worden beschouwd. Tevens kan worden afgeleid dat het bij die beoordeling gaat om de kennisname van de op het apparaaat opgeslagen of beschikbare gegevens.[480]

---

[478] HR 4-4-2017, ECLI:NL:HR:2017:588; HR 4-4-2017, ECLI:NL:HR:2017:592; HR 4-4-2017, ECLI:NL:HR:2017:584, *NJ* 2017,230 m.nt. T. Kooijmans.

[479] Hoewel de hiervoor weergegeven arresten veelal worden aangeduid als de "smartphone"-arresten blijken deze een breder bereik te hebben dan alleen smartphones, en betrekking te hebben op alle gegevensdragers en geautomatiseerde werken die zelfstandig door een opsporingsambtenaar in beslag kunnen worden genomen, zoals ook iPads, notebooks, gameconsoles, laptops en desktopcomputers (pc's).

[480] Immers ontstaat slechts dan een beeld, zie ook specifiek r.o. 2.6 van het bovengenoemde arrest: 'indien het onderzoek slechts bestaat uit het *raadplegen…*'.

Wordt er vervolgens echter een uitvoerig onderzoek ingesteld naar de inhoud van een inbeslaggenomen gegevensdrager[481], hetgeen in kinderpornozaken gebruikelijk is, dan zal daarvoor eerst een bevel van de officier van justitie moeten worden verkregen. In die gevallen waarin *op voorhand* te voorzien is dat de inbreuk op de persoonlijke levenssfeer zeer ingrijpend zal zijn is een machtiging van de rechter-commissaris vereist.[482] Ontbreekt een dergelijk bevel, waar zulks wel was vereist, dan levert dit een vormverzuim op als bedoeld in art. 359a Sv.[483]

Na de 'Smartphone-arresten'[484] volgden een aantal arresten van de Hoge Raad waarin het in die zaken (handmatig) uitgevoerde onderzoek niet meer dan een geringe inbreuk op de persoonlijke levenssfeer had opgeleverd. Deze arresten vormen daarmee een verdere verduidelijking van hetgeen de Hoge Raad verstaat onder een onderzoek waarvoor de bevoegdheid tot inbeslagname *sec* voldoende legitimatie biedt.[485] Zo heeft de Hoge Raad in het arrest van 10 juli 2018 het oordeel van het hof, waarin besloten lag dat het (kennelijk handmatig) gericht bekijken van foto's in de fotogalerij van de smartphone van de verdachte niet een meer dan beperkte inbreuk op de persoonlijke levenssfeer oplevert, in stand gelaten.[486]

De Hoge Raad heeft ook een aantal arresten gewezen in zaken waarin met een technisch hulpmiddel *alle gegevens* op de smartphone zijn onderzocht. Deze wijze van onderzoek is, zoals hiervoor reeds opgemerkt, in kinderpornozaken gebruikelijk. Er dient door de rechter in een voorkomend geval te worden vastgesteld of door *het onderzoek aan de hand van die gegevens* (de één-op-één kopie van een harde schijf of een logisch rapport van alle gegevens op een smartphone) een meer dan beperkte inbreuk op de persoonlijke levenssfeer is gemaakt.[487] Een machtiging van de rechter-commissaris is - indien zulks op voorhand te verwachten was - vereist. In de casus die leidde tot het arrest van de Hoge Raad van

---

[481] Daarmee is onzes inziens gelijk te stellen: onderzoek naar een (forensische) kopie of image van de inhoud van een *device*.
[482] Het moet daarbij gaan om meer dan bijvoorbeeld het enkele uitlezen van de een sim- of datakaart van een smartphone (vgl. r.o. 2.7.2. van HR 4-4-2017, ECLI:NL:HR:2017:588). De Hoge Raad geeft ook aan dat hierbij in het bijzonder te denken is aan gevallen waarin alle opgeslagen of beschikbare gegevens op de smartphone met gebruikmaking van een technische hulpmiddel en het onderzoek naar die gegevens zo verstrekkend is dat een min of meer compleet beeld van bepaalde aspecten van het persoonlijk leven van de gebruiker wordt verkregen.
[483] Aldus ook HR 4-4-2017, ECLI:NL:HR:2017:588, r.o. 2.7.2.
[484] Voor nadere beschouwingen verwijzen wij naar het artikel van J.W. van den Hurk & S.J. de Vries, "Onderzoek van gegevens(dragers)", *NJB* 2020/2806, alsmede naar Van den Hurk en De Vries Onderzoek aan digitale-gegevensdragers. Een technische en juridische verkenning (PWS nr. 15) 2021.
[485] Zie HR 14-11- 2017, ECLI:NL:HR:2017:2869 (smartphone is handmatig onderzocht, waarbij de verbalisant verscheidene gemiste telefoontjes, berichtjes en whatsappjes heeft gevonden. AG Harteveld stelt dat er slechts een gering aantal gegevens is geraadpleegd en geeft aan dat dit wijst in de richting van een beperkte inbreuk op de persoonlijke levenssfeer. HR: art. 81 RO); HR 23-1-2018, ECLI:NL:HR:2018:71 (niet-gelockte smartphone van een verdachte is handmatig doorzocht, waarbij door de verbalisant geklikt is op een app met de naam 'video' en vervolgens verschillende video's gemaakt met de smartphone door de verbalisant zijn bekeken. Eén van deze video's is tot het bewijs gebezigd. AG Bleichrodt kenmerkt dit als "beperkt onderzoek", waarvoor geen bevel OvJ of machtiging RC noodzakelijk was. HR: art. 81 RO);
[486] HR 10-7-2018, ECLI:NL:HR:2018:1121. Uit de inhoud van het arrest van het hof wordt niet duidelijk wat het onderzoek van de verbalisant precies heeft ingehouden. De verdediging heeft dit ook in het midden gelaten en gesteld dat het bekijken van alle foto's in de fotogalerij reeds een meer dan beperkte inbreuk op de persoonlijke levenssfeer oplevert. Het blijft daarom de vraag of – indien de verdediging meer concreet had aangegeven hoeveel foto's waren bekeken en wat daarop te zien was, met andere woorden waarin de inbreuk op de persoonlijke levenssfeer door het verrichte onderzoek precies was gelegen – de Hoge Raad de motivering van het hof ook toereikend had geacht.
[487] HR 18-12-2018, ECLI:NL:HR:2018:2323, *NJ* 2019,84 m. nt. T. Kooijmans.

9 juli 2019 is – naar het zich laat aanzien – een forensische (logische) kopie gemaakt van alle bestanden op de smartphone en de daarin aanwezige SD-kaart en is de kopie later op meerdere momenten nader onderzocht. Het oordeel van het hof, dat art. 94 Sv een toereikende wettelijke grondslag vormt voor het door de opsporingsambtenaren verrichte nadere onderzoek aan de inbeslaggenomen smartphone en de daarbij behorende SD-kaart van de verdachte, aangezien daarmee niet meer dan een beperkte inbreuk op de persoonlijke levenssfeer is gemaakt, is onvoldoende gemotiveerd. De Hoge Raad neemt daarbij in aanmerking dat door het hof in haar overwegingen is opgemerkt dat de politie wel selectief is geweest met het onderzoek , maar vervolgens niet heeft vastgesteld aan de hand waarvan en met het oog waarop een selectie is gemaakt, terwijl het onderzoek blijkbaar tenminste alle opgeslagen foto's en films omvatte.[488]

Indien door de rechter wordt vastgesteld dat voorafgaande toestemming door de officier van justitie of de rechter-commissaris was vereist maar niettemin ontbreekt, en daarmee dat sprake is van een onherstelbaar vormverzuim, dient de rechter daaraan één van de in art. 359a Sv genoemde rechtsgevolgen te verbinden.[489]

6.1.2.3 (Biometrische) ontgrendeling van devices

Naast de gebruikelijke beveiliging door middel van een wachtwoord of PIN-code komt de laatste jaren beveiliging van een device door middel van biometrische kenmerken van de gebruiker steeds meer in zwang. Het betreft met name apparaten die regelmatig zullen worden ontgrendeld, zoals smartphones en tablets, maar ook bij laptopcomputers[490] wordt deze wijze van ontgrendeling steeds vaker aangeboden. Veelgebruikte biometrische kenmerken zijn de vingerafdruk, gezichtsherkenning (door Apple 'Face ID' genaamd) en irisscan.

Sinds 2018 is een aantal vonnissen[491] gewezen die betrekking hebben op het door verdachten (al dan niet met toepassing van gepast geweld) doen ontgrendelen van smartphones met gebruik van biometrische kenmerken (in de praktijk steeds vingerafdrukken). Voor een goed begrip van de problematiek is het van belang om vast te stellen dat het zogenaamde 'decryptiebevel' zoals opgenomen in art. 125k Sv blijkens het derde lid van die bepaling niet gericht kan worden tot de verdachte.[492]

---

[488] HR 9-7-2019, ECLI:NL:HR:2019:1079.

[489] De rechter heeft kort gezegd drie opties, namelijk de enkele constatering van het verzuim, bewijsuitsluiting en in uitzonderlijke gevallen de niet-ontvankelijkheid van het Openbaar Ministerie uitspreken. De lat voor bewijsuitsluiting ligt reeds hoog en er is voor de rechter veel ruimte om te volstaan met de constatering van het vormverzuim. In HR 18-2-2020, ECLI:NL:HR:2020:123, *NJ* 2020/95 (vervolg op een van de Smartphone-arresten; HR 4-4- 2017, ECLI:NL:HR:2017:588), heeft de Hoge Raad geoordeeld dat de enkele omstandigheid dat een 'meer dan beperkte inbreuk op de persoonlijke levenssfeer van de verdachte is gemaakt' nog niet betekent dat bewijsuitsluiting noodzakelijk is als middel om toekomstige vergelijkbare vormverzuimen te voorkomen (zie voor de voorafgaande conclusie van AG Spronken van 5-11-2019 (contrair); ECLI:NL:PHR:2019:1121). Eerder heeft de Hoge Raad in HR 1-12-2020, ECLI:NL:HR:2020:1889, *NJ* 2021/169, de precieze formulering van enkele maatstaven in relatie tot art. 359a Sv genuanceerd en/of bijgesteld, waaronder de toepassingsvoorwaarden voor de rechtsgevolgen strafvermindering, bewijsuitsluiting en niet-ontvankelijkverklaring van het Openbaar Ministerie in de vervolging.

[490] Gebruikers van computers die draaien op het Windows 10-besturingssysteem kunnen Windows Hello activeren als de betreffende computer beschikt over bijvoorbeeld een webcam of een vingerafdrukscanner.

[491] Zie RB Rotterdam 28-1-2021, ECLI:NL:RBROT:2021:547, RB Den Haag 12-3-18 ECLI:NL:RBDHA:2018:2983, RB Rotterdam 14-12-18 ECLI:NL:RBROT:2018:10283, RB Noord-Holland 14-12-18 ECLI:NL:RBNHO:2018:11578 en in het bijzonder vanwege de meer uitvoerige overwegingen op dit punt RB Noord-Holland 28-2-19, ECLI:NL:RBNHO:2019:1568.

[492] Curieus is dat de wettekst er niet aan in de weg staat dat het bevel tot het ontsleutelen van gegevens in een op zichzelf niet-beveiligd of met toepassing van het eerste lid ontgrendeld device wel tot de verdachte wordt gericht. Dit is niet slechts een academische kwestie, denk bijvoorbeeld aan de situatie waarin een smartphone in

Uit de aangehaalde vonnissen valt op te maken dat het toepassen van fysiek geweld – of het daarmee dreigen – om een device langs biometrische weg te ontgrendelen, geoorloofd is zolang aan de eisen van proportionaliteit en subsidiariteit wordt voldaan. Kernelement in de gemaakte afweging vormt het *nemo tenetur*-beginsel. In het vonnis van de rechtbank Noord-Holland lezen we daaromtrent het volgende:

> *"Anders dan de situatie waarin verdachte wordt gedwongen de toegangscode van zijn telefoon te geven, hetgeen een verklaring van verdachte vereist, maakt het plaatsen van de duim van verdachte op zijn iPhone naar het oordeel van de rechtbank geen inbreuk op het nemo tenetur-beginsel. Het betreft hier namelijk het dulden van een onderzoeksmaatregel die geen actieve medewerking van verdachte vereist. Daar komt bij dat de vingerafdruk met een zeer geringe mate van dwang is verkregen. Dat met het plaatsen van de duim van verdachte op de iPhone toegang wordt verkregen tot mogelijk wilsafhankelijke en voor hem belastende gegevens, maakt dit naar het oordeel van de rechtbank niet anders."*

De mate van toegepast geweld wordt in diverse vonnissen afgezet tegen de ernst van het misdrijf waarop de verdenking ziet. Hoewel dit op het eerste gezicht begrijpelijk voorkomt, is aan deze benadering het gevaar verbonden dat een grote(re) mate van verzet door de verdachte ertoe kan leiden dat de mate van geweld die nodig is om de biometrische ontgrendeling te bewerkstelligen niet meer in redelijke verhouding zou zijn met de ernst van het feit waarop de verdenking ziet. Dat lijkt ons niet de bedoeling; veeleer zou sprake moeten zijn van een afweging van enerzijds het geweld dat benodigd zou zijn om een verdachte die zich louter passief verzet een device biometrisch te laten ontgrendelen en anderzijds de ernst van het feit waarop de verdenking ziet.

De factor van spoedeisendheid van het verkrijgen van inzicht in de gegevens op een device speelt onzes inziens een ondergeschikte rol. Het ontgrendelen van een modern device langs 'niet-natuurlijke weg', met andere woorden door het kraken van de code ervan, is een proces dat – indien het al succesvol verloopt – doorgaans veel tijd vergt.[493] Er is dus geen sprake van een afweging tussen het direct of binnen enkele dagen of weken over de gegevens kunnen beschikken maar van een afweging tussen het direct over de gegevens kunnen beschikken of op een moment dat deze naar verwachting minder relevant zullen zijn geworden.

De wetgever ontwikkelt plannen om voor deze materie in de modernisering van het Wetboek van Strafvordering een regeling op te nemen, welke als volgt zou komen te luiden[494]:

---

ontgrendelde toestand in handen van een opsporingsambtenaar komt. Deze opsporingsambtenaar zou de verdachte dan kunnen bevelen tot het ontgrendelen van bijvoorbeeld zijn of haar Dropbox-app door middel van het houden van een vinger op de vingerafdrukscanner. In onze visie is dit een niet door wetgever bedoelde ongerijmdheid die niet zou moeten worden geaccepteerd. Zie hieromtrent ook Vellinga-Schootstra, Handboek strafzaken onder 14.13.3. Het Wetsvoorstel Vaststelling nieuw Wetboek van Strafvordering geeft in art. 2.7.43 Sv (nieuw) twee uitbreidingen van het toepassingsbereik van het bevel toegangsverschaffing, namelijk de hiervoor besproken constructie waarin de officier van justitie het bevel richt tot een opsporingsambtenaar die vervolgens de verdachte een bevel geeft om mee te werken aan de ontgrendeling van het apparaat en de uitbreiding van gevallen waarin het bevel kan worden gegeven tot staandehouding en betreden ter aanhouding.

[493] RB Overijssel, 17-3- 2021, ECLI:NL:RBOVE:2021:1523 Klaagschrift tegen inbeslagneming telefoon gegrond. De rechtbank weegt in dit verband mee dat klager heeft verklaard dat hij de toegangscode van de telefoon niet aan de politie heeft verstrekt zodat anders dan door *destructief onderzoek* aan de telefoon geen gegevens beschikbaar kunnen komen uit de telefoon. De mogelijke toepassing van de niet-destructieve onderzoeksmethode *'brute-forcing'* lijkt hier over het hoofd te worden gezien.

[494] Wetsvoorstel Vaststelling van het nieuwe Wetboek van Strafvordering (versie: 20 maart 2023), art. 2.7.43 (p. 98/260 dig.).

> *Art. 2.7.43 lid 2*
> *In geval van biometrische beveiliging of versleuteling (…) kan de officier van justitie bevelen dat de opsporingsambtenaar deze beveiliging of versleuteling ongedaan maakt. De opsporingsambtenaar kan ter uitvoering van dat bevel tegen de wil van degene van wie redelijkerwijs kan worden vermoed dat hij deze beveiliging of versleuteling ongedaan kan maken, de maatregelen treffen die daartoe redelijkerwijs noodzakelijk zijn. (…).*

Voor de dogmatische verantwoording van dit voorstel verwijzen wij naar hetgeen door de Commissie modernisering opsporingsonderzoek in het digitale tijdperk in haar rapport "Regulering van opsporingsbevoegdheden in een digitale omgeving" (verder: 'de Cie. Koops' resp. 'het rapport Koops') wordt geschreven:

> *"(…) constateert de commissie dat er een belangrijk verschil bestaat tussen het meewerken in de vorm van het geven van een wachtwoord en meewerken via biometrische toegangsverschaffing. Dit verschil ligt in de kern van het Saunders-criterium dat een leidende rol speelt in de interpretatie van het nemo teneturbeginsel. (…) Het criterium is daarbij niet per se, of niet alleen, of iets onafhankelijk van de wil van de verdachte bestaat, maar vooral ook of iets onafhankelijk van de wil van de verdachte kan worden verkregen."*[495]

Als een reactie op het advies van de Cie. Koops is een interessante discussie tot stand gekomen in het Nederlands Juristenblad, waar wij kortheidshalve naar verwijzen voor het verkrijgen van een verdiepend inzicht in de problematiek.[496]

Inmiddels is op 1 oktober 2022 in het kader van de Innovatiewet Strafvordering art. 558 Sv in werking getreden, dat luidt:

> *In geval een inbeslaggenomen geautomatiseerd werk biometrisch is beveiligd of de gegevens biometrisch zijn versleuteld in de vorm van een vingerafdruk of een opname van de iris of het gezicht, kan de officier van justitie bevelen dat de opsporingsambtenaar deze beveiliging of versleuteling ongedaan maakt. De opsporingsambtenaar kan ter uitvoering van dat bevel tegen de wil van wie redelijkerwijs kan worden vermoed dat hij deze beveiliging of versleuteling ongedaan kan maken, de maatregelen treffen die daartoe redelijkerwijs noodzakelijk zijn.*

Naar verwachting is hiermee de dogmatische discussie rond dit onderwerp in belangrijke mate afgerond. In de rechtszaal zal het voornamelijk gaan over de vraag of de ter uitvoering van het bevel getroffen maatregelen redelijkerwijs noodzakelijk waren, waarbij uit een oogpunt van rechtsontwikkeling met name interessant zal zijn in hoeverre tegenwerking door de betrokkene (let wel: dat kan ook een ander dan een verdachte zijn) ertoe kan leiden dat geen sprake meer is van redelijkerwijs noodzakelijke maatregelen.

---

[495] Blz. 105.
[496] A. Bood, "Geef ze een vinger… Gedwongen ontgrendeling van een smartphone en het nemo tenetur-beginsel", NJB 2018/1880, blz. 2744-2748, L. Stevens, "Gedwongen biometrische toegangsverschaffing is niet in strijd met nemo tenetur", NJB 2019/315, blz. 400-403, M. Egberts & W. Ferdinandusse, "Reactie op Alex Bood", NJB 2019/316, blz. 404 en D. van Toor, "Het gedwongen ontgrendelen van een smartphone in het licht van het nemo-teneturbeginsel Reactie op Boods 'Geef ze een vinger'", NJB 2018/317, blz. 405-409.

Ons bereiken geluiden dat steeds meer verdachten in antwoord op de hiervoor omschreven ontwikkeling afzien van het gemak van biometrische ontgrendeling en terugvallen op het gebruik van vergrendelingscodes. Als reactie daarop zien we dat opsporingsdiensten zich inspannen om *devices* in ontgrendelde toestand in beslag te kunnen nemen, bijvoorbeeld door de verdachte op te bellen op het moment van de inbeslagneming.[497]

6.2. Behandeling en beoordeling van (mogelijk) bewijsmateriaal

6.2.1. Digitaal forensisch onderzoek in kinderpornozaken

Ingevolge de standaard werkwijze bij de politie en NFI dient zo veel mogelijk[498] een zogenaamde forensische kopie te worden gemaakt van de gegevens op een inbeslaggenomen gegevensdrager. Een dergelijke kopie komt *bit-for-bit* overeen met hetgeen op de gegevensdrager stond. Om te voorkomen dat er tijdens het kopiëren toch wijzigingen in het digitale materiaal optreden wordt er bij het kopieerproces ook een zogenaamde *write-blocker* gebruikt, zodat er alleen vanaf de gegevensdrager kan worden gelezen en er geen nieuwe gegevens naartoe kunnen worden geschreven. Om verder te controleren dat er bij het kopiëren geen wijzigingen zijn opgetreden worden zowel de brongegevensdrager als de kopie "gehasht", dat wil zeggen dat er met behulp van een algoritme een waarde wordt berekend over alle gegevens op de betreffende gegevensdragers. Als de forensische kopie inderdaad een exacte kopie is van het origineel, zullen de berekende hashwaarden overeenstemmen. Is er sprake van ook maar het geringste verschil tussen de bron en de kopie, dan zullen deze hashwaarden zeer significant verschillen.[499]

De reden dat er forensische kopieën worden gemaakt is dat er bij forensisch digitaal onderzoek een reëel risico bestaat dat door de gebruikte onderzoekstechnieken mogelijk wijzigingen optreden in het onderzochte digitale materiaal. Door altijd het origineel te bewaren kan desgewenst achteraf altijd worden nagegaan in hoeverre (en welk) materiaal inderdaad aanwezig was op de originele gegevensdrager, dan wel een mogelijk bijproduct is van het verrichte onderzoek. Hoewel de (aanwezigheid van de) oorspronkelijke harde schijf en de forensische kopie daarvan dus van (groot) belang kan zijn voor bijvoorbeeld het verrichten van nader onderzoek, maakt c.q. maken deze als regel geen onderdeel uit van het processtukken.[500]

De forensische kopie wordt vervolgens nader inhoudelijk onderzocht. Mede gezien de grote hoeveelheid gegevens die tegenwoordig op gegevensdragers wordt aangetroffen, wordt daarbij gebruik gemaakt van gespecialiseerde forensische software.[501] Met deze software kan

---

[497] RB Zeeland-West Brabant 17-5-19, ECLI:NL:RBZWB:2019:2195.

[498] Met name bij smartphones en dergelijke *devices* kan het zijn dat het technisch niet mogelijk is om een forensische kopie te maken. In dergelijke gevallen wordt een logische kopie gemaakt, die eveneens voor forensisch onderzoek geschikt is. Zie uitgebreider "Technische Toelichting, terug naar de bestanden" van het Nederlands Forensisch Instituut, 24 juni 2019, p. 16.

[499] Het valt op dat in het strafdossier nogal eens wordt volstaan met de vermelding van de berekende hashwaarde over de één-op-één kopie van de in beslag genomen gegevensdrager, welke door de digitaal rechercheur is onderzocht. De berekende hashwaarde over de bron ontbreekt dikwijls, waardoor bij bestudering van het strafdossier niet gecontroleerd kan worden of de waarden overeenkomen. Vgl. over een-op-een kopieën (Engels: images) van gegevensdragers en over 'hashes': "Technische Toelichting, terug naar de bestanden" van het Nederlands Forensisch Instituut, 24 juni 2019, p. 43-44 respectievelijk p. 18-19.

[500] Zie in dit verband ook HR 5-5-2001, ECLI:NL:HR:2001:AB1517 (oordeel Hof dat harde schijf geen onderdeel uitmaakte van processtukken juist). Zie over hoe dit uitgangspunt zich verhoudt tot het recht op tegenonderzoek/contra-expertise: hierna onder 7.5.

[501] Er wordt gebruik gemaakt van forensische *tools* van diverse leveranciers geschikt voor onderzoek aan de gegevens uit een één-op-één kopie of voor onderzoek aan gegevens op mobiele telefoons, waaronder

tegelijkertijd onderzoek worden verricht naar de aanwezigheid van kinderpornografisch materiaal op meerdere gegevensdragers . Over het algemeen is deze software in staat ook materiaal te vinden, dat voor de oorspronkelijke gebruiker niet meer benaderbaar was.[502]

6.2.2. Bewijswaarde van een match met Landelijke Database Kinderpornografie
De mogelijk vanuit de optiek van art. 240b Sr relevante inhoud van inbeslaggenomen gegevensdragers wordt ook vergeleken met de inhoud van de Landelijke Database Kinderpornografie. In deze Landelijke Database bevinden zich afbeeldingen (begin 2019 ruim 1,4 miljoen unieke afbeeldingen) die eerder zijn aangemerkt als kinderpornografisch.[503]
De precieze werkwijze met betrekking tot de vaststelling van het kinderpornografisch karakter van de afbeeldingen is voor zover bekend niet opgenomen in enig beleidsstuk.
Ook hierbij wordt weer, maar dan op bestands/afbeeldingsniveau, gebruik gemaakt van de techniek van het "hashen". Komt de hashwaarde van een bestand/digitale afbeelding op een gegevensdrager overeen met die van een bestand/digitale afbeelding uit de Landelijke database, dan kan met een extreem hoge mate van waarschijnlijkheid worden aangenomen dat het het-/dezelfde (kinderpornografische) bestand/afbeelding betreft.[504]

Technisch lemma: "hashen" en hashwaarde[505]

Hashen
Een digitaal bestand bestaat uit een reeks nullen en enen ("bits"). Het aantal en de posities van deze nullen en enen bepalen de inhoud van het bestand en zijn daarmee kenmerkend voor dat bestand. Door gebruikmaking van een zogenaamd hash-algoritme[506] kunnen de specifieke nullen en enen van een bepaald bestand zoals een afbeelding of video (of van een verzameling bestanden of zelfs een hele gegevensdrager) worden omgezet in een veel eenvoudiger en compactere (hexadecimale)[507] notatie. Het omzetten is éénrichtingsverkeer: de notatie kan niet meer worden omgerekend naar hetgeen is ingevoerd.

Het berekenen van een hashwaarde kan worden gebruikt om de integriteit te controleren of voor bestandsvergelijking. In processen-verbaal in kinderpornozaken komt men veelal gebruik van de hash-algoritmen MD5 (met een lengte van 128 bits) en SHA-1 (met een lengte van 160 bits).

---

bijvoorbeeld Magnet (waaronder Internet Evidence Finder en AXIOM), OpenText (EnCase), MSAB (XRY) en Cellebrite (UFED).
[502] Dit geldt met name voor materiaal in de zogenaamde *unallocated clusters* en in de *temporary internet files*; zie hierover verder hiervoor onder 4.2.1.5.
[503] Kamerbrief aanpak online seksueel kindermisbruik en bestuursrechtelijke handhaving, 3 juli 2019.
[504] Zie hierover verder hierna het technisch lemma: "hashen". In dit verband weinig gelukkig derhalve: RB Midden-Nederland 9-9-2013, ECLI:NL:RBMNE:2013:3688 (10 films; hashwaarde daarvan komt overeen met die van bestanden in de Landelijke Databank. "*De rechtbank is evenwel niet bekend met de bijzonderheden (aan de hand waarvan de betrouwbaarheid kan worden vastgesteld) van een vergelijking aan de hand van hashwaarden. Dit is te meer relevant omdat uit het proces-verbaal van verbalisant [verbalisant] niet volgt dat wanneer hashwaarden met elkaar overeenkomen dit ook zonder meer inhoudt dat het om identieke bestanden gaat. Daarom niet bewezen dat de 10 films ook een kinderpornografische inhoud hadden*"); hashwaarde als bewijs van kinderpornografisch karakter wel geaccepteerd in o.m. RB Utrecht 31-5-2010, ECLI:NL:RBUTR:2010:BN0067.
[505] Het navolgende is mede ontleend aan de NFI Vakbijlage forensisch gebruik van bestandskenmerken en bijbehorende hashalgoritmen, februari 2018.
[506] Een algoritme is een reeks instructies die vanuit een gegeven begintoestand aangeven welke (wiskundige en/of logische) stappen moeten worden uitgevoerd om tot een bepaald resultaat te geraken. Een algoritme kan door een computer automatisch uitgevoerd worden.
[507] Hexadecimaal betekent letterlijk 16-tallig. Het is een talstelsel waarbij niet, zoals gebruikelijk, met tien cijfers wordt gewerkt, maar met zestien cijfers. De cijfers 0 t/m 9 worden daarom uitgebreid met 'A' (=10) t/m 'F' (=16), ook wel 'a' t/m 'f'. In deze context zijn dat dus ook cijfers, geen letters. In de computerwereld wordt de hexadecimale notatie van getallen veel gebruikt, omdat deze manier van representeren goed aansluit bij de binaire representatie in de computer. Bron: Wikipedia. Een hexadecimaal getal bestaande uit twee posities volstaat om de waarde van een byte (8 bits) weer te geven.

De veiligheidsgarantie die ze bieden – de onwaarschijnlijkheid dat twee verschillende ingevoerde gegevens dezelfde notatie krijgen, zie hieronder – is nog steeds extreem hoog. Het NFI is in 2010 overgestapt op het nog veiligere SHA-256 algoritme. Omdat door de politie nog steeds MD5 en SHA-1 hashwaarden worden aangeleverd gebruikt het NFI ook deze algoritmes nog. Anders zou het NFI deze eerder gegenereerde hashwaarden namelijk, bijvoorbeeld na het maken van een kopie, niet meer kunnen verifiëren.

De algoritmes zijn zodanig geconstrueerd dat zelfs de allerkleinste verandering in bijvoorbeeld een bestand al een geheel ander omzettingsresultaat tot gevolg heeft. Een dergelijk omzettingsresultaat wordt een hash genoemd, maar ook wel aangeduid met de termen hashwaarde, hashcode of hashstring, of meer algemeen met de term: bestandskenmerk.

Een voorbeeld waarin twee vrijwel gelijke digitale teksten met behulp van de MD5-algoritme zijn omgezet:
Korpschef Nationale Politie wil politie nog dit jaar 'diverser' maken.
MD5 hash = da4d227eff91aa80cd57c71ced81c5e2.
Korpschef Nationale Politie wil politie nog dit jaar diverser maken.
MD5 hash = c3d0a318cd0e9037836be434244b29ad.

Een foto- of videobestand dat 100% identiek is aan een ander foto- of videobestand zal ook 100% dezelfde hash(waarde) hebben als dat andere bestand. Ook over foto- of videobestanden die door kinderpornospecialisten beoordeeld zijn kan dus zo'n hashwaarde gegenereerd worden. Wanneer alle hashwaarden van dergelijke reeds als kinderpornografisch gekwalificeerde afbeeldingen in een database worden gezet, dan krijg je feitelijk een grote verzameling van hexadecimale reeksen. Worden vervolgens bij een nieuw politieonderzoek gegevensdragers in beslag genomen, dan worden over de daarop aanwezige bestanden ook hashwaarden berekend. Daarna worden deze laatste hashwaarden met behulp van speciaal daarvoor ontwikkelde software vergeleken met de hashwaarden die zich al in de database bevinden. Aldus kan zeer snel, en grotendeels geautomatiseerd, worden vastgesteld of zich reeds eerder als kinderpornografisch gekwalificeerde afbeeldingen tussen de nieuwe gegevens bevinden.

Hashen wordt ook veel gebruikt als methode om te controleren of een bestand, of een verzameling bestanden na het maken van een (forensische) kopie inhoudelijk ongewijzigd is gebleven. Daartoe wordt alvorens een gegevensdrager door de politie of het NFI wordt benaderd of gekopieerd daarover eerst een hashwaarde berekend. Vervolgens wordt na het maken van de (forensische) kopie over de kopie wederom de hashwaarde berekend. Zijn deze hashwaarden identiek, dan kan ook worden aangenomen dat de gegevens op de kopie identiek zijn is aan de brongegevens.

Kans in de praktijk op een ander bestand met dezelfde hashwaarde/hetzelfde bestandskenmerk.
De kans dat twee verschillende bestanden bij toeval dezelfde hash(waarde) hebben (zo'n toevallige overeenkomst wordt ook wel een hashcollision genoemd) wordt extreem klein geacht. Het NFI heeft berekend dat de kans dat twee inhoudelijk verschillende bestanden bij toeval hetzelfde bestandkenmerk MD5, SHA-1 en/of SHA-256 hebben gelijk of kleiner is dan 1 op 2.9×10^{39} (dat is een 10 met 39 nullen). Deze laatste kans is extreem veel kleiner dan dat twee verschillende mensen bij toeval hetzelfde DNA-profiel hebben. Die kans is namelijk berekend op 1 op $1{,}6 \times 10^{10}$.

De uitkomsten van de totale vergelijking van de gegevens op de onderzochte gegevensdrager met die in de Landelijke Database kinderpornografie worden vervolgens als hulpmiddel gebruikt voor het schiften of prioriteren van het te beoordelen materiaal. Vervolgens wordt het relevant geachte materiaal beoordeeld door een (speciaal daarvoor opgeleide) verbalisant. De uitkomsten van dit selectie- en beoordelingsproces worden vervolgens neergelegd in een zogenaamde "collectiescan". In deze collectiescan werd (gewoonlijk per onderzochte gegevensdrager) een meer algemene, categorale beschrijving gegeven van hetgeen qua seksuele gedragingen op de aangetroffen afbeeldingen zichtbaar is. Idealiter behoren bij het proces-verbaal waar de collectiescan deel van uitmaakt ook bijlagen gevoegd waarin wordt aangegeven hoeveel kinderpornografische afbeeldingen zijn aangetroffen en of deze voor de gebruiker toegankelijk waren.

Deze werkwijze, die tot ongeveer 2015 zou worden gehanteerd[508], is in ieder geval juridisch problematisch, omdat uit de aldus opgestelde collectiescan normaliter zelf niet is te herleiden op welke concrete afbeelding(en) de beschrijving betrekking heeft en evenmin waar deze afbeelding op de gegevensdrager is gelokaliseerd. Op basis van vergelijking van meerdere dossiers met collectiescans rijst het vermoeden dat deze laatste gegevens echter wel (al dan niet tegelijk met het maken van de collectiescan) door de politie (kunnen) worden gegenereerd. Dat vermoeden wordt versterkt door de observatie van de oorspronkelijke auteur dat deze gegevens soms ook als bijlage met die collectiescan door de politie aan het OM zijn aangeleverd. Deze bijlagen werden echter vervolgens vrijwel nooit eigener beweging door het OM in het procesdossier gevoegd. Deze werkwijze droeg en draagt voor het Openbaar Ministerie risico's in zich, zowel in relatie tot de begrijpelijkheid van de tenlastelegging[509] als in relatie tot de bewezenverklaring.

Op basis van alleen de categorale uitkomsten als verwoord in de collectiescan zal immers in de regel niet zonder meer geconcludeerd kunnen worden dat die uitkomsten betrekking hebben op concrete, of op een concreet aantal, in de tenlastelegging aangeduide afbeeldingen.[510] De uitkomst van een collectiescan, indien de representativiteit daarvan tenminste voldoende aannemelijk is, zal in de regel overigens wel van aanzienlijk belang (kunnen) zijn voor de straftoemeting.[511]

Vanwege deze problematiek (en de daarmee samenhangende problematiek van de wijze van tenlasteleggen) hebben het OM en de Politie vanaf januari 2015 het standaard-proces-verbaal voor art. 240b-zaken aangepast.[512] In de aanpassing van januari 2015 is geïntroduceerd dat nu in de collectiescan de bestandsnamen worden opgenomen van de afbeeldingen die in de zogenaamde toonmap[513] worden opgenomen. Uitgangspunt lijkt daarbij te zijn dat de afbeeldingen die in de toonmap worden opgenomen afkomstig zijn uit de "*accessible*" bestanden, tenzij anders is geverbaliseerd.[514] Vanuit een oogpunt van rechterlijke beoordeling komt het echter voor dat telkenmale uit het strafdossier of het bredere onderzoek ter terechtzitting *expliciet* moet blijken dat een op een tenlastelegging aangeduide afbeelding al

[508] Blijkens mededelingen aan de oorspronkelijke auteur vanuit het Landelijk Parket zou deze werkwijze ondertussen aangepast zijn, en zouden bedoelde bijlagen in het vervolg dienen te worden opgenomen bij het proces-verbaal/het procesdossier.
[509] Zie hierover verder hierna onder 7.2.
[510] Zie bijvoorbeeld HR 1-7-2008, ECLI:NL:HR:2008:BC8645 (Het relaas van de verbalisant houdt in dat 299 van de onderzochte bestanden op de computer van de verdachte kinderporno bleken te bevatten. Dit relaas houdt echter niets in omtrent de wijze waarop de verbalisant is gekomen tot zijn bevindingen. Dat vrijwel alle kinderpornografische afbeeldingen bekend bleken in de Landelijke Database kinderpornografie maakt dat niet anders. Nu de verdachte wel heeft bekend kinderpornografie in bezit te hebben gehad, maar die erkenning geen betrekking heeft op alle 299 bewezenverklaarde afbeeldingen, is de bewezenverklaring ontoereikend gemotiveerd).
[511] In deze zin ook o.m. Reijntjes in zijn noot bij HR 24-6-2014, *NJ* 2014/339 (onder 7) en hierna onder 8.3.
[512] In oudere zaken kan derhalve de hiervoor genoemde problematiek nog onverkort actueel zijn.
[513] Zie hierover verder onder 7.4.1.
[514] Deze informatie is door het Landelijk Parket aan de oorspronkelijk auteur verstrekt. Deze kan niet uit openbare bronnen worden bevestigd.

dan niet *accessible* was[515], en dat niet kan worden aanvaard "dat de afbeelding in de toonmap zat, dus mag worden aangenomen deze *accessible* was".[516]

6.2.3. Bewijswaarde naam, format en plaats van aantreffen bestanden
Veelal wordt ook uit de aangetroffen hoeveelheid kinderpornografisch materiaal een beperkte selectie van 5 tot 25 afbeeldingen gemaakt die vervolgens gedetailleerder wordt beschreven in termen van bestandsnaam, locatie op de gegevensdrager en hetgeen op die afbeelding zichtbaar is. Soms wordt ook volstaan met het geven van laatstgenoemde inhoudelijke beschrijving in combinatie met het zogenaamde *filepath* (bijvoorbeeld: *C:\windows\[gebruiker]\afbeeldingen\jong.jpg*) waar de afbeelding is aangetroffen. Uit het *filepath* kan dan normaliter in samenhang met de rest van het dossier worden afgeleid op welke gegevensdrager en op welke locatie op die gegevensdrager het bestand is aangetroffen en wat de naam en format (in het voorbeeld: *jpg*[517]) van dat bestand was. Veelal kan uit het *filepath* – in ieder geval door een deskundige – ook worden afgeleid of dat bestand voor de gebruiker toegankelijk was of niet. Idealiter worden ook gegevens vermeld omtrent de datum van plaatsing van het bestand op de locatie, of omtrent data waarop het voor het laatst is benaderd en/of bewerkt.[518] Het is evident dat deze informatie relevant kan zijn voor de beantwoording van de (bewijs)vraag welke handelingen, en wanneer, met betrekking tot een bestand door een gebruiker/verdachte zijn verricht.[519]

Het valt echter op dat – met name bij processen-verbaal die niet afkomstig zijn van het Team Bestrijding Kinderporno en Kindersekstoerisme van de *Landelijke* Eenheid – de gegevensverstrekking over specifieke afbeeldingen, niet alleen in termen van locatie/filepath en toegankelijkheid[520], maar ook in termen van datering nogal eens ontbreekt, dan wel

---

[515] Onzes inziens zal daarbij tevens uit het dossier moeten zijn af te leiden *waarom* men tot die conclusie is gekomen; vermelding van de bestandslocatie (het "*filepath*") van de betreffende afbeelding(en) zal dan ook in veel gevallen zeer wenselijk zijn, aangezien daaruit veelal ook het al dan niet toegankelijk zijn van de afbeelding kan worden afgeleid (zie hierna onder 6.2.3.). *Opvallend:* RB Noord-Nederland 3-11-2022, ECLI:NL:RBNNE:2022:4093 (vaststellingen over toegankelijkheid van de op de (12) gegevensdragers van verdachte (o.a. harde schijven, een computer en 2 tablets) aangetroffen kinderpornografische bestanden, ontbreken).

[516] Vgl. in die zin RB Limburg 13-7-2021, ECLI:NL:RBLIM:2021:5591 ("*In totaal zijn op voornoemde gegevensdragers 63 foto's en 1 video aangetroffen, die op basis van de wet, de geldende jurisprudentie en de Aanwijzing Kinderpornografie van het College van procureurs-generaal, als kinderporno aan te merken zijn. De bestanden waren allemaal accessible (…). De 64 afbeeldingen zijn verwerkt in een collectiescan (…). Op de afbeeldingen zijn, kort samengevat, puberale meisjes (tussen de 11 en 17 jaar) te zien die poseren in erotisch getinte houdingen. (…)*." RB Overijssel 8-6-2021, ECLI:NL:RBOVE:2021:2291.

[517] *JPG* is een veel gebruikt format om afbeeldingen als foto's relatief compact ("gecomprimeerd") digitaal op te slaan. Bestanden waarbij dat format gebruikt is hebben de extensie: "*.jpg"*. Andere voor opslag van beeldmateriaal veelgebruikte formats c.q. extensies zijn "*.jpeg*" en "*.gif*", en voor video's onder meer "*.wmv*", ".mpeg" en ".avi".

[518] Zie over dergelijke metadata, waaronder de datum- en tijdgegevens betreffende (handelingen met) bestanden hierna onder 6.2.4.

[519] Zie voor het belang van datering van handelingen m.b.v. metadata o.m. RB Oost-Brabant 19-8-2015, ECLI:NL:RBOBR:2015:4938 (Uit het voormeld proces-verbaal Beschrijving kinderpornografisch materiaal volgt dat de onderzochte bestanden deels zijn weggeschreven onder het account van [verdachte] . Voorts blijkt uit dit proces-verbaal dat de bedoelde afbeeldingen met kinderporno op 24 augustus 2014 zijn geplaatst en voor het laatst zijn geopend op 22 oktober 2014, dus voordat [vader van slachtoffers] de laptop op 3 december 2014 uit het huis van verdachte heeft meegenomen. Gelet op het vorenstaande acht de rechtbank wettig en overtuigend bewezen dat verdachte op 3 december 2014 kinderporno in bezit heeft gehad, zoals hierna bewezenverklaard); en RB Utrecht 31-8-2011, ECLI:NL:RBUTR:2011:BR7588 (bezit kinderporno, voor het vaststellen van de pleegperiode gaat de rechtbank uit van de filedata van de bestanden).

[520] Zie bijv. RB Zeeland-West-Brabant 3-12-2021, ECLI:NL:RBZWB:2021:6175 ("*Vooropgesteld moet worden dat het niet duidelijk is op welke wijze het bestand op de telefoon terechtgekomen is. Er is namelijk in het dossier*

summier te noemen is. Dit kan ertoe leiden dat de strafrechter ten aanzien van bepaalde afbeeldingen of ten aanzien van gedragingen in een bepaalde tenlastegelegde periode tot vrijspraak moet besluiten.[521]

Los van de plaatsing in de tijd van gedragingen met bestanden kan het onder omstandigheden ook relevant zijn of bijvoorbeeld het *filepath* aanwijzingen bevat over hoe het bestand daar terecht gekomen is. Diverse communicatieprogramma's (zoals Windows Live Messenger) plaatsen bijvoorbeeld met chat-communicatie meegezonden afbeeldingen direct en zonder tussenkomst van de gebruiker[522] in een bepaalde map. Het *filepath* van deze map verwijst dan ook naar het gebruikte communicatie-programma. In het voorbeeld van Windows Live Messenger ziet zo'n filepath er dan bijvoorbeeld zo uit: C:\Users*[gebruikersnaam]*\AppData\Local\Temp\MessengerCache*afbeelding.jpg*. Een dergelijke map kan ook een toegankelijke map zijn. Uit het *enkele feit* dat afbeeldingen in een dergelijke bij een communicatie-applicatie behorende toegankelijke map zijn aangetroffen kan derhalve niet zonder meer worden afgeleid dat de gebruiker ook van de aanwezigheid van deze afbeeldingen op de hoogte was.[523] Daartoe zal derhalve in de regel nader onderzoek nodig zijn.

6.2.4. Bewijswaarde metadata

6.2.4.1. Gegevens over (afbeeldings)bestanden: datum- en tijdgegevens (tijdstempels)

Voor de strafrechtelijke beoordeling is tijdsinformatie een belangrijk gegeven. Gedragingen moeten bijvoorbeeld binnen een in de tenlastelegging genoemde periode kunnen worden gebracht. Daarnaast kan informatie over de vraag wanneer bestanden zijn gemaakt, geopend of bewerkt mede redengevend zijn voor het bewijs dat een verdachte wist van de aanwezigheid van een bepaald (afbeeldings)bestand. In dit kader is het van belang te weten dat nagenoeg alle computersystemen en -software extra gegevens over bijvoorbeeld een afbeelding opslaan. Deze extra informatie wordt metadata genoemd. Het kan daarbij gaan om datum- en tijdgegevens, maar bijvoorbeeld ook om gegevens omtrent het tijdstip waarop (en soms de plaats waar!) een bestand is gemaakt, bewerkt, geopend of geprint.

---

geen bewijs voorhanden waaruit blijkt dat verdachte een bewuste handeling heeft gepleegd om deze video op zijn telefoon op te slaan.").

[521] Zie bijv. RB Den Haag 12-12-2014, ECLI:NL:RBDHA:2014:15221 (verdachte heeft verklaard dat hij afbeeldingen van kinderpornografische aard heeft gedownload en vervolgens heeft opgeslagen in een map op zijn computer, waarna hij de afbeeldingen nog meerdere keren heeft bekeken. Verdachte heeft verklaard dat hij de afbeeldingen in september of oktober 2009 heeft verwijderd. De rechtbank is, evenals de raadsvrouw, van oordeel dat aan de hand van processen-verbaal van bevindingen en de bijbehorende bestandenlijst in het dossier met onvoldoende zekerheid kan worden vastgesteld of de bestanden ten tijde van de inbeslagneming nog zichtbaar en normaal te benaderen waren. De rechtbank zal daarom de verklaring van verdachte als uitgangspunt nemen en bewezen verklaren dat verdachte de afbeeldingen in de periode van 1 januari 2008 tot en met oktober 2009 in bezit heeft gehad en verdachte voor de overige tenlastegelegde periode vrijspreken).

[522] De gebruiker behoeft dus daarvoor niet de afbeelding (of het eventueel daarbij behorende bericht) ook te "openen". Wel moet de gebruiker voor de ontvangst ingelogd zijn op het WLM-netwerk, en veelal zal bij verzending de afbeelding ook binnen de gebruikte applicatie direct zichtbaar zijn voor de ontvanger. Bron: NFI-rapport (dr.ir. H.M.A. van Beek) 16 april 2015 in de zaak met parketnummer 09/757756-12.

[523] Dit lijkt te zijn miskend in RB Gelderland 29-2-2016, ECLI:NL:RBGEL:2016:1109 (verweer: "*ongevraagd toegezonden, niet geopend, en niet bekend met filmpjes*". "*De militaire kamer acht het een feit van algemene bekendheid dat alleen gedownloade en geopende filmpjes in het geheugen van een smartphone worden opgeslagen*"). Zie ook hiervoor onder 4.1.3.3.

Technisch lemma: tijdstempels (datum- en tijdsaanduidingen bij bestanden).

Computers houden bij de opslag en verwerking van gegevens bijna altijd ook automatisch bij wanneer die opslag en die verwerking heeft plaatsgevonden. Deze gegevens worden tijdstempels genoemd. Tijdstempels zijn zeer belangrijk in forensisch onderzoek en voor de beoordeling van de bewijswaarde van digitaal bewijsmateriaal. Het is daarom belangrijk er in ieder geval op hoofdlijnen enige kennis van te hebben.

Bij elk digitaal forensisch onderzoek moet, om de juistheid van de tijdstempels te kunnen beoordelen, gekeken worden naar de tijdsinstellingen van het te onderzoeken device. Tijdstempels worden afhankelijk van het besturingssysteem (Windows, Mac OSX) en het bestandssysteem (FAT, NTFS etc) verschillend verwerkt.[524] Het geautomatiseerde systeem van registratie van tijdstempels gaat uit van de instellingen in de zogenaamde systeemklok. Over de betrouwbaarheid van tijdstempels wordt hieronder het een en ander opgemerkt.

Betrouwbaarheid tijdstempels.
Computers ontlenen hun tijdsinformatie normaliter aan hun eigen systeemklok c.q. –tijd. Dat is de datum/tijd die is ingesteld op het systeem. In veel moderne computers zal het besturingssysteem daarvoor via internet contact leggen met een server die de juiste tijd als het ware doorgeeft.[525] Andere elektronische apparaten ontlenen de systeemtijd aan andere bronnen, te denken valt aan GPS-satellieten bij een sporthorloge. Het voert in dit verband te ver om uitputtend in te gaan op alle verschillende wijzen waarop elektronische apparaten en computers hun systeemtijd verkrijgen. In het volgende wordt met name ingegaan op de tijdsinformatie die computers gebruiken. De systeemklok c.q. -tijd kan echter veelal ook door de gebruiker/beheerder van een systeem gewijzigd worden (zij het dat deze dan in de regel bij het opnieuw opstarten van het systeem of na het verloop van een bepaalde tijdsinterval (in Windows 10 standaard ingesteld op zeven dagen) weer terugvalt op de juiste tijd). Elk digitaal forensisch onderzoek begint daarom met de controle van de systeemtijd.

De systeemtijd kan door de gebruiker gewijzigd worden en een apparaat kan door verschillende tijdzones reizen (denk aan de laptop die meegaat op vakantie naar een verre bestemming). Daarnaast bestaat de mogelijkheid om tijdstempels te manipuleren (*timestomping)*. In die gevallen wordt door onderzoekers vaak gepoogd om bestanden op een andere wijze te dateren, bijvoorbeeld door de inhoud van bestanden te koppelen aan bepaalde gebeurtenissen uit de fysieke wereld[526] of aan metadata in relatie tot het bestand die deels is gegeneerd vanuit andere systemen, zoals servers van websitehosters[527] of internetproviders[528], of die in andere systeem- of programmaonderdelen is opgeslagen. Ook kan worden onderzocht of er in de metadata van het bestand ook informatie staat over de computerlocatie waar het bestand vandaan komt, zodat eventueel vanuit die bron kan worden onderzocht wanneer het verzonden is. Ook de plaats waar een bepaald bestand op een gegevensdrager als een hard disk is opgeslagen kan iets zeggen over het moment waarop het is opgeslagen, omdat systemen bij de opslag van data bijvoorbeeld veelal ook een bepaalde volgorde aanhouden.

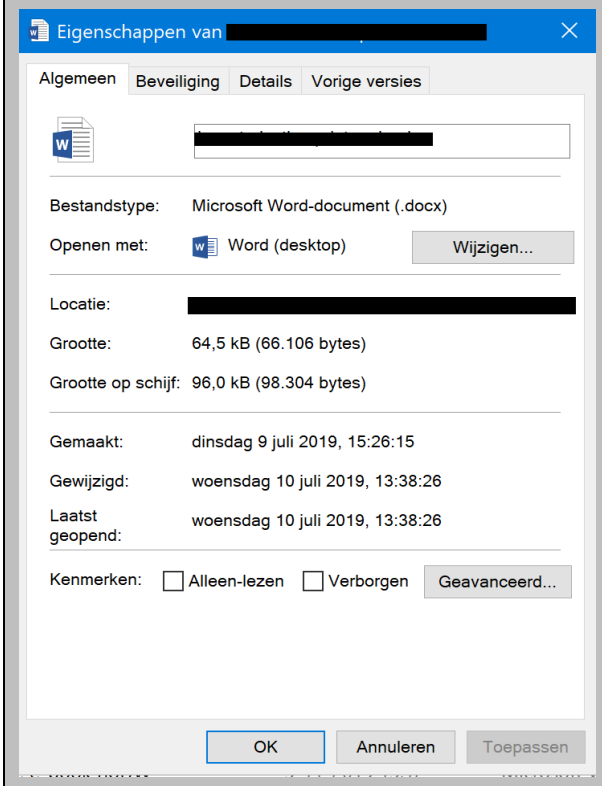
Als bestanden zijn "gewist" (ook regelmatig aangeduid als: "*deleted*") bevindt zich vaak nog wel meta(tijds)informatie over dat bestand in de logbestanden van het systeem of van het gebruikte programma. Daaruit kan dan bijvoorbeeld nog worden afgeleid dat een bepaald bestand op de computer heeft gestaan.

---

[524] Zie met name T. Knutson, "Filesystem Timestamps: What Makes Them Tick?", SANS 2016.
[525] Dat gebeurt over het algemeeen via het Network Time Protocol, zie: https://en.wikipedia.org/wiki/Network_Time_Protocol.
[526] Zie bijv. RB Den Haag 31-5-2017, ECLI:NL:RBDHA:2017:5839 (*file created date* gekoppeld aan moment van vrijkomen uit detentie en toegang tot computer en datum telefoongesprek over kopen van usb-stick om "rotzooi" te downloaden).
[527] Een voorbeeld kan zijn een zoekopdracht aan Google, gegeven in de webbrowser. De server van Google neemt in de URL van de pagina met zoekresultaten een tijdstempel op van het verzoek, al is deze vanwege de 'schrijfwijze' op het eerste oog niet te lezen. Een tijdstempel kan na analyse leesbaar worden gemaakt en vervolgens gebruikt worden in een vergelijking met digitale sporen op de betreffende computer rond hetzelfde moment. Zie voor meer – zeer technische – informatie: https://www.magnetforensics.com/resources/analyzing-timestamps-in-google-search-urls/ en http://cheeky4n6monkey.blogspot.com/2014/10/google-eid.html
[528] Zo zal als een opgeslagen afbeeldingsbestand oorspronkelijk was meegezonden als bijlage bij een emailbericht in de header van dat mailbericht veelal ook datum/tijdinformatie afkomstig van de verzender van het bericht c.q. de server van de provider zijn opgenomen. Als je vanaf het bestand terug rechercheert naar de mail waarbij deze was gevoegd, kan je dus mogelijk ook de datum van ontvangst van de afbeelding vaststellen.

Soms zijn na "wissen" ook de bestanden zelf aanwezig in de *unallocated* clusters, maar dan niet meer op een normale wijze toegankelijk. Lang niet altijd zijn dan echter ook de metadata van die bestanden nog beschikbaar. En als die er wel zijn, zijn die metadata (waaronder dus ook de tijdstempels) niet per definitie betrouwbaar. In die gevallen zal er eigenlijk – alvorens conclusies te trekken welke een relatie hebben met datum en tijd - altijd door een deskundige gericht nader onderzoek moeten worden gedaan, waarbij er een gerede kans bestaat dat ook een dergelijke deskundige niet tot duidelijke conclusies zal kunnen komen.

Algemene systematiek van tijdstempels (MAC-tijden)
Zeer veel programma's, waaronder Windows, registreren tijdstippen in de vorm van wat veelal MAC-tijden (MAC-times) wordt genoemd. MAC-tijden zijn een vorm van metadata waarbij wordt opgeslagen wanneer bestanden (of mappen) zijn gewijzigd (***m**odified*), laatst geopend (***a**ccessed*) of gemaakt (*c**reated***). Ook deze tijden zijn door een gebruiker op zichzelf overigens te manipuleren. Zo kan bijvoorbeeld in Windows eenvoudig het bijhouden van de laatst geopend-tijd worden uit- of aangezet.[529]
Aandacht verdient, dat verschillende besturingssystemen en programma's deze MAC-tijden veelal (net) iets anders bijhouden en/of opslaan. Het trekken van conclusies uit bij bestanden behorende (of in registers vermelde) MAC-tijden is derhalve zonder diepgaande kennis van zaken bepaald hachelijk. De metadata (waaronder de MAC-tijden) van een Word-bestand kunnen er op een Windowscomputer bijvoorbeeld uitzien als:



Relatie tussen tijdstempels en handelingen met een bestand (of map)
Voor opsporingsdiensten (en strafrechters!) is datum/tijdsinformatie bij bestanden vaak belangrijk om twee redenen:
a. de vaststelling of duiding van of en zo ja welke handelingen er met een bepaald bestand zijn uitgevoerd; en
b. de plaatsing in de tijd van die handelingen.
De MAC-tijden zijn hierbij veelal zeer belangrijk, omdat daaraan aanwijzingen kunnen worden ontleend over wanneer bijvoorbeeld een bestand op een bepaalde computer is opgeslagen, en wanneer het is gewijzigd en/of voor het laatst is geopend.

Een indicatie wat er met het tijdstempel-informatie (MAC-tijden) bij handelingen met bestanden in zijn algemeenheid in een Windowsomgeving gebeurt is te zien in het volgende overzicht.

[529] Als daarbij de standaardinstelling is veranderd is dat voor een deskundige echter in de regel eenvoudig vast te stellen. Wijziging van de standaardinstelling wijst op een zekere computerkennis en roept ook de vraag op waarom gebruiker die instelling heeft gewijzigd.

Handeling	(Last) Modified date	(Last) Accessed date	File Created date
Bestandsnaam wijzigen	Ongewijzigd	Ongewijzigd	Ongewijzigd
Verplaatsen/slepen naar een andere map	Ongewijzigd	Ongewijzigd	Ongewijzigd
Verplaatsen/slepen naar een andere gegevensdrager of partitie	Ongewijzigd	Verplaatsingstijdstip	Ongewijzigd
Kopiëren van een bestand	Ongewijzigd	Kopieertijdstip	Kopieertijdstip
Opslaan van nieuw bestand	Opslagtijdstip	Opslagtijdstip	Opslagtijdstip
Bewerken van bestaand bestand	Bewerkingstijdstip	Ongewijzigd	Ongewijzigd
Openen van bestaand bestand	Ongewijzigd	Aangepast/Ongewijzigd[530]	Ongewijzigd

Zo zal binnen Windows bij het kopiëren van een bestand de oorspronkelijke "*file created date*" van een bestand wijzigen in dat van het moment waarop dat bestand is gekopieerd. Dit betekent bijvoorbeeld dat uit een enkele *created* datum/tijdsaanduiding niet zonder meer kan worden afgeleid dat een bestand ook op die computer is "gemaakt", maar hooguit dat het op dat moment op die computer is opgeslagen. Dit onderscheid kan van belang zijn bij bijvoorbeeld de beoordeling of er naast bezit van bepaalde bestanden bijvoorbeeld ook sprake is geweest van het vervaardigen daarvan.

Ook volgt uit het voorgaande dat een *last modified* date in een tijdstempel van een bestand kan liggen voor een *created* date. Dat klinkt paradoxaal (hoe kan je iets bewerken dat nog niet eens gemaakt is) en wordt wellicht gevoeld als aanwijzing "dat er iets mis is" met het systeem en/of de (informatie over) dataopslag. Dat hoeft echter geenszins het geval te zijn. Zoals uit het overzicht blijkt zal namelijk in het tijdstempel van een bestand dat eerst is *bewerkt* en dan een week later wordt *gekopieerd* de oorspronkelijke bewerkingsdatum (*last modified* date) worden bewaard, maar bij de *file created* date de datum van het kopiëren van het bestand naar de schijf waar het is aangetroffen worden geregistreerd.

Welke tijdstempels bij een bestand worden gezet hangt af van de werking van het programma dat de betreffende handeling met het betreffende bestand heeft uitgevoerd. Er is daarbij veel variatie tussen softwarefabrikanten en zelfs tussen verschillende versies van eenzelfde programma. Bijzondere aandacht (en voorzichtigheid!) verdienen hierbij ook zogenaamde backup handelingen zoals het uitpakken (en inpakken) van bestanden in/uit archiefbestanden en -mappen (zoals .zip bestanden). Dergelijk in- of uitpakken kan namelijk leiden tot het overnemen van tijdstempels die (mogelijk al lang geleden) waren opgeslagen in het archiefbestand. Een voorbeeld: bij het downloaden en uitpakken met de zip-functie in de standaard windows explorer van een archiefbestand naar een laptop worden de uitgepakte bestanden voorzien van een *file created* date, *last modified* date en *last accessed* date gelijk aan de *last modified* date die al was opgeslagen in het oorspronkelijke zip (archief)bestand.[531]

Hoewel de wijze waarop tijdstempels worden geplaatst dus sterk software-specifiek is, kan wel in algemene zin gezegd worden dat het bij kopieer- en archief-toepassingen gebruikelijk is in ieder geval de *last modified* date te behouden.[532]

Het voorgaande maakt duidelijk dat het in individuele zaken op basis van tijdstempels trekken van conclusies met betrekking tot een gedraging met een bepaald bestand (de datum waarop dat gebeurd zou zijn daaronder begrepen) specifieke kennis vereist, onder meer van de werking van de in het specifieke geval gebruikte

[530] Afhankelijk van de (standaard)instelling van het systeem; als deze aldus is ingesteld dat deze de *access time* actualiseert, dan wordt de *access time* binnen een uur geactualiseerd, zo niet dan blijft de *access time* bij het openen van het bestand ongewijzigd.

[531] Dit lijkt onvoldoende te zijn onderkend in RB Midden-Nederland 10-10-2017, ECLI:NL:RBMNE:2017:5057 ("Naar het oordeel van de rechtbank sluit het samenvallen van de *file created* date en de *file last accessed* date de mogelijkheid uit dat met de term *file created* date een ander moment is bedoeld dan het tijdstip waarop verdachte de betreffende bestanden heeft opgeslagen"). Immers, ook als men op dit moment (2023) een zip-bestand met Windows Explorer uitpakt met daarin een afbeeldingsbestand met een "last modified" date in 2018 is sprake van het samenvallen van de "*file created*" date en "*file accessed*" date. Het afbeeldingsbestand is dan echter voorzien van een *file created* date en een *file accessed* date uit 2018 die evident *niet* het moment van opslag van het betreffende afbeeldingsbestand op de computer van degene die het zip-bestand heeft uitgepakt weergeeft. Hierbij kan worden opgemerkt dat ook in zeer veel processen-verbaal de bewijswaarde (in termen van moment van opslag op het betreffende systeem) van de *file created date* onvolledig (en daarmee onzes inziens ook onjuist) wordt weergegeven.

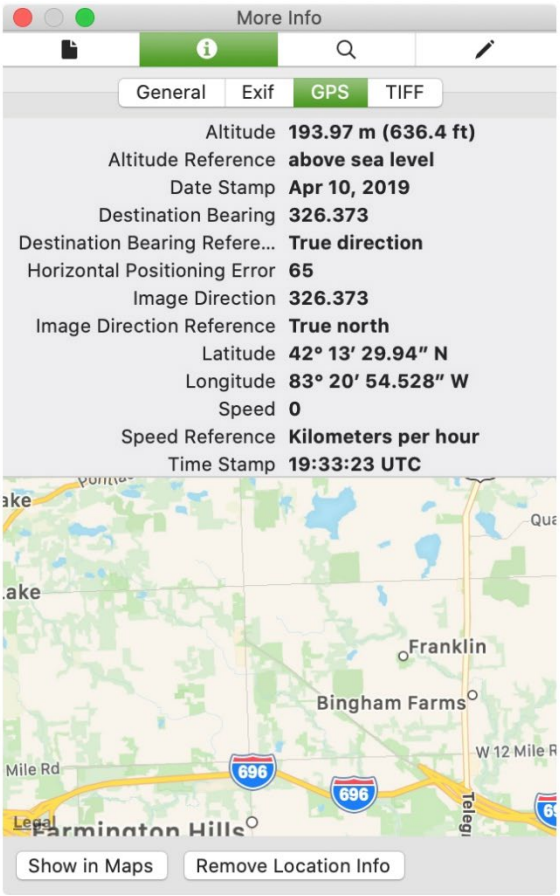
[532] Zie verder ook: "Technische Toelichting, terug naar de bestanden" van het Nederlands Forensisch Instituut, 24 juni 2019.

software. Het lijkt dan ook aangewezen dat de strafrechter indien die datering relevant wordt geacht voor de beoordeling van de zaak die conclusies eerst trekt nadat hij zich door een (digitaal) deskundige heeft laten voorlichten over de specifieke betekenis van de betreffende tijdstempels in *die* zaak.

Zoals uit het technisch lemma blijkt dienen uit metadata niet te snel stellige conclusies te worden getrokken. Dat geldt zeker ook voor metadata betreffende datum en tijd. Vooral als deze op zichzelf (dus los van andere informatie) wordt beschouwd, is voorzichtigheid bij het trekken van conclusies bepaald geboden. Wil men bewijsrechtelijke conclusies verbinden aan metadata, dan lijkt als regel inschakeling van een deskundige (al is het maar om de voorlopige eigen conclusies te verifiëren) de juiste weg te zijn. Daarmee is overigens niet gezegd dat de bewijswaarde voor wat betreft de plaatsing in de tijd van (gedragingen met) bestanden van in metadata opgeslagen datum- en tijdgegevens van bestanden gering moet worden geacht; zeker bezien in samenhang met andere digitale of tactische info kan deze bewijswaarde namelijk (zeer) hoog zijn.[533]

6.2.4.2. EXIF-informatie

Veel bestanden van digitale foto's of video's bevatten zogenaamde *EXIF*-informatie. Uit deze informatie kunnen in de regel diverse gegevens (waaronder naast de datum/tijd steeds vaker ook de geografische locatie waar de betreffende afbeelding gemaakt is) worden afgeleid.



[533] Zie bijv. ook Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520 (eigen verklaring dat bestanden "nieuw" waren i.c.m. datum in metadata bij bestand bewijzend voor moment waarop afbeelding is opgeslagen).

Deze *EXIF*-informatie is echter deels gerelateerd aan de (juistheid van de) basisinstellingen van de gebruikte camera, zodat het trekken van conclusies op basis van deze gegevens wel met de nodige voorzichtigheid zal dienen te geschieden.[534] Een bijzondere vorm van enigszins met *EXIF*-informatie gelijkende kenmerken die aan een foto kunnen zijn verbonden biedt de beeldsensor van de camera waarmee een onderzochte afbeelding is gemaakt. Deze blijkt volgens de politie op een wijze vergelijkbaar met een vingerafdruk het leggen van een verband tussen een foto en een specifieke camera mogelijk te maken.[535]

6.2.5. Bewijswaarde (doorgestuurde) e-mailberichten

Indien op een geautomatiseerd werk ingekomen e-mailberichten zijn aangetroffen, zal dat in de regel in voldoende mate bewijs vormen voor het *feitelijk* in het bezit hebben daarvan. Ook hier zal echter gelden dat daarmee nog niet ook de opzet op het bezit van die e-mailberichten is gegeven. E-mailberichten (en daarbij gevoegde bijlagen) kunnen immers net als vele andere vormen van digitale communicatie ook buiten de wil van de geadresseerde worden ontvangen. Bij in een verzendbox of in een "verzonden"-map aangetroffen e-mailberichten zal dat echter in de regel anders liggen, omdat het niet erg waarschijnlijk lijkt dat de gebruiker van de computer buiten zijn of haar wil dergelijke berichten zou hebben verzonden. Dat kan echter anders zijn, indien aannemelijk wordt dat in casu de betreffende computer gedurende de periode waarin de mailberichten zijn verstuurd, door een ander – al dan niet op afstand met behulp van bijvoorbeeld *remote access tools* – kon worden gebruikt.

Het is onzes inziens heden ten dage als een feit van algemene bekendheid aan te merken dat het bij het doorzenden van e-mailberichten eenvoudig is om wijzigingen aan te brengen ten opzichte van het oorspronkelijke e-mailbericht. Op zichzelf is dat echter nog geen reden om doorgezonden e-mailberichten niet als bewijsmiddel te bezigen. De door de rechter te beantwoorden vraag is ook hier of – alle feiten en omstandigheden in aanmerking nemend – aannemelijk is geworden dat van een dergelijke wijziging in het oorspronkelijke bericht ook in het concrete geval sprake is.[536] In sommige gevallen kan nader technisch onderzoek, met name naar de metadata van de betreffende e-mailberichten, eventueel handvatten voor die beoordeling aanreiken.

Voor wat betreft de mogelijkheden tot digitaal-forensisch onderzoek aan e-mailaccounts en daarin opgeslagen berichten is het onderscheid tussen web-based e-mail (of kortweg: webmail) en e-mailclients (of: e-mailprogramma's) relevant. Webmail is een verzamelnaam voor webapplicaties die het mogelijk maken om via een webgebaseerde gebruikersinterface e-mail te gebruiken.

---

[534] Zie bijv. RB Midden-Nederland 25-4-2022, ECLI:NL:RBMNE:2022:1578 ("*De foto's waarvan de medeverdachte verklaart deze gemaakt te hebben bevatten zogenaamde EXIF-data, onder andere inhoudende GPS gegevens waaruit blijkt dat deze op het woonadres van verdachte zijn gemaakt en waaruit blijkt dat deze zijn gemaakt met het cameramodel SM-G93F, welke hoort bij een Samsung S10. De medeverdachte was in bezit van een Samsung S10.*"). Uit informatie uit openbare bron blijkt dat het voormeld cameramodel niet bestaat (vermoedelijk betreft het cameramodel SM-930F of SM-935F). Merk voorts op dat de foto's zelf geen EXIF-data bevatten, maar dat de betreffende bestanden bestaan uit zowel de digitale foto zelf alsook de EXIF-data.

[535] RB Rotterdam 26-7-2018, ECLI:NL:RBROT:2018:6129.

[536] RB Dordrecht 3-8-2012, ECLI:NL:RBDOR:2012:BW0716 (verspreiden en in bezit hebben van kinderporno, verweer dat geforwarde e-mail niet als bewijs kan worden gebruikt, omdat dergelijk e-mails kunnen zijn bewerkt verworpen).

6.2.6. Bewijswaarde IP-adres

Zoals hiervoor al aangegeven vinden veel onderzoeken naar overtreding van art. 240b Sr hun grondslag in meldingen van het NCMEC of vergelijkbare meldpunten over aangetroffen kinderpornografisch materiaal op internet.[537] Veelal wordt dan ook met de informatie het IP-adres meegeleverd waarvandaan de communicatie of (bij cloudopslag) de gegevensopslag heeft plaatsgevonden, of waarmee ooit het betrokken account is geregistreerd.

De bewijswaarde van een IP-adres is op zichzelf nogal betrekkelijk. Het geeft in de kern slechts aan dat een bepaalde communicatie met internet van een bepaald device of via een bepaalde router is verlopen, en niet wie verantwoordelijk was voor die communicatie. In bepaalde gevallen, zoals in het geval aannemelijk is dat slechts één persoon toegang heeft tot dat device of die bepaalde router en/of er ander bewijs bestaat dat de betreffende communicatie, gezien bijvoorbeeld de inhoud, (waarschijnlijk) van een bepaalde verdachte afkomstig is, kan aan de combinatie van IP-adres en inhoud van de communicatie echter wel een sterke bewijswaarde worden toegekend.[538]

In de praktijk wordt het IP-adres vooral gebruikt als startpunt voor onderzoek, in het bijzonder voor het identificeren van de naam-, adres- en woonplaatsgegevens van een (mogelijke) verdachte, en voor het daarop aansluitend bezoeken van dat adres teneinde daar een doorzoeking te doen plaatsvinden of uitlevering te vragen. Zorgvuldigheid[539] en voorzichtigheid is daarbij (vooral voor officieren van justitie en rechter-commissarissen) wel geboden, omdat een IP-adres door de doorontwikkeling van de techniek op zichzelf niet altijd meer voldoende individualiseerbaar is. Dit speelt vooral bij het zogenaamde *Carrier Grade Network Address Translation* (CGN), waarbij in afwachting van de volledige transitie van het IPv4 naar het IPv6-protocol gebruik wordt gemaakt van (dynamische) IP-adressen die op meerdere individuele aansluitingen tegelijk betrekking kunnen hebben. In die gevallen zal om een voldoende mate van individualiseerbaarheid te krijgen veelal meer informatie aan de provider moeten worden gegeven en gevraagd (bijvoorbeeld precieze tijdstippen van de betreffende communicatie en de eventuele zogenaamde poortnummers) dan alleen het “kale” IP-adres.[540]

Ook wordt het IP-adres wel gebruikt als onderdeel van de bewijsvoering dat via een – veelal aan een bepaalde verdachte en/of computer te linken – internetverbinding gegevens zijn gedownload of verspreid. Hier wordt regelmatig het verweer gevoerd dat – in het bijzonder indien sprake is van een draadloos netwerk – “op afstand is ingebroken” in de wifirouter/modem van de verdachte, of dat deze router zonder in- of toestemming van de

---

[537] Zie hiervoor onder 6.1.1.

[538] RB Midden-Nederland 31-5-2021, ECLI:NL:RBMNE:2021:2257 (t.a.v. feit 1: “*uit het dossier blijkt ook dat de telefoon van verdachte ongeveer een half uur voor de inlogpoging verbinding heeft gemaakt met de laptop waarmee is geprobeerd in te loggen en met een IP-adres dat gekoppeld is aan het adres van verdachte*. ”)

[539] Illustratief zijn in dat kader ook de bevindingen van de Britse Interception of Communications Commissioner Sir Anthony May, waarvan de conclusies zijn samengevat in: https://www.security.nl/posting/435990/Onterechte+huiszoekingen+door+blunders+met+IP-adressen+in+VK.

[540] Zie hierover verder direct hierna in het Technisch lemma: Enige kanttekeningen bij de betrouwbaarheid van IP-adressen als grondslag voor rechterlijke beslissingen. In dat kader lijkt het in ieder geval verstandig om bij beslissingen welke mede zouden zijn gebaseerd op het gebruik van een bepaald IP-adres stelselmatig te bekijken c.q. na te vragen:
- welk IP-protocol is gebruikt bij het datacommunicatieverkeer waaraan via voormeld IP-adres is deelgenomen;
- in hoeverre is daarbij door de ISP gebruik gemaakt van Carrier Grade NAT;
- indien gebruik is gemaakt van Carrier Grade NAT: welke *source ports* zijn gebruikt op de tijdstippen dat het strafrechtelijk relevante datacommunicatieverkeer plaatsvond;
- of de verdachte c.q. een specifieke computer of locatie gelinkt kan worden aan de betreffende *source ports* en zo ja, op welke wijze.

normale gebruiker door een derde (bijvoorbeeld een gast) is gebruikt. Voor de meer technische kant van wifi en dit verweer wordt hier kortheidshalve verwezen naar het hiervoor onder 4.1.2.3. opgenomen technisch lemma "wifi". Zoals daaruit ook blijkt, hangt het van diverse factoren (maar met name van het beveiligingsniveau van de router en de bekendheid van anderen met eventuele wachtwoorden) af in hoeverre dergelijke verweren aannemelijk kunnen worden geacht. Ook andersoortige informatie, zoals bijvoorbeeld het tijdstip van de betreffende internetcommunicatie kan soms bijdragen aan de beoordeling van de aannemelijkheid van een dergelijk verweer.[541]
In sommige gevallen kan ook nader onderzoek aan de router/modem zelf aanvullende duidelijkheid geven over vragen als door welke computers en wanneer die router/modem is gebruikt. Een praktisch probleem is echter dat routers/modems bij doorzoekingen veelal niet in beslag worden genomen en evenmin als regel een forensische kopie van het werkgeheugen van dergelijke *devices* wordt gemaakt. Voor zover wel een forensische kopie van het werkgeheugen van een router/modem kan worden gemaakt, geldt als bijkomend probleem dat gegevens over apparaten die met de router verbonden zijn geweest (o.a. MAC-adressen) in het geheugen van de router slechts tijdelijk, of -indien het apparaat geen logging-functie kent- helemaal niet beschikbaar zijn.[542]

Technisch lemma: enige kanttekeningen bij de betrouwbaarheid van IP-adressen als grondslag voor rechterlijke beslissingen

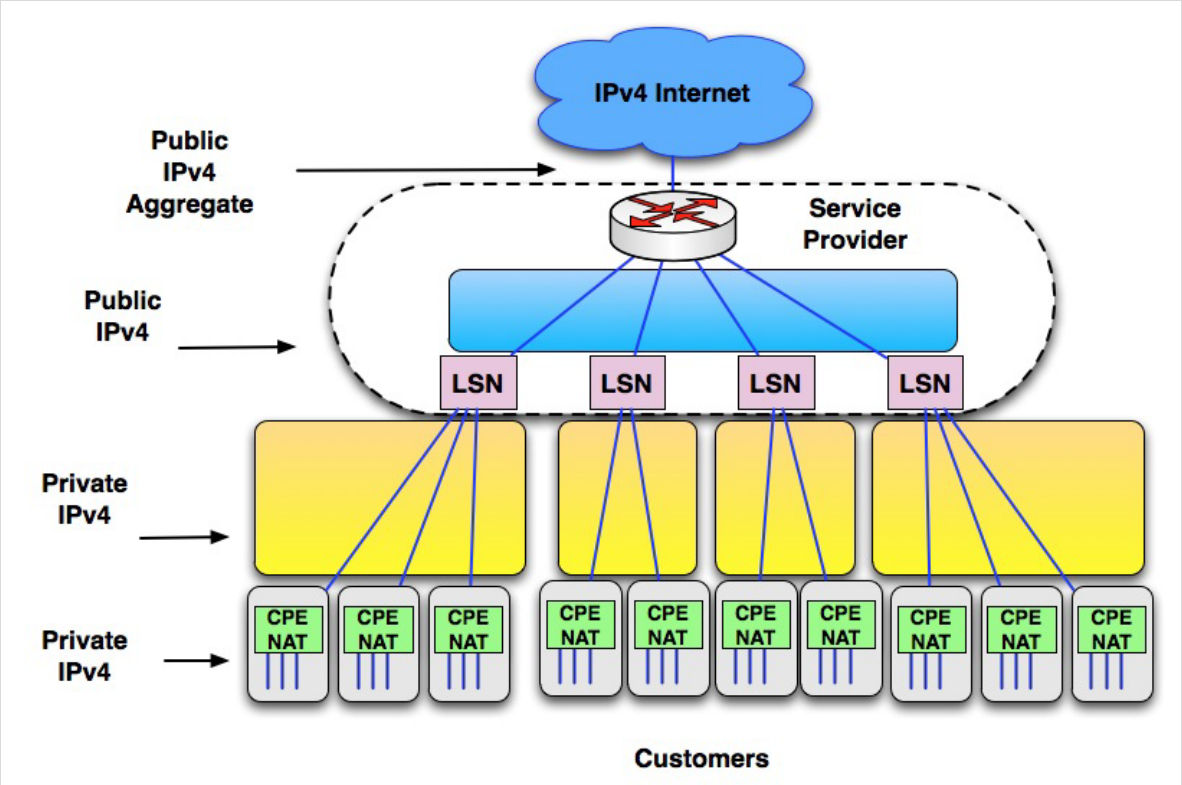
1. IP-Adres en Carrier Grade Network Address Translation
In nagenoeg alle strafzaken waarbij computers, smartphones en andere *devices* een rol spelen, wordt in het kader van de bepaling van de bestemming en herkomst van datacommunicatieverkeer door de opsporingsinstanties onderzoek gedaan naar IP-adressen. Met behulp van deze IP-adressen kunnen individuele computers (of andere *devices* binnen een netwerk[543]) worden geïdentificeerd. Elke computer of device krijgt namelijk als hij contact maakt met een internetserver een IP-adres toegewezen. Zo'n IP-adres heeft de vorm van een reeks cijfers (IPv4) en/of letters (IPv6). Elke IP-adres is gekoppeld aan een specifieke Internet Service Provider (ISP). Omdat de ISP's via hun abonnementenadministratie in de regel ook over de fysieke adressen van hun klanten beschikken, kan derhalve in veel gevallen via het IP-adres ook het fysieke adres van de eindgebruiker worden gevonden. Op dat fysieke adres kunnen vervolgens ook (veelal in het kader van een doorzoeking) opsporingshandelingen worden verricht, waarbij dan eventueel ook de betreffende computer in beslag kan worden genomen voor verder onderzoek.

Lange tijd gebruikte men bij de toekenning van IP-adressen, uitsluitend IP-adressen van het zogenaamde Internet Protocol versie 4-systeem (IPv4). Deze adressen zien er bijvoorbeeld als volgt uit: 159.46.196.29.[544] Door de explosieve groei van het aantal internetgebruikers, en van het aantal computers, smartphones, InternetofThings-devices etc., waarmee individuele gebruikers verbinding maken met het internet zijn er echter binnen het IPv4-protocol thans al te weinig adressen om aan de vraag naar IP-adressen te voldoen. De industrie heeft daarom een nieuw internetprotocol ontwikkeld: Internet Protocol versie 6 (IPv6). Een IP-adres volgens IPv6 ziet er bijvoorbeeld zo uit: 2001:db8:0:1234:0:567:8:1.

---

[541] Nogal eens wordt hierbij verwezen naar kinderen die het wifi- of routerpassword aan hun vrienden zouden hebben gegeven. Dergelijke vrienden zullen echter bijvoorbeeld in de regel dan niet ook 's nachts fysiek toegang hebben tot de betreffende wifi-router/modem.
[542] Zie meer uitvoerig hierover D. Blackman & P. Szewczyk, "The challenges of seizing and searching the contents of Wi-Fi devices for the modern investigator", *Australian Digital Forensics Conference* 2015, p. 37-48, i.h.b. p. 41 ("sixteen of the twenty devices inspected had little or no logging enabled by default, despite having the capability to log more extensive information").
[543] Via het IP-adres kan bovendien veelal ook de identiteit van de ISP via welke het datacommunicatieverkeer loopt c.q. heeft gelopen worden vastgesteld.
[544] Welk IP-adres door een bepaalde computer of netwerkapparaat wordt gebruikt (en waar die computer staat, en nog meer wellicht voor sommigen wat verontrustende informatie) is via bijvoorbeeld http://whatismyipaddress.com voor iedereen direct te achterhalen.

IPv6 wordt door een groot aantal ISP's in Nederland al gebruikt, maar door de met de overgang van IPv4 naar IPv6 is samenhangende technische complicaties, is IPv6 nog zeker niet algemeen ingevoerd. Omdat de ISP's en gebruikers ondertussen wel verder moeten, en daarvoor over IP-adressen moeten kunnen blijven beschikken, wordt nu gebruik gemaakt van een systeem dat voluit Carrier Grade Network Address Translation (Carrier Grade NAT, of CGN) wordt genoemd. Daarbij wordt allereerst het oorspronkelijke private IP-adres van (het apparaat van de) de eindgebruiker "vertaald" naar een meer algemeen (publiek) IP-adres van de ISP. Daarnaast wordt er gebruik gemaakt van het gegeven dat ook bij communicatie via een standaard IPv4 IP-adres gebruik kan worden gemaakt van een zeer groot aantal (theoretisch meer dan 65.000) onderscheiden poortnummers.[545] ISP's die momenteel gebruik maken van Carrier Grade NAT (en dat zijn in Nederland veruit de meeste) gebruiken deze laatste eigenschap om door middel van verdeling via deze poorten via slechts één IP-adres datacommunicatieverkeer naar verschillende eindgebruikers (dat kunnen er honderden of meer zijn) te sturen. Men kan dit enigszins vergelijken met het systeem van een interne telefooncentrale. Er is slechts één buitenlijn (één IP-adres) maar vele gebruikers die via die telefooncentrale verbonden zijn met de buitenwereld. Voor alle andere gebruikers op het internet is er maar één IP-adres zichtbaar. Achter dat ene IP-adres kunnen echter dus honderden verschillende individuele gebruikers zitten. Deze behoeven ook niet te behoren tot één organisatie of bijvoorbeeld in dezelfde woning of hetzelfde gebouw te verblijven. Schematisch ziet het er ongeveer zo uit:



Voor justitie brengt het gebruik van Carrier Grade NAT een probleem met zich. Bij gebruik van Carrier Grade NAT kan je eigenlijk alleen precies te weten komen naar welke individuele computer bepaald datacommunicatieverkeer is gegaan, als je naast de relevante tijdstippen van de communicatie ook beschikt over de informatie betreffende de daarbij gebruikte netwerkpoorten (de zogenaamde source ports). Op basis van thans beschikbare informatie lijkt het erop dat de meeste ISP's de informatie aangaande de gebruikte poorten niet, dan wel slechts kort, opslaan ("loggen"). Het kan dus, ook als een IP-adres beschikbaar is, heel lastig worden om achteraf nog te achterhalen naar welke individuele computer of via individuele internetaansluiting datacommunicatieverkeer heeft plaatsgevonden.

[545] Eén enkele computer kan meerdere sessies tegelijkertijd onderhouden die verbonden zijn met verschillende andere computers. Elke sessie wordt gedefinieerd met een bepaald poortnummer. Al deze sessies worden dan via een techniek die *multiplexing* wordt genoemd door dezelfde netwerkaansluiting gestuurd. In de meest gebruikte protocollen voor het transport van data via internet, TCP en UDP, wordt een poort aangeduid met een 16-bit-getal. Er zijn dus in principe 65536 mogelijke TCP- of UDP-poorten op één IP-adres. In werkelijkheid zijn dat er minder omdat een aanzienlijk aantal van deze poortnummers is gereserveerd voor gebruik door specifieke programma's (applicaties).

Nu de volledige invoering van IPv6 naar verwachting niet op korte termijn zal worden gerealiseerd[546] is dit een probleem dat zich nog enige tijd zal voordoen.

2. Misbruik van een IP-adres (spoofing)[547]
Het is technisch mogelijk internetverkeer (verder aan te duiden als datapakketten) vanaf het eigen IP-adres te versturen, en daarbij niet het eigen IP-adres maar een ander IP-adres als afzender in de kop (header) van het pakket te (laten) gebruiken. Dit wordt *spoofen* of *spoofing* genoemd.[548] Het lijkt op het voeren van een telefoongesprek waarbij de gebelde niet het telefoonnummer van de beller in het display ziet, maar van een derde persoon. Dit heeft in het systeem van het IP echter tot gevolg dat de ontvanger een eventuele reactie zal sturen naar het nummer van de beller, waardoor alles wat de gebelde zegt niet bij de beller maar bij de derde persoon te horen is. Het IP maakt dus een succesvolle uitwisseling van datapakketten moeilijk, omdat het antwoord zal uitkomen bij een andere partij dan de eigenlijke verzender. Daarnaast hebben providers (en breder: de internetgemeenschap) maatregelen genomen om *spoofing* tegen te gaan. Zo controleren bijvoorbeeld veel providers of het meegegeven IP-adres wel past bij het netwerk waar het pakket vandaan komt. Zo zal het dus niet lukken om vanuit een Nederlandse netwerk een datapakket te verzenden met een aan een Russische provider uitgeven IP-adres. Daarnaast wordt het IP-protocol doorgaans gebruikt tezamen met 2 aanvullende protocollen: TCP of UDP. Heel simpel samengevat zorgt het TCP-protocol ervoor dat een datapakket pas wordt verzonden als er eerst een naar het juiste “eigen” IP-adres verzonden antwoord van de geadresseerde computer is verkregen (ook wel bekend als *handshaking* of tweeweg-authenticatie). Als er dus een vals IP-afzenderadres wordt opgegeven zal het antwoord niet bij het “eigen” IP-adres aankomen, en wordt de verbinding verbroken. UDP kent op dit punt een minder sterke beveiliging maar wordt hoofdzakelijk gebruikt bij diensten die een grote gegevensstroom in één richting kennen, zoals videostreaming (Netflix etc.) of *online gaming*.

Bewijstechnisch leidt dit tot de volgende conclusies:
a. is een bericht alleen verzonden, dan kan men niet door alleen naar het bericht te kijken vaststellen of het bericht ook daadwerkelijk afkomstig is van het IP-adres dat als afzender in het bericht is opgenomen;
b. is er echter ook op een bericht gereageerd of is een website bezocht, dan is er een (geslaagde) TCP-verbinding nodig geweest, omdat er anders geen tweewegcommunicatie mogelijk was geweest. Wanneer dus bijvoorbeeld in de logbestanden van een website een IP-adres voorkomt, betekent dit in de regel dus ook dat sprake geweest moet zijn van (geslaagde) tweewegcommunicatie.

[546] https://www.telecompaper.com/nieuws/experts-luiden-noodklok-over-trage-transitie-naar-ipv6-in-nederland--1321312
[547] Het hierna gestelde m.b.t. *spoofing* is voor het overgrote deel ontleend aan het deskundigenrapport van Fox-It (K. Jonkers, MSc) d.d. 31 augustus 2015 in een zaak bij het Hof Den Haag met nummer 22-003589-14.
[548] Zie voor een beoordeling van een verweer dat header-informatie van een e-mailbericht met valse facturen niet voor het bewijs mocht worden gebruikt, nu het ‘X-Originating-IP’ van de afzender gespoofd zou zijn door een derde: Hof Den Haag 16-2-2022, ECLI:NL:GHDHA:2022:203.

HOOFDSTUK 7: STRAFVORDERLIJKE ASPECTEN

7.1. Vervolgingsbeleid

7.1.1. Aanwijzing Kinderpornografie (2016) / Indigo-beleid

Lang niet in alle zaken waarin in technisch-juridische zin sprake zou kunnen zijn van overtreding van art. 240b Sr wordt daadwerkelijk door het Openbaar Ministerie strafvervolging ingesteld. De hoofdlijnen van het vervolgingsbeleid zijn neergelegd in de Richtlijn voor strafvordering kinderpornografie (2021R002) en in de Aanwijzing Kinderpornografie (2016).[549] De meest recente versie van deze richtlijn is op 1 september 2021 in werking getreden. Verdachten kunnen dan ook in voorkomende gevallen ook in rechte een beroep op de inhoud daarvan doen.[550] De Richtlijn voor strafvordering kinderpornografie (2021R002) en de Aanwijzing Kinderpornografie (2016) zullen in 2024 worden geactualiseerd naar aanleiding van de verwachte inwerkingtreding van de Wet seksuele misdrijven.

In de Richtlijn voor strafvordering kinderpornografie (2013) werd nog gesteld dat:

> "*Uitgangspunt bij de vervolgingsbeslissing van het OM is dat op iedere overtreding van art. 240b Sr een betekenisvolle reactie van het OM dient te volgen. In de meeste gevallen betekent dat dat de zaak aan de rechter zal worden voorgelegd en een straf zal worden geëist*".[551]

In de Aanwijzing Kinderpornografie welke op 1 mei 2016 in werking is getreden wordt echter met betrekking tot de rol van het strafrecht en de vervolgingsbeslissing het volgende gesteld:

> *De focus van de strafrechtelijke aanpak van kinderpornografie is, naast het aanpakken van mensen die kinderpornografie downloaden of zich daar toegang toe verschaffen, met name gericht op verspreiders en producenten van kinderpornografie. Bij de verdenking van seksueel misbruik, vervaardiging van kinderpornografie, commerciële of grootschalige verspreiding, wordt in beginsel strafrechtelijk opgetreden. Eventuele instemming van minderjarigen maakt dit niet anders. Minderjarigen kunnen de (lange-termijn)gevolgen van deelname aan het maken en het in omloop brengen van pornografisch materiaal waar zij zelf op staan, anders dan de meeste volwassenen, niet altijd goed overzien en worden om die reden beschermd door de wet. Het strafrechtelijk optreden van het openbaar ministerie sluit hierbij aan. Waar sprake is van een verdenking van alleen downloaden, bezit of kleinschalige verspreiding, wordt maximaal ingezet op het voorkomen van herhaald daderschap. In deze gevallen kan vanuit het perspectief van het vergroten van de veiligheid gekozen*

---

[549] Volledigheidshalve wordt hierbij opgemerkt dat het vervolgingsbeleid in kinderpornozaken niet alleen wordt gevormd door de Richtlijn voor strafvordering kinderpornografie (2021R002) en de Aanwijzing Kinderpornografie (2016), maar ook door de Aanwijzing Zeden (2016) die er als het ware boven hangt. Daarnaast maken ook de hierna te bespreken OM-Richtlijn voor Strafvordering Kinderpornografie 2021 (2021R002) en de sexting richtlijn ("Pubers in beeld") deel uit van de beleidsstukken op dit onderwerp.

[550] M.J. Borgers, T. Kooijmans, *"Het Nederlands strafprocesrecht"*, Deventer: Kluwer 2021, p. 36: "(…) *dat rechtstreeks op een richtlijn (...) een beroep kan worden gedaan en de cassatierechter de richtlijn direct kan uitleggen. Het betreft immers recht, bij schending waarvan de Hoge Raad kan casseren*."

[553] Zie ook: Richtlijn voor strafvordering kinderpornografie (2016), V. De INDIGO-afdoening [Regeling vervallen per 01-09-2021], en ons bevestigd door het Expertisecentrum Kinderporno en Kindersekstoerisme van het Landelijk Parket Rotterdam.

> *worden voor een buitengerechtelijk traject, waarin snel ingrijpen en snel starten van adequate daderbehandeling prevaleren.*[552]

Aldus lijkt bij het OM bij "lichtere" vormen van overtreding van art. 240b Sr het accent te verschuiven van vervolging voor de strafrechter naar een buitengerechtelijke afdoeningsmodaliteit. De INDIGO-afdoening, waarvan de toepassingscriteria in hoofdstuk 5 van de Richtlijn voor strafvordering kinderpornografie (2016) werden beschreven, is per 1 september 2021 komen te vervallen.[553] Strafzaken die voor een INDIGO-afdoening in aanmerking kwamen kunnen thans wel bij OM-strafbeschikking worden afgedaan. Criteria daarvoor worden gegeven in hoofdstuk 5 van de Richtlijn voor strafvordering kinderpornografie (2021).[554]

7.1.2. Specifiek beleid consensuele minderjarigen / "sexting"

Voor het verschijnsel "sexting", waarbij met name minderjarigen, via communicatiediensten als Facebook, WhatsApp, Instagram, Snapchat e.d. of via internet erotische afbeeldingen (zowel video als foto) waarop (ook) zijzelf zijn afgebeeld aan een ander (dat kan ook een partner zijn) toezenden, geldt een specifiek opsporings- en vervolgingsbeleid.
Een meer gedetailleerde invulling van dit beleid is te vinden in de hierna meer gedetailleerd te bespreken Politie/OM-Leidraad afdoening sextingzaken "Pubers in beeld", welke leidraad op www.om.nl wordt omschreven als weergevende het "*OM-beleid bij door jongeren geproduceerde seksuele afbeeldingen van minderjarigen ('in de volksmond ook wel sexting genoemd')*".[555]

Uitgangspunt van dit "sextingbeleid" is dat na aangifte of melding van een door een jeugdige geproduceerde seksuele afbeelding (zoals een filmpje of een foto gemaakt met webcam of mobiele telefoon), allereerst de leeftijd wordt beoordeeld van degene die op de afbeelding te zien is. Als het gaat om een strafbare afbeelding van iemand onder de 12 jaar, dan wordt in beginsel uitgegaan van dwang of ontucht en wordt een volledig opsporingsonderzoek verricht. Betreft het een strafbare afbeelding van een minderjarige boven de 12 jaar, gezonden aan een andere minderjarige, dan wordt over het algemeen eerst een gesprek gevoerd met de jongere. De gegevensdragers waarop de afbeelding staat, worden in beslag genomen en het materiaal wordt bekeken en naar de landelijke eenheid van de politie gestuurd ter opname in de landelijke database met kinderpornografische afbeeldingen. Daarna worden de betrokkenen gehoord, waarbij aan een aantal hierna te noemen aspecten bijzondere aandacht wordt besteed. In eerdere versies van het beleid werd ook expliciet benoemd dat om verdere verspreiding tegen te gaan en ter bescherming van de minderjarige ook actie diende te worden ondernomen om de afbeeldingen (ook bij derden) te verwijderen. Opvallend genoeg komt dit actie/aandachtspunt in de meest recente versie van de Leidraad afdoening sextingzaken niet meer expliciet terug.

---

[553] Zie ook: Richtlijn voor strafvordering kinderpornografie (2016), V. De INDIGO-afdoening [Regeling vervallen per 01-09-2021], en ons bevestigd door het Expertisecentrum Kinderporno en Kindersekstoerisme van het Landelijk Parket Rotterdam.
[553] Zie ook: Richtlijn voor strafvordering kinderpornografie (2016), V. De INDIGO-afdoening [Regeling vervallen per 01-09-2021], en ons bevestigd door het Expertisecentrum Kinderporno en Kindersekstoerisme van het Landelijk Parket Rotterdam.
[554] Zie: Richtlijn voor strafvordering kinderpornografie (2021R002), V. OM-strafbeschikking. Merk op dat de genoemde criteria overeen stemmen met de criteria die werden gebruikt om te bepalen of een zaak in aanmerking kwam voor een INDIGO-afdoening, en die waren opgenomen in hoofdstuk V. van de Richtlijn voor Strafvordering Kinderpornografie (2016).
[555] De Leidraad afdoening sextingzaken "Pubers in beeld" is opgesteld door het Landelijk Expertisecentrum Kinderporno en Kindersekstoerisme, de meeste recente versie is op 1-11-2017 in werking getreden.

De officier van justitie beslist vervolgens of een betrokkene wordt vervolgd en voor welke feiten. Daarbij dient bij de afweging om wel of niet te vervolgen leidend te zijn de wijze waarop (en naar mag worden aangenomen: ook de mate waarin) de persoon op de afbeelding in zijn of haar belangen is geschaad, en de belangen van deze betrokkene, waaronder begrepen de gevolgen van eventuele vervolging van de verdachte voor de betrokkene.[556] In sommige gevallen zal de betrokkene immers meer gediend zijn met bijvoorbeeld het uit de circulatie halen van de betreffende afbeeldingen, dan met de vervolging van een verdachte. In het geval de verdachte minderjarig is, dienen de gevolgen van vervolging voor de verdachte (ook in termen van eventuele weigering van een Verklaring Omtrent het Gedrag) eveneens te worden meegewogen.[557]

Uit de Richtlijn en kader voor strafvordering jeugd en adolescenten (2021R001)[558] (gelezen in samenhang met de beleidsnota 'Pubers in Beeld) kan worden afgeleid dat het OM vervolging in gevallen van *sexting* waarbij afbeeldingen van minderjarigen betrokken zijn *niet* opportuun acht indien:

- sprake is van minderjarigen[559] onderling, of van minder- en meerderjarigen tussen wie een gering leeftijdsverschil bestaat; en
- er consensus tussen de betrokkenen is[560]; en
- de belangen van de betrokken minderjarige(n) door deze vorm van seksualiteit niet zijn geschaad[561]; en
- het gedrag gezien kan worden als leeftijdsadequaat.

Met betrekking tot minderjarige verdachten van *sexting*, die niet aan alle in de Aanwijzing Kinderpornografie genoemde criteria voor niet-vervolging voldoen is door het OM een nader specifiek beleidskader ontwikkeld, namelijk de hiervoor reeds benoemde beleidsnota "Pubers in beeld. Leidraad afdoening sextingzaken" (1 november 2017).[562]

Zakelijk weergegeven komt dit beleid erop neer dat de zaak ook anders dan via de weg van strafvervolging wegens overtreding van art. 240b Sr kan worden afgedaan indien:

---

[556] Aanwijzing Kinderpornografie (2016), a.w., par 1.4.; Beleidsnota "Pubers in Beeld", a.w., p. 4/5. Zie ook Gooren, *De strafrechtelijke bescherming van jongeren tegen seksuele contactlegging*, Tijdschrift voor Veiligheid, 2011, (10) nr. 2.

[557] Zie "Pubers in beeld" (2017), a.w., p. 2: "*Indien voor strafrechtelijk ingrijpen wordt geopteerd, verdient overweging dat een strafrechtelijke veroordeling op grond van 240b Sr (kinderpornografie) of een ander zedenfeit grote gevolgen heeft voor de toekomst van de veroordeelde. Onder andere de afgifte van een Verklaring omtrent gedrag (VOG) kan daardoor in de toekomst worden geweigerd, waardoor de arbeidsperspectieven van de veroordeelde behoorlijk worden beperkt*".

[558] Richtlijn en kader voor strafvordering jeugd en adolescenten, inclusief strafmaten Halt (2021R001) .

[559] Uit 'Pubers in Beeld' (2017), onder 2. kan worden afgeleid dat ingeval van een strafbare afbeelding van iemand onder de 12 jaar, als regel een volledig opsporingsonderzoek wordt verricht en veelal ook zal worden vervolgd.

[560] Dit criterium dient waarschijnlijk te worden gelezen in samenhang met het – hierna te bespreken - gestelde in de beleidsnota "Pubers in Beeld" (2017), a.w. onder 2., zodat daarbij meer in concreto ook aspecten als de vrijwilligheid van de seksuele gedraging (c.q. de aanwezigheid op enig moment van druk, dwang, misleiding of het bestaan van een afhankelijkheidsrelatie), de bewustheid van de afgebeelde minderjarige omtrent de vervaardiging van de afbeeldingen, en de (al dan niet affectieve) relatie tussen de afgebeelde minderjarige en de andere betrokkene(n) dienen te worden betrokken.

[561] Gezien de beleidsnota "Pubers in beeld" (2017), a.w., onder 2. gaat het daarbij onder meer om een aspect als "commerciële elementen". Anders dan voorheen wordt hierbij de mate van verspreiding van de afbeeldingen niet meer expliciet als criterium benoemd.

[562] "Pubers in beeld" (2017)

- verdachte en slachtoffer beiden minderjarig zijn (of het leeftijdsverschil tussen hen is minder dan vijf jaar, en de verdachte is jonger dan 23 jaar[563]); *én*
- het slachtoffer niet jonger is dan 12 jaar; *én*
- de verdachte niet handelde uit of met kwade intenties, zoals:
- commerciële overwegingen/bedoelingen of druk, dwang of misleiding of heimelijke opnames of vanuit een afhankelijkheidsrelatie; *én*
- geen sprake is van (aanwijzingen voor) een mogelijk ander zedenmisdrijf.

Aangaande de invulling van deze "andere afdoening" worden in de beleidsnota "Pubers in Beeld" een aantal (als "alternatieve interventies" aangeduide) voorbeelden met name genoemd, zoals:

- voorlichting door HALT of een andere instantie
- Mediation of bemiddeling
- Zorgmelding of doorverwijzing naar Veilig Thuis
- Strafbaar beeldmateriaal vrijwillig (laten) verwijderen door bezitter(s)
- Verwijzing naar informatieve en educatieve websites
- Het informeren van de school/ouders
- Groepsgesprek met betrokkenen, ten behoeve van toelichten normoverschrijding, waarschuwen voor gevolgen, toelichten consequenties bij recidive, etc.[564]

Uit "Pubers in beeld" kan tevens worden afgeleid dat niet wordt beoogd om andersoortige dan de hiervoor reeds genoemde niet-strafrechtelijke interventies (zoals bijvoorbeeld de inzet van jeugdbeschermingsmaatregelen, het inzetten van (behandel- of therapie)mogelijkheden uit de zorg of het opstarten van een mediationtraject) uit te sluiten. Integendeel, met name voor de lichtste categorie zaken[565], wordt aanbevolen om (alleen) "*alternatieve interventiemiddelen toe te laten passen door de politie, al dan niet in samenwerking met (keten)partners*."

Daarnaast geeft voormelde beleidsnota tevens aan dat voor een midden categorie van zaken[566] naast dagvaarding ook andere afdoeningsmodaliteiten zoals een Halt-afdoening[567], (voorwaardelijk) sepot dan wel OM-afdoening mogelijk zijn.[568] Ook kan in deze gevallen de vervolging wordt gebaseerd op andere strafbepalingen dan art. 240b Sr, zoals de artt. 261 Sr (smaad), 266 Sr (belediging) of de artt. 240 Sr (openbaar tentoonstellen/ongevraagd toezenden van pornografie) en 240a Sr (tonen van pornografie aan jongeren beneden de

---

[563] Uit "Pubers in beeld" (2017), a.w., onder 2. volgt dat indien de verdachte 23 jaar of ouder is, er in de visie van het OM automatisch sprake is van een zedenzaak waarbij vervolging voor de hand ligt.
[564] "Pubers in beeld" (2017), a.w., onder 3.
[565] In "Pubers in beeld" (2017), a.w., p. 4 nader omschreven als "categorie III zaken", dat zijn zaken waarin: "het beeldmateriaal op basis van vrijwilligheid tot stand lijkt te zijn gekomen, de betrokkenen minderjarig zijn (of er is een leeftijdsverschil van maximaal vijf jaar) en er is geen sprake van verzwarende omstandigheden".
[566] In "Pubers in beeld" (2017), a.w., onder 3. wordt deze zaakscategorie aangeduid als categorie II zaken, die verder (onder 2.) wordt omschreven als zaken waarin er aanwijzingen zijn dat er andere motieven dan genoemd onder categorie I een rol spelen, zoals pesten, smaad, laster of intimidatie.
[567] Ten aanzien van de (buitenstrafrechtelijke) HALT-straf verdient nog opmerking dat er sinds 1 november 2017 een specifieke interventie ("Respect online") is ontwikkeld ten aanzien van lichte vormen van online seksueel grensoverschrijdend gedrag, waaronder sexting. Zie https://www.halt.nl/samenwerken-met-halt/school/ongewenste-sexting.
[568] "Pubers in beeld" (2017), a.w., onder 3., p. 5.

16 jaar). Voordeel van de keuze voor dit laatste alternatief is dat de verdachte bij veroordeling een voor hem/haar in zijn/haar verdere leven belastend antecedent als zedendelinquent bespaard blijft.[569]

Voormelde criteria voor niet-vervolging c.q. buitengerechtelijke afdoening komen – in ieder geval thans – grotendeels overeen (maar vallen niet geheel samen) met die welke zijn af te leiden uit het arrest van de Hoge Raad van 9 februari 2016 inzake het niet als overtreding van art. 240b Sr kwalificeren van bepaalde in dat artikel omschreven gedragingen met seksueel getinte afbeeldingen van minderjarigen (met name *sexting*).[570] Naar verwachting zal – ook in deze context – over de interpretatie en waardering van al deze criteria nog wel het nodige debat worden gevoerd. Met name kan discussie bestaan over de vraag welk gewicht moet worden toegekend aan het antwoord op de vraag in hoeverre de minderjarige op het moment dat hij/zij toestemming gaf de gevolgen van de vervaardiging c.q. de verspreiding van de betreffende afbeelding(en) ook werkelijk kon overzien en/of in hoeverre die toestemming, alle omstandigheden afwegende, ook werkelijk in vrijheid kan geacht worden te zijn gegeven.[571]

Evenzo kunnen er – mede gezien de zich ontwikkelende opvattingen van onder meer de wetgever ter zake[572] – wel enige kanttekeningen worden geplaatst bij het naar het lijkt in de Afdoeningsleidraad "Puber in beeld" geformuleerde afdoeningsbeleid. Dat lijkt namelijk in het bijzonder voor die sextingzaken, waarbij uit wraak, pesterij, laster of intimidatie kinderpornografische afbeeldingen zijn verspreid, weinig punitief.[573] De vraag rijst of hierbij het belang van de betrokken minderjarige c.q. van een effectieve normhandhaving wel voldoende is meegewogen. Het is dan ook zeker denkbaar dat slachtoffers tegen sepot- en halt beslissingen uit hoofde van dit beleid door middel van een art. 12 Sv procedure bij het gerechtshof zullen opkomen.[574]

---

[569] Vgl. ook "Pubers in beeld" (2017), p. 3, 5e alinea. M.b.t. de art. 240 en 240a Sr wordt hierbij gesteld: "*Volgens huidig beleid van het COVOG wordt ten aanzien van de artt. 240 en 240a Sr , anders dan bij andere zedenartikelen, geen verlengde terugkijktermijn gehanteerd bij de beoordeling van een aanvraag voor een Verklaring Omtrent het Gedrag*". Betreffende een Halt-afdoening kan worden opgemerkt dat deze niet zichtbaar is op de justitiële documentatie, waardoor het later geen consequenties kan hebben voor de verstrekking van een VOG. Hetzelfde geldt voor een reprimande. Zie Richtlijn en kader voor strafvordering jeugd en adolescenten inclusief strafmaten Halt (2016R008).

[570] Zie hierover verder hiervoor onder 5.1.1. en 5.1.2.

[571] Relaties zijn immers lang niet altijd gelijkwaardig, en dat lijkt nog meer te gelden voor jongeren waar naast relationele onervarenheid en ongelijke ontwikkeling ook aspecten als groepsdruk en afhankelijkheid een grote rol kunnen spelen. Zeker ook bij minderjarigen wil een min of meer gelijke leeftijd nog geenszins impliceren dat ook sprake is van een gelijke ontwikkeling of gelijkwaardige relatie. In deze zin begrijpen wij ook: Hof Den Haag 7-6-2016, ECLI:NL:GHDHA:2016:1703.

[572] Op 8 oktober 2019 is bijvoorbeeld een aparte strafbaarstelling van de zogenaamde "wraakporno" in werking getreden, zie art. 139h Sr.

[573] Volgens de Leidraad komen dergelijke feiten "*over het algemeen in aanmerking voor een HALT-afdoening, (voorwaardelijk) sepot, OM-afdoening of dagvaarding*". Uit de context zou kunnen worden afgeleid dat dit laatste zeker niet als regel aan de orde zal zijn.

[574] Zie bijv. Hof Arnhem-Leeuwarden 20-12-2018, ECLI:NL:GHARL:2018:11697 (e-archief) (Afwijzing klacht, de officier van justitie kon in redelijkheid volstaan met oplegging van een strafbeschikking inhoudende een geldboete van 150 euro voor de verspreiding van naaktfoto's van het destijds 17-jarige slachtoffer, nu – ondanks de ernstige gevolgen van het feit voor het slachtoffer – de verdachte bij vervolging zou worden veroordeeld voor art. 240b Sr de gevolgen voor de toekomst voor de beklaagde te zwaar zullen zijn. Opvallend is dat het hof overweegt dat vervolging voor een lichter feit niet mogelijk zou zijn. Smaad wordt genoemd en kan als het enkel gaat om het doorsturen van een naaktfoto niet bewezen worden nu geen sprake is van 'tenlastelegging van een bepaald feit'. Waarom dan niet kon worden vervolgd voor belediging is niet nader aangeduid.)
Zie ook RB Overijssel 7-10-2019, ECLI:NL:RBOVE:2019:3530 (vervolging na geslaagde klachtprocedure nadat het slachtoffer van sexting zelfmoord pleegde(!)).

Uit het Wetsvoorstel seksuele misdrijven[575] blijkt dat niet is besloten tot een codificatie van de strafuitsluitingsgrond[576] sexting, nu volgens de wetgever "internationaalrechtelijke verplichtingen daarvoor niet voldoende ruimte laten". De wetgever stelt zich op het standpunt dat het vervolgingsbeleid voor de afdoening van sextingzaken, waarin rekening wordt gehouden met de mate van consensus bij de totstandkoming van het beeldmateriaal, en de opportuniteit van de vervolging per geval kan worden beoordeeld, voor een prudente toepassing van de nieuwe strafbaarstelling van digitale kinderpornografie (art. 252 Sr (nieuw)) in sextingzaken kan zorgen.[577]

7.2. Geldigheid tenlastelegging

Indien de officier van justitie besluit tot vervolging over te gaan, zal hij met het oog op de dagvaarding een tenlastelegging dienen op te stellen. Vooral bij gedragingen in verband met grootschaliger verzamelingen van kinderpornografisch materiaal (zoals: het bezit van honderdduizenden afbeeldingen) kan dit problematisch zijn. Reeds vanwege de omvang van het materiaal is dan immers volledige beschrijving van elk van de afbeeldingen ondoenlijk. Anderzijds dient de tenlastelegging ook voldoende feitelijk te zijn[578], met name op het punt van de omschrijving waarom de afbeeldingen kinderpornografisch zouden zijn, zodat de verdachte weet waartegen hij zich heeft te verweren.[579] Zowel het OM als de ZM hebben de laatste jaren duidelijk geworsteld met deze kwestie en dat heeft geleid tot vele varianten van tenlasteleggingen en beoordelingen. Niet zelden leidde dat ook tot tegenstrijdige uitspraken.

Het is daarom op zich niet verwonderlijk dat de Hoge Raad door het schetsen van een aantal hoofdlijnen herhaaldelijk heeft gepoogd meer lijn in de tenlasteleggingsmethodiek te brengen.[580]

7.2.1. Vindplaats, omschrijving en aantal afbeeldingen op de tenlastelegging

De huidige jurisprudentiële lijn is te kennen uit een reeks arresten van de Hoge Raad.[581] Hoewel deze lijn inmiddels als enige tijd geleden is uitgezet, werkt deze nog steeds – zowel in positieve als in negatieve zin – door in recente jurisprudentie. Om die reden gaan we er toch relatief uitgebreid op in. Zakelijk weergegeven komt de lijn op het volgende neer.

---

[575] Wijziging van het Wetboek van Strafrecht en andere wetten in verband met de modernisering van de strafbaarstelling van verschillende vormen van seksueel grensoverschrijdend gedrag (Wet seksuele misdrijven), Kamerstukken II, 2022-2023, 36 222, nr. 2.

[576] De wetgever merkt sexting aan als strafuitsluitingsgrond (en niet, zoals de Hoge Raad in zijn arrest van 9 november 2016 heeft gedaan, als buitenwettelijke kwalificatieuitsluitingsgrond). Zie: Memorie van Toelichting bij de Wet seksuele misdrijven, Kamerstukken II 2022-2023, 36 222, nr. 3, p. 57.

[577] Idem.

[578] Zie ook art. 261 Sv. Zie o.m. RB Limburg 14-12-2021, ECLI:NL:RBLIM:2021:9530 ("*In de tenlastelegging is echter maar één van de kinderpornografische video's feitelijk omschreven. De andere video's en de afbeeldingen zijn in de tenlastelegging niet nader uitgewerkt en in de tenlastelegging staat ook niet vermeld dat de wél beschreven video slechts een selectie van het aangetroffen materiaal betreft. Om die reden is de rechtbank van oordeel dat de dagvaarding ten aanzien van de niet gespecificeerde afbeeldingen en video's niet voldoet aan de eisen gesteld door art. 261 lid 1 Sr.*")

[579] Zie hierover o.m. HR 20-12-2011, ECLI:NL:HR:2011:BS1739 (HR herhaalt relevante overwegingen uit HR ECLI:NL:HR:2004:AQ3710 m.b.t het onvoldoende feitelijke betekenis hebben van de term 'afbeelding van een seksuele gedrag' en het voor de 'opgave van het feit' als bedoeld in art. 261 Sv vereist zijn van een feitelijke omschrijving van de afbeelding in de tenlastelegging. Zie ook de conclusie van de AG).

[580] Een goede samenvatting van het jurisprudentieverloop tot en met 2015 is te vinden in de Notitie van het LOVS-stafbureau van 17 november 2015, getiteld: Wijze van tenlasteleggen van art. 240b Sr en geldigheid van de dagvaarding.

[581] HR 20-12-2011, ECLI:NL:HR:2011:BS1739; HR 26-6-2014, ECLI:NL:HR:2014:1497; HR 17-11-2015, ECLI:NL:HR:2015:3322 en HR 12-12-2017, ECLI:NL:HR:2017:3124.

A. Beschrijving van slechts enkele afbeeldingen in de tenlastelegging

1. bij voorkeur worden ten hoogste vijf afbeeldingen in de tenlastelegging beschreven, "*zonder in de tenlastelegging zelf enige aanduiding van of verwijzing op te nemen naar een wellicht grotere hoeveelheid waarvan die afbeeldingen deel uitmaken*."[582]

2. Is in de tenlastelegging niet volstaan met de beschrijving van ten hoogste vijf afbeeldingen, dan geldt – op straffe van (partiële) nietigheid van de dagvaarding – dat de tenlastelegging "*ten aanzien van elk van die afbeeldingen hetzij een voldoende concrete beschrijving dient te bevatten, hetzij de vindplaats van die beschrijving in het dossier dient te vermelden*".[583]

   Overeenkomstig advocaat-generaal Aben[584] komt het ons voor dat dit niet betekent dat er niet meer gecategoriseerd mag worden en evenmin dat elke in de tenlastelegging bedoelde afbeelding bijvoorbeeld moet zijn genummerd of van een naam moet zijn voorzien.[585]
   Het impliceert echter wel dat de in de tenlastelegging bedoelde afbeeldingen voor de verdachte aanwijsbaar (en daarmee ook in het dossier en/of in het bewijsmateriaal in bredere zin) vindbaar moeten zijn.[586] Denkbaar is hierbij bijvoorbeeld dat de tenlastelegging de mapnaam vermeldt waarin de betreffende afbeeldingen gezamenlijk zijn opgeslagen, waarna de daarin opgenomen afbeeldingen (bij voorkeur met vermelding van de bestandsnaam) in de tenlastelegging worden beschreven, dan wel aldaar wordt aangegeven waar deze in het proces-verbaal zijn beschreven. Of omgekeerd: dat diverse categorieën gedragingen worden weergeven, met daarbij per categorie de vermelding van een of meer bestandsnamen en de gegevensdragers waarop deze zich zouden bevinden.[587]
   Aangenomen mag worden dat het omschrijven van de seksuele gedragingen ook categoraal mag gebeuren[588], mits de omschrijving daarbij dan wel voldoende feitelijk blijft. Zo oordeelde de Hoge Raad dat een omschrijving met betrekking tot afbeeldingen van personen beneden de leeftijd van 16 jaar "*die op zodanige wijze poseren en/of zijn afgebeeld, dat hun ontblote geslachtsdelen nadrukkelijk en/of*

---

[582] O.m. HR 12-12-2017, ECLI:NL:HR:2017:3124, r.o. 2.5. en HR 17-11-2015, ECLI:NL:HR:2015:3322, r.o. 2.5.
[583] HR 12-12-2017, ECLI:NL:HR:2017:3124, r.o. 2.6.; HR 17-11-2015, ECLI:NL:HR:2015:3322, r.o. 2.6.
[584] Zie de conclusie van AG Aben (ECLI:NL:PHR:2015:2267) bij het in de vorige noot genoemde arrest.
[585] Om diverse redenen lijkt dit laatste overigens wel de voorkeur te verdienen. De vermelding van bestandsnamen en filepaths van de betreffende afbeeldingen geeft niet alleen veel duidelijkheid over welke afbeeldingen nu precies de inzet van de zaak vormen, maar geeft veelal ook een indicatie over bijvoorbeeld de toegankelijkheid van de betreffende bestanden.
[586] Zie ook de conclusie van AG Machielse (ECLI:NL:PHR:2017:1346) bij HR 12-12-2017, ECLI:NL:HR:2017:3124, alwaar hij stelt: "*dat de rechtspraak niet als eis stelt dat de afbeeldingen worden aangeduid met kenmerk of vindplaats kan ik niet onderschrijven*".
[587] Zie bijv. Hof Den Bosch 17-10-2017, ECLI:NL:GHSHE:2017:4433 (De seksuele gedragingen zijn daarbij in vier categorieën onderverdeeld en per categorie is een nadere feitelijke omschrijving van de seksuele gedraging weergegeven, waarbij telkens als toelichting aan het eind van deze omschrijving wordt verwezen naar één of meer bestandsnamen van afbeeldingen uit de in beslag genomen collectie, met daarbij al dan niet genoemd het bronproces-verbaal waarin die afbeeldingen zouden worden beschreven. Bovendien zijn de specifieke gegevensdragers waarop zich de in de tenlastelegging genoemde afbeeldingen zouden bevinden in de tenlastelegging opgenomen. Een en ander is in het procesdossier terug te vinden. Zodoende is naar het oordeel van het hof sprake van zowel een voldoende concrete beschrijving als een vermelde vindplaats) en RB Amsterdam 28-11-2017, ECLI:NL:RBAMS:2017:8681.
[588] Vgl. ook de conclusie van AG Knigge (ECLI:NL:PHR:2012:BY4852, nr. 5.12.).

uitdagend in beeld zijn gebracht (op een wijze kennelijk bedoeld althans mede bedoeld om seksuele prikkeling op te wekken" voldoende feitelijk is.[589]

Het blijft dan echter wel scherp zeilen, want in hetzelfde arrest brak de Hoge Raad de staf over een omschrijving met betrekking tot soortgelijke afbeeldingen, die luidde: "*die (een) seksuele gedraging(en) met zichzelf en/of een of meer andere personen verrichten en/of laten verrichten (op een wijze kennelijk bedoeld althans mede bedoeld om seksuele prikkeling op te wekken en/of bestaande die seksuele gedraging(en) onder meer uit het plegen van (een) ontuchtige handeling(en) met zichzelf*".
Samengevat zou men kunnen concluderen dat de feitelijke omschrijvingen van afbeeldingen in de tenlastelegging wel in zekere mate als categorieën mogen worden aangeduid, maar dat deze categorieaanduidingen ook dan nog wel enige details van de op de afbeeldingen zichtbare seksuele gedragingen moeten bevatten.[590] In de praktijk (b)lijken de eisen met betrekking tot de omschrijving van de bestanden – ook door een soms weinig alert opereren vanuit het OM – nog steeds tot problemen te leiden. Te verwachten is echter dat deze problemen op termijn zullen afnemen, omdat het OM er thans bij het aanbrengen van nieuwe strafzaken vrijwel altijd voor kiest om in de tenlastelegging van een aantal specifiek benoemde afbeeldingsbestanden een zakelijke weergave[591] op te nemen van hetgeen op die afbeeldingen te zien is.

Voldoet de tenlastelegging niet aan de hiervoor genoemde eisen ten aanzien van de omschrijving (en vindplaats) van de afbeeldingen, dan is deze in beginsel nietig.
In voorkomende gevallen kan echter volledige nietigheid achterwege blijven als de tenlastelegging naast bijvoorbeeld meer generieke aanduidingen als "een groot aantal afbeeldingen" of "onder meer bevattende" tevens ten aanzien van een aantal afbeeldingen een voldoende concrete beschrijving bevat. Dan zal de tenlastelegging in ieder geval ten aanzien van die afbeeldingen wel als geldig kunnen worden beschouwd.[592] Voor het overige is deze dan (partieel) nietig.[593]

B. Grootschalig karakter van het delict te betrekken bij de *straftoemeting*

1. "*In geval van bewezenverklaring van het handelen van de verdachte met betrekking tot een of meer van die in de tenlastelegging omschreven afbeeldingen kan vervolgens bij de straftoemeting rekening worden gehouden met het grootschalige karakter van het delict, bijvoorbeeld op grond van de erkenning door de verdachte van het grootschalige karakter, hetgeen betekent dat de concrete afbeeldingen of de exacte hoeveelheid kinderporno niet behoeven te worden besproken, of op grond van de uitkomst van een in het voorbereidend onderzoek uitgevoerde steekproef uit het aangetroffen materiaal, mits de verdachte in de gelegenheid is gesteld de bij de steekproef gehanteerde methode aan de orde te stellen.*"

---

[589] HR 28-9-2004, ECLI:NL:HR:2004:AQ3710.
[590] In dezelfde zin: AG Aben (ECLI:NL:PHR:2015:2267) in zijn conclusie bij HR 17-11-2015, ECLI:NL:HR:2015:3322 en A.J. Machielse in Noyon, Langemeijer & Remmelink e.a. (red.), *Het Wetboek van Strafrecht (online)*, aant. 9 bij art. 240b Sr.
[591] Deze zakelijke weergave in de tenlastelegging is dan in de regel gebaseerd op een in het dossier aanwezige veel gedetailleerdere beschrijving van diezelfde afbeelding.
[592] Zie ook de conclusie van AG Aben (ECLI:NL:PHR:2017:1227) bij HR 14-11-2017, ECLI:NL:HR:2017:2854 (art. 81.1 RO) en bijv. RB Noord-Nederland 6-6-2017, ECLI:NL:RBNNE:2017:1996
[593] O.m. RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (De rechtbank verklaart de dagvaarding wat betreft de zinsnede '(onder meer)' (partieel) nietig, nu deze niet voldoet aan de eisen van art. 261 lid 1 Sv); RB Noord-Nederland 6-6-2017, ECLI:NL:RBNNE:2017:1996;

2. Volgens de Hoge Raad mag de strafrechter ook in bepaalde andere gevallen niet in de tenlastelegging feitelijk vermelde en omschreven afbeeldingen bij de straftoemeting betrekken. De Hoge Raad formuleert zulks als volgt: :
"Te denken valt aan de situatie waarin het gaat om een verzameling waarvan op grond van een in het voorbereidend onderzoek ingesteld summier onderzoek in redelijkheid mag worden verondersteld dat het gaat om materiaal dat geheel of grotendeels uit kinderporno bestaat, terwijl de verdachte hetzij die veronderstelling weliswaar niet heeft erkend doch ook niet heeft betwist, hetzij wel heeft betwist doch de juistheid van die betwisting op grond van het in het voorbereidend onderzoek verrichte onderzoek onaannemelijk is."

7.2.2. Enige kritische noten bij de huidige lijn van de Hoge Raad

Hoewel de pogingen van de Hoge Raad om lijn te brengen in de moeizame discussie over de tenlastelegging van grootschalige handelingen met betrekking tot kinderpornografisch materiaal bepaald waardering verdienen, is de wijze waarop hij dat heeft gedaan vanuit het oogpunt van zowel de feitenrechter als vanuit dat van de verdachte, het OM en benadeelde partijen/slachtoffers, niet onproblematisch. Diverse auteurs hebben zich daarover dan ook in meer of mindere mate kritisch uitgelaten.[594]

Een van de kritiekpunten is dat hetgeen de Hoge Raad (voor)schrijft ten aanzien van zaken van grootschalige kinderpornografie slechts soelaas biedt als de discussie over de niet op de tenlastelegging vermelde en omschreven afbeeldingen zich toespitst op de vraag of deze afbeeldingen als kinderpornografisch zijn te kwalificeren of niet.[595] In de recht(er)spraktijk is dat aspect in de regel echter niet het punt van discussie. Daar gaat het vaker om de vraag of de verdachte *opzet* had op het bezit/verspreiden (etc.) van (ook) het niet op de tenlastelegging omschreven materiaal. De lijn van de Hoge Raad geeft echter voor de oplossing van deze problematiek geen bruikbare handvatten, met name niet in de veel voorkomende gevallen dat de verdachte zich op zijn zwijgrecht beroept en het dossier zelf te weinig gedetailleerde informatie bevat om te kunnen beoordelen in hoeverre er (ook) ten aanzien van de gedragingen met de grote aantallen niet op de tenlastelegging opgenomen/uitgeschreven afbeeldingen (in beginsel) opzet aanwezig kan worden geacht.[596] In dit verband wordt opgemerkt dat inbeslaggenomen afbeeldingen vaak op verschillende gegevensdragers/partities/bestandsmappen staan, zodat niet zonder meer kan worden aangenomen dat wat ten aanzien van de in de tenlastelegging/bewezenverklaring genoemde afbeeldingen geldt, evenzeer geldt voor die afbeeldingen die *niet* in de tenlastelegging zijn genoemd.

---

[594] Zie o.m. Reijntjes in zijn noot bij *NJ* 2014/339: "*Dit is niet alleen onduidelijk, maar - voor zover begrijpelijk - ook erg ruim geformuleerd*"; M.J. Borgers, Vervolging en bestraffing van grootschalig bezit van kinderpornografie , DD 2014/47 (afl. 7), p. 499-511. Zie met betrekking tot de gevolgen van de lijn van de Hoge Raad voor benadeelde partijen/slachtoffers: Mr. C.E. Dettmeijer-Vermeulen en mr. L. van Krimpen, *Schadevergoeding voor bezit van kinderpornografie: juridische mogelijkheden en praktische obstakels*, Tijdschrift Praktijkwijzer Strafrecht (TPWS) 2014/26, onder 2.1.

[595] Zie bijv. Gerechtshof 's-Hertogenbosch 10-02-2014, ECLI:NL:GHSHE:2014:317; Vgl. ook Reijntjes in zijn noot bij *NJ* 2014/339, onder 6.

[596] Politieprocessen-verbaal hebben m.b.t. de niet op de tenlastelegging omschreven afbeeldingen in de regel niet het vereiste detailniveau (qua bestandsnaam, *filepath* (of andere aanduiding van vindplaats op de computer/gegevensdrager), datering en toegankelijkheid) om zelfs op hoofdlijnen te kunnen beoordelen of (ook) ten aanzien van die afbeeldingen (waarschijnlijk) sprake is van opzet; een dergelijke weergave is bij grote aantallen ook problematisch omdat zulks – bij een ontkennende c.q. zwijgende verdachte − feitelijk een gedetailleerde beschrijving van (alle) vindplaatsen (o.m. in de vorm van *filepaths)* van (al) die afbeeldingen op de computer/gegevensdrager met zich zou brengen.

Daarbij komt dat de door de Hoge Raad dringend geadviseerde beperking tot (slechts) vijf afbeeldingen, het debat op de zitting feitelijk wordt verengd tot een bespreking en beoordeling van (alleen) die vijf afbeeldingen. De eventuele aanwezigheid van veel grotere aantallen kinderpornografische afbeeldingen wordt namelijk alleen relevant als in ieder geval de op de tenlastelegging omschreven gedragingen met betrekking tot (tenminste één van) deze vijf afbeeldingen bewezen kunnen worden verklaard. Zo niet, dan volgt immers zonder meer vrijspraak, ook als er verder honderdduizenden andere afbeeldingen zouden zijn aangetroffen.[597]
Dit leidt er toe dat ten aanzien van de vijf wél vermelde afbeeldingen er in toenemende mate zeer uitvoerig en (technisch) gedetailleerd verweer wordt gevoerd. Het strafdossier is echter veelal niet geschreven op een dergelijk gedetailleerd niveau. Dat is immers zeer bewerkelijk als het gaat om grote aantallen afbeeldingen, terwijl het gecompliceerd is om reeds in een vrij vroeg stadium van het politieonderzoek een verantwoorde keuze te maken uit een beperkt aantal afbeeldingen ten aanzien waarvan wel uitvoeriger gedetailleerde gegevens in het proces-verbaal worden weergegeven. Daardoor doen zich vervolgens nogal eens aanzienlijke bewijsproblemen (ook ten aanzien van de strafverzwarende kwalificatie “een gewoonte maken van”) voor. In dat verband blijkt het ook nogal eens belemmerend te werken dat de strafrechter door de tenlastelegging feitelijk gedwongen wordt tot een vorm van blikvernauwing, en dat hetgeen met betrekking tot (soms: duizenden) andere afbeeldingen blijkt niet of slechts zeer beperkt bij zijn bewijsbeoordeling ten aanzien van de op de tenlastelegging vermelde afbeeldingen kan worden betrokken. Deze “blikvernauwing” leidt bovendien tijdens het onderzoek ter terechtzitting tot het ondersneeuwen van de omvang van de gepleegde feiten, zowel voor de verdachte als voor het publiek.[598]

Een derde kritiekpunt betreft de gevolgen van de lijn van de Hoge Raad. Deze heeft al geleid tot een groot aantal (partieel) nietig verklaarde dagvaardingen[599] en (deel)vrijspraken.[600] Daardoor komt allereerst de effectieve normhandhaving ter zake van overtreding van art. 240b Sr in het geding. Aan de andere kant leidt hetgeen de Hoge Raad voorschrijft soms tot veroordelingen tot aanzienlijke gevangenisstraffen waar *de jure* en *de facto* slechts het bezit (etc.) van slechts 1 of 2 concrete afbeeldingen bewezen is verklaard. Zeker vanuit een verdedigingsoogpunt is deze onbalans niet onproblematisch; de verdachte wordt dan feitelijk voor veel meer veroordeeld dan hij in ieder geval op grond van de tenlastelegging kon verwachten.

Concluderend lijkt het erop dat door voormelde lijn van de Hoge Raad de problemen rond de tenlastelegging van grootschalige kinderpornografie nog zeker niet zijn opgelost en deze

---

[597] Zie in dit verband bijvoorbeeld Hof Arnhem-Leeuwarden 11-12-2019, ECLI:NL:GHARL:2019:11285, waarin een partiële vrijspraak volgde ten aanzien van de ten laste gelegde gedragingen verspreiden en aanbieden. In die zaak bleek weliswaar aan de hand van screenshots dat de verdachte bestanden met kinderpornografische termen in de bestandsnamen had verzonden via P2P-programma Gigatribe, maar waren de betreffende bestanden niet ten laste gelegd en evenmin nader aangeduid of omschreven in het dossier.
[598] Vgl. in deze ook Reijntjes in zijn noot bij HR 24-6- 2014, ECLI:NL:HR:2014:1497, *NJ* 2014/339.
[599] Het aantal gepubliceerde uitspraken waarin een dagvaarding ter zake art. 240b Sr (partieel) nietig wordt verklaard, is echter gering. Een zoekslag op rechtspraak.nl op de zoektermen “240b Sr”, “geldigheid dagvaarding” en “nietig” levert voor de periode van 1 januari 2014 tot 1 april 2023 ‘slechts’ 8 uitspraken op, namelijk: Hof Den Bosch 28-1-2022, ECLI:NL:GHSHE:2022:232, RB Rotterdam 14-12-2020, ECLI:NL:RBROT:2020:11534, RB Rotterdam 7-7-2016, ECLI:NL:RBROT:2016:5146, RB Noord-Holland 21-5-2015, ECLI:NL:RBNHO:2015:6391, RB Noord-Holland, 9-4-2015, ECLI:NL:RBNHO:2015:2987, RB Noord-Holland, 25-9-2014, ECLI:NL:RBNHO:2014:13120, RB Noord-Holland 27-5-2014, ECLI:NL:RBNHO:2014:4798, RB Noord-Holland 13-5-2014, ECLI:NL:RBNHO:2014:13124.
[600] Een zoekslag op rechtspraak.nl op de zoektermen “kinderporno en “240b Sr” voor de periode van 1 november 2022 tot 1 april 2023 leert dat het voor die periode (reeds) 15 uitspraken betreft (van in totaal 104 doorgenomen uitspraken; aldus een percentage van ruim 14%).

vanuit het oogpunt van de (effectiviteit van de) strafrechtspleging zelfs een aantal negatieve gevolgen heeft gehad. De oplossing moet hier wellicht worden gezocht in het bij grote aantallen afbeeldingen binnen zekere kaders aanvaarden van een meer categorale aanduiding en omschrijving van de afbeeldingen en de daarop zichtbare seksuele gedragingen in de tenlastelegging.[601] Het komt ons voor dat zulks in veruit de meeste gevallen voor een verdachte voldoende (en zelfs meer dan thans) duidelijk zal maken, waartegen hij zich dient te verdedigen.
Het is aannemelijk dat de Hoge Raad ook reeds thans onder zekere condities een dergelijke meer categorale tenlastelegging mogelijk acht[602], maar vastgesteld kan worden dat een dergelijke opvatting op dit moment in ieder geval feitelijk door het OM niet meer wordt toegepast[603] en door de feitenrechters niet als zodanig wordt (h)erkend.[604] Meer duidelijkheid daaromtrent zou daarom wenselijk zijn.

7.3. Rechtmatigheid verkrijging bewijsmateriaal

Regelmatig wordt in art. 240b-zaken een beroep gedaan op gesteld onrechtmatige verkrijging van het bewijs. Dit is ook begrijpelijk in het licht van het feit dat in deze zaken het bewijs overwegend wordt verkregen door onderzoek aan onder de verdachte inbeslaggenomen computersystemen en gegevensdragers. Uitsluiting van het bewijs van de resultaten van onderzoek aan deze systemen c.q. gegevensdragers zal dan ook in zeer veel gevallen tot vrijspraak leiden. Hoewel de Hoge Raad thans hoge eisen stelt aan bewijsuitsluiting als reactie op eventuele vormverzuimen[605], is er derhalve toch aanleiding een aantal meer op art. 240b Sr toegespitste situaties nader onder de loep te nemen.

7.3.1. "Voldoende verdenking"

---

[601] Voorbeelden van tenlasteleggingen langs deze lijn, die in ieder geval genade bij de feitenrechters konden vinden, zijn bijvoorbeeld Hof Amsterdam 9-5-2016, ECLI:NL:GHAMS:2016:1777 (OM-appel na nietigverklaring inleidende dagvaarding. Tenlastelegging kleinschalig bezit van kinderporno. Er is geen uitgebreide beschrijving van de verweten afbeeldingen in de tenlastelegging of in een proces-verbaal. De verdachte stelde dat hij niet weet waartegen hij zich moet verdedigen. In hoger beroep heeft de advocaat-generaal hierop de afbeeldingen achter gesloten deuren aan het hof en de verdachte getoond. *Hof: tenlastelegging voldoende feitelijk*, *gelet op verhandelde ter terechtzitting in hoger beroep*. Volgt terugwijzing); Hof Arnhem-Leeuwarden 29-4-2015, ECLI:NL:GHARL:2015:3878); RB Rotterdam 10-11-2015, ECLI:NL:RBROT:2015:8250, deels ook Hof Amsterdam 29-10-2015, ECLI:NL:GHAMS:2015:4435.
[602] Zie r.o. 2.6. in HR 17-11-2015, ECLI:NL:HR:2015:3322, AG Aben in zijn conclusie (ECLI:NL:PHR:2015:2267) bij HR 17-11-2015, ECLI:NL:HR:2015:3322 en het hiervoor in deze paragraaf onder A.2. gestelde.
[603] Blijkens vanuit het OM aan de oorspronkelijk auteur in juni 2017 verstrekte informatie is het dringende advies aan officieren van justitie thans dat een beperkt aantal afbeeldingen in de tenlastelegging dient te worden opgenomen. Dat mogen er meer dan 5 zijn indien dat nodig is i.v.m. het aantal gegevensdragers, de pleegperiode, de bewijsbaarheid van opzet of de verschillende aard van de afbeeldingen. Van deze afbeeldingen worden ook in de tenlastelegging de bestandsnamen benoemd en waar mogelijk de vindplaats in het dossier aangegeven.
[604] Zie bijv. RB Midden-Nederland 4-5-2016, ECLI:NL:RBMNE:2016:2523 (De rechtbank verklaart, gelet op het arrest van de Hoge Raad van 17-11- 2015 (ECLI:NL:HR:2015:3322), de dagvaarding nietig omdat deze niet voldoet aan de eisen van het Wetboek van Strafvordering. In de onderhavige tenlastelegging wordt *een zakelijke weergave gegeven* van wat er op de *63019* afbeeldingen te zien is. De tenlastelegging beperkt zich hiermee niet tot een beschrijving van een beperkte selectie afbeeldingen. Uit het arrest van de Hoge Raad volgt dat de tenlastelegging zich bij voorkeur zou moeten beperken tot het beschrijven van een selectie van een gering aantal afbeeldingen – zo mogelijk ten hoogste vijf – zonder in de tenlastelegging zelf enige aanduiding van of verwijzing op te nemen naar een wellicht grotere hoeveelheid waarvan die afbeeldingen deel uitmaken. De rechtbank zal om die reden de tenlastelegging nietig verklaren.) en Hof Den Bosch 24-8-2016, ECLI:NL:GHSHE:2016:3767 (Ambtshalve partiële nietigheid van de dagvaarding t.a.v. de aantallen kinderporno).
[605] Zie Hoge Raad 19-2-2013, ECLI:NL:HR:2013:BY5321, *NJ* 2013/308.

Zoals hiervoor[606] omschreven worden de meeste politieonderzoeken in verband met kinderpornografisch materiaal geïnitieerd door meldingen vanuit NCMEC of derden zoals buitenlandse justitiële autoriteiten, burgers en bedrijven zoals internetserviceproviders en communicatiedienstenaanbieders. Gewoonlijk via het IP-adres komt dan meestal ook (de naam en het adres van) een bepaalde verdachte in beeld, waarna de politie de verdachte benadert, hetzij met een verzoek tot uitlevering hetzij in het kader van een doorzoeking. De rechtspraak lijkt er geen moeite mee te hebben om – al dan niet met verwijzing naar het interstatelijke vertrouwensbeginsel[607] – een melding als hier bedoeld in combinatie met een concrete link (bijvoorbeeld de link IP-adres – naam, adres, woonplaats van een bepaalde persoon) aan te merken als voldoende feitelijke grondslag om een redelijk vermoeden van schuld aan een strafbaar feit (en de inzet van dwangmiddelen) op te baseren.[608] Evenmin lijken daarbij hoge eisen te worden gesteld aan de actualiteit van de melding.[609]

7.3.2. Doorzoeking woning na toestemming

In voorkomende gevallen wordt wel het verweer gevoerd, dat de verdachte weliswaar toestemming heeft gegeven voor een betreding of doorzoeking, maar dat deze toestemming niet gevraagd had mogen worden en mitsdien het verkregen bewijs onrechtmatig zou zijn. In dit kader wordt allereerst opgemerkt, dat volgens vaste rechtspraak van de Hoge Raad bij toestemming van een bewoner voor de doorzoeking van zijn woning (of voor enige andere onderzoekshandeling) niet van het gebruik van een dwangmiddel kan worden gesproken zodat ook de daarvoor in de wet neergelegde voorwaarden (waaronder het aanwezig zijn van een redelijk vermoeden van schuld) niet van toepassing zijn.[610]

Het voorgaande impliceert echter niet dat het doorzoeken van de woning van een bewoner met diens toestemming geheel van rechterlijke toetsing is gevrijwaard. Ook in het geval van gegeven toestemming kan de reden van doorzoeking zodanig vaag zijn of kan doorzoeking van zodanige mate van willekeur getuigen dat een ontoelaatbare inbreuk op de persoonlijke levenssfeer moet worden aangenomen.[611] Bij de toetsing van de rechtmatigheid van een

---

[606] Zie par. 6.1.1.

[607] Zie hieromtrent HR 31-1-2006, ECLI:NL:HR:2006:AU3426 en meer specifiek met betrekking tot kinderporno o.m. RB Rotterdam 31-3-2011, ECLI:NL:RBROT:2011:BP9776.

[608] Zie bijvoorbeeld RB Utrecht 5-4-2013, ECLI:NL:RBMNE:2013:BZ7922 (redelijk vermoeden van schuld t.t.v. doorzoeking, ondanks dat vier jaar was verstreken tussen moment van toegang tot kinderpornografische website en moment doorzoeking. "*Het is een feit van algemene bekendheid dat mensen die kinderporno bekijken en downloaden daar in de meeste gevallen niet zomaar mee stoppen en dat men de afbeeldingen pleegt te bewaren. De rechtbank is dan ook van oordeel dat in de onderhavige zaak door de aard van het feit het tijdsverloop het redelijk vermoeden van schuld niet wegneemt*.". Zie voor een nadere bespreking van de mogelijke kwetsbaarheid van (alleen) een IP-adres als basis voor het aannemen van een redelijke verdenking ook hiervoor 6.2.6.

[609] Zie bijv RB Oost-Brabant 16-9-2021, ECLI:NL:RBOBR:2021:4921 ("*In de periode van 2016 t/m 2019 heeft de politie meldingen ontvangen van onder meer voetbalverenigingen over een onbekend persoon die zich als voetbalscout voordeed en minderjarige voetballers benaderde met het voorstel om zich naakt te filmen zodat hij kon beoordelen of ze geschikt waren voor een voetbalschool. In diezelfde periode ontving het Amerikaanse National Center for Msising and Exploited Children (NCMEC) via haar cybertiplijn meldingen over kinderpornografie op het internet, die zijn doorgeleid naar de Nederlandse politie. (...) In 2019 volgden verschillende NCMEC-meldingen met uiteindelijk ook gegevens betreffende de identiteit van verdachte*."). en RB Utrecht 22-6-2010, ECLI:NL:RBUTR:2010:BN2195 ("Niet ten aanzien van alle strafbare feiten in het algemeen kan worden gezegd dat het tijdsverloop het redelijk vermoeden van schuld wegneemt. De aard van het feit is daarbij van belang. Door de aard van het onderhavige feit is de rechtbank van oordeel dat op basis van de CIE-startinformatie (van meer dan *een jaar* daarvoor; *auteurs*) van de politie op 15 februari 2007 rechtmatig in de woning is binnengetreden."

[610] Zie o.m. HR 18-12-2012, ECLI:NL:HR:2012:BY5315 en HR 1-2-2000, *NJ* 2000/264.

[611] Aldus AG Machielse in zijn conclusie ECLI:NL:PHR:2008:BC5944 bij HR 8-4-2008, ECLI:NL:HR:2008:BC5944.

doorzoeking kan door de strafrechter bovendien tevens worden beoordeeld in hoeverre de toestemming van een bewoner voor doorzoeking van zijn woning daadwerkelijk in vrijheid is gegeven.

7.3.3. Doorzoeking computer/smartphone zonder toestemming

Er is echter discussie ontstaan over de vraag of het door de politie in beslag nemen en onderzoeken van computers en andere gegevensdragers (waaronder een smartphone) zonder specifieke wettelijke grondslag[612] of rechterlijke toetsing in overeenstemming is met art. 8 EVRM. In dat kader is van belang dat kinderpornografisch materiaal tegenwoordig ook op dergelijke *devices* aanwezig kan zijn, en dat daarvan bijvoorbeeld ook in het kader van de opsporing van andersoortige strafbare feiten kan blijken.

Genoemde discussie is mede ingegeven door het gegeven dat *smartphones* zich hebben ontwikkeld tot hoogwaardige elektronische apparaten met aanzienlijke opslagcapaciteit en diverse communicatiemethoden, die bij uitstek worden gebruikt voor het opslaan en uitwisselen van zeer persoonlijke informatie.

Op 4 april 2017 heeft de Hoge Raad een aantal arresten gewezen met betrekking tot deze problematiek. Deze arresten zijn reeds besproken in paragraaf 6.1.2., waarnaar hier dan ook kortheidshalve wordt verwezen.

7.3.4. "Uitlokking" door Nederlandse opsporingsinstanties

Ingevolge de Nederlandse wet en de jurisprudentie van het EHRM is "uitlokking" van een strafbaar feit door opsporingsautoriteiten niet toegestaan. "Uitlokking" dient hierbij te worden verstaan als "een verdachte brengen tot andere handelingen dan die waarop zijn opzet reeds was gericht".[613] Acties waarbij zogenaamde lokmiddelen zoals bijvoorbeeld het neerzetten van een (niet afgesloten) lokfiets, worden ingezet, vallen hier niet onder omdat door het neerzetten van een dergelijke fiets een verdachte niet wordt gebracht tot andere handelingen dan die waarop zijn opzet reeds tevoren was gericht. Dergelijke ongerichte uitlokking met behulp van lokmiddelen is door de Hoge Raad in algemene zin aanvaard.[614]

In dit kader verdient opmerking dat de politie in het verleden zogenaamde lokwebhops heeft opgezet waarop illegaal vuurwerk werd aangeboden om het adres en het e-mailadres van potentiële kopers te achterhalen.[615] Betrokkenen kregen daarop persoonlijk een waarschuwing omtrent hun illegale gedrag. Er zijn thans echter geen aanwijzingen dat Nederlandse opsporingsambtenaren zich ook in het kader van de opsporing van art. 240b-feiten zouden (willen) bedienen van lokmiddelen zoals bijvoorbeeld het op internet aanbieden van (pseudo-) kinderpornografisch materiaal. Het kan echter niet worden uitgesloten dat zulks in navolging van buitenlandse opsporingsactiviteiten en/of in Europol verband in de toekomst wel het geval zal zijn.[616]

---

[612] Het lijkt niet onwaarschijnlijk dat de juist in het kader van art. 240b-onderzoeken gehandhaafde mogelijkheid om ex art. 551 Sv uitlevering te vragen in het specifieke kader van dergelijke zaken wel als een wettelijke grondslag voor inbeslagname en onderzoek kan worden aangemerkt.

[613] HR 4-12-1979, ECLI:HR:1979:AB7429 (n.g.); *NJ* 1980/356 met annotatie van Th.W. van Veen (*Tallon*-arrest).

[614] HR 28-10-2008, *NJ* 2009, 224 m.nt. M.J. Borgers (lokfiets-arrest); HR 6-10-2009, ECLI:NL:HR:2009:BI7084 (lokauto-arrest).

[615] Zie de webpublicatie Na lokfiets en lok-oma nu lokwebshop van politie d.d. 16 december 2013.

[616] Zie daarover hierna onder 7.3.5.
Een voorbeeld van hoe vergaand deze praktijk kan zijn betreft de overname van Child Play, een *hidden service* op het darkweb. De Australische politie nam deze in het geheim over na arrestatie van de oprichter. Vervolgens

Wel is er sprake van geweest dat een NGO beelden van een virtuele minderjarige vervaardigde en op het internet plaatste met de bedoeling te onderzoeken in hoeverre daarop door personen met seksuele intenties zou worden gereageerd.[617] De beelden zelf waren echter niet als kinderpornografisch aan te merken, zodat een en ander buiten het bereik van art. 240b Sr bleef. Evenzo is niet direct een relatie te leggen tussen de opsporing van art. 240b-feiten en de thans nog niet juridisch werkbaar gebleken[618] inzet van politieambtenaren die zich in chatrooms voordoen als minderjarigen om zicht te krijgen op personen die zich mogelijk schuldig zouden maken aan "*grooming*" of andere seksuele misdrijven met minderjarigen. Ondenkbaar is echter een dergelijke relatie niet, met name niet indien in het kader van de contacten tussen een niet als zodanig herkenbare opsporingsambtenaar en "geïnteresseerde" door de laatste (ook) kinderpornografisch materiaal met de opsporingsambtenaar wordt gedeeld of wordt voorgesteld dergelijk materiaal te delen. Of dan sprake is van uitlokking zal via de hiervoor besproken gebruikelijke maatstaf van het *Tallon*-criterium moeten worden beoordeeld.

Sinds 1 maart 2019 is art. 248e Sr (betreffende "*grooming*") zodanig gewijzigd dat daarin uitdrukkelijk strafbaar is gesteld "*grooming*" door "iemand die zich, al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van zestien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van zestien jaren nog niet heeft bereikt (…)"[619]. Hiermee is het in beginsel wel mogelijk geworden om zich als minderjarigen voordoende opsporingsambtenaren als bijvoorbeeld "lokpuber" in te zetten[620]. Minister Grapperhaus van Justitie en Veiligheid heeft in een Kamerbrief van 1 maart 2019 meegedeeld dat alleen opsporingsambtenaren onder voorwaarden bevoegd zijn tot het voor opsporingsdoeleinden inzetten van lokmiddelen omdat hun optreden met waarborgen omkleed en aan wettelijke regels gebonden is, om burgers te beschermen tegen ongerechtvaardigde

---

heeft men gedurende een jaar de site in de lucht gehouden en ook kinderpornografisch materiaal gedeeld om argwaan te voorkomen. Zie The Guardian 7-10-2017. In toenemende mate wordt ook gebruik gemaakt van *forensic linguistic techniques* om de gebruikers van kinderpornofora op het darkweb door middel van interactie (chatten) te kunnen ontmaskeren. Een recenter voorbeeld van die succesvolle aanpak vormt de ontmaskering van een *administrator* van een forum op het darkweb genaamd Babyheart. Aannemelijk is dat in dat geval van de zijde van de verdediging zal worden betoogd, dat zulks een vorm van niet toelaatbare uitlokking inhoudt, vgl. S.F.J. Smeets, *De 'lokpuber': een mislukt experiment*, Strafblad 2013/4.

[617] Het zogenaamde Sweetie-project van Terre des Hommes wordt omschreven op: https://www.terredeshommes.nl/nl/programmas/sweetie.

[618] Het Hof Den Haag honoreerde op 25 juni 2013 een bezwaarschrift tegen de dagvaarding (wegens *grooming*) omdat communicatie met de volwassen verbalisanten niet kon worden aangemerkt als "*grooming* van een minderjarige". Deze uitspraak is niet gepubliceerd maar grotendeels te kennen uit S.F.J. Smeets, *De 'lokpuber': een mislukt experiment*, Strafblad 2013/4, p. 333..

[619] Interessant in dit verband is RB Overijssel 16 juli 2021, ECLI:NL:RBOVE:2021:2881. Ontslag van alle rechtsvervolging (OVAR) wegens niet-kwalificeerbaarheid van het feit, i.v.m. de tussentijds (per 1 maart 2019) gewijzigde delictsomschrijving van art. 248e Sr. Het onderdeel "*enige handeling onderneemt gericht op het verwezenlijken van die ontmoeting*" ontbreekt in de tenlastelegging. Tevens is in de tenlastelegging niet omschreven welke handelingen de man zou hebben verricht tot het verwezenlijken van die ontmoeting.

[620] Een interessant geval deed zich voor in RB Midden-Nederland 17-11-2015, ECLI:NL:RBMNE:2015:9631. In casu had de vader van aangeefster zich voorgedaan als aangeefster (zijn minderjarige dochter). De raadsman heeft onder verwijzing naar een brief van de minister van Justitie van 23 september 2015 bepleit dat de inzet van meerderjarige opsporingsambtenaren die zich "online" voordoen als minderjarige inmiddels zou zijn gestaakt, hetgeen consequenties heeft voor de ontvankelijkheid. De rechtbank heeft het niet-ontvankelijkheidsverweer van de raadsman als onvoldoende onderbouwd verworpen, en daartoe onder meer overwogen dat de door de raadsman aangehaalde brief enkel ziet op de inzet van opsporingsambtenaren en niet op handelen van burgers. De rechtbank overwoog voorts: "*hierbij heeft het gesprek zich tussen de vader en de verdachte bovendien zodanig inhoudelijk ontwikkeld, dat niet gesteld kan worden dat de verdachte andere vragen zou hebben gesteld of andere opmerkingen zou hebben gemaakt, dan hij heeft gedaan, indien verdachte wel daadwerkelijk met [slachtoffer 2] had gecommuniceerd tijdens het betreffende gesprek. De vader heeft enkel vragen van de verdachte beantwoord, alsof hij zijn dochter was*."

inbreuken op hun recht op privacy en het recht op een eerlijk proces, en dat hij hierover met Terre des Hommes in gesprek is.[621]

7.3.5. Bewijsmateriaal afkomstig van buitenlandse autoriteiten
Zoals hierboven reeds aangegeven komt het met enige regelmaat voor dat de verdenking tegen een verdachte mede is gebaseerd op informatie van buitenlandse justitiële instanties.[622]

Sommige van deze instanties hanteren (ook) in het kader van de bestrijding van kinderpornografie soms andere (en verdergaande) methoden dan in Nederland gebruikelijk dan wel toegestaan. Met name gaat het dan om de inzet van middelen die naar Nederlands recht mogelijk als niet rechtmatige infiltratie of uitlokking zouden worden aangemerkt. Zo is bijvoorbeeld gebleken dat de Amerikaanse FBI fakelinks naar niet bestaande kinderpornovideo's heeft gebruikt om "geïnteresseerden" in kinderpornografisch materiaal in beeld te krijgen[623] of met dezelfde bedoeling kinderporno-sites na overname door de politie nog enige tijd in de lucht heeft gehouden.[624] Ook komt het voor dat men undercover-agenten inzet in chatfora.[625] Indien daarbij tot Nederland te herleiden personen in beeld komen wordt deze informatie normaliter ook gedeeld met de Nederlandse opsporingsautoriteiten.

In zijn algemeenheid zal dergelijke van buitenlandse autoriteiten rechtmatig verkregen informatie in het kader van het Nederlandse strafproces als rechtmatig kunnen worden aangemerkt. Het is daarbij in beginsel niet aan de Nederlandse strafrechter om de rechtmatigheid van de verkrijging van de betreffende gegevens door de buitenlandse autoriteiten op grondslag van het Nederlandse recht (zoals bijvoorbeeld het Tallon-criterium) te onderzoeken. Uitgangspunt is immers het interstatelijke vertrouwensbeginsel, dat inhoudt dat de strafrechter er op mag vertrouwen dat deze autoriteiten van die vreemde staat de hun toegekende opsporingsbevoegdheden overeenkomstig hun wettelijke systeem zullen uitoefenen.[626] Dit kan echter anders zijn indien de bewijsgaring door de buitenlandse autoriteiten een kennelijke inbreuk oplevert op verdragsrechtelijk beschermde mensenrechten[627], waarbij mede van belang is of de verdachte daardoor is geschaad in een jegens hem te respecteren belang. Een uitzondering op genoemde hoofdregel kan voorts aan de orde zijn indien sprake is van een als ontoelaatbaar aan te merken eigen betrokkenheid van

---

[621] Brief d.d. 1 maart 2019 aan de Voorzitter van de Tweede Kamer der Staten-Generaal. Zie ook: A. de Hingh, "Grooming in het wetsvoorstel Computercriminaliteit III. Over het verbod op sexchatten met kinderen, robots en politieambtenaren.", Computerrecht 2018/162.
[622] Zie bijvoorbeeld RB Overijssel 28-11-2017, ECLI:NL:RBOVE:2017:4443 (uit een Nieuw Zeelands politieonderzoek is informatie verkregen, afkomstig uit chatberichten van een forum op het "darknet". Op dat forum hebben liefhebbers van seksueel misbruik van kinderen in de leeftijd tussen de 5 en 16 jaar contact met elkaar. Uit de verkregen chatberichten bleek onder meer dat aan deze chatcommunicatie werd deelgenomen door een persoon, waarvan het vermoeden was gerezen dat het een persoon met de Nederlandse nationaliteit betrof. Gedurende het strafrechtelijk onderzoek is de TOR-site van verdachte benaderd en is een grote hoeveelheid kinderpornografische afbeeldingen (113.425 foto's en 58 video's) gedownload.
[623] Bron: CNET, FBI posts fake hyperlinks to snare child porn suspects d.d. 20 maart 2008.
[624] Bron: The Independent, International child abuse ring dismantled by police who ran fake sites to identify abusers, d.d. 5 maart 2016.
[625] Zie bijv. RB Den Haag 24-8-2017, ECLI:NL:RBDHA:2017:9578 (zaak komt uit FBI-onderzoek, verdachte chatte met undercover agent via chatprogramma).
[626] Aldus ook bijv. RB Noord-Nederland 27-7-2017, ECLI:NL:RBNNE:2017:2882 (n.o.-verweer inzake onderzoekresultaten uit Zwitserland verworpen onder verwijzing naar interstatelijk vertrouwensbeginsel).
[627] Gedacht kan daarbij worden aan situaties waarin sprake is of zou kunnen zijn van het niet respecteren van verdedigingsrechten zoals die voortvloeien uit het EVRM (vgl. EHRM 27 juni 2000, *NJ* 2002, 102 en HR 31 januari 2006, ECLI:NL:HR:2006:AU3446, *NJ* 2006, 365), of waarin sprake is van bijvoorbeeld overtreding van het *nullem crimen*-beginsel door toepassing van een als marteling aan te merken verhoormethode.

de Nederlandse opsporingsautoriteiten bij de buitenlandse bewijsverkrijging.[628] Daarbij kan gedacht worden aan een verzoek aan de betreffende buitenlandse autoriteit om een bepaalde verdachte "uit te lokken" tot een bepaalde gedraging, of het erin bewilligen dat een dergelijke gedraging op Nederlands grondgebied plaatsvindt.

7.4. Voorbereidend onderzoek

In algemene zin zijn kinderpornozaken strafzaken als alle andere en zijn dus in beginsel ook de algemene strafvorderlijke regels omtrent bijvoorbeeld de inhoud van het dossier, het horen van getuigen en deskundigen en het laten verrichten van een tegenonderzoek door deskundigen van toepassing. Maar er bestaan ook een aantal verschillen, die te maken hebben met de specifieke aard van het betreffende (gestelde) kinderpornografische materiaal en met het in sommige gevallen specifieke rechterlijke toetsingskader.

7.4.1. Onderzoeksmateriaal/gegevensdragers/toonmap: processtuk?

Lange tijd is gediscussieerd over de vraag in hoeverre gesteld kinderpornografisch materiaal deel moet uitmaken van het procesdossier waarop de strafrechter recht doet. Aan de ene zijde van de discussie bevond zich over het algemeen het Openbaar Ministerie, dat zich principieel verzette tegen de toevoeging van door hen als kinderpornografisch gekwalificeerde afbeeldingen aan het strafdossier. Dat verzet was ingegeven door de wens dergelijke afbeeldingen niet verder te willen verspreiden en/of wederom (ook) aan de verdachte te openbaren.[629]

Aan de andere zijde vond men veelal raadslieden, NGO's die zich sterk maken voor jeugdige slachtoffers van seksueel misbruik en soms ook een bewindspersoon. De redenen waarom men toevoeging aan het dossier wenste waren overigens nogal uiteenlopend. Zo voerden kinderbeschermingsorganisaties, opsporingsdiensten[630] en bedoelde bewindspersoon[631] wel aan dat kennisname door de rechter van het – veelal schokkende – materiaal zou leiden tot hogere straffen. Raadslieden voerden veelal aan dat zij zelf wilden kunnen (laten) beoordelen of een afbeelding als (kinder)pornografisch moet worden beschouwd.

In de recht(er)spraktijk lijkt thans echter zeer breed aanvaard, dat de gesteld kinderpornografische afbeeldingen niet standaard door het OM in het procesdossier behoeven te worden gevoegd. Evenmin wordt aangenomen dat de raadsman recht heeft op toezending van papieren of digitale afschriften van de betreffende afbeeldingen. De gegevensdragers zelf worden om die reden evenmin als processtuk aan het dossier toegevoegd of aan de raadsman verstrekt.[632]

---

[628] Vgl. in die zin ook bijv. RB Haarlem 2-8-2012, ECLI:NL:RBHAA:2012:BX4050.

[629] Aanwijzing Kinderpornografie (2016A005), onder 2.4. Hoewel de afbeeldingen formeel geen processtuk zijn zou vanuit de gedachte dat hetgeen is toegestaan ten aanzien van processtukken zeker ook heeft te gelden voor niet-processtukken kunnen worden betoogd dat de wettelijke grondslag voor de hier bedoelde niet verstrekking is gelegen in het gestelde in art. 32, lid 2 Sv.

[630] Zie bijv. H. Schaafsma, "*Ik kijk alleen maar*", Blauw - Opsporing, 6-2-2010, nr. 3, p. 10.

[631] De toenmalige minister van justitie Hirsch Ballin maakte bijv. in oktober 2010 in de media kenbaar dat hij aan de "beroepsgroep van de rechtspraak" had meegedeeld om deze reden van mening te zijn dat rechters de beelden van kinderporno zelf moesten bekijken als ze een maker daarvan moeten berechten, hoe "erg, akelig en afstotend" dit ook is.

[632] De Hoge Raad laat eerder echter wel de mogelijkheid open dat de raadsman om toevoeging van de gegevens aan het dossier verzoekt; zie HR 5-5-2001, ECLI:NL:HR:2001:AB1517, *NJ* 2001/479 (harde schijf i.c. geen onderdeel van de processtukken; geen verzoek verdediging om toevoeging harde schijf aan dossier).

De raadsman kan echter wel desgewenst voor de zitting (op het parket of kort voor aanvang van de zitting) kennisnemen van een door de politie in overleg met het OM samengestelde zogenaamde toonmap met een representatieve selectie van aangetroffen afbeeldingen. In deze selectie bevinden zich normaliter ook alle op de tenlastelegging expliciet genoemde en uitgeschreven afbeeldingen. De in de map opgenomen afbeeldingen worden door het OM beschouwd als stukken van overtuiging. Deze map dient vervolgens ook tijdens de zitting beschikbaar te zijn voor eventuele kennisname door de strafrechter en de verdediging. De verdediging kan vanzelfsprekend de rechter gemotiveerd verzoeken om bepaalde afbeeldingen uit de toonmap, of andere relevant geachte afbeeldingen, alsnog aan het dossier toe te voegen en/of te bekijken. Omdat ingevolge deze werkwijze de toonmap en de zich daarin bevindende afbeeldingen zelf geen processtuk is/zijn, kunnen de in de toonmap aanwezige afbeeldingen alleen via de rechterlijke waarneming bijdragen tot het bewijs.[633]

Kan het OM de betreffende afbeeldingen niet produceren, bijvoorbeeld doordat deze zoek zijn geraakt (of gemaakt), terwijl het strafbare karakter daarvan wordt betwist, dan zal – tenzij de inhoud en het karakter van de afbeeldingen uit andere wettige bewijsmiddelen[634] kan worden afgeleid – in beginsel vrijspraak volgen.[635]

7.4.2. Verzoeken om een slachtoffer en/of andere getuigen te horen

Hiervoor is al aangegeven, dat voor de beoordeling van de overgrote meerderheid van art. 240b-zaken het niet relevant is of, en in hoeverre een op een afbeelding zichtbare minderjarige toestemming heeft gegeven voor de vervaardiging en/of verspreiding van de betreffende afbeelding, en evenmin of deze daardoor schade heeft geleden.[636] Verzoeken om het slachtoffer (of anderen) als getuige ter zake te horen zullen dan ook reeds hierom niet kunnen worden gehonoreerd.

Een uitzondering kan zich evenwel voordoen indien sprake zou kunnen zijn van een situatie van consensuele *sexting*, zoals hiervoor omschreven in paragraaf 5.1. e.v. Het element van instemming door de afgebeelde minderjarige is dan namelijk een onderdeel van het door de Hoge Raad genoemde samenstel van factoren, welke de strafrechter bij zijn beoordeling van de kwalificeerbaarheid van de bewezenverklaring van een art. 240b Sr-gedraging dient te betrekken. Zulks maakt dat met een verzoek om de betreffende minderjarige te horen in een dergelijk geval een reëel verdedigingsbelang gemoeid kan zijn.

---

[633] Zie omtrent de (voorwaarden voor de) rechterlijke waarneming als bruikbaar hierover verder hierna onder 7.6.1.1. Zie o.m. ook: RB Midden-Nederland 9-12-2016, ECLI:NL:RBMNE:2016:7765 (De rechtbank heeft ter zitting kennisgenomen van de inhoud van de toonmap en waargenomen dat het materiaal kinderpornografisch is).

[634] Te denken valt hier met name aan voldoende gedetailleerde verklaringen van verbalisanten of getuigen omtrent hetgeen op die afbeeldingen te zien was. Denkbaar is ook dat indien de hashcode van een niet meer beschikbare afbeelding nog wel beschikbaar is, vanuit de Landelijke database kinderporno een identieke afbeelding kan worden gegenereerd.

[635] Aldus bijv. RB Zeeland-West-Brabant 28-4-2016, ECLI:NL:RBZWB:2016:2601 (Vrijspraak, vd heeft foto's en filmopnames gemaakt van een jongen die bij hem thuis onder de douche stond. De afbeeldingen zijn door de vd gewist en derhalve is aan de rechtbank de mogelijkheid ontnomen om een oordeel te geven over de vraag of de afbeeldingen zijn te scharen onder 240b Sr); vgl. ook RB Den Haag 26-1-2018, ECLI:NL:RBDHA:2018:772 en 2018:771 (Geen van de beschreven filmpjes in het dossier opgenomen en slechts een enkele afbeelding is aan het dossier toegevoegd; geen beoordeling mogelijk; vrijspraak**)**
Onder omstandigheden kan dat anders liggen; zie bijv. RB Gelderland 27-10-2016, ECLI:NL:RBGEL:2016:5747 (Bewijs verspreiden kp-afbeeldingen d.m.v. smartphone o.m. afgeleid uit whatsapp-berichten over verzending en verklaringen van getuigen dat zij de betreffende afbeeldingen hebben gezien en waarin zij de afbeeldingen omschrijven).

[636] Zie hiervoor onder 5.3.

Evenzo is hiervoor reeds uiteengezet dat het voor de rechterlijke beoordeling irrelevant is of een afgebeelde persoon in werkelijkheid al de leeftijd van 18 jaren heeft bereikt.[637] Er is dan ook geen plaats voor tegenbewijs van verdachte inhoudende dat betrokkene de leeftijd van 18 jaar al heeft bereikt.[638] Verzoeken om het slachtoffer (of getuigen dan wel deskundigen) op dit punt te horen kunnen dan ook slechts worden afgewezen.

7.5. Recht op tegenonderzoek/contra-expertise

7.5.1. Algemene uitgangspunten
In het kader van art. 240b-zaken worden met enige regelmaat de bevindingen of conclusies van de politie of een deskundige van het NFI ten aanzien van bepaalde technische aspecten door de verdachte betwist. Onder omstandigheden kan dan aan de verdachte een recht op een vorm van tegenonderzoek toekomen. De regeling van het tegenonderzoek (ook wel contra-expertise genoemd) is in het Nederlandse strafprocesrecht complex en onderhevig aan voortdurende beïnvloeding vanuit "Straatsburg". Hieronder zullen daarom eerst een aantal hoofdlijnen uiteen worden uiteengezet.

"Beoordelend onderzoek" ex art. 230 Sv
Allereerst kent art. 230 Sv aan een verdachte aan wie kennis is gegeven van de uitslag van een in het kader van het vooronderzoek door een deskundige verricht onderzoek *de bevoegdheid* toe een deskundige te laten benoemen voor het verrichten van een zogenaamd beoordelend onderzoek. Bij een dergelijk beoordelend onderzoek is het object van onderzoek het onderzoeksverslag dat door de eerdere deskundige is uitgebracht. Het houdt dus *niet* in dat de tweede deskundige het onderzoek "nog eens helemaal over mag doen".[639]
Bij een verzoek geldt tevens als formele voorwaarde dat de verdachte wel aangeeft wie die tegendeskundige dan moet zijn. De uitvoering verloopt via de rechter- of raadsheer-commissaris. Daarbij wordt vanzelfsprekend het eerdere deskundigenrapport overgedragen, maar de eigenlijke onderzoeksobjecten (zoals gegevensdragers) normaliter niet.
Breed wordt aangenomen dat de kosten van een dergelijk beoordelend onderzoek voor rekening van de staat zijn.[640]

Opmerking verdient hier voorts dat, hoewel (politie)deskundigen ten aanzien van onderzoeken die zij in het kader van technisch opsporingsonderzoek als bedoeld in art. 150, tweede lid, Sv hebben verricht, niet immer als deskundige in de zin van strafvordering worden aangemerkt, uit de wetsgeschiedenis kan worden afgeleid dat de wetgever heeft beoogd de (beperkte) regeling ex art. 230 Sv van het "beoordelend onderzoek" ook tot processen-verbaal van deze categorie "specialistische opsporingsambtenaren" uit te strekken.[641]

Nader (aanvullend) onderzoek ex art. 231 Sv
Daarnaast kan sprake zijn van nader (of: aanvullend) onderzoek als bedoeld in art. 231, eerste lid, Sv. In dat geval wordt voorgebouwd op het al uitgevoerde onderzoek. Dit kan

---

[637] Zie hiervoor onder 3.3.1.
[638] HR 18-11-2008, ECLI:NL:HR:2008:BF0170.
[639] Vgl. Hof Arnhem-Leeuwarden 19-7-2018, ECLI:NL:GHARL:2018:6616 ("*Anders dan de verdediging betoogt, schept dit artikel (KCC: art. 230, tweede lid, Sv) naar het oordeel van het hof geen onbeperkte bevoegdheid voor de verdachte om ieder deskundigenonderzoek in elk stadium van het proces te laten (tegen-)onderzoeken*.").
[640] Aldus ook o.m. Cleiren e.a., *Tekst en Commentaar Strafrecht*, in het commentaar bij art. 230 Sv.
[641] Zie hierover uitgebreider; Cleiren/Crijns/Verpalen, *Tekst en Commentaar Strafvordering (11e druk)*, art. 150, aantekening 2.; zie omtrent deze problematiek ook: AG Aben in zijn conclusie d.d. 16-06-2015, ECLI:NL:PHR:2015:1826 (HR: gevolgd (81.1 RO), ECLI:NL:HR:2015:2774).

bijvoorbeeld inhouden dat andere technieken worden ingezet, of uitgebreider onderzoek plaatsvindt, om zo te proberen om meer relevante informatie van een gegevensdrager of anderszins vastgelegde data[642] te verkrijgen. Om een nader/aanvullend onderzoek te kunnen uitvoeren heeft de deskundige de onderzoeksvraag nodig zoals gesteld in het oorspronkelijke onderzoek alsook het onderzoeksmateriaal, de rapportages en de resultaten van het oorspronkelijke onderzoek.[643]
Het nader onderzoek kan worden uitgevoerd door de deskundige/onderzoeksinstelling die het eerdere onderzoek heeft uitgevoerd of door een andere deskundige of onderzoeksinstelling. In het laatste geval is het de bedoeling dat de rechter- of raadsheer-commissaris een opdracht tot overdracht opmaakt zodat de documenten en monsters bij het eerste instituut kunnen worden overdragen naar het uitvoerende instituut. Afhankelijk van wie de formele opdracht uitgaat zijn de kosten van het nader onderzoek voor de staat of voor de verdachte.[644]

(Volledig) Tegenonderzoek
Tegenonderzoek is een onafhankelijk en onbevooroordeeld onderzoek dat *(geheel) opnieuw* wordt uitgevoerd door een andere deskundige en/of bij een ander instituut dan die resp. dat het vorige onderzoek heeft verricht. Uit art. 150c, tweede lid, Sv volgt dat een deskundige die het tegenonderzoek gaat verrichten toegang krijgt tot het onderzoeksmateriaal en de desbetreffende gegevens uit het eerste onderzoek. Het gaat hier dan bijvoorbeeld om gegevensdragers die door het NFI worden bewaard voor een eventueel tegenonderzoek en om gegevens die de eerste deskundige in het kader van zijn onderzoeksopdracht heeft ontvangen (de onderzoeksvraag, delictsomschrijving, overzicht van reeds verricht onderzoek enz.). Het onderzoek dient gelijkwaardig te zijn aan het eerste onderzoek.[645]

Voor de overdracht van onderzoeksmaterialen en/of gegevens is een *opdracht tot overdracht* ondertekend door een rechter- of raadsheer-commissaris nodig (dit geldt in elk geval voor het NFI, zonder een dergelijke opdracht verstrekt het NFI geen materialen of gegevens aan derden).

Een tegenonderzoek moet een onafhankelijk en onbevooroordeeld onderzoek zijn. Daarom is het niet gewenst dat de onderzoeks*rapportages* en *-resultaten* van de eerste deskundige worden meegezonden. Dit laat onverlet dat het in een later stadium van de procedure nuttig kan zijn om de visie van de verschillende deskundigen tegenover elkaar te zetten, bijvoorbeeld door hen ter zitting, al dan niet in elkaars bijzijn, te horen.

Uit het voorgaande blijkt dat er verschillende vormen van “tegenonderzoek” zijn, welke onderling zowel qua aard, omvang als uitvoering aanzienlijk verschillen. Dat betekent dat van de verdediging kan worden gevraagd, dat zij indien zij “een tegenonderzoek” wenst, duidelijk aangeeft welke vorm van tegenonderzoek zij op het oog heeft, en zo nodig ook motiveert waarom niet met een andere (minder omvangrijke) vorm van tegenonderzoek zou kunnen worden volstaan. Een algemeen geformuleerd verzoek als: “ik verzoek u een tegenonderzoek te gelasten” zal dus in de regel niet als voldoende gemotiveerd kunnen worden beschouwd.[646]

---

[642] Bijvoorbeeld metadata die is meegekomen met onderschepte of afgetapte communicatie.
[643] Zie art. 231, lid 2, Sv, alsook Cleiren e.a., *Tekst en Commentaar Strafrecht*, in het commentaar bij art. 231 Sv.
[644] Zij het dat als de verdachte opdrachtgever is, deze kosten mogelijk via art. 591 Sv na afloop van de zaak voor vergoeding in aanmerking komen; in bepaalde gevallen kan in dit verband ook een voorschot worden verkregen (zie art. 51j, lid 4 Sv).
[645] Zie art. 150a, lid 3, Sv.
[646] Aldus ook AG Machielse in zijn conclusie d.d. 15-5-2014, ECLI:NL:PHR:2014:478 voorafgaand aan HR 3-6-2014, ECLI:NL:HR:2014:1305.

Hoewel dit niet expliciet uit de wetstekst blijkt, kan een verdachte, zijn raadsman of de officier van justitie/advocaat-generaal, indien de zaak reeds aanhangig is bij de zittingsrechter, ook de zittingsrechter vragen tegenonderzoek te laten verrichten.[647] De strafrechter kan daartoe ook ambtshalve besluiten. Indien de rechter bepaalt dat een tegenonderzoek dient plaats te vinden, kan hij hiertoe op basis van art. 315 Sv zelf opdracht geven of kan hij de zaak ingevolge art. 316 Sv daarvoor terug verwijzen naar de rechter- of raadsheer commissaris.[648]

De beoordeling van een verzoek tot het verrichten van een tegenonderzoek is niet altijd even eenvoudig. Formeel uitgangspunt is echter dat het Nederlandse strafprocesrecht geen algemeen recht op contra-expertise kent. Wel bestaat wetgeving waarin dit voor specifieke situaties is vastgelegd.[649] In dat verband is ook de rechterlijke maatstaf voor de beoordeling van dergelijke verzoeken formeel nog steeds het noodzakelijkheidscriterium. Hoewel ook uit art. 6 EVRM niet zonder meer een recht op (volledige) contra-expertise voortvloeit[650], zijn voormelde uitgangspunten onder invloed van de Straatsburgse jurisprudentie wel steeds verder genuanceerd. Naast de hiervoor reeds genoemde mogelijkheid tot tegenonderzoek van het onderzoeksverslag, volgt namelijk uit de rechtspraak van de Hoge Raad dat de eis van een eerlijke procesvoering kan meebrengen dat aan een verzoek tot het doen verrichten van een tegenonderzoek gevolg behoort te worden gegeven.[651] Of zich zo een geval voordoet is afhankelijk van de omstandigheden van de desbetreffende zaak. Daarbij kan worden gedacht aan onder meer[652]:

a) de gronden waarop het verzoek steunt[653];

---

[647] Dit wordt afgeleid uit artt. 328 jo. 315 en 316 Sv; zie o.m. HR 8-2- 2005, ECLI:NL:HR:2005:AR7228; *NJ* 2005/514.
[648] In hoger beroep zijn deze bepalingen dienovereenkomstig van toepassing (art. 415 Sv).
[649] Zie in dit kader o.m. Hof Amsterdam 16-7-2013, ECLI:NL:GHAMS:2013:2124 (tegenonderzoek ademanalyse uitdrukkelijk in regeling vastgelegd).
[650] Zie onder meer EHRM 30-10-1991, *Brandstetter*, Serie A nr. 214-A; EHRM 2-10-2001, *G.B. vs Frankrijk,* 44069/98 par. 68 ; EHRM 11-12-2008, *Mirilashvili vs. Rusland,* nr. 6293/04 par. 189 e.v.
[651] Vaste jurisprudentie zie o.m. HR 8-9-2009, ECLI:NL:HR:2009:BI5746, HR 19-6-2007, ECLI:NL:HR:2007:BA2104; HR 8-2-2005, ECLI:NL:HR:2005:AR7228, *NJ* 2005/514 m.nt. Pme; HR 2-2-1993, *NJ* 1993/476.
[652] Zie o.m. HR 8-9-2009, ECLI:NL:HR:2009:BI5746; HR 12-3-2013, ECLI:NL:HR:2013:BZ3886, r.o. 3.3; HR 16-4-2013, ECLI:NL:HR:2013:BZ7150; idem o.m.: Hof Arnhem-Leeuwarden 05-07-2013, ECLI:NL:GHARL:2013:4825.
[653] Vgl. ook HR 8-5-2001, ECLI:NL:HR:2001:AB1517, waarbij het oordeel van het hof dat geen sprake was van inbreuk op het beginsel van equality of arms door de Hoge Raad in stand werd gelaten, waarbij de Hoge Raad o.m. in aanmerking nam (r.o. 3.7): a) hetgeen het Hof heeft overwogen omtrent de gang van zaken tijdens het onderzoek ter terechtzitting in hoger beroep, waaronder de aldaar aan de verdediging geboden mogelijkheid om de getuige-deskundige vragen te stellen omtrent het aan de harde schijf verrichte onderzoek, en b) de omstandigheid dat de verdediging ter terechtzitting niet heeft aangegeven welke onderdelen van dat door de politie aan dat inbeslaggenomen voorwerp verrichte onderzoek onjuist of onvolledig zouden zijn, terwijl zij voorts niet om een nader onderzoek heeft verzocht, noch ook om de verstrekking van een kopie van de harde schijf teneinde het door haar noodzakelijk geachte onderzoek aan dit inbeslaggenomen voorwerp alsnog te (doen) verrichten. Zie ook: Hof Amsterdam 30-1-2018, ECLI:NL:GHAMS:2018:240 (Afwijzing verzoeken tot horen van deskundige van het NFI en uitvoeren van contra-expertise. Blijkens de motivering van de verzoeken gaat de raadsman er klaarblijkelijk van uit dat het “kraken” van het wachtwoord en de pincode van de telefoon in kwestie door het NFI gevolgen kan hebben gehad voor de integriteit van de data op die telefoon. Daarin is, zo moet uit de toelichting worden opgemaakt, ook het belang van de verdediging bij het verzochte verhoor en onderzoek gelegen. Het hof stelt vast dat in de gegeven toelichting is volstaan met het enkele opwerpen van die theoretische voorstelling dat mutaties in de data kunnen zijn opgetreden als gevolg van de ontsleuteling van wachtwoord en pincode. Dat vormt evenwel een onvoldoende onderbouwing voor deze verzoeken. Het hof wijst beide verzoeken dan ook af. Voor het verzochte verhoor van de deskundige en onderzoek in de vorm van contra-expertise is de noodzaak niet gebleken).

b) het belang van het gevraagde tegenonderzoek in het licht van – bijvoorbeeld – de aanwezigheid van ander bewijsmateriaal dan wel de overtuigende kracht die pleegt te worden toegekend aan het bestreden onderzoeksresultaat[654];
c) de omstandigheid dat het verzoek is gedaan op een zodanig tijdstip dat een dergelijk onderzoek nog mogelijk is; en
d) de omstandigheid dat het verzoek redelijkerwijs eerder had kunnen worden gedaan.

Deze criteria zullen voor de feitenrechter leidend moeten zijn bij de beoordeling van verzoeken om contra-expertise. Bij de meer materiële invulling daarvan kan overigens ook de wetsgeschiedenis behulpzaam zijn. In de memorie van toelichting bij de Wet Deskundige in strafzaken wordt in dit kader namelijk gerefereerd aan Kwakman[655] die op basis van de uitleg van het EHRM en de Hoge Raad van het fair-trialbeginsel tot de conclusie komt dat de verdachte ook tijdens het onderzoek op de terechtzitting in beperkte mate recht op tegenonderzoek heeft, indien (min of meer cumulatief)[656] aan de volgende voorwaarden is voldaan:

– de resultaten van het deskundigenonderzoek zijn gemotiveerd betwist of roepen vragen op omtrent de betrouwbaarheid van de gehanteerde methode;
– aangetoond is dat de door de rechter benoemde deskundige objectief bezien niet als onpartijdig kan worden beschouwd;
– gemotiveerd is aangetoond dat de op zijn verzoek te benoemen deskundige een relevante bijdrage kan leveren aan het strafproces;
– het verzoek is tijdig en uitdrukkelijk gedaan (met het oog daarop moet onderzoeksmateriaal op passende wijze worden bewaard);
– tegenonderzoek moet technisch en praktisch mogelijk zijn.

Wij zien het zo dat aan de laatste drie voorwaarden in beginsel altijd moet zijn voldaan, en daarnaast tenminste aan één van de twee eerstgenoemde voorwaarden.

7.5.2. Contra-expertise met betrekking tot onderzoek naar gegevensdrager(s)
In het licht van het voorgaande is het denkbaar dat een verdachte de rechter verzoekt om hem toe te staan zelf door een deskundige onderzoek aan de betreffende gegevensdrager te laten verrichten. Zeker als reeds een eerder onderzoek door een onafhankelijk deskundige (zoals die van het NFI) aan die gegevensdrager heeft plaatsgevonden, zullen in de regel hoge eisen aan de onderbouwing van een dergelijk verzoek kunnen worden gesteld. Zo zal met name moeten worden toegelicht waarom niet met een beoordelend onderzoek als bedoeld in art. 230 Sv of met een (nadere) bevraging van de deskundige die reeds heeft gerapporteerd zou kunnen worden volstaan. Ook zal kritisch moeten worden nagegaan in hoeverre de voorgestelde deskundige over de kennis, faciliteiten en tijdruimte beschikt om het gevraagde tegenonderzoek verantwoord en binnen een redelijke termijn te kunnen uitvoeren. Tenslotte dient in de afweging te worden betrokken in hoeverre (door de deskundige of anderszins) kan worden gewaarborgd dat eventueel op de gegevensdrager(s) opgeslagen strafbaar materiaal niet verder verspreid wordt dan in het kader van het te verrichten onderzoek strikt noodzakelijk is.

---

[654] Vgl. ook HR 12-03-2013, ECLI:NL:HR:2013:BZ3886; *NJ* 2013/179.
[655] N.J.M. Kwakman, *De deskundige in het strafproces*, Onderzoeksproject Strafvordering 2001 van prof. M.W. Groenhuijsen en prof. mr. G. Knigge - Het onderzoek ter terechtzitting, pag. 365.
[656] N. J. M. Kwakman – De deskundige in het strafproces, onderdeel van het eerste deel van het onderzoeksproject Strafvordering 2001, blz. 365.

Wordt het verzoek toegewezen, dan verdient het de voorkeur een ICT-deskundige te benoemen die is opgenomen in het deskundigenregister van het Nederlands Register Gerechtelijk Deskundigen (NRGD).[657] Als een deskundige is benoemd, blijken er nog wel eens problemen te ontstaan rond de afgifte van het onderzoeksmateriaal. In zaken waar het gaat om onderzoeksmateriaal in de vorm van gegevensdragers ligt dat veelal wat eenvoudiger dan in het algemeen omdat het dan mogelijk is een forensische kopie te verstrekken van het oorspronkelijke materiaal. Daardoor bestaat in deze gevallen geen risico van destructie of modificatie van het oorspronkelijke (bewijs)materiaal. Wat betreft het tegengaan van de verdere verspreiding van eventueel strafbaar materiaal op de gegevensdrager lijkt het raadzaam te overwegen met de benoemde deskundige daarover uitdrukkelijke afspraken te maken[658], zodat deze zich ook bewust is van de eventuele beperkingen (zoals het mogelijk beperkter kunnen consulteren van collega's, al dan niet via fora) die dit specifieke onderzoekskader met zich kan brengen.

7.6. Onderzoek ter terechtzitting

7.6.1. Tonen ter terechtzitting/kennisname door rechter van tenlastegelegd materiaal

7.6.1.1. Moet de rechter ook zelf de afbeeldingen bekijken?

Er is langere tijd discussie geweest over de vraag of de strafrechter aan wie een art. 240b-zaak is voorgelegd ook immer zelf kennis diende te nemen van de betreffende afbeeldingen. Deze discussie werd deels gevoed door een arrest van de Hoge Raad van 7 december 2004[659], waarin de Hoge Raad casseerde, omdat hij vond dat de verantwoording van de feitenrechter van zijn oordeel dat bepaalde afbeeldingen kinderpornografisch van aard waren tekort schoot. In casu bleek namelijk niet uit het proces-verbaal van het onderzoek ter terechtzitting dat het Hof ter terechtzitting zich door eigen waarneming een beeld had gevormd van de afbeeldingen (die zich in die zaak in een fotomap bevonden). De Hoge Raad leidde daaruit af dat het Hof zich kennelijk niet op eigen waarneming had gebaseerd, maar was afgegaan op de inhoud van een proces-verbaal van een opsporingsambtenaar. Dat proces-verbaal hield in "*dat de verbalisanten de door hen bekeken afbeeldingen hebben aangemerkt als kinderpornografie omdat de afbeeldingen personen betroffen die kennelijk jonger waren dan zestien jaar, onderscheidenlijk dat een aantal afbeeldingen in het onderzoek gemarkeerd was als kinderpornografie*". Het is in dit licht dan ook weinig verrassend dat de Hoge Raad vervolgens oordeelde: "*Het relaas houdt niet in op grond waarvan de verbalisanten tot die bevinding zijn gekomen. Een dergelijke conclusie kan niet bijdragen tot het bewijs. Dat kan slechts anders zijn indien in een geval als het onderhavige de rechter op grond van andere bewijsmiddelen, waaronder de eigen waarneming van afbeeldingen door de rechter, heeft geoordeeld en heeft kunnen oordelen dat een zodanige conclusie terecht is getrokken. Daarvan is hier echter geen sprake.*" en de uitspraak van het Hof casseerde.

---

[657] Met ingang van 1 januari 2017 bevat dit register namelijk ook ICT-deskundigen.

[658] Deze afspraken kunnen zich onder meer uitstrekken over geheimhouding (incl. een verbod op het vermenigvuldigen en/of het delen met derden van de data op de gegevensdrager), de wijze van opslag van en de (fysieke en digitale) beperking van toegang tot de gegevensdrager, de communicatie met derden over de inhoud van de gegevensdrager en de wijze waarop de gegevensdrager na afloop van het onderzoek zal worden geretourneerd.

[659] HR 7-12-2004, ECLI:NL:HR:2004:AQ8936, *NJ* 2006, 62.

Bij dit arrest passen derhalve twee kanttekeningen:

1. In de betreffende zaak was de kwalificatie van de afbeeldingen als kinderpornografisch door verbalisanten niet onderbouwd, terwijl thans in processen-verbaal door verbalisanten, nagenoeg altijd onder verwijzing naar onder meer de 'Aanwijzing kinderpornografie' van het College van Procureurs-Generaal een dergelijke onderbouwing wel wordt gegeven.
2. In de betreffende zaak was door de verdediging de kwalificatie van het materiaal als "kinderpornografie" nadrukkelijk betwist.

Uit dit arrest kan derhalve niet worden afgeleid dat de zittingsrechter in kinderpornozaken altijd ook zelf naar het materiaal zou moeten kijken. Integendeel zelfs. Indien zich in het dossier reeds voldoende gedetailleerde in pv's vervatte beschrijvingen van het in de tenlastelegging omschreven materiaal bevinden en daarin tevens is onderbouwd op basis van welke criteria dit materiaal is gekwalificeerd als kinderporno, behoeven rechters het materiaal in beginsel niet ook zelf nog te bekijken. Dit is slechts anders, indien de verdediging de juistheid van de beschrijving of van de daaraan door de politie gegeven kwalificatie, voldoende gemotiveerd betwist[660], dan wel de beschrijving in het proces-verbaal en/of de tenlastelegging daartoe reeds op zichzelf aanleiding geeft. Dan zal de strafrechter ook zelf de betwiste afbeeldingen moeten bekijken (en indien dat ter terechtzitting heeft plaatsgevonden zal in het proces-verbaal van de terechtzitting moeten worden opgenomen dat die afbeeldingen zijn getoond/bekeken). In dat geval vormt de waarneming door de rechter van die afbeeldingen ook een (eventueel aanvullend) zelfstandig bewijsmiddel, waarbij het wat ons betreft de voorkeur heeft om als uitgangspunt te nemen dat de rechter – kort en zakelijk en zo objectief mogelijk – weergeeft wat hij meent te zien, zodat de andere procesdeelnemers daarop desgewenst kunnen reageren. Vanzelfsprekend zal het een en ander vervolgens in het proces-verbaal van de terechtzitting dienen te worden opgenomen.[661]

In het geval de officier van justitie of de verdediging de strafrechter nadrukkelijk verzoekt om ter terechtzitting kennis te nemen van de afbeeldingen, dan zal de strafrechter daarop gemotiveerd dienen te antwoorden[662], waarbij naar mag worden aangenomen de in de voorgaande alinea genoemde aspecten zullen (moeten) worden betrokken.

---

[660] Vgl. ook: HR 7-7-2015, ECLI:NL:HR:2015:1801 (afwijzing (met verwijzing naar noodzakelijkheidscriterium) verzoek tot ter terechtzitting beluisteren bepaalde tapgesprekken gezien onderbouwing onvoldoende gemotiveerd afgewezen) en HR 10-4-2012, ECLI:NL:HR:2012:BW1450 (verzoek tot tonen beelden ter terechtzitting omdat herkenning door verbalisanten wordt betwist; ten onrechte niet door hof op beslist).

[661] Vgl. o.m. de conclusie van AG Jörg (ECLI:NL:PHR:2010:BL8772) bij HR 6-4-2010, ECLI:NL:HR:2010:BL8772; Van belang hierbij is te onderscheiden dat de rechterlijke waarneming weliswaar in beginsel bij het onderzoek ter terechtzitting moet zijn gedaan, maar de inhoud van die waarneming niet reeds ter terechtzitting behoeft te worden uitgesproken c.q. ter sprake te worden gebracht door de rechter, mits partijen daardoor niet worden verrast (zie o.m. HR 24-9-2019, ECLI:NL:HR:2019:1414**.** Indien aan een aantal specifieke voorwaarden is voldaan acht de Hoge Raad overigens ook een *na* de terechtzitting in raadkamer gedane rechterlijke waarneming van materiaal uit de toonmap als bewijsmiddel toelaatbaar (HR 17-10-2017, ECLI:NL:HR:2017:2639), maar uit het arrest wordt duidelijk dat de Hoge Raad (en de AG) er de voorkeur aan geeft dat zulks zoveel mogelijk *tijdens* het onderzoek ter terechtzitting plaatsvindt. Zie voor een iets afwijkende situatie de CAG vóór ECLI:NL:PHR:2018:248, hier waren wel tijdens het onderzoek ter terechtzitting foto's aan de verdachte getoond waarvan het de vraag was of daarop het slachtoffer te zien was. Die vaststelling heeft het Hof in de bewijsmiddelen opgenomen, terwijl niet uit het proces-verbaal van het verhandelde ter zitting bleek dat die waarneming aan verdachte was voorgehouden. Uit de feitelijke gang van zaken, waarbij ook de behandeling van de zaak in eerste aanleg wordt betrokken, trekt de AG de conclusie dat van een verrassing geen sprake kon zijn.

[662] Vgl. de reeds hiervoor genoemde uitspraken HR 10-4-2012, ECLI:NL:HR:2012:BW1450 en HR 7-7-2015, ECLI:NL:HR:2015:1801.

7.6.1.2. Toevoeging door de rechter van de afbeeldingen aan het procesdossier
Buruma heeft onzes inziens op goede gronden betoogd dat een zuivere beoordeling door zowel de feiten- als de cassatierechter met zich brengt dat ingeval de rechter zelf de beelden heeft beoordeeld of als de zaak feitelijk draait om de beoordeling van het al dan niet kinderpornografische karakter van de afbeeldingen, de betreffende afbeeldingen dan ook (alsnog) door de rechter aan het strafdossier dienen te worden toegevoegd.[663] Denkbaar is daarbij dat om het risico van verspreiding of onverhoedse confrontatie zoveel mogelijk tegen te gaan de betreffende afbeeldingen dan eerst op een (met een wachtwoord beveiligde en versleutelde) gegevensdrager worden geplaatst, vervolgens de gegevensdrager zelf in het dossier wordt opgenomen, en het wachtwoord vervolgens afzonderlijk aan een functionaris van het volgende rechtscollege wordt verstrekt.[664]

7.6.2. Feiten van algemene bekendheid en internetinformatie
In art. 240b-zaken komt het regelmatig voor dat de rechter, bijvoorbeeld om zich een nader beeld te verschaffen van de betekenis van bepaalde in de stukken gebruikte technische termen, of van de werking van (delen van) *devices* of software, bronnen op internet raadpleegt.

Als hetgeen de rechter vervolgens langs die weg ter kennis komt als "*feit (of omstandigheid) van algemene bekendheid"* kan worden gekwalificeerd, kan en mag de rechter die informatie ook mede aan zijn beslissing ten grondslag leggen.[665]
Ingevolge de jurisprudentie van de Hoge Raad zijn van algemene bekendheid *"die gegevens die ieder van de rechtstreeks bij het geding betrokkenen geacht moet worden te kennen of die hij zonder noemenswaardige moeite uit algemeen toegankelijke bronnen kan achterhalen*."[666]
Voorts moet het bij dergelijke feiten of omstandigheden gaan om "*gegevens die geen specialistische kennis veronderstellen en waarvan de juistheid redelijkerwijs niet voor betwisting vatbaar is*".[667]

Voorgaande uitgangspunten gelden ook voor informatie afkomstig van internet(bronnen). Bedacht moet echter worden dat de enkele omstandigheid dat bepaalde informatie aan internetbronnen is ontleend nog niet maakt dat die informatie ook kan worden aangemerkt als een feit of omstandigheid van algemene bekendheid in de zin van art. 339, tweede lid, Sv. Deze enkele omstandigheid zegt namelijk op zichzelf nog niet of de betreffende informatie ook inhoudelijk kan worden beschouwd als te zijn "van algemene bekendheid".[668] Je zou zelfs het tegendeel kunnen betogen. Als het gaat om het nazoeken van meer dan eenvoudige begripsomschrijvingen is al snel per definitie geen sprake meer van feiten van algemene bekendheid. Het voert te ver om in het kader van dit boek dieper op dit onderwerp in te gaan,

---

[663] Y. Buruma, *Plaatjes kijken*, Blog NJB 14 december 2015, NJB 2015/2221.
[664] Overigens zou een dergelijke werkwijze wel de nodige aanpassingen en nadere maatregelen vragen om te voorkomen dat (sporen van) het materiaal op gegevensdragers en/of het netwerk binnen OM en ZM achterblijven. Zou zullen de afbeeldingen gescand moeten worden en dan buiten het netwerk op een gegevensdrager geplaatst moeten worden. Die gegevensdrager zal vervolgens zelf alleen via een niet aan het netwerk verbonden computer geraadpleegd kunnen worden, die dan vervolgens feitelijk "besmet " moet worden geacht met kinderporno (bv. omdat thumbnails zullen zijn aangemaakt) en dan ook direct na gebruik geschoond zal moeten worden. Op dit moment lijken OM en ZM qua kennis en faciliteiten niet nog in staat een dergelijk proces praktisch uit te voeren. Toevoeging aan het procesdossier is op dit moment derhalve geen reële mogelijkheid.
[665] Zie art. 339, lid 2, jo. art. 338 Sv.
[666] Zie o.m. HR 11-1-2011, ECLI:NL:HR:2011:BP0291, *NJ* 2011/116 met lezenswaardige noot van P.A.M. Mevis (ACAB-I)**;** Hoge Raad 12-07-2011, ECLI:NL:HR:2011:BQ6555.
[667] HR 29-3-2016, ECLI:NL:HR:2016:522 , *NJ* 2016/249 m.nt. P.A.M. Mevis.
[668] Aldus HR 29-3-2016, ECLI:NL:HR:2016:522, *NJ* 2016/249 m.nt. P.A.M. Mevis.

maar een interessant punt van overdenking is in hoeverre specialisatie van een rechter, bijvoorbeeld op het gebied van cybercrime, ertoe leidt dat hem of haar bekende technische informatie zonder meer in een uitspraak gebruikt kan worden. Het zou immers ongewenst zijn als een dergelijke rechter in iedere zaak waarin een bepaald technisch aspect speelt opnieuw een deskundige moet benoemen om iets uiteen te zetten wat bijvoorbeeld uit de behandeling van eerdere strafzaken of uit cursussen al genoegzaam bekend is. Anderzijds moeten de andere procesdeelnemers wel op de hoogte zijn van hetgeen de rechter aan een beslissing ten grondslag zal leggen, bijvoorbeeld om aan te kunnen voeren dat die informatie onjuist of onvolledig is. Het verdient daarom aanbeveling om ook waar geen sprake is van "gegoogelde" informatie, bij enige twijfel aan de kant van de rechter of de informatie waar hij of zij niet op grond van het dossier over beschikt ook bij de andere procesdeelnemers bekend is, de hierna te noemen processuele regels die gelden voor "gegoogelde informatie", te volgen.

Daarbij wordt opgemerkt dat als procespartijen meer dan gemiddelde ICT-technische kennis hebben, het aannemelijk is dat in de betreffende strafzaak bepaalde technische gegevens ook eerder en meer dan gebruikelijk door de rechter als zijnde van algemene bekendheid zullen kunnen worden gekwalificeerd. Dat volgt uit voornoemde rechtspraak, in het bijzonder waar de Hoge Raad mede verwijst naar gegevens "*die ieder van de rechtstreeks bij het geding betrokkenen geacht moet worden te kennen"*.[669]

Een en ander betekent geenszins dat de strafrechter door hem betrouwbaar geachte informatie van internet niet bij zijn beoordeling zou mogen betrekken. Zo laat de rechtspraak bijvoorbeeld vele voorbeelden zien van door de rechter als feit van algemene bekendheid aan *Google maps* of de *ANWB-routeplanner* ontleende informatie omtrent afstanden en reistijden. De rechter moet er hierbij wel op bedacht zijn dat het wel moet gaan om *in Nederland* van algemene bekendheid zijnde feiten en omstandigheden, zodat bijvoorbeeld het aantal treffers op Google[670] met betrekking tot een bepaalde zoekterm, indien ook anderstalige websites in de zoekslag zijn betrokken, daarvoor onvoldoende redengevend is.[671] De (aanvullende) eis dat het gegevens zijn "die geen specialistische kennis veronderstellen en waarvan de juistheid redelijkerwijs niet voor betwisting vatbaar is" is overigens niet altijd even eenvoudig toe te passen. Zo casseerde de Hoge Raad het op internetinformatie gebaseerde oordeel van de feitenrechter dat (de plant) "*aloe capensis* niet hetzelfde is als *aloe vera*", omdat niet aan deze maatstaf was voldaan[672], maar liet zeer kort daarna het oordeel van een ander Hof in stand dat het een feit van algemene bekendheid is "dat PIN-nummers unieke nummers van BlackBerry smartphones zijn, waarmee de gebruikers van deze toestellen met elkaar kunnen communiceren ('pingen'), en het PIN-nummer gekoppeld is aan het toestel en niet kan worden gewijzigd".[673]

---

[669] Zie o.m. HR 12-07-2011, ECLI:NL:HR:2011:BQ6555 en HR 11-1-2011, ECLI:NL:HR:2011:BP0291.
[670] Het zoeken op internet wordt vaak aangeduid als 'googelen'. Er zijn echter ook zoekmachines beschikbaar die andere resultaten opleveren dan Google. Rechtspraakmedewerkers dienen zich te realiseren dat zij - tenzij zij uitdrukkelijk voor een andere zoekmachine hebben gekozen - in beginsel gebruik maken van Bing als zoekmachine. Dat kan leiden tot geheel andere resultaten dan het gebruik van Google. Men dient zich hiervan bewust te zijn alvorens ter zitting mee te delen dat een zoekslag 'op Google' een bepaald resultaat heeft opgeleverd.
[671] HR 11-1-2011, ECLI:NL:HR:2011:BP0291, *NJ* 2011/116 (ACAB-1).
[672] HR 29-3-2016, ECLI:NL:HR:2016:522.
[673] HR 26-4-2016, ECLI:NL:HR:2016:746 (opmerkelijk is ook dat de AG in zijn conclusie ook verwijst naar zoekmachines op internet/wikipedia, en stelt dat deze informatie een feit van algemene bekendheid is, omdat zij "zonder noemenswaardige moeite uit algemeen toegankelijke bronnen zijn te achterhalen" terwijl de Hoge Raad 4 weken daarvoor nog oordeelde dat dit laatste op zichzelf een te beperkt toetsingscriterium inhield.

Het gebruik door de strafrechter van *gegoogelde* informatie kan dus een zeker materieel-juridisch risico inhouden. Daarnaast dient de strafrechter die een dergelijk "algemeen bekend feit" bij zijn beslissing wil betrekken ook aan een aantal eisen van formele/procesrechtelijke aard te voldoen. Uit de rechtspraak van de Hoge Raad zijn in ieder geval de volgende processuele regels af te leiden[674]:

1. Geen rechtsregel dwingt de rechter ertoe een algemeen bekend gegeven bij het onderzoek op de terechtzitting ter sprake te brengen; *maar*
2. Indien echter niet zonder meer duidelijk is of het gaat om een algemeen bekend gegeven, behoort de rechter dat gegeven aan de orde te stellen bij de behandeling van de zaak op de terechtzitting.
3. Indien bij dat onderzoek op de terechtzitting vervolgens het uitdrukkelijk onderbouwde standpunt wordt ingenomen dat en waarom het gegeven niet van algemene bekendheid is, zal de rechter in geval van afwijking van dat standpunt in zijn uitspraak op de voet van art. 359, tweede lid, Sv de redenen dienen op te geven die daartoe hebben geleid.

Aangezien vooral technische informatie op ICT-gebied al snel als specialistisch zal hebben te gelden, zal de strafrechter er derhalve zeker in die gevallen wijs aan doen om door hemzelf van internet(bronnen) verkregen informatie (inclusief vermelding van de bronnen waaruit deze afkomstig is) ook ter zitting met partijen te bespreken.

7.7. Ontoegankelijk maken, beslag, onttrekking en verbeurdverklaring

7.7.1. Ontoegankelijk maken (artt. 125o, 125p (nieuw) en 126cc, lid 5, Sv)

7.7.1.1. Art. 125o Sv: ontoegankelijkmaking van bij doorzoeking aangetroffen gegevens

Uit art. 125o Sv volgt dat, indien bij een doorzoeking in een geautomatiseerd werk[675] strafbare gegevens (zoals bijvoorbeeld kinderpornografisch materiaal) worden aangetroffen, door de officier van justitie, dan wel de rechter-commissaris, kan worden bepaald dat die gegevens ontoegankelijk worden gemaakt. Het gaat dan om het treffen van maatregelen om te voorkomen dat de beheerder van een geautomatiseerd werk of een derde verder van die gegevens kennisnemen of gebruikmaken. Ook de verdere verspreiding van die gegevens moet door de maatregel kunnen worden voorkomen. Onder het ontoegankelijk maken van gegevens wordt mede verstaan het verwijderen van de gegevens, met behoud van een kopie ten behoeve van de strafvordering. In dat geval zal er echter meestal voor worden gekozen om de relevante gegevens te laten kopiëren naar gegevensdragers onder volledige controle van de opsporingsdiensten, en deze daarna te verwijderen uit de oorspronkelijke omgeving. In iedere situatie zal moeten worden beoordeeld welke maatregel het meest effectief is, rekening houdend met de eisen van proportionaliteit en subsidiariteit.[676] Het gaat hier om een tijdelijke maatregel die kan voortduren tot het moment dat het belang van strafvordering zich niet meer verzet tegen de opheffing van de maatregel. Daarom is de maatregel in zekere zin vergelijkbaar met die van inbeslagname ter onttrekking aan het verkeer.

---

[674] Zie Hoge Raad 12-7-2011, ECLI:NL:HR:2011:BQ6555, r.o. 2.5 en HR 11-1-2011, ECLI:NL:HR:2011:BP0291.

[675] Merk op dat onder doorzoeking in een geautomatiseerd werk mede te verstaan kan zijn het tijdens doorzoeking uit te voeren onderzoek in een geautomatiseerd werk ter vastlegging van gegevens ex art. 125i Sv en de netwerkzoeking ex art. 125j Sv, indien de rechter-commissaris voor een dergelijke doorzoekingen machtiging heeft verleend.

[676] Kamerstukken II 1998/99, 26 671, nr. 3, blz. 21.

7.7.1.2. Art. 126cc, lid 5, Sv: ontoegankelijkmaking van aangetroffen gegevens bij onderzoek in een geautomatiseerd werk
Met dit artikel wordt voorzien in de mogelijkheid de bovengenoemde maatregel tot ontoegankelijkmaking van aangetroffen gegevens ook toe te passen in het geval waarin een geautomatiseerd werk onderzocht wordt buiten de situatie van de doorzoeking.[677] Hiervoor is een bevel van de officier van justitie toereikend. Het artikel volgt verder, door art. 125o Sv tweede en derde lid van overeenkomstige toepassing te verklaren, hetzelfde regime als hierboven beschreven.

7.7.1.3. Art. 125p Sv: ontoegankelijkmaking van aangetroffen gegevens bij verdenking
Uit het voorgaande blijkt dat de maatregel van ontoegankelijkmaking in art. 125o Sv alleen kon worden genomen, indien in het kader van een doorzoeking strafbare gegevens in een geautomatiseerd werk werden aangetroffen. De regeling in art. 126cc, vijfde lid, Sv ziet enkel op een reeds uitgevoerd onderzoek aan een geautomatiseerd werk. Deze beperkingen, de omstandigheid dat een andere mogelijkheid tot het ontoegankelijk maken van gegevens via de zogenaamde notice-and-takedown procedure uit art. 54a Sr (oud) niet effectief afdwingbaar was en enkele wetssystematische overwegingen[678] hebben ertoe geleid dat thans een zelfstandige bevoegdheid tot ontoegankelijkmaking van gegevens in art. 125p Sv is opgenomen. Deze bevoegdheid bestaat naast de hiervoor besproken ontoegankelijkmaking van bij doorzoeking aangetroffen gegevens.

Met deze zelfstandige bevoegdheid tot ontoegankelijkmaking van gegevens kan de officier van justitie, na voorafgaande schriftelijke machtiging van de rechter-commissaris aan een aanbieder van een telecommunicatiedienst[679] een bevel richten strekkende tot onmiddellijke ontoegankelijkmaking van gegevens. De bevoegdheid is in principe bedoeld voor die gevallen waarin de bestaande notice-and-takedown procedure niet afdoende is voor de verwijdering van gegevens, zoals ten aanzien van die aanbieders die de gedragscode niet hebben ondertekend of niet naleven.[680] Het geeft een aanzienlijke uitbreiding van de mogelijkheden om strafbaar materiaal te verwijderen van bijvoorbeeld een website of uit een cloudomgeving indien aldaar – voor zover hier relevant – kinderpornografisch materiaal aanwezig is.[681]

7.7.1.4. De rol van de strafrechter bij beoordeling maatregelen tot ontoegankelijkmaking
De systematiek van rechterlijke controle op de toepassing van de hierboven besproken maatregelen tot ontoegankelijkmaking volgt eenzelfde regime.[682] De maatregelen tot ontoegankelijkmaking dienen te worden opgeheven, zodra het belang van strafvordering zich niet meer verzet tegen de opheffing van de genomen maatregelen. Heeft een verdachte bezwaren tegen de betreffende maatregelen of tegen het uitblijven van opheffing daarvan, dan kan hij zich met een klaagschrift tot de raadkamer wenden. Volgt er geen strafzaak of

---

[677] Te denken valt aan het onderzoek door een verbalisant aan een gegevensdrager, al dan niet in een situatie van inbeslagname. Tevens is dit artikel van toepassing op art. 126nba Sv, de hackbevoegdheid, indien deze wordt ingezet met oog op de in lid 1, sub e, opgenomen onderzoekshandeling.
[678] Kamerstukken II 2015-2016, 34 372, nr. 3 (MvT), p. 56 e.v.
[679] Zie art. 138g Sv dat een zeer ruime definitie geeft, o.a. techbedrijven en internetserviceproviders zijn aan te merken als een aanbieder van een communicatiedienst.
[680] Kamerstukken II 2015-2016, 34 372, nr. 3 (MvT), p. 57.
[681] In de parlementaire behandeling is terecht veel aandacht geweest voor de gevaren van te vergaande inperking van de vrijheid van meningsuiting als gevolg van de maatregel. Twee beperkingen moeten voorkomen dat het OM 'in de rol van een censurerende internetpolitie wordt gedrongen', te weten de voorafgaande rechterlijke machtiging en de beperking ten aanzien van een verdenking van een strafbaar feit als bedoeld in art. 67 Sv.
[682] Dit volgt uit het bij WCC-III in art. 354 Sv toegevoegde derde lid, luidende:
"*In de gevallen, bedoeld in artikel 353, eerste lid, neemt de rechtbank tevens een beslissing over het bevel, bedoeld in artikel 125p, indien een dergelijk bevel nog niet is opgeheven*".

klaagschrift, dan kan desgewenst de officier van justitie bij de raadkamer een vordering indienen tot afgifte van een last tot vernietiging van de ontoegankelijk gemaakte gegevens.[683] Leidt het onderzoek tot een concrete strafzaak, dan zal, indien de betreffende maatregel tot ontoegankelijkmaking nog niet is opgeheven, de strafrechter een beslissing moeten nemen over de toepassing van de maatregel.[684] De strafrechter kan daarbij, voor zover zulks noodzakelijk is ter voorkoming van nieuwe strafbare feiten, bepalen dat de betreffende gegevens worden vernietigd. Is dat niet het geval, dan dient te worden bepaald dat de gegevens weer aan de beheerder van het geautomatiseerde werk ter beschikking dienen te worden gesteld.[685]

7.7.2. Beslagbeslissingen: verbeurdverklaring en onttrekking aan het verkeer
In veel, zo niet nagenoeg alle, strafzaken waarbij (tevens) een verdenking bestaat van overtreding van art. 240b Sr zijn ook gegevensdragers (met daarop gegevens) en computersystemen in beslag genomen. Voor zover daarvan niet reeds afstand is gedaan, zal vervolgens ook door het OM dan wel de strafrechter een beslissing omtrent dit beslag moeten worden genomen.

Aandacht hierbij verdient dat onder het huidige Wetboek van Strafvordering gegevens slechts bij (grote) uitzondering zelfstandig in beslag kunnen worden genomen[686]; het zijn immers in beginsel geen goederen of vorderingen.[687] Uitzonderingen zijn echter wel denkbaar, maar doen zich uitsluitend voor ten aanzien van gegevens met een zekere reële/economische waarde, waardoor bespreking daarvan hier achterwege kan blijven.

7.7.2.1. Het OM-beleid
Blijkens de Aanwijzing kinderpornografie 2016[688] is het OM-beleid ter zake helder: indien op een *gegevensdrager* bestanden inhoudende afbeeldingen zoals bedoeld in art. 240b Sr staan, zal onttrekking aan het verkeer van die gegevensdrager gevorderd worden.[689]
Omdat het OM blijkens de Aanwijzing een computer met daarin een of meer harde schijven beoordeelt als één gezamenlijkheid van voorwerpen met betrekking tot welke het bewezenverklaarde feit is begaan (ook als de harde schijven in de loop van het onderzoek

[683] Zie art. 552fa, lid 1, Sv
[684] Zie artt. 354 jo. 353 Sv.
[685] Zie art. 354, lid 2 Sv.
[686] Het Wetboek van Strafvordering kent echter wel een maatregel die lijkt op de onttrekking aan het verkeer en die inhoudt dat de rechter kan beslissen dat bepaalde gegevens *die als voorlopige maatregel ontoegankelijk zijn gemaakt*, definitief worden vernietigd. Dit betekent dat de rechthebbende van die gegevens geen aanspraak kan maken op de "teruggave" van die gegevens en daarover niet meer kan beschikken. Dit is geregeld in de huidige artt. 354 en 552fa Sv. Een dergelijke beslissing kan de rechter nemen ten aanzien van gegevens met betrekking tot welke of met behulp waarvan het strafbare feit is begaan en als de vernietiging van die gegevens noodzakelijk is ter voorkoming van nieuwe strafbare feiten.
[687] Zie HR 3-12-1996, ECLI:NL:HR:1996:ZD0584 (n.g. op rechtspraak.nl); *NJ* 1997, 574 m.nt. van 't Hart. In dit arrest stelde de Hoge Raad vast dat gegevens geen goederen zijn, nu daarvan slechts sprake kan zijn als degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest als een ander zich de macht erover verschaft. Zie meer recent HR 4-12-2018, ECLI:NL:HR:2018:2244. De Hoge Raad stelt in dit arrest vast dat de opvatting dat afzonderlijke bestanden/gegevens op gegevensdrager evenzovele voorwerpen zijn waarop beslag rust en zijn te beschouwen als afzonderlijke voorwerpen a.b.i. in art. 36b Sr geen steun vindt in het recht.
[688] Zie de Aanwijzing Kinderpornografie (2016) van het College van Procureurs-Generaal d.d. 1 mei 2016, onder 3.2.4.
[689] De achtergrond van de focus in dit beleid op de gegevensdrager (en niet primair op de daarop aanwezige afbeeldingen) is dat uit het feit dat ingevolge art. 240b Sr niet alleen de kinderpornografische afbeelding, maar ook de gegevensdrager bevattende die afbeelding het voorwerp van strafbaarstelling is. Dit maakt dat de gegevensdrager zelf ook een strafbaar voorwerp is. In de visie van het OM brengt zulks met zich dat zij m.b.t. een gegevensdrager waarop zich kinderpornografische afbeeldingen bevinden wel onttrekking aan het verkeer *moet* verzoeken.

wellicht gescheiden zijn geweest van de computerkast), zal het OM derhalve als regel ook onttrekking vorderen van het (gehele) geautomatiseerd werk c.q. de computer of het device[690] waarin zich de gegevensdrager bevindt c.q. met welke de betreffende gegevensdrager met kinderpornografisch materiaal verbonden is (geweest).[691] Aandacht verdient hier dat het in dit opzicht gaat om de *technisch/operationele* samenhang tussen de diverse *voorwerpen*.

Dergelijke vorderingen leverden ten aanzien van *gegevensdragers* waarop zich kinderpornografische afbeeldingen bevinden in de rechtspraktijk langere tijd relatief weinig problemen op. In dat geval is immers in beginsel sprake van een voorwerp van zodanige aard dat het ongecontroleerde bezit daarvan in strijd is met de wet of het algemeen belang.[692]

Daarnaast blijkt de Hoge Raad geen al te hoge eisen te stellen aan wat als een (voor collectieve onttrekking vatbare) niet deelbare verzameling van kinderpornografisch materiaal kan worden aangemerkt. Voorwaarde is dan wel dat er wat betreft inhoudelijke kenmerken en/of de wijze van totstandkoming een zodanige samenhang bestaat met wel als zodanig gekwalificeerd kinderpornografisch materiaal dat het geheel als kinderporno dient te worden aangemerkt.[693] Meestal gaat het hierbij om series afbeeldingen van eenzelfde kind. Let wel: het gaat hier om de vraag in hoeverre op zichzelf niet als kinderpornografisch te beschouwen afbeeldingen, vanwege genoemde samenhang toch (ook) als kinderpornografisch kunnen worden aangemerkt.[694] Het gaat hier derhalve om de *inhoudelijke* samenhang van de *afbeeldingen*.

Een geheel andere vraag is echter of de enkele aanwezigheid van kinderpornografisch materiaal op een gegevensdrager met zich brengt dat de betreffende gegevensdrager sowieso onttrokken kan (of in de visie van het OM zelfs: *moet*) worden, met als consequentie dat *de facto* ook alle andere op die gegevensdrager aanwezige niet-strafbare gegevens worden onttrokken (en normaliter: vernietigd).

Steun voor het OM-standpunt is te vinden in het arrest van de Hoge Raad van 7 december 2010, waar de Hoge Raad onder meer overwoog:[695]

> *5.1. Het middel bevat de klacht dat het Hof afbeeldingen aan het verkeer heeft onttrokken die niet onder art. 240b Sr vallen.*

---

[690] Hierbij valt te denken aan andere geautomatiseerde werken met een geheugen(kaart) of harddisk, zoals bijvoorbeeld digitale fotocamera's, gameconsoles, tablets etc.
[691] Aanwijzing Kinderpornografie (2016), *a.w*, onder 3.2.1 en 3.2.4.
[692] Dat het hier gaat om een eigenschap van het materiaal/het object zelf, en zulks dus los staat van de vraag naar opzet of schuld bij de verdachte, lijkt te zijn miskend in o.m. Hof Den Bosch 25-4-2017, ECLI:NL:GHSHE:2017:1786
(Met betrekking tot het bezit van kinderporno is verweten dat verdachte een gegevensdrager bevattende een kinderpornografische afbeelding in bezit heeft gehad etc. Het betreft een laptop die regelmatig in een restaurant werd gebruikt door personeel, en daarnaast ook door de partner van verdachte. Vrijspraak ter zake van bezit van kinderporno. *De laptop wordt, gelet op dat oordeel, teruggegeven aan verdachte* (curs. auteur).
[693] HR 7-12-2010, ECLI:NL:HR:2010:BO6446, r.o. 5.4.
[694] Deze samenhang kan o.i. met zich brengen dat zelfs afbeeldingen op een gegevensdrager die op zichzelf beschouwd niet-kinderpornografisch zijn vanwege hun relatie tot wel als kinderpornografisch aan te merken materiaal op een *andere* gegevensdrager toch als kinderpornografisch worden aangemerkt, en dat dientengevolge ook de gegevensdrager waarop die afbeeldingen zich bevinden kan worden onttrokken.
[695] HR 7-12-2010, ECLI:NL:HR:2010:BO6446, r.o. 5.1 - 5.3.

> *5.2. De bestreden beschikking houdt dienaangaande in hetgeen reeds onder 2 is weergegeven, te weten:*
> *"Waar negatieven of dia's in de vorm van 'stroken' zijn inbeslaggenomen, of verschillende opnamen op één blad zijn afgedrukt - die derhalve niet zonder beschadiging of knippen van elkaar te scheiden zijn - heeft het hof - indien het tot het oordeel kwam dat een der opnamen van die strip of dat blad moest worden gekwalificeerd als kinderporno - het geheel als kinderporno aangemerkt. Het hof heeft dus niet zelf geknipt of gescheurd. Mutatis mutandis geldt hetzelfde voor de filmrol en de videocassette, op welke gegevensdragers twee van de vijf opnamen - ook volgens beslagene - kinderporno bevatten. In het geval dat verschillende opnamen van dezelfde jongen naar het oordeel van het hof de indruk maken tot stand te zijn gekomen in één fotosessie, heeft het hof vanwege dit onderlinge verband de hele serie als kinderporno aangemerkt."*
>
> *5.3. 's Hofs oordeel dat de uit negatieven of dia's bestaande stroken en de opnamen die op één blad zijn afgedrukt alsook de filmrol en videocassette moeten worden aangemerkt als niet deelbare voorwerpen welke vatbaar zijn voor onttrekking aan het verkeer, getuigt niet van een verkeerde rechtsopvatting.*

Men kan zich echter de vraag stellen of een “filmrol” en “videocassette” zich heden ten dage nog wel laten voldoende laten vergelijken met de meer moderne digitale gegevensdragers zoals bijvoorbeeld een geheugenkaart van 1TB of een harddisk van 4 TB. Dit klemt te meer als op die gegevensdrager ook zeer veel niet-strafbare (en geheel niets met kinderprorno te maken hebbende) gegevens (met een soms zeer waardevol en onvervangbaar karakter) en/of gegevens van derden aanwezig zijn. In die gevallen zal een onttrekkingsbeslissing die de facto ook de onttrekking van al deze andere gegevens inhoudt spanning oproepen met de eisen van proportionaliteit en subsidiariteit, en wellicht ook met de in het EVRM gegarandeerde rechten op eigendom en op eerbiediging van het familie- en privéleven.
Zoals hierna zal blijken is er thans dan ook in de rechtspraak verschil van inzicht over de vraag hoe moet worden omgegaan met de onttrekking van een gegevensdrager waarop zich naast kinderpornografisch materiaal ook evident niet-strafbare waardevolle of onvervangbare gegevens bevinden, zoals bijvoorbeeld administratieve gegevens of familiefoto’s. Hierop wordt hierna onder 7.7.2.2. ingegaan.

Opmerking verdient hier dat in de praktijk ook vorderingen tot onttrekking worden gedaan ten aanzien van gegevensdragers, zoals dvd’s en externe hard drives, die zijn aangetroffen bij een verdachte die (ook) kinderpornografisch materiaal op andere gegevensdragers in zijn bezit had, maar welke gegevensdragers zelf niet zijn onderzocht op de aanwezigheid van kinderpornografisch materiaal. Tenzij op enigerlei wijze aannemelijk wordt dat de betreffende gegevensdragers zijn gerelateerd aan het bezit (etc.) van kinderpornografisch materiaal (bijvoorbeeld blijkens opschriften, plaats van opbergen etc.) en de gegevensdragers aldus kunnen worden aangemerkt als behorende tot de gezamenlijkheid van voorwerpen waarmee het strafbare feit is begaan, is er dan waarschijnlijk geen rechtsgrond voor de onttrekking van voormelde gegevensdragers.[696] Een bijzonder geval betrof de onttrekking aan het verkeer van

[696] Vgl. in deze zin ook de conclusie van AG Vegter 11-1- 2011, ECLI:NL:PHR:2011:BP1285 (gevolgd door HR (81.1 RO), ECLI:NL:HR:2011:BP1285): “*In de hiervoor weergegeven overwegingen ligt evenwel besloten dat het Hof voornoemde 212 videobanden en 9 cd-roms - gelet op de aard van de bewezenverklaarde feiten - kennelijk heeft opgevat als een gezamenlijkheid van voorwerpen met betrekking tot welke de bewezenverklaarde feiten zijn begaan, op grond waarvan ook gezegd kan worden dat die gezamenlijkheid van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd is met de wet of met het algemeen belang. In aanmerking genomen dat de verdachte onder meer is veroordeeld ter zake van - kort gezegd - het vervaardigen van en het in bezit hebben van videobanden met kinderpornografie, heeft het Hof de onttrekking aan het verkeer van voornoemde gezamenlijkheid van voorwerpen kunnen gelasten*.” In deze zin niet geheel onproblematisch lijken dan ook: RB

een computer (merk: Medion) die was gebruikt voor het maken van back-ups van een andere computer (merk: HP) waarop kinderpornografisch materiaal aanwezig was. Het hof achtte onttrekking aan het verkeer noodzakelijk, nu "een geenszins denkbeeldige kans bestaat dat er op die computer kinderpornografisch materiaal staat, omdat niet blijkt dat het onderzoek door de politie van de computer (…) zodanig volledig is geweest dat voldoende kan worden uitgesloten dat daarop nog – verborgen of alleen bij uitvoeriger onderzoek traceerbaar – kinderpornografisch materiaal staat."[697] De Hoge Raad was evenals AG Spronken van oordeel dat de voormelde beslissing tot onttrekking aan het verkeer niet toereikend was gemotiveerd.[698] AG Spronken overwoog in dit verband onder meer dat niet was gebleken op grond waarvan volgens het hof aanwijzingen bestonden die het vermoeden konden rechtvaardigen dat mogelijk toch kinderpornografisch materiaal op de Medion-computer aanwezig was. Deze beslissing roept de vraag op of en zo ja, onder welke voorwaarden onttrekking aan het verkeer van geautomatiseerde werken/gegevensdragers waarop geen kinderpornografisch materiaal is aangetroffen, maar die wel verbonden zijn geweest met een geautomatiseerd werk waarop kinderpornografisch materiaal is aangetroffen, mogelijk is.
De uitvoering van het OM-beleid ten aanzien van het *onttrekken* van *geautomatiseerde werken* is overigens, zoals uit het volgende zal blijken, niet erg consistent. Weliswaar wordt in de Aanwijzing kinderpornografie (2016) aangegeven dat ook ten aanzien van dergelijke goederen onttrekking aan het verkeer dient te worden gevorderd, maar tegelijkertijd blijken steeds meer OM-functionarissen ter zitting aan te sturen op de *verbeurdverklaring* van geautomatiseerde werken.

7.7.2.2. Onttrekking aan het verkeer: ook ten aanzien van niet-strafbare gegevens?

De werkelijkheid ten aanzien van onttrekking blijkt weerbarstiger dan de eenvoud van de OM-aanwijzing doet vermoeden. Zoals hiervoor uiteengezet blijken op in beslaggenomen *gegevensdragers* ook andere gegevens dan strafbare kinderpornografische afbeeldingen te staan. Ongeclausuleerde onttrekking van de gegevensdrager impliceert dan tevens de automatische vernietiging van deze gegevens. Dat schuurt, zeker ook in die gevallen waarin bijvoorbeeld de verdachte wel wordt vrijgesproken, bijvoorbeeld omdat de opzet op het bezit van kinderpornografische afbeeldingen niet bewezen kan worden.
De rechtspraak worstelt blijkens de jurisprudentie thans zichtbaar met deze problematiek.[699] In hoofdlijnen beweegt de rechtspraak zich daarbij tussen twee uitersten: van "kale"

Amsterdam 26-1-2017, ECLI:NL:RBAMS:2017:537 (Bezit kinderporno; onttrekking aan het verkeer van 334 dvd's; de bewezenverklaarde kinderporno stond echter op een (eveneens onttrokken) computer en hard disk; toch onttrekking van ook alle dvd's omdat computer, hard disc en dvd's door Rb. worden opgevat als "een gezamenlijkheid van voorwerpen" met betrekking tot welke de strafbare feiten zijn begaan; voor dit laatste wordt echter geen enkele feitelijke onderbouwing in de uitspraak gegeven) en RB Arnhem (militaire kamer) 20-7-2009, ECLI:NL:RBARN:2009:BJ3015 (Kennelijk zeer grote hoeveelheid op de gegevensdragers aanwezige bestanden, slechts een relatief klein gedeelte daarvan is gecontroleerd op de aanwezigheid van kinderporno. Vaststaat dat op een aantal van de wel gecontroleerde gegevensdragers/bestanden een grote hoeveelheid materiaal is aangetroffen dat als kinderporno kan worden aangemerkt. Voorts staat vast dat verdachte zich gedurende een lange tijd bezig heeft gehouden met het digitaal zoeken naar kinderporno en dat hij bestanden met die inhoud heeft gedownload. In hoeverre dergelijk materiaal behalve op de voornoemde voorwerpen ook op de andere door verdachte gebruikte gegevensdragers terecht is gekomen kan de militaire kamer niet vaststellen. Naar het oordeel van de militaire kamer bestaat er een reëel risico dat de rest van de verzameling van bij verdachte in beslaggenomen digitale gegevensdragers niet (geheel) vrij is van kinderporno. De militaire kamer acht het ongecontroleerde bezit van die voorwerpen en de daarop aanwezige digitale bestanden daarom in strijd met het algemene belang zodat ook voornoemde voorwerpen onttrokken dienen te worden aan het verkeer).

[697] Hof Den Haag 9-2-2021, ECLI:NL:GHDHA:2021:2884.

[698] HR 6-12-2022, ECLI:NL:HR:2022:1815; en CAG Spronken, 18-10-2022, ECLI:NL:PHR:2022:960.

[699] Zie voor een beschrijving van de probleempunten (en een duidelijke stellingname): J. van den Bos, *Strafrechtelijke beslissingen inzake in beslag genomen gegevensdragers*, In: Trema 2017/10; zie voor een

onttrekking van de gehele gegevensdrager[700] tot opdracht aan de politie om de strafbare gegevens van de gegevensdrager te verwijderen en deze daarna te retourneren[701]. Problematisch hierbij is dat gegevensdragers, en in het bijzonder hard drives, tegenwoordig zeer grote hoeveelheden informatie bevatten[702]. Het is daarom voor de opsporingsdiensten redelijkerwijs niet praktisch uitvoerbaar om van dergelijke gegevensdragers alleen de strafbare gegevens te verwijderen, dan wel om daarvan alleen de niet-strafbare gegevens te kopiëren[703]. Deze omstandigheid c.q. dit gegeven wordt in de rechtspraak - onzes inziens ten

---

kritische beschrijving van de huidige regelgeving ook: S. Royer en J.J. Oerlemans, *Naar een nieuwe regeling voor beslag op gegevensdragers*, Computerrecht 2017/5.

[700] Hof Amsterdam 6-4-2016, ECLI:NL:GHAMS:2016:1274 (Bezit kinderpornografie. "*Anders dan de rechtbank heeft beslist, kan niet worden overgegaan tot teruggave van de genoemde harde schijven na verwijdering van de kinderpornografische beeltenissen, omdat niet gegarandeerd kan worden dat (delen van) de strafbare bestanden niet achterblijven op de gegevensdragers en met (tegenwoordig vrij algemeen verkrijgbare software) weer teruggehaald kunnen worden*"; RB Amsterdam 20-10-2016, ECLI:NL:RBAMS:2016:8065 (Veroordeling voor bezit kinderpornografie, overweging m.b.t. de onttrekking aan het verkeer van drie gegevensdragers: "*Op alle drie de gegevensdragers is kinderpornografisch materiaal aangetroffen. (..) Technisch is niet te garanderen dat de gegevensdragers volledig schoon van kinderporno teruggegeven kunnen worden. Wanneer de gegevensdragers desondanks worden teruggegeven aan verdachte, zou het strafbare materiaal opnieuw in omloop worden gebracht, wat voorkomen dient te worden. Om die reden worden gegevensdragers waarop kinderporno aanwezig is, aan het verkeer onttrokken. Wanneer naast strafbaar materiaal ook niet-strafbaar materiaal op een gegevensdrager aanwezig is, komt het voor rekening en risico van de verdachte dat het niet-strafbare materiaal samen met de kinderporno wordt vernietigd. Het maatschappelijke belang bij de vernietiging van de kinderporno weegt zonder meer zwaarder dan het belang van verdachte bij het beschikbaar houden van zijn privé-bestanden*."; Hof Arnhem Leeuwarden 1-2-2017, ECLI:NL:GHARL:2017:1124 (n.g. op rechtspraak.nl*):* Het hof begrijpt en onderschrijft de overwegingen van het openbaar ministerie die leiden tot bezwaar mee te werken aan het verkrijgen van bepaalde foto's op de externe harde schijf van de verdachte, waar ook kinderpornografisch materiaal aanwezig is, en onttrekt de externe harde schijf aan het verkeer zonder opdracht om de betreffende foto's er af te halen ten behoeve van de verdachte. Oordeel blijft in stand na cassatie: HR 4-12-2018, ECLI:NL:HR:2018:2244.

[701] Zie bijv**.** RB Zeeland-West-Brabant 25-3-2021, ECLI:NL:RBZWB:2021:1421 (vrijspraak van bezit van 80 kinderpornografische afbeeldingen (65 foto's en 15 video's). Beslag: *"(…) dat de andere gegevens ter beschikking van de verdachte moet worden gesteld en in zoverre zal een last worden gegeven tot teruggave aan de verdachte. Het is aan het OM om te besluiten op welke feitelijke wijze dit plaatsvindt. De rechtbank zal daarvoor een paar handvatten geven (…)*." De rechtbank noemt daarna twee 'methoden van verstrekking': het zodanig wissen van de kinderpornografische bestanden dat terughalen niet meer mogelijk is waarna de computer aan verdachte kan worden teruggegeven, en dat verdachte een lege gegevensdrager aanlevert waarop de politie de niet-strafbare gegevens kopieert.; RB Rotterdam 22-11-2017, ECLI:NL:RBROT:2017:9328 (veroordeling voor bezit en vervaardigen kinderpornografie. Beslag: "*de computer, externe harddisk en geheugenkaart moeten worden onttrokken aan het verkeer. De daarop opgeslagen privébestanden moeten worden gekopieerd en aan verdachte ter beschikking worden gesteld. Het is aan het OM te bepalen op welke wijze dit plaatsvindt"*); RB Rotterdam 25-1-2017, ECLI:NL:RBROT:2017:642 (laptop met daarop 9 kinderpornobestanden, opdracht aan OM: *of* teruggave laptop na verwijdering kinderporno, *of* niet kinderpornobestanden van laptop overzetten op een door verdachte aan te leveren gegevensdrager).

[702] Zo passen bijvoorbeeld op een tegenwoordig heel gebruikelijke hard disk van 1 TB 200.000 digitale foto's van 5 Mb (of 400.000 van 2,5 Mb) of ruim 88 *miljoen* Word-A4-tjes. Vgl. ook Hengeloër voor rechter om een miljoen kinderpornoplaatjes.

[703] Om dat te realiseren zou men namelijk dan eerst ieder individueel bestand moeten bekijken. In die zin ook de Aanwijzing Kinderpornografie (2016), onder 3.2.4 en o.m. Hof Arnhem-Leeuwarden 7-9-2017, ECLI:NL:GHARL:2017:7920 (De laptop wordt onttrokken aan het verkeer, aangezien het ongecontroleerde bezit daarvan in strijd is met het algemeen belang en de wet en het onevenredig veel werk is om deze laptop gegarandeerd vrij van kinderporno te krijgen); RB Den Haag 25-9-2017, ECLI:NL:RBDHA:2017:11341 (Verwijdering van aanwezig strafbaar materiaal zoals door de raadsman voorgesteld, is dermate ingewikkeld dat dit zoveel tijd en moeite kost dat dit in redelijkheid niet van het Openbaar Ministerie kan worden gevergd); RB Midden-Nederland 7-2-2017, ECLI:NL:RBMNE:2017:2874 **(**Klaagschrift 552a Sv, verzoek teruggave van een aantal bestanden die staan opgeslagen op (de harde schijf van) de in beslag genomen computer, waaronder familiefoto's en digitaal lesmateriaal dat aan klager verstrekt is in het kader van zijn behandeling. De rechtbank overweegt dat de computer in beslag is genomen en dat daarop bestanden zijn aangetroffen die volgens het

onrechte - nogal eens onderschat of als "uitvoeringsprobleem" beschouwd.[704] Daar komt nog bij dat het in het eerste geval technisch bijzonder moeilijk, zo niet onmogelijk, is te garanderen dat de alsdan verwijderde gegevens niet via speciale (tegenwoordig ruim en eenvoudig beschikbare) software kunnen worden "teruggehaald".[705]

De Hoge Raad heeft in zijn arrest van 4 december 2018[706] geoordeeld dat de opvatting dat afzonderlijke bestanden/gegevens op een gegevensdrager evenzovele voorwerpen zijn waarop het beslag rust en zijn te beschouwen als afzonderlijke voorwerpen als bedoeld in art. 36b Sr., geen steun vindt in het recht. Het teruggeven van losse bestanden/gegevens is daarom juridisch gezien onmogelijk. Aan de andere kant kan niet worden ontkend dat een verdachte of derden soms een zwaarwegend belang kunnen hebben bij het niet verloren gaan van bepaalde, soms onvervangbare, gegevens.[707]

Openbaar Ministerie aan te merken zijn als kinderporno. Het strafvorderlijk belang verzet zich daarom tegen de teruggave van die computer, inclusief de harde schijf. Daarbij wordt onderscheid gemaakt tussen het digitaal lesmateriaal (niet valt in te zien waarom dit niet nogmaals aan klager kan worden verstrekt) en de familiefoto's (op dit punt is het klaagschrift onvoldoende concreet/niet helder om welke bestanden het gaat en waar deze opgeslagen staan). Er volgt, gelet op de zeer omvangrijke hoeveelheid bestanden, en de motivering van het OM dat zulks uitzoeken veel capaciteit vergt en niet uit te sluiten is dat strafbaar materiaal zal worden mee gekopieerd, ongegrondverklaring); RB Maastricht (raadkamer) 21-2-2008, ECLI:NL:RBMAA:2008:BC5445 en RB Arnhem 29-4-2005, ECLI:NL:RBARN:2005:AT4918 (kinderporno; geen teruggave aan de verdachte van niet-strafbare gegevensbestanden om reden van onevenredige bewerkelijkheid voor de politie).

[704] Zie bijv. RB Midden-Nederland, 8-3-2017, ECLI:NL:RBMNE:2017:1117 (bewezenverklaard: gewoonte maken van vervaardigen en bezit kinderporno; verzoek teruggave van niet-kinderpornografische bestanden op laptop. "*Anders dan de officier van justitie beschouwt de rechtbank deze gegevens wel als voorwerpen waarover de rechtbank afzonderlijk kan beslissen. In deze zaak ziet de rechtbank hiertoe aanleiding. Zij zal bevelen dat de laptop zal worden onttrokken aan het verkeer nadat de niet-kinderpornografische inhoud daarvan aan verdachte ter beschikking is gesteld*."); RB Noord-Nederland 21-1-2013, ECLI:NL:RBNNE:2013:BZ9663 (Namens verdachte is terechtzitting verzocht om teruggave van de inbeslaggenomen computer en de daarbij behorende harde schijf. "*De officier van justitie heeft zich ter terechtzitting niet verzet tegen teruggave van de genoemde computer en harde schijf, doch heeft aangegeven dat teruggave van de computer en harde schijf pas kan plaatsvinden nadat het gewraakte kinderpornografische materiaal ervan is verwijderd. De rechtbank is gelet hierop van oordeel dat de inbeslaggenomen computer en de daarbij behorende harde schijf aan de verdachte moeten worden teruggegeven, doch eerst nadat door of vanwege het openbaar ministerie deze zijn ontdaan van het gewraakte kinderpornografische materiaal*."); RB Zutphen 27-4-2011, ECLI:NL:RBZUT:2011:BQ2758 (kinderporno; onttrekking van *3* (?) harde schijven, met gelijktijdige opdracht tot kopiëren en afgifte aan verdachte van daarop aanwezige privébestanden) en RB Breda 6-9-2012, ECLI:NL:RBBRE:2012:BX6898 (bezit kinderporno, onttrekking computer en harde schijf; last tot teruggave aan verdachte van "*alle zich op genoemde gegevensdragers bevindende bestanden die niet vallen onder de kinderpornobestanden*").

[705] Aldus ook o.m.: Hof Amsterdam 6-4-2016, ECLI:NL:GHAMS:2016:1274; RB Amsterdam 20-10-2016, ECLI:NL:RBAMS:2016:8065; Gerechtshof Leeuwarden, 24-5-2011, ECLI:NL:GHLEE:2011:BQ5793; RB Gelderland 6-3-2017 ECLI:NL:RBGEL:2017:1223 (telefoons worden onttrokken aan het verkeer. "*Gelet op de huidige technieken is het niet ondenkbaar dat de kinderpornografische foto's – ook na het wissen van de gegevens op de telefoon – toch nog teruggehaald kunnen worden. Het ongecontroleerde bezit van de telefoons is dan ook in strijd met het algemeen belang en de wet*."). Hierbij kan worden opgemerkt dat de meest gebruikelijke methode om hard drives *volledig* te schonen (door deze met behulp van een speciaal programma te "*wipen*"; (her)formatteren wist namelijk in Windows slechts de verwijzingstabel, niet ook de overige data op de schijf)) in dit geval niet mogelijk is, omdat dan ook de gegevens die zouden moeten worden geretourneerd, zouden worden overschreven/vernietigd.

[706] Hoge Raad 4-12-18, ECLI:NL:HR:2018:2244.

[707] Vergelijk in dit verband ook Nationale Ombudsman, rapport 2010/259 (Klacht over niet-teruggave foto's op inbeslaggenomen harde schijf; geen vervolging maar ook geen (gedeeltelijke) teruggave door OM, terwijl beklagtermijn is verlopen. "*De Nationale ombudsman beveelt het OM aan om óf de onttrekking aan het verkeer te vorderen van de harde schijf óf verzoeker inzage te geven in de kopie van de harde schijf (als deze nog aanwezig is) en hem die foto's terug te geven die voor hem van grote emotionele waarde zijn, zodat hij daarna afstand van de (kopie) harde schijf kan doen en deze vernietigd kan worden. Mocht het OM alles reeds vernietigd hebben, beveelt de Nationale Ombudsman het OM aan om een passende compensatie aan te bieden*."

Het Hof Den Haag heeft in een arrest van 14 februari 2019[708] - dat voortbouwde op een tussenarrest van 3 mei 2018[709] - vastgesteld en overwogen:

> *"dat de Nederlandse wetssystematiek vooralsnog geen expliciete juridische grondslag biedt om gegevens los te zien van de in beslag genomen gegevensdrager waarop zij zich bevinden (...) Dat betekent dat het hof in de onderhavige zaak onder het huidige recht gezien geen andere beslissing kan nemen dan de ongeclausuleerde onttrekking aan het verkeer van de in beslag genomen laptop, nu zich daarop ook kinderpornografisch materiaal bevindt en het ongecontroleerde bezit daarvan in strijd is met de wet."(...)*
> *Naar het oordeel van het hof vloeit uit de (...) verplichtingen voortvloeiende uit artikel 8 EVRM en artikel 1 van het Eerste Protocol bij het EVRM voort dat een verdachte zijn bezwaren tegen c.q. verzoeken ten aanzien van een voorgestelde wijze van afdoening met betrekking tot een inbeslaggenomen gegevensdrager, ook als het toeziet op de daarop aanwezige gegevens, aan de (straf)rechter moet kunnen voorleggen. Deze dient bij de beoordeling daarvan een belangenafweging te maken tussen de strafvorderlijke en maatschappelijke belangen bij onttrekking enerzijds en de persoonlijke belangen van de verdachte bij behoud c.q. verkrijging van de betreffende gegevens anderzijds, waarbij ook proportionaliteits- en subsidiariteitsaspecten dienen te worden betrokken. Naar het oordeel van het hof impliceert zulks eveneens de mogelijkheid dat de rechter beveelt dat specifieke bestanden die zich op een inbeslaggenomen gegevensdrager bevinden aan de verdachte zullen worden verstrekt. (...)*
> *Het hof is derhalve van oordeel dat het thans geldende Wetboek van Strafvordering voor waar het betreft het ontbreken van de mogelijkheid om gegevens(bestanden) die zich op een inbeslaggenomen gegevensdrager bevinden te onttrekken aan het verkeer (c.q. vanwege het ontbreken van een rechterlijke bevoegdheid om te bepalen dat specifieke gegevens(bestanden) die zich op een dergelijke gegevensdrager bevinden aan de verdachte moeten worden verstrekt) in zijn algemeenheid niet in overeenstemming is met het uit artikel 8 EVRM en artikel 1 van het Eerste Protocol bij het EVRM voortvloeiende vereiste dat er een "meaningful review of the lawfulness of and the justification for the measure" moet kunnen plaatsvinden van de betreffende inbeslagname van de gegevensdrager c.q. van de de facto inbeslagname van de zich daarop bevindende of daarvan overgenomen gegevens."*

Waar leidt dit volgens het Hof vervolgens praktisch toe?

> *"Het hof stelt in dit verband overigens voorop dat, indien sprake is van een gegevensdrager waarop strafbare gegevens zijn opgeslagen, als uitgangspunt heeft te gelden dat deze gegevensdrager aan het verkeer zal moeten worden onttrokken. Gezien de grote hoeveelheden data die zich vandaag de dag op gegevensdragers (kunnen) bevinden en in aanmerking nemende de huidige stand van de techniek, vormt het naar het oordeel van het hof een onevenredig grote belasting voor de opsporingsdiensten om gegevensdragers feitelijk op bestandsniveau te moeten onderzoeken teneinde vast te stellen of sprake is van strafbaar dan wel niet-strafbaar materiaal. Het hof laat daarbij in het midden dat ook al zou die exercitie wel plaatsvinden nog allerminst kan worden uitgesloten dat niet toch strafbaar materiaal op de betreffende gegevensdrager is achtergebleven.*

---

[708] Hof Den Haag 14-2-19, ECLI:NL:GHDHA:2019:391.
[709] Hof Den Haag 3-5-18, ECLI:NL:GHDHA:2018:1074.

Indien echter, zoals in het onderhavige geval, een verdachte gemotiveerd verzoekt om verstrekking van een of meer door hem (duidelijk) omschreven gegevensbestanden die op de betreffende inbeslaggenomen gegevensdrager zijn opgeslagen, dient een belangenafweging plaats te vinden tussen de strafvorderlijke en maatschappelijke belangen bij onttrekking enerzijds en de persoonlijke belangen van de verdachte bij behoud c.q. verkrijging van de verzochte gegevensbestanden anderzijds.

Bij deze belangenafweging kunnen naar het oordeel van het hof onder meer de navolgende aspecten worden betrokken:
- of, en zo ja: de mate waarin, door de verdachte informatie is verstrekt over het aantal gegevensbestanden waarop zijn verzoek toeziet alsmede over de daarop betrekking hebbende bestandsnamen en bestandslocaties;
- de (geschatte) technische en personele uitvoerbaarheid voor de betrokken opsporingsdienst die met het verzoek samenhangt alsmede het daarmee gemoeide tijdbeslag;
- het belang van de verdachte bij behoud c.q. verkrijging van de betreffende gegevensbestanden alsmede de mate waarin hij dat belang heeft onderbouwd;
- de omstandigheid of de verdachte door zijn wijze van handelen c.q. wijze van opslag moet worden geacht zelf het risico te hebben aanvaard van vermenging van strafbare en niet-strafbare gegevensbestanden en/of dat (daardoor) de gegevensbestanden waarop het verzoek betrekking heeft niet dan wel slechts op onevenredig arbeidsintensieve wijze weer van de strafbare gegevensbestanden kan worden gescheiden."

Nadien is in enkele uitspraken[710] met toepassing van het door het Hof uiteengezette beoordelingskader een verzoek om teruggave van een in beslag genomen gegevensdrager beoordeeld. Voor zover ons bekend heeft dit in één geval geleid tot het verstrekken van een kopie van de oorspronkelijk veiliggestelde gegevens teruggeven van gegevens aan een verdachte.[711] Het is wellicht goed om er op te wijzen dat de in het algemeen spraakgebruik gehanteerde terminologie 'teruggeven van gegevens' in juridische zin niet juist is. De gegevens blijven immers aanwezig op de inbeslaggenomen gegevensdrager (totdat die eventueel vernietigd wordt) en mogelijk ook in een gemaakte forensische kopie. Formuleringen als 'verstrekken van een kopie' verdienen daarom de voorkeur.

---

[710] RB Midden-Nederland 19-6-18, ECLI:NL:RBMNE:2018:2762, RB Rotterdam 20-6-18, ECLI:NL:RBROT:2018:4807, RB Rotterdam 26-6-18, ECLI:NL:RBROT:2018:6130 en Hof Den Haag 25-9-18, ECLI:NL:GHDHA:2018:2489. Vgl. minder gelukkig: RB Rotterdam, 11-10-2021, ECLI:NL:RBROT:2021:9956 (Afwijzing van het verzoek, nu geen schatting kan worden gemaakt van het gemoeide tijdsbeslag omdat de verdachte zijn verzoek niet concreet heeft gemaakt; de mate van onderbouwing van het verzoek lijkt hier ten onrechte als zelfstandig gezichtspunt in de belangenafweging te worden betrokken, terwijl ingeval van een onvoldoende gemotiveerd verzoek in het geheel niet aan de belangenafweging wordt toegekomen).

[711] Hof Den Haag 26-11-2019, ECLI:NL:GHDHA:2019:3149, "*In onderhavige strafzaak heeft het hof op 1 maart 2019 een tussenarrest gewezen. Het hof heeft daarin - kort gezegd - bepaald dat de verdachte in staat moet worden gesteld om op het politiebureau zijn reisverslagen (in woord en/of beeld) die zich op de harde schijf van de laptop bevinden aan te wijzen en in kopie te ontvangen, mits deze gang van zaken voor de politie werkbaar en uitvoerbaar is. Op 1 april 2019 is de verdachte op het politiebureau ontvangen en heeft hij voornoemde reisverslagen, bestaande uit enkele documenten en een aantal mappen met daarin een hoeveelheid afbeeldingen, in kopie ontvangen op een door hemzelf meegebrachte USB-stick.*"

7.7.2.3. Onttrekking aan het verkeer: behalve van losse gegevensdragers ook van computers en andere devices?

In voorkomende gevallen worden ook wel *geautomatiseerde werken* (computers, smartphones en vergelijkbare *devices*) die zijn gebruikt bij het begaan van een art. 240b-feit onttrokken aan het verkeer verklaard. Wij merken hierbij op dat er een overgang valt waar te nemen van de wijze waarop kinderpornografisch materiaal wordt opgeslagen en verzameld. Dit vond in het verleden vrijwel zonder uitzondering plaats met behulp van een traditionele computer, die het materiaal opsloeg op een (interne en/of externe) harde schijf. Tegenwoordig zien we steeds vaker opslag in de cloud, en ook gevallen waarin dergelijke opslag via een smartphone is bewerkstelligd. Denk daarbij aan het geautomatiseerd opslaan in een cloudomgeving van via social media-applicaties ontvangen afbeeldingen. De enkele omstandigheid dat niet kan worden uitgesloten dat in een cloudaccount opgeslagen strafbaar materiaal na teruggave van het geautomatiseerd werk alsnog daarop terecht komt, biedt onvoldoende grond voor de onttrekking aan het verkeer van dat geautomatiseerd werk.[712]

Bij beslissingen omtrent het onttrekken aan het verkeer lijkt het springende punt dan overigens niet te zijn dat het geautomatiseerde werk daarbij geen voorwerp zou betreffen met behulp van welke het feit is begaan. Dat lijkt in veruit de meeste gevallen voor de hand te liggen. Allereerst omdat in veel gevallen de onderdelen van een computer, waaronder in ieder geval een harde schijf, veelal als één gezamenlijkheid van voorwerpen zal kunnen worden beschouwd.[713] Voor externe harde schijven geldt wel dat vastgesteld zal moeten worden dat daarop voorkomend kinderpornografisch materiaal via de betreffende computer daarop terechtgekomen is. Dat het geautomatiseerd werk een voorwerp betreft met behulp waarvan het feit is begaan lijkt ook voor de hand te liggen omdat "zich via een geautomatiseerd werk toegang verschaffen tot kinderpornografie" naar zijn aard slechts kan worden begaan met behulp van een geautomatiseerd werk en voorts digitaal kinderpornografisch materiaal slechts met behulp van (het geheel van overige componenten van) een computer of een ander device op een gegevensdrager kan worden vastgelegd en in het overgrote deel van de gevallen ook slechts daarmee kan worden verspreid, gekopieerd, enzovoorts.[714] Hier lijkt echter ook wel anders over te worden gedacht.[715]

---

[712] HR 24-1-2023, ECLI:NL:HR:2023:85.

[713] Dat brengt zich dat in beginsel ook het *gehele* computersysteem waarin zich een harde schijf met kinderpornografische schijf als een te onttrekken gegevensdrager kan worden aangemerkt. Zie hiervoor verder echter ook hierna en hiervoor onder 7.7.2.1.

[714] Betoogd kan dan ook worden dat - tenzij aannemelijk wordt gemaakt dat de betreffende op een met de inbeslaggenomen computer verbonden gegevensdrager aanwezige strafbare gegevens (alleen) met een andere dan de inbeslaggenomen computer op die gegevensdrager zijn geplaatst - er vanuit gegaan kan worden dat de betreffende gegevens *met behulp van* de inbeslaggenomen computer op die gegevensdrager zijn geplaatst. Onzes inziens is er slechts indien de gewraakte gegevens zijn aangetroffen op een losse/mobiele gegevensdrager zoals een USB-stick aanleiding om eventueel ter zake nader onderzoek in te (laten) stellen.

[715] Zie bijvoorbeeld AG Knigge zijn conclusie (ECLI:NL:PHR:2016:156) bij HR 29-3-2014, ECLI:NL:HR:2016:526 waar hij o.m. stelt: "*Mogelijk heeft de Rechtbank geoordeeld dat het verwerven van de kinderporno met behulp van de computer is begaan. Dat oordeel is dan niet zonder meer begrijpelijk, in aanmerking genomen dat de klager in raadkamer verklaarde dat hij de (map met) bestanden van iemand anders had gekregen en dat hij geen internet heeft in de Tbs-kliniek zodat de bestanden niet door hem kunnen zijn gedownload*." Deze redenering leunt sterk op de verklaring van verdachte en gaat voorbij aan het feit dat de betreffende -beweerdelijk gekregen- bestanden vervolgens wel op de kennelijk aan verdachte toebehorende (naar moet worden aangenomen in de computer van verdachte aanwezige) hard disk zijn geplaatst, hetwelk toch bezwaarlijk op andere wijze kan zijn geschiedt dan door het met behulp van de computer van verdachte kopiëren van of verplaatsen van die gegevens vanaf een gegevensdrager van de gestelde derde naar de hard disk in de computer van verdachte. In zoverre is het toch niet zo onbegrijpelijk dat de rechtbank mogelijk heeft geoordeeld dat het verwerven van de kinderporno *met behulp van* de computer van verdachte was begaan.

Problematischer is echter wel de beantwoording van vraag in hoeverre een computer of andere *devices* zoals mobiele telefoons en digitale camera's waarop (al dan niet na verwijdering van de gegevensdrager met kinderpornografisch materiaal) zelf geen kinderpornografische afbeeldingen (meer) staan, (nog) van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd is met de wet of in strijd met het algemeen belang moet worden geacht. Gezien zijn arresten van 29 maart 2016[716] en 30 januari 2018[717] blijkt de Hoge Raad dit geenszins vanzelfsprekend te vinden. Het arrest van 29 maart 2016 betrof de onttrekking van een computer en een (vermoedelijk oorspronkelijk wel, maar op het moment van de beslagbeslissing niet meer in die computer aanwezige) harddisk met op die harddisk kinderpornografische afbeeldingen. De verdachte kwam daarbij op tegen de onttrekking van de computer(kast), waarop verder geen kinderpornografisch materiaal was aangetroffen. De Hoge Raad overwoog daarin: "*Het oordeel van de Rechtbank dat de computer vatbaar is voor onttrekking aan het verkeer is niet begrijpelijk, reeds omdat uit die beslissing van de Rechtbank niet blijkt met welk strafbaar feit de computer in verband staat of waarom de computer van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd is met de wet of met het algemeen belang*."[718] Het arrest van 30 januari 2018 betrof de (ongemotiveerde) onttrekking van 2 mobiele telefoons en 2 digitale camera's door het hof, welke beslissing met een nagenoeg gelijke formulering als die in het arrest van 29 maart 2016 werd gecasseerd.

Hieruit volgt dat de strafrechter in ieder geval de onttrekking aan het verkeer van een computer of ander device waarvan niet al reeds uit de bewijsmiddelen blijkt dat daarop (nog) strafbaar materiaal aanwezig is, goed zal dienen te motiveren. Daarbij kan waarschijnlijk een onderscheid worden gemaakt tussen de situatie waarin op het moment van de beslagbeslissing een gegevensdrager nog onderdeel uitmaakt van een computer, of daarmee min of meer vast verbonden is (of is geweest) en de situatie waarin dat niet (meer) het geval is (of was).[719]

In het eerste geval gaat het dan om de vraag of de strafrechter bij zijn beslagbeslissing een splitsing zou moeten aanbrengen tussen de computer en de zich nog daarin bevindende of daarmee verbonden gegevensdrager. Vanuit de zijde van verdachten wordt dit wel bepleit met de redenering dat na verwijdering van de gegevensdrager(r) uit de computer c.q. het verbreken van de verbinding tussen beide, er ten aanzien van de computer geen sprake meer zou zijn van een voorwerp dat van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd is met de wet of het algemeen belang.

In dit kader wordt allereerst opgemerkt dat het in dergelijke gevallen alleszins verdedigbaar lijkt om de computer en de gegevensdrager aan te merken als een als eenheid (of: als een gezamenlijkheid van voorwerpen) te beschouwen systeem/netwerk waarmee de in art. 240b Sr strafbaar gestelde gedragingen zijn begaan.[720]

---

[716] HR 29-3-2016, ECLI:NL:HR:2016:526.
[717] HR 30-1-2018, ECLI:NL:HR:2018:116.
[718] Opmerking verdient hier dat de Hoge Raad met dit arrest niet zozeer wilde uitsluiten dat naast gegevensdragers ook de computers waarin deze zich bevinden/bevonden onttrokken kunnen worden verklaard, maar veeleer problemen had met de wijze waarop de rechtbank dat in het concrete geval (zonder verwijzing naar bijvoorbeeld de criteria in art. 36c Sr) en zonder verwijzing naar de (mogelijke) relatie tussen de computer en het op de harddisk aanwezige materiaal had gemotiveerd.
[719] In het eerste geval lijkt immers aannemelijk, dat het geautomatiseerde werk en de betreffende gegevensdrager(s) moeten worden beschouwd als een gezamenlijkheid van voorwerpen met betrekking tot welke het bewezenverklaarde is begaan. Zie in dit verband o.m. HR 12-7-2011, ECLI:NL:HR:2011:BQ2488; Hof Amsterdam 26-4-2013, ECLI:NL:GHAMS:2013:BZ8885; AG Knigge in zijn conclusie (ECLI:NL:PHR:2013:2390) bij HR 14-1-2014, ECLI:NL:HR:2014:56; Hof Den Bosch, 10-2-2014, ECLI:NL:GHSHE:2014:317.
[720] Vgl. HR 23-12-1980, *NJ* 1981/208.

Bovendien zijn er in de rechtspraak van de Hoge Raad weinig tot geen aanknopingspunten te vinden voor het standpunt dat in dergelijke gevallen voorwerpen zouden moeten worden gesplitst in niet en wél voor onttrekking vatbare deelvoorwerpen[721] (i.c. bijvoorbeeld een systeemkast en een daarin geplaatste harde schijf).[722] Het lijkt dan ook reeds hierom onwaarschijnlijk dat de Hoge Raad ook in geval gecompromitteerde harddrives uit een computer kunnen worden gehaald, een beslissing van de feitenrechter om de gezamenlijkheid van computer en gegevensdrager(s) onttrokken te verklaren, zal casseren.

Dit laat echter onverlet dat er onder omstandigheden toch redenen kunnen zijn voor de strafrechter om een dergelijke splitsing te gelasten. Daarbij kan vooral worden gedacht aan situaties waarin op een gegevensdrager wel kinderpornografisch materiaal is aangetroffen, maar de verdachte desondanks wordt vrijgesproken van het bezit van dit materiaal. Indien en voor zover dat ook redelijkerwijs uitvoerbaar is, en kan worden uitgesloten dat er zich op eventueel terug te geven (onderdelen van) de computer nog strafbare afbeeldingen bevinden, dan is voorstelbaar dat de strafrechter beslist om (alleen) de gegevensdrager met de afbeeldingen te onttrekken aan het verkeer en de computer zelf (minus die gegevensdrager) te retourneren.[723]

Anders lijkt het te liggen indien het computers betreft waarop zelf geen strafbare gegevens zijn opgeslagen en waarvan ook anderszins niet kan blijken dat zij min of meer vast verbonden zijn (geweest) met de gegevensdrager waarop de gewraakte afbeeldingen zijn aangetroffen. Aangenomen moet worden dat in dat geval niet kan worden gezegd dat deze computer op zichzelf (het is dan immers een “gewone” computer als alle andere..) van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd zou zijn met de wet of het algemeen belang.[724] Ingeval er in die gevallen een veroordeling voor overtreding van art. 240b Sr voorligt en men om moverende redenen niet tot teruggave van het geautomatiseerde werk wil overgaan, lijkt het daarom meer aangewezen om de maatregel van verbeurdverklaring te overwegen.

---

[721] Aldus ook Meijer, *Tekst en Commentaar Strafrecht*, 14e druk, art. 33a, aantekening 5.

[722] Vgl. in dit verband ook RB Rotterdam 12-4-2017, ECLI:NL:RBROT:2017:3051 (verzoek om teruggave laptop met uitzondering van de harddisk (waarop kinderpornografie was aangetroffen); verdachte is onduidelijk over welke documenten nog op de laptop zouden staan en wat het belang daarvan nog is. Belangen van verdachte wegen niet op tegen de werklast voor de politie bij toewijzing van het verzoek; Onttrekking gehele laptop.) Wij tekenen hierbij wel aan dat niet was gevraagd om teruggave van de harddisk na het door de politie verwijderen van de kinderporno, of om teruggave van bepaalde bestanden. Betoogd was dat de harddisk zelf eenvoudig uit de laptop te verwijderen was (dat is inderdaad vaak binnen een paar minuten te doen), daar heeft de rechtbank niet op gerespondeerd. Dat er na verwijdering van de harddisk elders op de laptop nog bestanden zullen staan is geen realistisch scenario. Voorts overweegt de rechtbank dat de bestanden bevattende kinderporno aan het verkeer zullen worden onttrokken, aldus miskennende dat gegevens als zodanig in beginsel geen “goed” in strafrechtelijke zin zijn en dus niet kunnen worden onttrokken aan het verkeer.

[723] Aldus ook RB Den Bosch 27-1-2009, ECLI:NL:RBSHE:2009:BH0895 (vrijspraak bezit kinderporno op *unallocated clusters*; onttrekking hard disk afbeeldingen; last tot teruggave desktop computer); zie voor de discussie of de strafrechter wel bevoegd is een dergelijke “gesplitste” last te geven hiervoor onder 7.7.2.2.

[724] Zie HR 29-3-2016, ECLI:NL:HR:2016:526 (“*Het oordeel van de Rb dat de computer vatbaar is voor onttrekking aan het verkeer is niet begrijpelijk, reeds omdat uit die beslissing van de Rb niet blijkt met welk strafbaar feit de computer in verband staat of waarom de computer van zodanige aard is dat het ongecontroleerde bezit daarvan in strijd is met de wet of met het algemeen belang*.”; Zie ook art. 36c, laatste bijzin, Sr en art. 36d Sr. Zie in dit verband ook bijv. Hof Arnhem-Leeuwarden 3-5-2017, ECLI:NL:GHARL:2017:3682
(Beslag: twee mobiele telefoons niet onttrokken aan het verkeer zoals gevorderd door de AG, omdat niet vastgesteld kan worden dat deze voorwerpen van zodanige aard zijn dat het ongecontroleerde bezit daarvan in strijd is met de wet of het algemeen belang); HR 28-1-2014, ECLI:NL:HR:2014:187 (ontoereikende motivering *onttrekking* navigatiesysteem) en ouder: HR 2-11-1999, *NJ* 2000/37 (ontoereikende motivering *onttrekking* koffer waarin cocaïne is vervoerd).

7.7.2.4. Verbeurdverklaring van een geautomatiseerd werk.
Regelmatig is er in rechte ook discussie over een gevorderde verbeurdverklaring van *geautomatiseerde werken (computers)*. In het bijzonder indien daaruit de gegevensdragers met strafbare afbeeldingen zijn of kunnen worden verwijderd, of zelfs daarvan geen vast onderdeel hebben uitgemaakt (zoals bij externe harddrives of bij gebruik van cloudboxen). Er wordt dan wel betoogd dat (het bezit van) dit geautomatiseerde werk zelf niet in strijd met de wet is en/of dat verbeurdverklaring de verdachte onevenredig (extra) zou bestraffen.

Bij de beoordeling van dergelijke verweren zal allereerst de grondslag van de verbeurdverklaring kritisch moeten worden getoetst. Normaliter zal deze zijn dat met (behulp van) het betreffende geautomatiseerde werk de strafbare feiten zijn begaan. In de praktijk blijkt echter dat in het kader van het strafrechtelijk onderzoek veelal meerdere geautomatiseerde werken in beslag worden genomen, ten aanzien waarvan vervolgens ook vrijwel "automatisch" door het OM verbeurdverklaring wordt gevorderd. Lang niet van al deze geautomatiseerde werken blijkt vervolgens echter met voldoende zekerheid te kunnen worden vastgesteld dat deze zijn gebruikt bij de aan de verdachte verweten strafbare gedragingen ex art. 240b Sr.[725] De strafrechter zal derhalve in dergelijke gevallen bij zijn beoordeling van de vordering tot verbeurdverklaring veelal dienen te differentiëren tussen de onderscheiden in beslag genomen geautomatiseerde werken.[726]

Een tweede kwestie is of verbeurdverklaring van een geautomatiseerd werk achterwege dient te blijven als blijkt (wat in de regel het geval zal zijn) dat gecompromitteerde gegevensdragers uit dat geautomatiseerde werk kunnen worden verwijderd en het geautomatiseerde werk dus aldus "geschoond" zou kunnen worden geretourneerd. Of zelfs dat er in het geautomatiseerde werk zelf geen gegevensdragers met strafbare inhoud zijn aangetroffen, maar dat het geautomatiseerde werk gebruikt is om zich (via internet) toegang te verschaffen tot kinderpornografische afbeeldingen, dan wel om afbeeldingen op interne (hard drives) dan wel externe geheugenlocaties (zoals externe hard drives en cloudomgevingen) te plaatsen.
In dit kader wordt allereerst opgemerkt dat ook in laatstgenoemde gevallen in ieder geval voldaan is aan een van de wettelijke gronden voor verbeurdverklaring, te weten dat het een voorwerp betreft met behulp van welke het feit is begaan.[727] Het enkele gegeven dat een geautomatiseerd werk ook zonder hard drives met strafbare afbeeldingen kan worden geretourneerd, of dat een externe drive separaat zou kunnen worden verbeurdverklaard of onttrokken, doet hieraan op zich niet af. Zeker niet indien men in aanmerking neemt dat zulks nog niet maakt dat de betreffende geautomatiseerde werken niet meer zouden behoren tot het als eenheid te beschouwen systeem/netwerk c.q. tot een gezamenlijkheid van voorwerpen waarmee de in art. 240b Sr strafbaar gestelde gedragingen zijn begaan.[728]

---

[725] Zo worden bij doorzoekingen meestal alle computers in een woning in beslag genomen, dus ook die welke later overwegend of geheel in gebruik blijken te zijn geweest bij bijvoorbeeld een partner of kinderen.
[726] Zie in deze zin ook: HR 6-12-2016, ECLI:NL:PHR:2016:1200 (Ontoereikende motivering van de verbeurdverklaring van voorwerpen (telefoons, simkaarten, PC, iPod en Nintendo DS-doos) nu het hof niet heeft vastgesteld dat is voldaan aan de voorwaarden voor verbeurdverklaring ex art. 33a Sr. I.c. had het hof niet vastgesteld aan wie de verbeurdverklaarde voorwerpen toebehoren en wat de relatie was met (één van) de bewezenverklaarde feiten).
[727] Zie ook het hiervoor gestelde onder 7.7.2.1. in het bijzonder de mogelijk andere opvatting ter zake van AG Knigge in zijn conclusie (ECLI:NL:PHR:2016:156) bij HR 29-3-2014. ECLI:NL:HR:2016:526.
[728] Vgl. HR 23-12-1980, *NJ* 1981/208 en meer recent: Hof Amsterdam 18-10-2017, ECLI:NL:GHAMS:2017:4214 (gegevensdragers, telefoons en fototoestellen in beslag genomen. Uit het dossier blijkt dat een aantal van deze voorwerpen is gebruikt voor het (doen) opnemen van zijn seksuele handelingen met de slachtoffers en het bewaren van die opnames en het maken en opslaan van kinderpornografische

Zoals hiervoor al onder 7.7.2.1. gesteld, wordt als regel evenmin van de rechter verwacht dat hij bij zijn beslissing omtrent verbeurdverklaring van een voorwerp differentieert tussen bepaalde onderdelen van dat voorwerp, dus tussen bijvoorbeeld de computer zelf en een daarin aanwezige gegevensdrager (zoals een hard disk).

Het lijkt dan ook reeds hierom onwaarschijnlijk dat de Hoge Raad een beslissing van de feitenrechter om indien aannemelijk is geworden dat een computer feitelijk betrokken is geweest bij het begaan van de in art. 240b Sr omschreven feiten en gedragingen[729] tot verbeurdverklaring van die *gehele* computer (inclusief de daarop aanwezige gegevens) over te gaan, zal casseren.[730]

7.8. Benadeelde partij en schadevergoeding[731]

In art. 240b-zaken stelt zich slechts zelden een benadeelde partij en wordt (dus) ook zelden schadevergoeding gevorderd. De oorzaak daarvoor is allereerst gelegen in het feit dat de slachtoffers veelal niet bekend zijn, of niet met de rechtszaak tegen de verdachte bekend zijn, omdat zij bijvoorbeeld elders op de wereld wonen.

Voor zover ons bekend is er in Nederland nog geen rechtspraak (civiel- of strafrechtelijk) waarbij (bijvoorbeeld op vordering van een belangenorganisatie) aan anonieme slachtoffers van kinderpornografie schadevergoeding werd toegekend.[732] Er is in 2011-2012 wel sprake geweest van de oprichting van een overheidsfonds voor dergelijke anonieme slachtoffers. De gedachte daarbij was om de rechter de mogelijkheid te geven om een verdachte bij veroordeling te verplichten betalingen aan dat fonds te doen; deze betalingen zouden dan vervolgens ten goede komen aan de hulpverlening aan slachtoffers van kindermisbruik en aan de bestrijding van dat type criminaliteit. Anders dan in andere landen[733] is een dergelijk fonds er echter nooit gekomen.

In voorkomende gevallen kan echter – ook in het kader van bezit van kinderporno – wel sprake zijn van een identificeerbaar slachtoffer en van rechtstreekse[734] schade. Deze schade

---

afbeeldingen. Op grond hiervan beschouwt het hof voormelde voorwerpen als een gezamenlijkheid van voorwerpen met behulp waarvan het onder 9 (= kinderpornografie vervaardigen en in bezit hebben). bewezenverklaarde feit is begaan. Deze voorwerpen zullen worden verbeurd verklaard.) en RB Noord-Nederland 23-10-2017, ECLI:NL:RBNNE:2017:4057 (verzoek teruggave 3 computers waarop geen kinderporno is aangetroffen wordt niet gehonoreerd, verbeurdverklaring nu de feiten met de computers zijn begaan en deze toebehoren aan verdachte).

[729] Indien dat niet zo is, is er waarschijnlijk ook geen rechtsgrond (bij vrijspraak kan ook de bijkomende straf van verbeurdverklaring niet worden opgelegd) om tot verbeurdverklaring van de computer over te gaan.

[730] Zie bijv. ook RB Noord-Nederland 4-5-2017, ECLI:NL:RBNNE:2017:1681 **(“***De in beslag genomen computer met een harddisk is vatbaar voor verbeurdverklaring, nu feit 3 (bezit kinderporno en verschaffen toegang tot kinderporno) daarmee is begaan*”).

[731] Zie hierover uitgebreider: Mr. C.E. Dettmeijer-Vermeulen en mr. L. van Krimpen*, Schadevergoeding voor bezit van kinderpornografie: juridische mogelijkheden en praktische obstakels*, Tijdschrift Praktijkwijzer Strafrecht (TPWS) 2014/26.

[732] In de VS wordt in veel staten (en ook federaal) echter ook een *bezitter* van kinderpornografisch materiaal aansprakelijk geacht voor de schade bij het afgebeeld kind, ook voor die schade die het gevolg is van het afgebeelde misbruik). Regelmatig worden in geval van anonieme slachtoffers (aanzienlijke) forfaitaire bedragen toegewezen, welke dan in bepaalde fondsen dienen te worden gestort.

[733] Zoals bijvoorbeeld het Verenigd Koninkrijk en Canada (The Justice for victims of child pornography act (Canada), https://web2.gov.mb.ca/bills/39-5/b220e.php).

[734] In voorkomende gevallen kan ook sprake zijn van verplaatste schade ex art. 6:107 BW, met name immateriële schade bij de ouders en/of de kosten die zij als gevolg van het delict voor hun daarbij als slachtoffer betrokken kind hebben gemaakt. Uit HR 16-9-2014, ECLI:NL:HR:2014:2668 kan worden afgeleid dat een in het kader van

zal dan veelal zijn oorzaak vinden in de wetenschap dat die afbeeldingen voor anderen zichtbaar zijn, en in de daarmee samenhangende gevoelens van schaamte (en soms depressiviteit en suïcidaliteit). In die optiek, welke ook in de – in dit opzicht overigens zeer schaarse – rechtspraak is gevolgd, is het bezitten en bekijken van kinderpornografie ook een inbreuk op het fundamentele recht op privacy (ex art. 8 EVRM) en de daaruit voortvloeiende schade dus ook het rechtstreekse en voorzienbare gevolg daarvan.[735] Deze benadering kan tevens als voordeel in zich dragen dat niet telkenmale de benadeelde partij ook dient aan te tonen dat hij/zij door voormeld handelen immateriële schade heeft geleden bestaande uit aantasting in zijn persoon[736], maar onder omstandigheden kan volstaan met het vragen van schadevergoeding voor voormelde aantasting van zijn recht op privacy *sec*.

De hoogte van de toegekende schadevergoeding lijkt daarbij ook af te hangen van de omvang en de aard van het handelen van een verdachte. Grosso modo lijken de door de strafrechter toegekende vergoedingen zich te bewegen in een bandbreedte van € 500 tot € 1.000, indien alleen sprake is van bezit van afbeeldingen van de benadeelde partij[737] en van € 1.100 tot € 3.500, indien daarnaast ook sprake is van verspreiding (al dan niet via internet).[738]

---

een vordering benadeelde partij ingediende vordering tot vergoeding van verplaatste schade niet zonder meer kan worden afgewezen op de enkele grond dat de ouder(s) niet zelf slachtoffer zijn c.q. dat dergelijke schade jegens hen niet als rechtstreekse schade als bedoeld in art. 51f Sv kan worden aangemerkt. Zoals ook uit genoemd arrest blijkt zal echter de behandeling van een dergelijke vordering, waaronder het maken van onderscheid welke schade moet worden toegerekend aan het kind zelf, en welke aan de ouder(s), veelal een onevenredige belasting van het strafgeding opleveren. Zie over de problematiek van de verplaatste schade verder: T.J.C. Bueters, *Verplaatste schade in de strafprocedure na Robert M.,* Tijdschrift Letselschade in de rechtspraktijk, 2015, aflevering 3 (23 mei 2015).

[735] Aldus RB Amsterdam (tussenvonnis) 21-6-2012, ECLI:NL:RBAMS:2012:BW9108 en RB Amsterdam (eindvonnis) 23-7-2012, ECLI:NL:RBAMS:2012:BX2325 in de zgn. Robert M.-zaak. Zie ook Hof Amsterdam 26-4-2013, ECLI:NL:GHAMS:2013:BZ8895 m.b.t. de met deze zaak verband houdende zaak van de partner van Robert M. die in hoger beroep alleen werd veroordeeld voor het medeplegen van bezit van kinderporno.

[736] Met alle daarmee verband houdende eisen qua (medische) bewijsvoering van dien.

[737] RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (€ 1.000) Hof Amsterdam, 26-4-2013, ECLI:NL:GHAMS:2013:BZ8895 (€ 500); RB Amsterdam 19-1-2017, ECLI:NL:RBAMS:2017:225 (deels heimelijk vervaardigen kinderporno; geen verspreiding; toekenning van schadevergoeding aan diverse BP's ter hoogte van € 1.000 tot € 1.500 (indien ook psychische druk etc. bij vervaardiging).

[738] RB Noord-Nederland 12-9-2019, ECLI:NL:RBNNE:2019:4203 (€ 1.250, verspreiding van naaktfoto's van 2-jarig zoontje onder chatcontacten); RB Overijssel 16-3-2018, ECLI:NL:RBOVE:2018:811 (€ 2.000, onduidelijk is in hoeverre m.b.t. deze benadeelde ook sprake was van verspreiden); RB Gelderland 25-11-2013, ECLI:NL:RBGEL:2013:4849 (verspreiding via internet; € 1.100,00); RB Midden-Nederland 23-8-2016, ECLI:NL:RBMNE:2016:4673 (verspreiding, ook plaatsing op facebookaccount van slachtoffer; € 1500); RB Oost-Brabant 19-8-2016, ECLI:NL:RBOBR:2016:4488 (openbaarmaking plaatsing kinderpornografische afbeelding met vernederende bijschriften; toekenning € 2500); Hof Den Haag 27-10-2016, ECLI:NL:GHDHA:2016:3213, (ernstige o.m. psychische gevolgen door openbaarmaking op Facebook; immateriële schadevergoeding € 3.500).

HOOFDSTUK 8: VOORLOPIGE HECHTENIS EN STRAFTOEMETING

8.1. Voorlopige hechtenis

In beginsel is bij verdenking van overtreding van art. 240b Sr voorlopige hechtenis toegelaten.[739] De praktijk blijkt echter genuanceerd. Indien het zaken betreft waarin de verdenking lijkt te zijn beperkt tot het enkele in bezit hebben van niet al te grote aantallen afbeeldingen, blijkt terughoudend gebruik te worden gemaakt van het instrument van de voorlopige hechtenis. In die gevallen zal het voorarrest veelal beperkt blijven tot maximaal 3 dagen inverzekeringstelling of zal de verdachte weliswaar worden voorgeleid aan de rechter-commissaris, maar zal de bewaring – zeker als de verdachte tevens zwaarwegende persoonlijke belangen heeft (bijv. werk) – vervolgens worden geschorst.[740] Bij recidive, als ernstig aan te merken gedragingen zoals het (tevens) produceren en/of verspreiden van een grote hoeveelheid kinderporno of het in bezit hebben van grote aantallen afbeeldingen, blijkt over het algemeen wel voor langere duur voorlopige hechtenis te worden toegepast.
Als grond voor de voorlopige hechtenis wordt dan gewoonlijk herhalingsgevaar (en incidenteel ook: collusiegevaar) genoemd.

Herhalingsgevaar als grond voor voorlopige hechtenis is in deze gevallen overigens juridisch niet onproblematisch. Op overtreding van art. 240b Sr (zonder de strafverzwarende omstandigheden genoemd in art. 240b, tweede lid, Sr en art. 248 Sr) is namelijk een maximumstrafbedreiging gesteld van *4* jaar (en niet de in art. 67a, tweede lid, onder 2, Sv genoemde strafbedreiging van *6* jaar of meer), terwijl er voorts discussie over bestaat in hoeverre met name door het *bezit* van kinderpornografie de gezondheid of veiligheid van personen (i.c. minderjarigen) in gevaar kan komen.[741]

Bij bezit van grotere aantallen afbeeldingen of indien sprake (b)lijkt te zijn van een zich over een langere periode en/of veelvuldig voordoen van in art. 240b Sr strafbaar gestelde gedragingen zal derhalve een officier van justitie er in de regel verstandig aan doen te overwegen om in zijn vordering(en) met betrekking tot de voorlopige hechtenis, tevens "het gewoonte maken" als omschreven in art. 240b, tweede lid, Sr op te nemen.[742]

8.2. Straf- en sanctiemodaliteiten

Bij veroordeling wegens overtreding van art. 240b Sr kan de strafrechter in beginsel alle in het Wetboek van Strafrecht genoemde sanctiemodaliteiten toepassen.
Voor wat betreft de oplegging van de taakstraf gelden daarbij ten aanzien van feiten gepleegd voor 3 januari 2012[743] ingevolge art. 22b Sr echter wel beperkingen. Daarop wordt in de volgende paragraaf in gegaan.

---

[739] Zie art. 67, lid 1 onder a Sv.
[740] Hier komt ook art. 67a, lid 3, Sv in beeld, omdat – zoals hierna zal blijken – bij *first offenders* die worden veroordeeld voor alleen het bezit van niet al te grote hoeveelheden kinderporno in de praktijk lang niet altijd een onvoorwaardelijke gevangenisstraf van enige duur wordt opgelegd.
[741] Dit verband is namelijk immers veelal slechts indirect te leggen. Vgl. ook Cleiren, Crijns en Verpalen, *Tekst en Commentaar Strafrecht*, 11e druk, art. 240b, aantekening 1. ("*Seksueel misbruik van jeugdigen moet worden tegengegaan en daarom ook de digitale exploitatie van dergelijk misbruik. Centraal staat de bescherming van de (afgebeelde) minderjarige*"). Zie ook hierna onder 8.4.3. met betrekking tot de criteria voor directe uitvoerbaarheid van bijzondere voorwaarden.
[742] De maximumstrafbedreiging wordt dan immers verhoogd naar 8 jaar gevangenisstraf, waardoor dan in ieder geval wel voldaan wordt aan de in art. 67a, lid 2, onder 2, Sv genoemde minimale strafbedreiging van 6 jaar.
[743] Zie HR 29-1-2014, ECLI:NL:HR:2014:186 (invoering art. 22b heeft geen terugwerkende kracht.)

8.2.1 Oplegging van de Tbs-maatregel
Er kan twijfel bestaan over de mogelijkheid om *alleen* voor overtreding van art. 240b Sr een Tbs- of PIJ-maatregel op te leggen, aangezien de wet daarvoor tevens bepaalt dat "*de veiligheid van anderen, dan wel de algemene veiligheid van personen (...) het opleggen van die maatregel eist*". Met name indien het *alleen* om bezit of andere vormen van meer passieve gedragingen met betrekking tot kinderpornografie gaat is het niet aanstonds vanzelfsprekend dat de strafrechter zal aannemen dat aan deze maatstaf is voldaan. Lange tijd waren op rechtspraak.nl dan ook geen uitspraken te vinden waarbij *alleen* voor overtreding van art. 240b Sr de Tbs-maatregel is opgelegd.[744]

Er lijkt echter meer recent sprake te zijn van een zekere uitbreiding van de toepassing van Tbs, met name in zaken waarin het gaat om méér dan enkel bezit (ook verspreiden en/of vervaardigen), sprake is van recidive en ook de strafverzwarende omstandigheid "een gewoonte maken" aan de orde is. Het blijkt daarbij dan met name te gaan om oplegging van de Tbs met voorwaarden.[745]

Oplegging van een Tbs-maatregel met dwangverpleging voor (alleen) art. 240b-feiten is echter ook voorgekomen.[746] Zou een Tbs-maatregel met dwangverpleging worden opgelegd of is sprake van een (toekomstige) omzetting van een Tbs met voorwaarden naar een Tbs met dwangverpleging, dan is een vervolgvraag of deze Tbs-maatregel dan gemaximeerd is tot maximaal 4 jaar of niet. In het verleden is veelal aangenomen dat "het voorhanden hebben van kinderporno op zichzelf, hoe onwenselijk dergelijke gedragingen ook zijn, geen handelen oplevert dat gericht is tegen of gevaar oplevert voor de onaantastbaarheid van het lichaam van een of meer personen, en dat derhalve de duur van de aan de terbeschikkinggestelde opgelegde maatregel beperkt is tot vier jaar".[747]

---

[744] Uit Hof Arnhem 7-5-2012, ECLI:NL:GHARN:2012:BW7191 is echter wel af te leiden dat dit wel voorkwam. Er zijn bovendien wel diverse uitspraken waarbij bij gelijktijdige veroordeling voor overtreding van art. 240b Sr en nog andere (meestal zeden-gerelateerde) feiten de Tbs-maatregel is opgelegd, zoals: RB Rotterdam 7-11-2016, ECLI:NL:RBROT:2016:8473 (Tbs met dwangverpleging voor o.m. 240b Sr), Hof Den Bosch 24-8-2016, ECLI:NL:GHSHE:2016:3767 (idem) en RB Den Haag 22-3-2018, ECLI:NL:RBDHA:2018:3316 (veroordeling wegens mensenhandel, ontucht en 240b Sr. m.b.t. één slachtoffer).
[745] Zie bijv. RB Midden-Nederland 22-11-2016, ECLI:NL:RBMNE:2016:6168 (zie bijv. verspreiden, aanbieden, verwerven, bezit van en zich toegang verschaffen tot kinderporno, 3.000 foto's en 82 films. Recidive. Gebruik anonieme netwerken en versleutelde gegevensdragers. Voeren van chatgesprekken met een – vermoedelijke – vervaardiger van kinderporno. Oplegging van zowel gevangenisstraf als Tbs met voorwaarden); RB Oost-Brabant 22-2-2017, ECLI:NL:RBOBR:2017:893 (gewoonte gemaakt van het verzamelen van kinderpornografie; oplegging van de maatregel Tbs met voorwaarden); RB Overijssel 12-1-2016, ECLI:NL:RBOVE:2016:72 (Bezit en verspreiding kinderporno (jonger dan 12 jaar) 15 maanden cel en Tbs met voorwaarden) en Hof Den Haag 11-04-2019, ECLI:NL:GHDHA:2019:848 (gedurende twee periodes van 7 jaar misbruik van nichtje resp. dochter alsmede bezit van kinderporno, gevangenisstraf van 4 jaar en dadelijk uitvoerbaar verklaarde Tbs met dwangverpleging). Zie met betrekking tot de motivering van de beslissing van oplegging van Tbs met voorwaarden ook HR 30-1-2018, ECLI:NL:HR:2018:116 (HR komt terug op ECLI:NL:HR:2013:BY8434 m.b.t. motiveringsplicht of sprake is van een geweldsmisdrijf indien Tbs is opgelegd zonder dwang. Met het oog op de mogelijke, in art. 38c Sr voorziene, omzetting van Tbs zonder dwang in Tbs met dwang en vervolgens de verlenging daarvan, moet thans worden aanvaard dat, in het geval dat Tbs met voorwaarden is opgelegd, eenzelfde motiveringsvoorschrift geldt. Oordeel hof dat aan verdachte de maatregel van Tbs met voorwaarden is opgelegd ter zake van een geweldsmisdrijf is gezien veroordeling voor (gewoonte maken van) gedragingen met kinderporno niet begrijpelijk (vgl. ECLI:NL:HR:2017:524).
[746] Zulks blijkt o.m. uit Hof Arnhem 7-5-2012, ECLI:NL:GHARN:2012:BW7191. Bij oplegging van de Tbs-maatregel met dwangverpleging gaat het echter meestal om zaken waarin niet enkel sprake is van gedragingen met kinderpornografie maar ook van ontucht met minderjarigen; zie bijv. RB Overijssel 28-11-2017, ECLI:NL:RBOVE:2017:4443 (gevangenisstraf van 5 jaar en tot de maatregel van terbeschikkingstelling met dwangverpleging voor langdurige ontucht met 2 minderjarige meisjes en het maken en het wereldwijd verspreiden van kinderporno).
[747] Aldus Hof Arnhem 7-5-2012, ECLI:NL:GHARN:2012:BW7191.

Zoals hierna onder 8.4.1. nader zal worden besproken, is ten aanzien van strafbare gedragingen met kinderpornografisch materiaal de laatste jaren in de lagere rechtspraak steeds breder aangenomen dat deze gedragingen wel *gericht zijn tegen of gevaar opleveren voor de onaantastbaarheid van het lichaam van een of meer personen*. A fortiori werd daaruit ook wel afgeleid dat in dergelijke gevallen ook oplegging van een ongemaximeerde Tbs-maatregel mogelijk was.[748]

Bij arrest van 28 maart 2017 heeft de Hoge Raad echter geoordeeld dat het (een gewoonte maken van) verwerven en zich toegang verschaffen tot, alsmede het in bezit en voorraad hebben van kinderporno *geen* gedragingen bevat die onmiskenbaar zijn gericht tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen.[749] Dit brengt met zich dat ongemaximeerde Tbs voor (alleen) deze gedragingen met kinderporno *niet* kan worden opgelegd.[750]

8.2.2. Art. 22b / 77ma Sr (in beginsel geen taakstraf bij veroordeling voor art. 240b Sr)
Ingevolge de artt. 22b, lid 1, onder b, en 77ma, lid 1, onder b, Sr mag bij veroordeling voor overtreding van art. 240b Sr in beginsel geen taakstraf worden opgelegd. Daarvan kan bij meerderjarigen[751] echter worden afgeweken, indien naast de taakstraf een *onvoorwaardelijke* vrijheidsstraf of vrijheidsbenemende maatregel wordt opgelegd. De tekst van de bepalingen laat derhalve toe dat de rechter bij de straftoemeting een taakstraf combineert met een (soms: zeer korte) onvoorwaardelijke gevangenisstraf of jeugddetentie (bijv. 1 dag[752]). Deze strafcombinatie wordt met name bij *first offenders* ten aanzien van wie alleen *bezit* van kinderporno bewezen is verklaard regelmatig toegepast.

---

[748] In deze zin ook expliciet: Hof Arnhem-Leeuwarden 26-8-2016, ECLI:NL:GHARL:2016:6883 (Oplegging TBS met voorwaarden voor bezit, toegang verschaffen tot en verspreiden (plaatsen op forum) van grote hoeveelheden (626.818 foto's en 6.551 filmpjes) kinderporno, waaronder zeer extreem materiaal); overweging hof dat bij eventuele omzetting naar dwangverpleging de feiten moeten worden aangemerkt als zijnde delicten die gericht zijn tegen of een gevaar veroorzaken voor de onaantastbaarheid van het lichaam van personen en derhalve dan de TBS ongemaximeerd zal zijn).

[749] HR 28-3-2017, ECLI:NL:HR:2017:524, r.o. 2.5.3.; zie ook HR 30-1-2018, ECLI:NL:HR:2018:116, r.o. 3.4.2. (een gewoonte maken van (i) het verwerven, in bezit hebben en zich toegang verschaffen en (ii) het verspreiden, aanbieden en openlijk tentoonstellen van kinderporno - kunnen niet zonder meer worden gekarakteriseerd als misdrijven die onmiskenbaar zijn gericht tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen in de zin van art. 38e, eerste lid, Sr).

[750] Aannemelijk is dat RB Den Haag 30-3-2018, ECLI:NL:RBDHA:2018:3541, waarin anders werd geoordeeld (oplegging voorwaardelijke TBS voor alleen gewoonte maken van bezit en toegang verschaffen kinderporno) is gewezen voordat men kennis had genomen van voormeld arrest van de Hoge Raad van 28-3-2018.

[751] Voor minderjarigen geldt namelijk dat in art. 77ma Sr de in art. 22b, lid 3 Sr opgenomen beperking dat de naast de taakstraf opgelegde sanctie een *onvoorwaardelijke* gevangenisstraf of vrijheidsbenemende maatregel moet zijn, ontbreekt. Derhalve kan ook bij veroordeling van minderjarigen voor overtreding van art. 240b (en/of andere zedenfeiten) wel een werkstraf in combinatie met een *voorwaardelijke* jeugddetentie worden opgelegd; zie bijv. RB Den Haag 14-9-2017, ECLI:NL:RBDHA:2017:10942 (Jeugdzaak. Seksueel misbruik 5 jarig buurmeisje door 13-jarige verdachte, welk misbruik door verdachte is gefilmd en via social media tweemaal is doorgestuurd naar een vriendin van hem. Bewezenverklaring van o.m. ontucht (binnendringen) en het vervaardigen en verspreiden van kinderporno. Sanctie: 40 uur ws en 1 wk jd voorwaardelijk (met bijzondere voorwaarden).

[752] Veelal wordt daarbij aangesloten bij de duur van de ondergane inverzekeringstelling of voorlopige hechtenis. Zie bijv. RB Gelderland 15-6-2017, ECLI:NL:RBGEL:2017:3152 (gevangenisstraf van 181 dagen waarvan 180 voorwaardelijk en werkstraf van 240 uur voor het plegen van ontucht met een minderjarige en het vervaardigen, verwerven en bezitten van kinderporno); RB Amsterdam 1-8-2017, ECLI:NL:RBAMS:2017:5532 (bezit kinderporno; 180 dagen gevangenisstraf waarvan 179 voorwaardelijk).

Er zijn echter ook meerdere voorbeelden uit de rechtspraak, waarbij aan het gestelde in art. 22b c.q. art. 77ma Sr door de strafrechter geheel voorbij is gegaan[753] en waarbij de strafrechter dus – naar mag worden aangenomen: opzettelijk – *contra legem* handelt.

8.3. Straftoemeting

8.3.1. Wettelijke strafbedreiging, strafvermeerderende factoren en bijkomende straffen en maatregelen.
De maximum wettelijke strafbedreiging op overtreding van art. 240b Sr is een gevangenisstraf voor de duur van vier jaren en/of een geldboete van de vijfde categorie. Indien bewezen is verklaard dat de verdachte een beroep of gewoonte heeft gemaakt van handelen als bedoeld in art. 240b, tweede lid Sr, wordt de maximumstraf verhoogd tot een gevangenisstraf van acht jaren (en/of een geldboete van de vijfde categorie).

In de praktijk blijken de wettelijke strafvermeerderende omstandigheden die zijn genoemd in art. 248b Sr weinig aandacht te krijgen. Art. 248 Sr bepaalt dat de straffen genoemd in art. 240b met een derde kunnen worden verhoogd, indien het feit:

- wordt gepleegd door twee of meer personen;
- wordt begaan tegen zijn kind, een kind over wie hij het gezag uitoefent, een kind dat hij verzorgt of opvoedt als behorend tot zijn gezin, zijn pupil, een aan zijn zorg, opleiding of waakzaamheid toevertrouwde minderjarige of zijn minderjarige bediende of ondergeschikte;
- wordt begaan tegen een persoon waarbij misbruik van een kwetsbare positie wordt gemaakt;
- is voorafgegaan, vergezeld of gevolgd van geweld.[754]

Indien overtreding van art. 240b Sr zwaar lichamelijk letsel ten gevolge heeft, of daarvan levensgevaar voor een ander te duchten is, wordt het strafmaximum verhoogd tot 15 jaar. Heeft het feit de dood tot gevolg dan wordt het strafmaxima verhoogd tot 18 jaar.

---

[753] Zie bijv. RB Noord-Nederland, 1-7- 2021, ECLI:NL:RBNNE:2021:2863 ("*Al met al acht de rechtbank oplegging van een onvoorwaardelijke straf niet passend gelet op de problematiek van verdachte, het tijdsverloop in deze zaak, het feit dat verdachte al drie jaar op eigen initiatief een behandeling volgt en sinds het bewezenverklaarde feit niet nogmaals met politie of justitie in aanraking is gekomen. De rechtbank zal dan ook volstaan met oplegging van een voorwaardelijke gevangenisstraf*."); RB Zeeland-West-Brabant 21-6-2021, ECLI:NL:RBZWB:2021:3066 ("*De rechtbank stelt vast dat art. 22b van het Wetboek van Strafrecht een onvoorwaardelijke gevangenisstraf eist in het geval van een veroordeling op grond van art. 240b van het Wetboek van Strafrecht. In beginsel acht de rechtbank een gevangenisstraf, mede gelet op de oriëntatiepunten voor straftoemeting, die voor het in bezit hebben van deze hoeveelheid kinderporno uitgaan van een gevangenisstraf, passend voor een delict als het onderhavige. De rechtbank houdt echter in grote mate rekening met de persoon van verdachte zoals naar voren komt uit het advies van de reclassering van 3 juni 2021. Hieruit blijkt dat verdachte verstandelijk beperkt is en (mogelijk) behept met pedofiele neigingen*."). RB Rotterdam 21-4-2016, ECLI:NL:RBROT:2016:3009 (Bezit en toegang verschaffen tot kinderporno. (15 afbeeldingen); oplegging "kale taakstraf") en RB Rotterdam 21-1-2016, ECLI:NL:RBROT:2016:547 (veroordeling wegens bezit over lange periode van deels als ernstig te waarderen kinderpornografisch materiaal tot taakstraf van 150 uur en een voorwaardelijke gevangenisstraf van 3 maanden (met bijzondere voorwaarden) en; RB Gelderland 22-11-2016, ECLI:NL:RBGEL:2016:6315 (Bezit kinderporno, 60 afbeeldingen. *Recidive*, geen oplegging onvoorwaardelijke gevangenisstraf, maar voorwaardelijke gevangenisstraf voor de duur van 181 dagen **en** werkstraf);

[754] Deze omstandigheden hebben in het kader van art. 240b Sr geen andere betekenis dan die zij ook elders in het Wetboek van Strafrecht met betrekking tot andersoortige feiten, zoals art. 312 Sr, hebben, zodat hierop in het kader van deze uitgave niet specifiek nader wordt ingegaan.

Het valt op dat zelfs in zaken, waarin daartoe gezien de inhoud van het proces-verbaal gerede aanleiding zou bestaan, deze strafverzwarende omstandigheden veelal niet in de tenlastelegging worden opgenomen. Indien zulks wordt nagelaten, zal de strafrechter daarmee – althans in formele zin[755] – bij de straftoemeting geen rekening kunnen houden.

Naast genoemde hoofdstraffen kunnen bij veroordeling wegens overtreding van art. 240b Sr ook bijkomende straffen worden opgelegd. Zo kan een veroordeling tot ontzetting uit bepaalde rechten worden uitgesproken. Daarbij kan het gaan om het bekleden van een ambt, het dienen bij de gewapende macht en het zijn van raadsman of gerechtelijke bewindvoerder.[756] Als de overtreding van art. 240b Sr is begaan in het kader van de beroepsuitoefening van de verdachte, kan hij ook uit dat beroep ontzet worden.[757] Op rechtspraak.nl zijn echter geen uitspraken te vinden waarbij deze laatste bijkomende straf is opgelegd voor alleen overtreding van art. 240b Sr. Wel zijn enkele uitspraken bekend waarbij zulks is gebeurd ingeval de verdachte niet alleen voor overtreding van art. 240b Sr, maar ook voor andere (zeden)feiten werd veroordeeld.[758]

Daarnaast kan als bijkomende straf ook verbeurdverklaring van bijvoorbeeld gegevensdragers en geautomatiseerde werken worden uitgesproken of de maatregel van onttrekking aan het verkeer van bijvoorbeeld gegevensdragers met pornografische afbeeldingen worden uitgesproken. In kinderpornozaken worden zowel de verbeurdverklaring als de onttrekking veelvuldig uitgesproken. De verbeurdverklaring en onttrekking zijn reeds hiervoor onder 7.7.2.1 tot en met 7.7.2.3. besproken, waarnaar hier kortheidshalve wordt verwezen.

8.3.2. Richtlijnen en Oriëntatiepunten

Zowel het College van Procureurs-Generaal als het Landelijk Overleg Vakinhoud Strafsectoren (hierna: 'LOVS') hebben met betrekking tot de straftoemeting in strafzaken betreffende kinderpornografie specifieke richtlijnen respectievelijk oriëntatiepunten ontwikkeld.

De OM-Richtlijn voor Strafvordering Kinderpornografie (2016R010) bevat een redelijk fijnmazig overzicht van voor de bepaling van de strafeis relevant geachte factoren. Tevens bevat deze Richtlijn voor een aantal "kale" basisdelicten ook de strafeis die daarbij vanuit het OM als basiseis wordt gezien.[759] Indien sprake is van bezit/verwerving/toegang verschaffen met betrekking tot een geringe hoeveelheid afbeeldingen *en* verdachte is first offender *en* het betreft een eenmalig gepleegd feit *en* het feit is onbewust/door nalatigheid gepleegd bedraagt de basiseis: een korte onvoorwaardelijke gevangenisstraf + 240 uur taakstraf + een

---

[755] In die zin dat de strafrechter dan niet het (verhoogde) strafmaximum dat zou hebben voortgevloeid uit de toepassing van art. 248 Sr mag hanteren. Hij mag natuurlijk wel bij de meer generale straftoemeting bijvoorbeeld een aspect als dat het feit is begaan tegen een aan de verdachte toevertrouwd kind in zijn beoordeling betrekken.
[756] Art. 251, lid 1, Sr jo. art. 28, lid 1, sub 1, Sr.
[757] Art. 251, lid 2, Sr. Zie ook art. 28, lid 1, sub 5, Sr.
[758] Zie RB Leeuwarden 25-8-2011, ECLI:NL:RBLEE:2011:BR5799 (veroordeling voor feitelijke aanranding van de eerbaarheid van leerlingen/pupillen door leraar/voetbaltrainer en bezit kinderporno; O.m. ontzetting uit het beroep van leraar voor een periode van twee jaar en achttien maanden; Hof Amsterdam 12-10-2005, ECLI:NL:GHAMS:2005:AU4229 (veroordeling voor schuld aan de dood van een baby en wegens het een gewoonte maken van het in voorraad hebben van kinderpornografie. O.m. voorwaardelijke ontzetting uit het beroep van arts voor een periode van drie jaar met een proeftijd van drie jaar; RB Den Bosch 19-6-2001, ECLI:NL:RBSHE:2001:AB2182 (veroordeling voor het in voorraad hebben van kinderpornografie, meermalen gepleegd, ontucht met een patiënt en ontucht met een pupil. O.m. voorwaardelijke ontzetting uit het beroep van huisarts voor een periode van vier jaar.
[759] Richtlijn voor strafvordering Kinderpornografie (2016R010), in werking getreden 1 oktober 2016.

voorwaardelijke gevangenisstraf met bijzondere voorwaarden.[760] In andere gevallen liggen de basiseisen op een niveau van 12 maanden onvoorwaardelijke gevangenisstraf of meer.

Door het LOVS zijn ook met betrekking tot art. 240b Sr-zaken oriëntatiepunten voor de straftoemeting bekend gemaakt.[761] Deze oriëntatiepunten zijn weliswaar in overleg met strafrechters tot stand gekomen maar binden de individuele rechter in een concrete zaak niet. Qua inhoud wijken de oriëntatiepunten weinig af van de richtlijnen van het OM. Voor het enkele door een *first offender* bezitten/verwerven van, en/of zich toegang verschaffen tot, een geringe hoeveelheid kinderporno waarop zeer jonge kinderen en/of geweldselementen zijn afgebeeld wordt bijvoorbeeld een oriëntatiepunt genoemd van 240 uur taakstraf + 6 maanden gevangenisstraf, waarvan een kort gedeelte onvoorwaardelijk, met bijzondere voorwaarden. In andere gevallen liggen de oriëntatiepunten op het niveau van 1 jaar onvoorwaardelijke gevangenisstraf of (aanmerkelijk) meer.

8.3.3. Voor de bepaling van de strafmaat relevante factoren

8.3.3.1. In de OM-Richtlijn en LOVS-Oriëntatiepunten genoemde factoren
Zowel de OM-Richtlijn als de LOVS-Oriëntatiepunten noemen ook met zoveel woorden een aantal – niet limitatieve – feiten en omstandigheden die bij de formulering van een strafeis respectievelijk de strafbepaling in een concreet geval zouden kunnen worden betrokken. Allereerst speelt hierbij de aard van de gedraging met betrekking tot het kinderpornografisch materiaal een rol. Het uitsluitend voor eigen gebruik in bezit hebben van strafbaar materiaal, het verwerven daarvan of zich daartoe toegang verschaffen wordt daarbij in zowel de OM- als ZM-uitgangspunten als een minder zware gedraging aangemerkt dan het zelf *vervaardigen* of voor eigen gewin *verspreiden* of *aanbieden* (waarbij het gewin ook kan bestaan uit het zich door de verspreiding/aanbieding een bepaalde positie, privileges of status verwerven).[762] Als bijzonder ernstig worden voorts die gedragingen ten aanzien van kinderpornografie aangemerkt die een structureel, doelbewust en georganiseerd (al dan niet met een commercieel oogmerk) karakter hebben en/of die vallen onder de strafverzwarende omstandigheden van art. 240b, tweede lid, Sr (het “een gewoonte maken van”) en/of 248 Sr.[763]

---

[760] Het valt op dat deze criteria grotendeels overeenkomen met die voor buitengerechtelijke afdoening ingevolge het zogenaamde Indigo-beleid (zie hiervoor onder 7.1.1. en de OM-Richtlijn zelf). Nu het hier voorts gaat om gepubliceerd beleid zou in voorkomende gevallen dan ook ter terechtzitting de vraag kunnen rijzen waarom aan de verdachte niet alvorens te dagvaarden deze afdoeningsmodaliteit is aangeboden. Niet ondenkbaar is dat indien vanuit het OM geen bevredigend antwoord op deze vraag kan worden gegeven het OM vanwege handelen in strijd met eigen gepubliceerd beleid niet-ontvankelijk zal worden verklaard.
[761] Oriëntatiepunten straftoemeting en LOVS-afspraken (laatstelijk gewijzigd: december 2016).
[762] Zie voor bijv. RB Haarlem 22-03-2011, ECLI:NL:RBHAA:2011:BQ1647 (verdachte heeft zich schuldig gemaakt aan het invoeren van kinderporno, vastgelegd op twee cd-roms en een dvd, lagere straf dan geëist, omdat verdachte het pakket naar zichzelf heeft verzonden kennelijk voor eigen gebruik en het niet aannemelijk is dat het aangetroffen kinderpornografisch materiaal bestemd was voor verdere verspreiding dan wel handel).
[763] Zie bijv. RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735 (bezit kinderporno en maken van gewoonte daarvan alsmede verspreiding kinderpornografisch materiaal. Bewijsoverwegingen o.m. m.b.t. *gewoonte* (gezien de hoeveelheid afbeeldingen, de lengte van de periode waarin verdachte deze afbeeldingen verzamelde en de frequentie waarmee hij zich met het verzamelen van deze afbeeldingen bezig hield). Opgelegde straf: 12 maanden gevangenisstraf waarvan 4 maanden voorwaardelijk, proeftijd 3 jaren met oplegging van diverse bijzondere voorwaarden); vgl. ook RB Gelderland, 4-7-2017, ECLI:NL:RBGEL:2017:3525 (gedurende een periode van meer dan 2,5 jaar schuldig maken aan het verspreiden, vervaardigen en in het bezit hebben van kinderpornografisch materiaal en eenmaal aan grooming en ontucht met minderjarige. GS 20 mnd wv. 16 mnd vw pt 3 jrn met bijz vw dadelijk uitvoerbaar en TS 240 uur)
Zie hiervoor onder 8.3.1.

Daarnaast is een aantal factoren van belang die betrekking hebben op (de aard van) het materiaal zelf, of de persoon van de verdachte. Zo noemen de Oriëntatiepunten bijvoorbeeld naast de reeds genoemde omstandigheden de volgende factoren:

- Aantal afbeeldingen (fysiek en/of digitaal);[764]
- Periode waarin de verzameling van afbeeldingen is opgebouwd;
- Leeftijd slachtoffer(s);[765]
- Het feit wordt gepleegd met een slachtoffer dat in staat van bewusteloosheid, verminderd bewustzijn of lichamelijke onmacht verkeert, dan wel aan een zodanige gebrekkige ontwikkeling of ziekelijke stoornis van zijn geestvermogens lijdt dat hij/zij niet of onvolkomen in staat is zijn/haar wil daaromtrent te bepalen of kenbaar te maken of daartegen weerstand te bieden;[766]
- Aard van de afbeelding(en) (bijv. alleen poserend, vernederende of zeer expliciete pose, ontuchtige handelingen, seksueel binnendringen, geweld);[767]
- Type afbeelding (bijv. echt of virtuele productie);[768]
- Professionaliteit (bijv. commercieel doeleinde, winstbejag);
- Recidive;
- Herhalingsgevaar;
- Bereidheid tot gedragsverandering, erkenning en inzicht in problematiek gedrag.[769]

---

[764] Opvallend is dat in de Richtlijn voor strafvordering Kinderpornografie (2016R010) (onder IV) het belang van het aantal bij een verdachte in bezit zijnde afbeeldingen enigszins wordt gerelativeerd. Daarbij wordt verwezen naar "*de ontwikkelingen op digitaal en internetgebied en het relatieve gemak waarmee tegenwoordig in korte tijd bijzonder grote aantallen kinderpornografische afbeeldingen kunnen worden gedownload, gekopieerd, opgeslagen en bewaard*". De vraag kan worden gesteld of het feit dat iets technisch relatief eenvoudig is afdoet aan de strafwaardigheid daarvan.

[765] Zie bijv. RB Overijssel 29-1-2016, ECLI:NL:RBOVE:2016:290 (veel afbeeldingen van zeer vergaande handelingen met zeer jonge kinderen; 18 mnd gv wv 8 vw); Hof Arnhem-Leeuwarden 26-8-2016, ECLI:NL:GHARL:2016:6883 (zeer extreme afbeeldingen; ook van kinderen van 0 tot 2 jaar; TBS met voorwaarden); Hof Den Haag 3-3-2010, ECLI:NL:GHSGR:2010:BL6582 (strafmaatappel OM; seksuele handelingen met zeer jonge kinderen). *Zie echter ook*: RB Noord-Holland 4-4-2017, ECLI:NL:RBNHO:2017:2692 (bezit aanzienlijk aantal kinderpornografische afbeeldingen, waarop ook zeer jonge kinderen en baby's te zien zijn, pleegperiode van ruim 2 jaar. Bovendien is verdachte tijdens de schorsing van de bewaring gerecidiveerd; 198 dagen gv wv 180 vw, en bijzondere voorwaarden).

[766] Het hier gestelde is vermoedelijk een meer verfeitelijkte weergave van het in art. 248, lid 3, Sr bepaalde ten aanzien van het begaan van het feit tegen een persoon bij wie misbruik van een kwetsbare positie wordt gemaakt.

[767] Zie bijv. ook RB Overijssel 29-1-2016, ECLI:NL:RBOVE:2016:290 (veel afbeeldingen van zeer vergaande handelingen met zeer jonge kinderen; RB Arnhem 4-8-2011, ECLI:NL:RBARN:2011:BR4170 (groot aantal afbeeldingen en filmpjes waaronder met zeer vergaande seksuele handelingen) vs. RB Utrecht 6-10-2011, ECLI:NL:RBUTR:2011:BT8700 (geringe hoeveelheid, geen verdergaande handelingen of afbeeldingen dan poseren).

[768] Zie bijv. ook RB Gelderland 2-3-2017, ECLI:NL:RBGEL:2017:1090 (afwijking van oriëntatiepunten, nu het merendeel van het aangetroffen beeldmateriaal bestond uit virtuele kinderpornografie, waarbij geen sprake is van het misbruik van kinderen).

[769] Hof Leeuwarden 19-7-2010, ECLI:NL:GHLEE:2010:BN1787 (bezit aanzienlijke hoeveelheid kinderporno, oplegging werkstraf i.p.v. gevangenisstraf o.m. n.a.v. gegeven dat verdachte reeds 2,5 jaar op vrijwillige basis een ambulante forensisch psychiatrische behandeling volgt); Zie ten aanzien van deze factor ook: Conclusie AG Harteveld (ECLI:NL:PHR:2014:2095) bij HR 18-11-2014, ECLI:NL:HR:2014:3304 (verwerping cassatiemiddel tegen strafmaatoverweging waaruit bleek dat de "proceshouding" van de verdachte in voor hem negatieve zin in de straftoemeting was betrokken).

De Richtlijn voor strafvordering kinderpornografie (2016)[770] noemt daarnaast ook met zoveel woorden als relevante factor:

- De pleegperiode/ouderdom van de feiten; en
- De herkomst van de afbeeldingen, in de zin van: of de afbeeldingen zijn gekocht of anderszins tegen tegenprestatie geleverd en/of toegankelijk gemaakt en/of alleen toegankelijk waren na gebruik van codes, wachtwoorden e.d.;

Een viertal andere, in de rechtspraak genoemde factoren bij de straftoemeting zijn:

- (Ernst van de) bij slachtoffers ontstane schade;[771]
- Openbaarmaking van de identiteit van afgebeelde personen;[772]
- Bij de verdachte gewekte verwachtingen omtrent sepot op basis van het Indigo-beleid;[773] en
- Media-aandacht.[774]

Uit de rechtspraak blijkt dat deze factoren (zij het niet altijd allemaal, en niet altijd allemaal tezamen) ook feitelijk een belangrijke rol spelen bij de straftoemetingsbeslissing.

Bij de bestudering van de rechtspraak valt op dat de strafrechter in geval alleen "bezit" bewezen wordt verklaard en het een *first offender* betreft vrijwel nooit een *on*voorwaardelijke gevangenisstraf van langere duur dan het ondergane (veelal zeer korte) voorarrest oplegt, maar als regel een (nagenoeg) geheel voorwaardelijke gevangenisstraf, gecombineerd met een onvoorwaardelijke werkstraf. Dit geldt ook als het om grotere hoeveelheden kinderpornografisch materiaal gaat en/of daarop zeer jonge kinderen zijn afgebeeld. Geconcludeerd kan dan ook worden dat de oriëntatiepunten (en deels ook de wet in de zin van art. 22b Sr[775]) in dit opzicht in de praktijk voor in ieder geval deze specifieke categorie zaken/verdachten veelal niet lijken te worden gevolgd.

---

[770] Richtlijn voor strafvordering Kinderpornografie (2016R010), onder IV.
[771] RB Gelderland 25-11-2013, ECLI:NL:RBGEL:2013:4849 (vervaardigen, bezit en verspreiden kinderporno, in strafmotivering opgenomen dat het slachtoffer aanzienlijke schade is toegebracht doordat één van de filmpjes op internet circuleert).
[772] RB Oost-Brabant 19-8-2016, ECLI:NL:RBOBR:2016:4488.
[773] RB Amsterdam 1-8-2017, ECLI:NL:RBAMS:2017:5532 (Bezit kinderporno. In de strafmaat is ten voordele van verdachte rekening gehouden met het feit dat er vanuit het OM de indruk gewekt dat er voor verdachte grote kans bestond dat de zaak zou worden geseponeerd omdat verdachte in aanmerking zou komen voor een zogenaamde INDIGO afdoening. Bij de doorzoeking is door de politie een INDIGO folder uitgereikt aan verdachte, tezamen met een folder van De Waag. Er wordt in dit materiaal te weinig aandacht besteed aan de mogelijkheid dat verdachte niet in aanmerking komt voor deze afdoeningsvorm. Het OM heeft vervolgens op meerdere verzoeken van de raadsman niet gereageerd en telkens geen duidelijkheid willen verschaffen over de vraag of verdachte wel of niet in aanmerking zou komen voor de INDIGO afdoening).
[774] Zie onder meer RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735 (gevolgen media aandacht bij straftoemeting betrokken); Zie echter ook RB Amsterdam 22-11-2017, ECLI:NL:RBAMS:2017:8564 (rector middelbare school die o.m. foto's van leerlingen bewerkte tot kinderporno; beroep op strafmatiging wegens uitvoerige media-aandacht grotendeels verworpen, omdat de "*media-aandacht een voorzienbaar gevolg is geweest van het eigen handelen van verdachte*"; echter wel rekening gehouden met de omstandigheid dat door de politie gedetailleerde berichtgeving aan slachtoffers is verspreid, "*voor welke schending van privacy geen aanleiding was*").
[775] Zie hierover verder hiervoor onder 8.2.2.

8.3.3.2. De Verklaring omtrent het gedrag (VOG) als strafbeïnvloedende factor[776].
Sinds enkele jaren wordt bij de beoordeling van de afgifte van een Verklaring omtrent het gedrag (VOG) ten aanzien van een veroordeling voor zedendelicten, waartoe ook overtreding van art. 240b Sr wordt gerekend, onbeperkt teruggekeken[777]. Dat impliceert dat veroordeling en bestraffing voor dit feit, ook bij minderjarigen, kan leiden tot weigering van een VOG met alle consequenties ten aanzien van het kunnen volgen/afronden van opleidingen of het verkrijgen of behouden van werk van dien.

Er wordt dan ook met enige regelmaat door de verdachte c.q. raadslieden betoogd dat zulks moet leiden tot een lagere strafoplegging. Hierbij past een aantal kanttekeningen. Allereerst doet zich hier het probleem voor dat voor de strafrechter weinig inzichtelijk is of, en zo ja onder welke omstandigheden, een bepaalde strafoplegging in de praktijk leidt tot daadwerkelijke weigering van een VOG[778]. Ten aanzien van zedendelicten is echter wel bekend dat het beleid daaromtrent zeer streng is en de uitvoering van dat beleid zo mogelijk nog strenger[779]. Duidelijk is evenwel dat een strafrechtelijke veroordeling niet per definitie betekent dat een VOG wordt geweigerd. Zo kregen in 2018 186.042 personen met antecedenten een VOG en werden in dat jaar van de 1.220.100 aanvragen er slechts 3.251 geweigerd.[780] Evenzeer blijkt echter dat motiveringen van de strafrechter omtrent bijvoorbeeld de ernst van het feit kunnen doorwerken in de besluitvorming omtrent de afgifte van een VOG.[781]

---

[776] Zie voor meer uitgebreide besprekingen van dit onderwerp: E.G. Kurtovic en M.D. Rijnsburger, *De straf- en bestuursrechter als communicerende vaten in VOG-zaken*, DD 2016 (70), nr. 9, p. 62-70 en S. Meijer, *De invloed van de strafrechter op de bijkomende gevolgen van de straf, Pleidooi voor een meer integrale benadering tussen de straftoemetingsbeslissing en de bestuursrechtelijke beslissing*, DD 2017(16), nr. 3, p. 15-22.

[777] Art. 3.1.1. van de Beleidsregels VOG.

[778] Weliswaar zijn de Beleidsregels VOG openbaar (Stcrt. 2013, 5409), maar dat zegt op zich nog niet al te veel over de uitvoeringspraktijk.

[779] Zie hierover uitgebreider S. Meijer, *De Verklaring Omtrent Gedrag; enkele kanttekeningen bij recente rechtspraak*, DD 2015 (32), nr. 4, p. 22-32, par. 4, alsook Afdeling bestuursrechtspraak Raad van State, 12-2-2014, ECLI:NL:RVS:2014:382, onder 5.1,. waaruit onder meer blijkt dat in paragraaf 3.3.2 van de Beleidsregels is bepaald, dat in het geval van zedendelicten aan de hand van de omstandigheden van het geval wordt beoordeeld of de weigering van een VOG *evident disproportioneel* is, maar dat de staatssecretaris dit zo uitlegt, dat in het geval van door een meerderjarige gepleegde zedendelicten, ongeacht de aard van die delicten, de omstandigheden van het concrete geval *niet* bepalend zijn voor de vraag of een risico voor de samenleving bestaat en of de weigering van een VOG evident disproportioneel is. De Afdeling achtte deze laatste uitleg overigens onjuist.

[780] Bron: Justis.nl; zie ook Hoge Raad 9-2-2016, ECLI:NL:HR:2016:213 ("*In het middel wordt tot uitgangspunt genomen dat sprake is van schending van art. 3 EVRM, omdat aan de verdachte als gevolg van zijn veroordeling "in elk geval gedurende een zeer lange periode – geen VOG zal worden verstrekt, waardoor hij het beroep van zijn keuze nooit zal kunnen uitoefenen en ook, in feite, levenslang zal zijn uitgesloten van de uitoefening van tal van andere beroepen", waarbij het middel zonder nadere onderbouwing ervan uitgaat dat een door verdachte gedane aanvraag van een VOG nimmer zal worden ingewilligd, ook niet na bezwaar en beroep tegen een weigering. Deze stellingen zijn evenwel onjuist, zodat de juistheid van genoemd uitgangspunt onbesproken kan blijven*").

[781] Zie bijv. Afdeling bestuursrechtspraak Raad van State 11-12-2013, ECLI:NL:RVS:2013:2331, onder 4.3. (vernietiging weigering VOG, ernst van de zedendelicten blijkt niet uit de veroordeling); vgl. ook RB Zeeland-West-Brabant 29-6-2017, ECLI:NL:RBZWB:2017:3913 (e-archief) (afwijzing VOG na veroordeling voor onder meer bezit kinderpornografie; VOG nodig voor een functie als priesterstudent; in afweging mede betrokken oordeel strafrechter dat bezit kinderporno geen licht vergrijp betreft en dat risico op recidive bestaat; beroep tegen weigering VOG ongegrond).

Naar huidig recht lijkt er echter geen rechtsplicht voor de strafrechter te bestaan om zich in zijn uitspraak desgevraagd dan wel ambtshalve uit te spreken over (de gevolgen van zijn straftoemeting voor) de VOG.[782]

In de literatuur is er echter wel voor gepleit dat de strafrechter zich desondanks – al dan niet desgevraagd – in voorkomende gevallen wel uitlaat over zijn opvatting ter zake van de doorwerking van de veroordeling op een eventuele VOG-aanvraag.[783] Een van de redenen in die publicaties genoemd is dat het COVOG[784] zich slechts blijkt te baseren op de gegevens die in het Justitieel Documentatiesysteem zijn verwerkt en deze vervolgens slechts marginaal toetst.[785] Indien impliciete of expliciete aanwijzingen van de strafrechter in de uitspraak zijn opgenomen, kan betrokkene echter de uitspraak in de strafzaak inbrengen in de procedure bij het verkrijgen van een VOG, en aldus een betere belangenafweging bewerkstelligen.[786]
In dit licht is het niet geheel verrassend dat in de jurisprudentie meerdere voorbeelden zijn te vinden van uitspraken waarin de strafrechter zich tevens (al dan niet als *obiter dictum*) uitspreekt over de consequenties van zijn uitspraak voor de VOG.[787] In hoeverre dergelijke *obiter dicta* echter ook daadwerkelijk invloed hebben op de beslissing omtrent afgifte van de VOG is onduidelijk.

8.4. Proeftijd en bijzondere voorwaarden

8.4.1. (Duur van de) Proeftijd

Er is discussie mogelijk over de vraag wat bij veroordeling tot een voorwaardelijke straf wegens overtreding van art. 240b Sr[788] de maximaal te bepalen proeftijd is. Ingevolge art. 14b, tweede lid, Sr bedraagt deze namelijk drie jaren, maar kan deze op ten hoogste tien jaren worden bepaald "*indien er ernstig rekening mee moet worden gehouden dat de veroordeelde wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen*".
Dit laatste criterium komt ook op diverse plaatsen elders in het Wetboek van Strafrecht voor.[789] Een wettelijke definitie van genoemd begrip ontbreekt echter in het Wetboek van Strafrecht, zodat we voor duiding aangewezen zijn op de wetsgeschiedenis en de jurisprudentie. Helaas verschaft – mede door zijn gedateerdheid (1992; 1999) – ook de

---

[782] Zie o.m. Hof Amsterdam 31-3-2016, ECLI:NL:GHAMS:2016:1210; Vgl. ook HR 9-2-2016, ECLI:NL:HR:2016:213 r.o. 3.4.
[783] Zo o.m. P.M. Schuyt, *De VOG als strafbeïnvloedende omstandigheid – of juist niet, niet,* TREMA, 2014/1, p. 10-15 en de in de voorgaande noten genoemde auteurs.
[784] Thans wordt de screening uitgevoerd door screeningautoriteit Justis.
[785] Aldus S. Meijer *De Verklaring Omtrent Gedrag; enkele kanttekeningen bij recente rechtspraak*, DD 2015/32 onder 6. Uit de op de website van Justis geplaatste brochure over screening lijkt te volgen dat deze praktijk niet is gewijzigd.
[786]Aldus Schuyt, a.w.; Vgl. ook Hof Den Haag 21-6-2011, ECLI:NL:GHSGR:2011:BQ8697.
[787] Zie bijv. Hof Den Haag 7-6-2016, ECLI:NL:GHDHA:2016:1703 ("Het weigeren van de afgifte van een VOG aan de verdachte op grond van - uitsluitend - de onderhavige strafzaak komt het hof voor, gelet op de jeugdige leeftijd van de verdachte en gelet op de bijzondere omstandigheden in de onderhavige zaak waar het geen kinderpornografie betreft maar afbeeldingen van leeftijdgenoten, als een dermate grote inbreuk op het privéleven van de verdachte, dat een dergelijke beslissing naar het oordeel van het hof strijdig zou zijn met art. 8 van het Europees Verdrag tot bescherming van de Rechten van de Mens en art. 3 van het Verdrag inzake de Rechten van het Kind"); Soortgelijk: Hof Den Haag 5-9-2017, ECLI:NL:GHDHA:2017:2520; Hof Den Haag 25-8-2016, ECLI:NL:GHDHA:2016:2466 en Hof Arnhem-Leeuwarden 4-2-2013, ECLI:NL:GHARL:2013:CA0478.
[788] Opmerkelijk genoeg heeft de wetgever met betrekking tot het misdrijf van art. 254a Sr (bezit etc. van *dieren*porno) in art. 14b, lid 3 Sr wel expliciet bepaald dat ingeval van veroordeling voor dat misdrijf een proeftijd van maximaal 10 jaar kan worden opgelegd.
[789] Zie art. 38e Sr (limitering verlenging Tbs met dwangverpleging); art. 77t, lid 3 Sr (limitering verlenging PIJ-maatregel); art. 14e en art. 77za Sr: (bevel "dadelijke uitvoerbaarheid"; i.w.tr. 1 april 2012).

wetsgeschiedenis slechts beperkt duidelijkheid ten aanzien van welke misdrijven kan worden aangenomen dat zij gericht zijn tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen.

Indertijd is in de Memorie van Toelichting gesteld dat het in ieder geval mede gaat om de misdrijven die worden omschreven in de titel XIV (zedenmisdrijven) van het Tweede Boek van het Wetboek van Strafrecht. Meer specifiek worden daarbij ook de seksuele delicten genoemd, waarin het bestanddeel "geweld" is opgenomen (zoals de misdrijven omschreven in de artt. 242 en 246 Sr), maar ook ten aanzien van de misdrijven omschreven in de artt. 243, 244, 245, 247, 248a (als "opvolger" van art. 248ter) , 249, 250, eerste lid, aanhef en onder 1, of 250, eerste lid, aanhef en onder 2, en tweede lid, Sr kan op basis van diezelfde wetsgeschiedenis worden aangenomen dat voldaan is aan het lichamelijke onaantastbaarheidcriterium.[790] Art. 240b Sr wordt daarbij echter niet genoemd.

Bijkomend probleem in art. 240b Sr-zaken is dat, zeker waar de bewezenverklaring een meer passieve vorm van handelen betreft (zoals het geval is bij 'in bezit hebben' en 'zich toegang verschaffen tot'), het verband tussen het handelen van verdachten en de risico's voor de onaantastbaarheid van het lichaam van (jeugdige) personen relatief ver verwijderd is. Aan de andere kant dient te worden onderkend dat dergelijk kinderpornografisch materiaal in overgrote mate het gevolg is van de exploitatie van seksueel misbruik. Ook passieve handelingen ten aanzien van dergelijk materiaal dragen derhalve bij aan de instandhouding van "de markt" voor dat materiaal en daarmee aan het daarmee direct verband houdende misbruik. Sinds enige tijd wordt geaccepteerd dat niet alleen het in omloop brengen, maar ook het in bezit hebben van kinderpornografisch materiaal schadelijk is c.q. kan zijn voor de afgebeelde minderjarigen, nu reeds daardoor bij hen psychische schade kan ontstaan.[791]

Vermoedelijk om laatstgenoemde redenen was in de jurisprudentie een brede tendens zichtbaar om het misdrijf van art. 240b Sr aan te merken als een misdrijf dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen.[792]

---

[790] Aldus ook Nota naar aanleiding van het Eindverslag, als weergegeven in Hof Arnhem 06-06-2011, ECLI:NL:GHARN:2011:BQ9476.

[791] In het bijzonder door de wetenschap dat anderen daarvan kennis (kunnen) nemen. Zie daarover verder hiervoor onder 7.8.

[792] Voldaan aan lichamelijke onaantastbaarheidscriterium o.m.: Hof Arnhem-Leeuwarden 26-08-2016, ECLI:NL:GHARL:2016:6883; RB Oost-Brabant 12-12-2016, ECLI:NL:RBOBR:2016:6847; RB Overijssel 6-12-2018, ECLI:NL:RBOVE:2018:4679 ("*Naast de pedofiele stoornis bestaan er bij verdachte ook psychische disfuncties die voortkomen uit de borderline persoonlijkheidsstoornis. Dit bestaat uit impulsiviteit, een gebrek aan voldoende afweer en controlemechanismen, gebrek aan zelfvertrouwen, negatief zelfbeeld, identiteitsproblemen, stemmingsregulatieproblematiek, gevoelens van leegte, afwijzing en eenzaamheid. (...) Er is sprake van forse problematiek op meerdere leefgebieden en van problematisch middelengebruik*.") . Anders echter: Hof Arnhem 7-5-2012, ECLI:NL:GHARN:2012:BW7191 (tbs opgelegd wegens overtreding art. 240b; "*Het voorhanden hebben van kinderporno levert op zichzelf, hoe onwenselijk dergelijke gedragingen ook zijn, geen handelen op dat gericht is tegen of gevaar oplevert voor de onaantastbaarheid van het lichaam van een of meer personen*". Vgl. ook RB Rotterdam 6-10-2011, ECLI:NL:RBROT:2011:BT7601 (bewezenverklaard: een gegevensdrager, bevattende een afbeelding waarvan de vertoning schadelijk is te achten voor personen beneden de leeftijd van zestien jaar (opm. auteurs: betreft dus kennelijk tonen van 'gewone' porno), vertonen aan een minderjarige van wie hij weet of redelijkerwijs moet vermoeden, dat deze jonger is dan zestien jaar, meermalen gepleegd; art. 240a Sr). RB: "*het thans bewezen verklaarde feit betreft niet een misdrijf dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen, derhalve geen wettelijke grond om te komen tot een proeftijd van langer dan twee jaren*".

Dit bracht met zich dat ook langere proeftijden dan drie jaren werden bepaald.[793] In 2017 en 2018 heeft de Hoge Raad echter – in ieder geval waar het betreft de gedragingen "in bezit hebben" en "verwerven" van, respectievelijk het "zich toegang verschaffen tot" kinderpornografisch materiaal – de staf over deze benadering gebroken. De Hoge Raad oordeelde – met verwijzing naar de wetsgeschiedenis – dat deze gedragingen geen gedragingen zijn "*die onmiskenbaar zijn gericht tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen*" in de zin van art. 14b, tweede lid, Sr en dat deze gedragingen ook niet zonder meer kunnen worden gekarakteriseerd als misdrijven die dergelijke gedragingen omvatten.[794] Voor deze gedragingen kan derhalve geen langere proeftijd (meer) dan drie jaren worden opgelegd.[795] Recent heeft echter de rechtbank Oost-Brabant in tegenstelling tot en zonder verwijzing naar voorgaand besproken jurisprudentie van de Hoge Raad overwogen dat "*de strekking van artikel 240b van het Wetboek van Strafrecht is gelegen in het tegengaan van seksueel misbruik van jeugdigen en van de exploitatie daarvan, waaronder te begrijpen het verleiden van minderjarigen om hieraan (tegen betaling) deel te nemen en de overtreding van dit artikel is reeds om die reden aan te merken als een misdrijf dat is gericht tegen, of gevaar veroorzaakt voor, de onaantastbaarheid van het lichaam van een of meer personen, een en ander zoals in artikel 14b, tweede lid van het Wetboek van Strafrecht bedoeld*".[796] Dientengevolge achtte de rechtbank Oost-Brabant een langere proeftijd dan drie jaren in dat geval passend en geboden en heeft de rechtbank een proeftijd voor de duur van vijf jaren opgelegd. Het is de auteurs van dit e-book onbekend of in deze zaak hoger beroep is ingesteld. Nu deze uitspraak ingaat tegen de lijn van de Hoge Raad wordt een toelichting in het vonnis node gemist.

8.4.2. Algemene en bijzondere voorwaarden

Bij veroordeling wegens overtreding van art. 240b Sr kunnen in beginsel alle in art. 14c Sr genoemde algemene en bijzondere voorwaarden worden opgelegd.
In de recht(er)spraktijk rijzen er echter regelmatig vragen over de wenselijkheid en uitvoerbaarheid van bepaalde meer specifiek met de aard van dit specifieke (zeden)delict samenhangende bijzondere voorwaarden. Daarom wordt in het navolgende een aantal bijzondere voorwaarden met name vanuit dit perspectief besproken.

8.4.2.1. Toezicht door de reclassering ex art. 14d, tweede lid, Sr

Allereerst volgt uit het wettelijk systeem en de formulering van art. 14c, eerste lid, Sr dat in geval van veroordeling tot een (deels) voorwaardelijke strafsanctie in ieder geval tevens (van rechtswege) sprake zal zijn van de plicht tot medewerking aan reclasseringstoezicht, de medewerking aan huisbezoeken daaronder begrepen. Van belang is echter zich te realiseren

---

[793] Zie bijv. RB Noord-Nederland 13-7-2017, ECLI:NL:RBNNE:2017:2583 (gevangenisstraf voor de duur van 15 maanden, waarvan 12 maanden voorwaardelijk met een proeftijd van 5 jaren, met oplegging van bijzondere voorwaarden voor het in bezit hebben van kinderpornografische bestanden (terwijl de verdachte nog in de proeftijd liep van een eerdere veroordeling voor bezit van kinderpornografisch materiaal).
RB Oost-Brabant 12-12-2016, ECLI:NL:RBOBR:2016:6847 (Gewoonte maken van het verzamelen en verspreiden van kinderporno. Extreem grote hoeveelheid kinderporno. Proeftijd 7 jaar); RB Gelderland 22-11-2016, ECLI:NL:RBGEL:2016:6315 (alleen bezit kinderporno; proeftijd 5 jaar); RB Oost-Brabant 19-8-2016, ECLI:NL:RBOBR:2016:4488 (bezit en verspreiden kinderporno; proeftijd 5 jaar).
[794] HR 28-3-2017, ECLI:NL:HR:2017:524, r.o. 2.5.3., HR 30-1-2018, ECLI:NL:HR:2018:116, r.o. 3.4.2 en HR 12-6-2018, ECLI:NL:HR:2018:894.
[795] Aandacht verdient hierbij echter dat daarmee onzes inziens nog niet gezegd is dat hetzelfde geldt voor andersoortige gedragingen met kinderporno, zoals het vervaardigen, verspreiden, tentoonstellen (enz.) daarvan. AG Hofstee stelt in zijn conclusie (ECLI:NL:PHR:2017:195, r.o. 57) bij HR 28-3-2017, ECLI:NL:HR:2017:524 dat bij 'hands on' "vervaardigen" (waarbij ook sprake is van fysieke betrokkenheid bij het misdrijf) van kinderporno uit de wetsgeschiedenis kan worden afgeleid dat in dat geval wel aan het zwaardere proeftijdcriterium is voldaan.
[796] RB Oost-Brabant 18-10-2021, ECLI:NL:RBOBR:2021:5459.

dat zulks niet tevens inhoudt dat de reclasseringsmedewerker daarmee ook het recht verkrijgt om zonder toestemming van de veroordeelde diens woning te betreden. Dat recht is immers, binnen de toepasselijke wettelijke kaders, uitsluitend voorbehouden aan politie en justitie. De voorwaarde van reclasseringstoezicht impliceert derhalve niet dat de reclassering bijvoorbeeld ook tegen de wil van de veroordeelde (het gebruik van) de computerapparatuur van een veroordeelde kan controleren. Daartoe zal een meer specifieke grondslag, in de vorm van een daartoe strekkende bijzondere voorwaarde, noodzakelijk zijn.

8.4.2.2. Behandeling (al dan niet bij "De Waag")

In een aanzienlijk aantal zaken waarin een veroordeling voor overtreding van art. 240b Sr wordt uitgesproken, wordt als bijzondere voorwaarde een vorm van ambulante behandeling gesteld. Meestal houdt deze behandeling een (groeps)behandeling bij "De Waag" in, welke instelling onder meer voor deze specifieke groep veroordeelden (zowel jeugdigen als volwassenen) een behandeltraject heeft ontwikkeld.[797]

Over de vraag in hoeverre een dergelijke behandeling ook in termen van voorkoming van recidive effectief is, bestaat weinig duidelijkheid. Genoemde behandeling bij de Waag is in ieder geval (nog?) niet door het Ministerie van Veiligheid en Justitie (na *evidence based*–onderzoek) als "erkende gedragsinterventie" aangemerkt.[798]

Weigert een verdachte reeds op voorhand deelname aan een dergelijk behandeltraject, dan wordt ook wel gekozen voor oplegging van een langere proeftijd dan twee jaren.[799]

8.4.2.3. Internetverbod / internetfilter / verplichting tot het laten controleren van geautomatiseerde werken en/of gegevensdragers.

Teneinde recidive van art. 240b-feiten zoveel mogelijk tegen te gaan leggen rechters regelmatig bijzondere voorwaarden op die er toe strekken te bewerkstelligen dat een verdachte geen toegang meer zal hebben tot internet en/of zo veel mogelijk te voorkomen dat hij een dergelijke toegang gebruikt om wederom strafbare handelingen met kinderpornografisch materiaal te plegen. Meer specifiek gaat het dan om het opleggen van een "internetverbod"[800] respectievelijk een verplichting tot het gebruik van een specifiek internetfilter[801] dan wel van een specifieke internetprovider die gebruikt maakt van specifieke informatiefilters.[802] Deze verplichtingen worden veelal gecombineerd met de bijzondere

---

[797] Zie verder: https://www.dewaagnederland.nl/clienten-en-familie/behandeling-volwassenen/seksueel-grensoverschrijdend-gedrag/.

[798] Zie voor de lijst van erkende gedragsinterventies (voor jeugd): http://www.nji.nl/nl/Databank/Databank-Effectieve-Jeugdinterventies/Erkende-interventies en (voor volwassenen): https://www.justitieleinterventies.nl/erkende-interventies.

[799] RB Zutphen 18-10-2011, ECLI:NL:RBZUT:2011:BU1269. Ingevolge de hiervoor onder 8.4.1. reeds gememoreerde rechtspraak van de Hoge Raad is deze in ieder geval voor *in bezit hebben van*, *verwerven van* en *toegang verschaffen tot* kinderpornografisch materiaal maximaal *drie jaren*

[800] Zie bijv. RB Oost-Brabant 12-12-2016, ECLI:NL:RBOBR:2016:6847 (bijz. vw.: verboden gebruik te maken van internet.)

[801] RB Gelderland 13-08-2015, ECLI:NL:RBGEL:2015:5251 (bijz. vw., o.m.: gebruik internetfilter en meewerken aan controle apparatuur); RB Gelderland 12-12-2014, ECLI:NL:RBGEL:2014:7698 (bezit kinderporno, strafoplegging met o.a. als bijz.vw. dat verdachte op iedere gegevensdrager gebruik maakt van een filter van FilterNet).

[802] RB Zutphen 22-11-2011, ECLI:NL:RBZUT:2011:BU5322 (bezit kinderporno, bijz. vw.: aanwijzingen van reclassering opvolgen ook als deze inhouden het gebruik van internetprovider Kliksafe).

voorwaarde[803] dat de verdachte controle moet toestaan van bij de hem in gebruik zijnde computerapparatuur en gegevensdragers.[804]

Hier werpt zich allereerst de vraag op naar de zin van het stellen van dergelijke voorwaarden, nu internet thans via allerlei wegen, waaronder gebruik van smartphones met anonieme simkaarten of met tablets en laptops via zogenaamde wifi-hotspots ook buiten de woon- en werkomgeving van een veroordeelde eenvoudig en anoniem toegankelijk is. Ook zijn er al langere tijd serieuze wetenschappelijke twijfels over bijvoorbeeld de bruikbaarheid en betrouwbaarheid van internetfilters.[805] De effectiviteit van een controle van geautomatiseerde werken en/of gegevensdragers is eveneens beperkt.[806] Waar bovendien toegang tot internet steeds meer een conditio sine qua non is voor deelname aan de samenleving, kan een internetverbod ook de re-integratie van veroordeelden op een onwenselijke wijze bemoeilijken. De rechter zal zich derhalve steeds als hij overweegt een dergelijke bijzondere voorwaarde op te leggen de vraag moeten stellen in hoeverre controle van geautomatiseerde werken en/of gegevensdragers in het voorliggende geval in redelijkheid zinvol en wenselijk moet worden geacht.

Legt de strafrechter een dergelijke bijzondere voorwaarde op, dan dringt zich de vraag op naar de uitvoerbaarheid van de controle op computers/gegevensdragers door de reclassering op de naleving daarvan.[807] Blijkens informatie van Reclassering Nederland zijn daarvoor speciale afspraken met de politie gemaakt. Deze houden in dat, als een dergelijke controle wenselijk wordt geacht, de toezichthouder contact opneemt met de politie. Samen met de politie wordt dan een onaangekondigd huisbezoek gepland. De toezichthouder en de politiefunctionaris gaan vervolgens samen naar de veroordeelde cliënt. De leiding ligt daarbij bij de toezichthouder terwijl de politiefunctionaris die in dit soort onderzoeken is gespecialiseerd en toegerust, het onderzoek feitelijk uitvoert. Deze rolverdeling is enerzijds zo afgesproken omwille van de digitale expertise bij de politie en anderzijds omdat het controleren van

---

[803] Een verplichting tot het laten controleren van de gegevensdragers wordt soms ook opgelegd als tbs-voorwaarde; zie o.m. RB Rotterdam, 29-3-2022, ECLI:NL:RBROT:2022:2305 ("*9. De veroordeelde verleent haar medewerking aan de controle van digitale gegevensdragers. Hiertoe verstrekt de veroordeelde wachtwoorden of toegangscodes aan de reclassering, de kliniek en/of de politie.*") en RB Rotterdam 11-10-2021, ECLI:NL:RBROT:2021:9956. Wij menen dat nu de privacyinbreuk door controles in een Tbs-setting niet wezenlijk anders is dan de privacyinbreuk die ontstaat door controles die als bijzondere voorwaarde worden uitgevoerd, de jurisprudentie van de Hoge Raad over bijzondere voorwaarden strekkend tot controle van gegevensdragers onverkort op Tbs-voorwaarden die strekken tot controle van de gegevensdragers van de Tbs-gestelde van toepassing is.

[804] Zie bijv. RB Noord-Holland 11-7-2017, ECLI:NL:RBNHO:2017:5735 (verbod op internetomgevingen met kinderen of met kinderpornografisch materiaal; "*waarbij de reclassering het recht heeft, in het kader van toezicht controle uit te oefenen op computer(s) en andere apparatuur van betrokkene waarop afbeeldingen (kunnen) worden opgeslagen of waarmee het internet kan worden benaderd*"); RB Gelderland 11-7-2017, ECLI:NL:RBGEL:2017:3599 (o.m. onthouden van digitaal communiceren met minderjarigen. "*Het daarop uitgeoefende toezicht kan mede bestaan uit controles van zijn computer(s), digitale gegevensdragers en andere apparatuur*"); RB Noord-Holland 4-4-2017, ECLI:NL:RBNHO:2017:2692; RB Den Haag 08-09-2016, ECLI:NL:RBDHA:2016:10833; RB Overijssel 31-5-2016, ECLI:NL:RBOVE:2016:1852; RB Rotterdam 21-04-2016, ECLI:NL:RBROT:2016:3009; RB Overijssel 29-01-2016, ECLI:NL:RBOVE:2016:290; RB Oost-Brabant 17-12-2015, ECLI:NL:RBOBR:2015:7343; RB Gelderland 1-5-2015, ECLI:NL:RBGEL:2015:2897; RB Noord-Nederland 12-12-2014, ECLI:NL:RBNNE:2014:6406; RB Den Haag 09-08-2012, ECLI:NL:RBSGR:2012:BX4810.

[805] Zie bijv. W.Ph. Stol, H.W.K. Kaspersen, J. Kerstens, E.R. Leukfeldt, A.R. Lodder, *Filteren van kinderporno op internet; een verkenning van technieken en regulieringen in binnen- en buitenland*, WODC, mei 2008.

[806] Zie nader: Controle van gegevensdragers: toezicht of opsporing? J.W. van den Hurk en S.J. de Vries, NJB 2020/571.

[807] Idem.

gegevensdragers impliciet een opsporingshandeling is, hetgeen een politietaak is.[808] In december 2022 stonden er circa 300 veroordeelden onder toezicht met een geregistreerd zedendelict, waarbij het toezicht op de bijzondere voorwaarden door middel van controle van gegevensdragers kan plaatsvinden.[809] Vanwege capaciteitsbeperkingen bij de politie kunnen op jaarbasis maximaal 50 controles worden uitgevoerd.[810]

Deze werkwijze van reclassering en politie is vanuit het oogpunt van uitvoerbaarheid goed te begrijpen, maar duidelijk is dat deze tevens met zich brengt dat de veroordeelde feitelijk gedurende de gehele proeftijd zou moeten gedogen dat op elk willekeurig moment de politie en/of de reclassering zijn woning betreedt om vervolgens zijn computer(s) te onderzoeken. In dit licht is het dan ook onzes inziens niet geheel verrassend dat de Hoge Raad begin 2016 een bijzondere voorwaarde als: *dat "de verdachte gedurende de proeftijd zal meewerken aan politiële controles van zijn computer(s) en andere apparatuur waarop afbeeldingen (kunnen) zijn opgeslagen*" in strijd heeft geacht met de wet, en meer in het bijzonder in strijd met art. 14c, tweede lid, onder 14º, Sr.[811] De Hoge Raad nam daarbij mede in aanmerking dat het Hof weliswaar kennelijk het oog had op gedrag dat met – kort gezegd – kinderporno verband hield, maar oordeelde dat de voorwaarde niet als een voldoende precies gedragsvoorschrift was geformuleerd, alsmede dat het toezicht op de naleving van voorwaarden separaat is geregeld en een bijzondere voorwaarde in de zin van art. 14c, tweede lid, onder 14º, Sr niet geacht kan worden gedrag te omvatten dat in feite overeenkomt met het meewerken aan door de politie uit te oefenen dwangmiddelen op de veelomvattende en ingrijpende wijze, zoals in de onderhavige voorwaarde is geformuleerd. In 2020, 2021 en 2022 heeft de Hoge Raad in vergelijkbare zaken expliciet verwezen naar het arrest van 2016 en de daarin geformuleerde overwegingen herhaald.[812] De in 2016 ingezette lijn van de Hoge Raad is dus nog steeds van toepassing.

De formuleringen van de Hoge Raad roepen wel de vraag op, onder welke condities een controle-voorwaarde wel de juridische toets der kritiek zou kunnen doorstaan, of dat moet worden aangenomen dat het opleggen van een controlevoorwaarde sinds dit arrest feitelijk is uitgesloten. Het is wat dat betreft te betreuren dat de Hoge Raad in voormeld arrest de feitenrechter niet meer werkbare aanknopingspunten en duidelijkheid heeft geboden. Het is dan ook niet verwonderlijk dat het arrest van de Hoge Raad minder effect op de rechtspraak heeft gehad dan aanvankelijk werd verwacht. Zo blijkt uit een verkennend onderzoek naar nadien verschenen uitspraken dat veel rechtbanken en hoven op de oude voet verder zijn gegaan, zonder het arrest in acht te nemen.[813] In enkele andere zaken gaf het arrest de rechter aanleiding om de gevorderde controle van gegevensdragers juist in het geheel niet als bijzondere voorwaarde op te nemen vanwege de potentieel zeer ingrijpende inbreuk op de persoonlijke levenssfeer van de verdachte.[814] Met name interessant zijn die zaken waarin de rechter aan de slag is gegaan met het (her)formuleren van de gedragsvoorwaarde om zo

---

[808] Bron: informatie per mail (2017) aan de oorspronkelijk auteur van S. van Gennip, algemeen directeur Reclassering Nederland.
[809] Deze informatie is door Reclassering Nederland in mei 2023 per mail aan het KCC verstrekt.
[810] Deze informatie is door Reclassering Nederland verstrekt in een informeel overleg van 18 januari 2023 met onder meer auteurs.
[811] HR 23-2-2016, ECLI:NL:HR:2016:302.
[812] HR 31-5-2022, ECLI:NL:HR:2022:807, HR 15-3-2022, ECLI:NL:HR:2022:338, HR 7-7-2020, ECLI:NL:2020:1215 en HR 9-03-2021, ECLI:NL:HR:2021:248 (herhaling arrest HR 7-7-2020).
[813] Een greep uit recentere rechtspraak: RB Noord-Nederland 16-7-2018, ECLI:NL:RBNNE:2018:2764, RB Rotterdam 15-11-2018, ECLI:NL:RBROT:2018:9416, RB Overijssel 23-5-2019, ECLI:NL:RBOVE:2019:1766, RB Den Haag 4-4-2019, ECLI:NL:RBDHA:2019:3445 en Hof Den Bosch 26-2-2019, ECLI:NL:GHSHE:2019:690.
[814] Bijv. RB Limburg 18-5-2018, ECLI:NL:RBLIM:2018:4685.

tegemoet te komen aan de door de Hoge Raad verwoorde bezwaren.

In diverse na het arrest van de Hoge Raad door de feitenrechter gewezen uitspraken zien we dat de bijzondere voorwaarde wordt geformuleerd langs de lijnen van het voorstel van de advocaat-generaal in zijn conclusie bij dit arrest.[815] Een voorbeeld zien we in een vonnis van de rechtbank Gelderland[816]:

> *"- zich onthoudt op welke wijze dan ook van gedragingen die zijn gericht op het verkrijgen en/of verspreiden van kinder- en dierenpornografisch materiaal - al dan niet in een digitale omgeving -, terwijl het daarop uitgeoefende toezicht mede kan bestaan uit controles van zijn computer(s) en andere apparatuur. Veroordeelde dient in dat kader mee te werken aan controle van digitale gegevensdragers tijdens een huisbezoek en is tijdens de gesprekken met de reclassering open over de wijze waarop hij denkt dit gedrag te voorkomen."*

De rechtbank motiveert dit als volgt:

> *"Deze voorwaarde kan worden aangemerkt als een voorwaarde die strekt goed levensgedrag van de veroordeelde te bevorderen of die een gedraging betreft waartoe hij uit een oogpunt van maatschappelijke betamelijkheid gehouden moet worden geacht (HR 26 november 1968, ECLI:NL:HR:1968:AB6079, NJ 1970/123). Naar het oordeel van de rechtbank is toezicht op deze gedragsaanwijzing middels controle van computers en andere apparatuur gezien het bewezenverklaarde noodzakelijk en proportioneel. De noodzaak is gelegen in de omstandigheid dat de gedragsaanwijzing zonder controle zinloos is. Controle is ook proportioneel nu dit is beperkt tot controle van gegevensdragers op aanwezigheid van kinder/dierenpornografisch materiaal. In casu is er sprake van een gedragsaanwijzing waarvan de naleving bij huisbezoeken (door de reclassering) kan worden gecontroleerd."*

We merken op dat de rechtbank geen begrenzing heeft gegeven met betrekking tot de frequentie waarmee controles kunnen plaatsvinden, zodat naar onze inschatting reeds op die grond potentieel sprake is van een meer dan geringe inbreuk op de grondrechten van de verdachte, hetgeen niet toelaatbaar wordt geacht. Onze inschatting, gebaseerd op kennisneming van een significante hoeveelheid beslissingen op dit punt, is dat in het merendeel daarvan geen frequentiebegrenzing is opgenomen.

In een aantal uitspraken is een formulering gekozen die meer tegemoet komt aan de bezwaren die de Hoge Raad in zijn arrest heeft genoemd. De rechtbank Amsterdam heeft in een vonnis overwogen dat zij uit het arrest van de Hoge Raad afleidt dat controle van gegevensdragers als bijzondere voorwaarde mogelijk is, indien sprake is van een bijzondere voorwaarde die een voldoende duidelijk gedragsvoorschrift bevat en niet een te veelomvattend en te ingrijpend dwangmiddel is.[817] In het dictum is te lezen dat de rechtbank de voorwaarde als volgt vorm heeft gegeven:

> *"- wordt verplicht zich te onthouden van:*

---

[815] Conclusie AG 1-12-2015, ECLI:NL:PHR:2015:2693 (overweging 15 e.v.).
[816] RB Gelderland 19-7-2018, ECLI:NL:RBGEL:2018:3213, RB Gelderland 29-11-2018, ECLI:NL:RBGEL:2018:5103.
[817] RB Amsterdam 26-1-2018, ECLI:NL:RBAMS:2018:517.

(a) gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen en
(b) gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met kinderen wordt gecommuniceerd.

Ten behoeve van de naleving van deze laatstgenoemde verplichting is veroordeelde verder verplicht zijn medewerking te verlenen aan het steekproefsgewijs laten controleren van zijn digitale gegevensdragers. De reclassering bepaalt in welke gevallen, op welke manier, door wie en wanneer de feitelijke controle plaatsvindt. De medewerking dient uit het volgende te bestaan:
• Veroordeelde moet maximaal tweemaal per jaar in het kader van die controle aan de reclassering en eventueel door de reclassering uitgenodigde politiemedewerkers de toegang verschaffen tot zijn woning;
• Veroordeelde moet dan op verzoek van de reclassering al zijn digitale gegevensdragers ter beschikking stellen dan wel overhandigen aan de reclasserings- of politiemedewerkers;
• Veroordeelde moet de reclassering dan wel de door hen uitgenodigde politiemedewerkers de toegang verschaffen tot alle aanwezige digitale gegevensdragers, bijvoorbeeld door het geven van de benodigde wachtwoorden."

De rechtbank heeft gekozen voor een expliciete tweedeling door de verplichting tot onthouding van bepaald gedrag als voorwaarde te stellen en daaraan de verplichting tot het meewerken aan die controle te koppelen. Belangrijk is dat de rechtbank daarnaast precies heeft omschreven waaruit de medewerking tot controle precies moet bestaan en dat de controle een bepaalde maximale frequentie per jaar van de proeftijd heeft. Deze wijze van formuleren heeft navolging gevonden in uitspraken van andere rechtbanken[818] en is tevens (integraal) overgenomen in onder meer een arrest van het hof Den Haag.[819]

Het voorgaande komt echter onvoldoende tegemoet aan de bezwaren van de Hoge Raad. Op 7 juli 2020 casseerde de Hoge Raad een ander arrest van het hof Den Haag waarin de volgende bijzondere voorwaarde was opgenomen.[820]

"Stelt als bijzondere voorwaarde dat de veroordeelde zich gedurende de proeftijd op welke wijze dan ook:
- onthoudt van het op digitale wijze met een seksuele intentie communiceren met minderjarigen/kinderen,
- zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen,
- zich onthoudt van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd, terwijl het daarop uitgeoefende toezicht de afspraak omvat dat de veroordeelde geen wisprogramma's op zijn digitale apparatuur mag hebben of gebruiken."
En:
"Stelt als bijzondere voorwaarde dat de veroordeelde maximaal tweemaal per jaar in het kader van controle van zijn digitale gegevensdragers aan de reclassering en eventueel door de reclassering uitgenodigde politiemedewerkers de toegang verschaft

[818] RB Oost-Brabant 27-3-2018, ECLI:NL:RBOBR:2018:1428 en RB Gelderland 10-4-2018, ECLI:NL:RBGEL:2018:1680.
[819] Hof Den Haag 25-9-2018, ECLI:NL:GHDHA:2018:2490.
[820] HR 7-7-2020, ECLI:NL:HR:2020:1215.

> *tot zijn woning, waarbij de veroordeelde dan op verzoek van de reclassering, al zijn digitale gegevensdragers ter beschikking moet stellen dan wel overhandigen aan de reclasserings- of politiemedewerkers. De veroordeelde moet de reclassering dan wel de door hen uitgenodigde politiemedewerkers de toegang verschaffen tot alle aanwezige digitale gegevensdragers, bijvoorbeeld door het geven van de benodigde wachtwoorden."*

De gedragsvoorwaarde is langs dezelfde lijn opgebouwd als de hiervoor besproken oplossing van de rechtbank Amsterdam. Het kon echter niet op goedkeuring van de Hoge Raad rekenen. De Hoge Raad herhaalt, zoals reeds eerder vermeld, de uitgangspunten uit eerder genoemd arrest uit 2016 en overweegt dat de bijzondere voorwaarde niet voldoet aan deze maatstaven. Het hof heeft niet voldoende duidelijk tot uitdrukking gebracht dat is beoogd het toezicht op de naleving van de gedragsvoorwaarde te regelen en evenmin voldoende precies geformuleerd dat het onderzoek aan de gegevensdragers (en daarmee verbonden het verlenen van toegang tot de woning en de gegevensdragers) beperkt dient te blijven tot toezicht op de naleving van de gedragsvoorwaarde. Daarnaast heeft het hof evenmin voldoende precies geformuleerd op welke wijze dat onderzoek aan de gegevensdragers mag worden uitgevoerd en welke functionarissen daarbij de reclassering (technische) ondersteuning mogen bieden, teneinde te waarborgen dat de persoonlijke levenssfeer van de verdachte niet meer dan nodig voor het beoogde toezicht wordt beperkt. Na terugverwijzing door de Hoge Raad heeft het hof Den Haag derhalve in 2021 opnieuw arrest gewezen in deze zaak.

Het hof Den Haag heeft in dit arrest, waarbij het aansluiting heeft gezocht bij het arrest van ditzelfde hof van 9 februari 2021[821], het volgende overwogen[822]:

> "*Het hof is van oordeel dat het noodzakelijk is om de maximale hoeveelheid en de frequentie van controles van geautomatiseerde werken en digitale gegevensdragers te beperken ter voorkoming van een te ingrijpende inbreuk op het privéleven van de verdachte, maar beoogt met de hierna weer te geven modaliteit te bereiken dat maximale vrijheid wordt gegeven aan de reclassering om te voorkomen dat de verdachte zijn gedrag kan aanpassen aan het aantal en de frequentie van deze controles.*
> *Het voorgaande leidt tot het volgende.*
> *Het toezicht op de hierna onder 4 vermelde voorwaarde [opmerking auteurs: deze voorwaarde betreft het zich onthouden van het op digitale wijze met een seksuele intentie communiceren met minderjarigen/kinderen, het zich onthouden van gedragingen die zijn gericht op internetomgevingen waarin kinderpornografisch materiaal kan worden verkregen, het zich onthouden van gedragingen die zijn gericht op internetomgevingen waarin over seksuele handelingen met minderjarigen/kinderen wordt gecommuniceerd en het zich onthouden van het aanwezig hebben of gebruiken van wisprogramma's op zijn digitale apparatuur] kan onder andere bestaan uit controles van geautomatiseerde werken en digitale gegevensdragers. De verdachte dient daaraan mee te werken tijdens een huisbezoek. Deze controles mogen gedurende de proeftijd, die wordt gesteld op 3 jaren, maximaal 3 keer worden uitgevoerd en mogen – voor zover het gedrag bedoeld onder het tweede en derde gedachtestreepje van de onder 4 gestelde voorwaarde betreft – **slechts op zodanige wijze worden uitgevoerd dat niet door een persoon kennis wordt genomen van de inhoud van afbeeldingen (geautomatiseerde controle is derhalve wel toegestaan). Tot slot***

[821] Hof Den Haag, 9-2-2021, ECLI:NL:GHDHA:2021:193.
[822] Hof Den Haag, 24-3-2021, ECLI:NL:GHDHA:2021:569.

bepaalt het hof dat ten behoeve van deze controle een deskundige (niet zijnde een opsporingsambtenaar) de reclassering (technische) ondersteuning mag bieden. ”[823]

Nu dit zeker niet in alle gevallen in latere rechtspraak terugkeert lijkt het nuttig om er op te wijzen dat in voormeld arrest een uitdrukkelijk onderscheid wordt gemaakt tussen enerzijds de specifieke gedragsvoorwaarde (gericht op kortweg het zich onthouden van digitaal gedrag met betrekking tot kinderpornografie) en anderzijds de wijze waarop het daartoe te houden toezicht kan worden uitgeoefend. Dat laatste is van geheel andere aard dan de voorwaarde betreffende het gedrag van de veroordeelde als bedoeld in artikel 14c, lid 2 sub 14 Sr., en gebaseerd op art. 14c lid 6 Sr. In veel uitspraken zien wij deze twee elementen door elkaar lopen.

De Hoge Raad heeft in zijn arrest van 29 november 2022[824] geoordeeld dat de hierboven weergegeven randvoorwaarden zoals geformuleerd in het arrest van het hof Den Haag van 9 februari 2021 (ECLI:NL:GHDHA:2021:569) niet van een onjuiste rechtsopvatting getuigen en toereikend gemotiveerd zijn. In dit arrest overweegt de Hoge Raad voor het eerst expliciet dat het ontbreken van een specifieke wettelijke regeling voor de vormgeving van het toezicht op de naleving van bijzondere voorwaarden die strekken tot controle van gegevensdragers, niet eraan in de weg staat dat de rechter zelf invulling geeft aan de wijze waarop dat toezicht kan plaatsvinden[825]. Voordien bestond in de rechtspraak geen consensus over de vraag of de strafrechter zich met de vormgeving van het toezicht zou mogen bemoeien.[826] Tevens heeft de Hoge Raad overwogen dat het aspect “welke (politie)functionarissen bij de controle betrokken mogen zijn” onverkort relevant is voor de vormgeving van het toezicht.

---

[823] Deze formulering is o.m. gevolgd in: Hof Arnhem-Leeuwarden 22-11-2022, ECLI:NL:GHARL:2022:9671, Hof Arnhem-Leeuwarden 26-10-2021, ECLI:NL:GHARL:2021:10329 (onder expliciete verwijzing naar de voormelde 2 arresten van het Hof Den Haag); RB Overijssel 7-4-2023, ECLI:NL:RBOVE:2023:1252, RB Den-Haag 2-3-2023, ECLI:NL:RBDHA:2023:3469, RB Den Haag 7-12-2022, ECLI:NL:RBDHA:2022:13114, RB Zeeland-West-Brabant 14-7-2022, ECLI:NL:RBZWB:2022:3852, RB Den Haag 30-8-2022, ECLI:NL:RBDHA:2022:8626 en RB Rotterdam 29-3-2022, ECLI:NL:RBROT:2022:2304, RB Rotterdam 10-3-2022, ECLI:NL:RBROT:2022:1743, RB Midden-Nederland, 19-1-2022, ECLI:NL:RBMNE:2022:101, RB Rotterdam, 28-10-2021, ECLI:NL:RBROT:2021:10779.

[824] HR 29-11-2022, ECLI:NL:HR:2022:1763 (zie ook: CPG Vegter, 11-10-2022, ECLI:NL:PHR:2022:915).

[825] Zie i.h.b. r.o. 2.4 van het arrest: “*Het ontbreken van zo’n specifieke wettelijke regeling betekent niet dat de rechter bij het geven van een toezichtsopdracht geen nadere invulling kan geven aan de manier waarop dat toezicht kan plaatsvinden. Wel zal bij het geven van zo’n opdracht moeten zijn gewaarborgd dat het toezicht niet leidt tot een meer dan beperkte inbreuk op de persoonlijke levenssfeer van de veroordeelde. Daarbij komt betekenis toe aan de vraag met welke frequentie en hoe de controles van de gegevensdragers mogen worden uitgevoerd en welke (politie)functionarissen daarbij betrokken mogen zijn*.”

[826] Vgl. o.m. Hof ’s-Hertogenbosch, 22-2-2022, ECLI:NL:GHSHE:2022:520: “*Het hof zal, anders dan door de rechtbank is bepaald en door de advocaat-generaal is gevorderd, niet bepalen dat de verdachte zijn medewerking zal verlenen aan het steekproefsgewijs laten controleren van zijn digitale gegevensdragers op de aanwezigheid van kinderporno, waarbij de reclassering bepaalt in welke gevallen, op welke manier, door wie en wanneer de feitelijke controle plaatsvindt, nu een dergelijke voorwaarde naar het oordeel van het hof niet voldoet aan de eisen van art. 14c, lid 2 sub 14 Sr, inhoudende dat de voorwaarde het gedrag van de veroordeelde dient te betreffen, waarbij voldoende precies het daarin vervatte gedragsvoorschrift dient te worden geformuleerd*.”

Ondertussen gaat een aantal gerechten nog steeds op de oude voet verder.[827] Nu dit zonder nadere onderbouwing gebeurt, is het de vraag of dit het gevolg is van een andere rechtsopvatting – hetgeen uiteraard mogelijk is – of van het niet op de hoogte zijn van de recente jurisprudentie (waarvan na lezing van dit boek geen sprake meer kan zijn).

Wat opvalt in de meer recente jurisprudentie is dat met enige regelmaat nieuwe of anders geformuleerde voorwaarden opduiken. Van eenvormigheid is zeker geen sprake.
Als voorbeelden kunnen worden genoemd:

- De verhoging van de frequentie van het aantal mogelijke controles per jaar. Waar lange tijd twee keer per jaar gemeengoed was, zien we nu ook een maximum van drie keer per jaar.[828] Onduidelijk is waar dit op gebaseerd is, enige onderbouwing zijn wij nog niet tegengekomen.
- "Kan het digitaal onderzoek onvoldoende ter plaatse plaatsvinden, dan kan de deskundige na goedkeuring van de reclassering een digitale kopie maken van de geautomatiseerde werken en gegevensdragers. De kopie wordt zo spoedig mogelijk elders onderzocht, waarna de deskundige het onderzoeksresultaat uitsluitend rapporteert aan de reclassering. (…). Binnen twee weken nadat de reclassering is gebleken dat geen schending van de gedragsvoorwaarde heeft plaatsgevonden wordt de digitale kopie vernietigd."[829] Curieus is dat het maken van een kopie van geautomatiseerde werken en/of gegevensdragers in het kader van het toezicht op de naleving van bijzondere voorwaarden zonder enige beperking wordt toegestaan, terwijl dergelijke onderzoekshandelingen in het kader van de opsporing strikt genormeerd zijn (zie: de smartphone-jurisprudentie[830]). Volstrekt onduidelijk is op welke wijze de reclassering achteraf zou kunnen controleren of de kopie daadwerkelijk door de politie is vernietigd.
- "De zedenrechercheur rapporteert uitsluitend aan de reclassering".[831] Met andere woorden wordt het de betreffende rechercheur verboden om een proces-verbaal op te maken. Behalve dat het de (retorische) vraag is in hoeverre een dergelijk verbod kan worden gebaseerd op art. 14c lid 2 sub 14 Sr, kan worden betwijfeld of het een opsporingsambtenaar vrij staat om geen proces-verbaal op te maken van het aantreffen van kinderpornografisch materiaal.
- "De veroordeelde (…) meldt welke gegevensdragers hij gebruikt en stemt in met controle op deze gegevensdragers."[832] Hoewel de formulering "stemt in met" vrijwilligheid suggereert, kan zij onzes inziens niet anders worden opgevat dan als een meewerkverplichting. Afgedwongen instemming is immers geen instemming.

---

[827] Zie o.a.: RB Amsterdam 2-2-2022, ECLI:NL:RBAMS:2022:351, RB Oost-Brabant 14-09-2021, ECLI:NL:RBOBR:2021:4920; RB Gelderland 22-06-2021 ECLI:NL:RBGEL:2021:3130; RB Oost-Brabant 11-8-2020, ECLI:NL:RBOBR:2020:3971, RB Overijssel 6-8-2020, ECLI:NL:RBOVE:2020:2599, RB Limburg 5-8-2020, ECLI:NL:RBLIM:2020:5774, RB Noord-Nederland 28-7-2020, ECLI:NL:RBNNE:2020:2624, RB Midden-Nederland 17-7-2020, ECLI:NL:RBMNE:2020:2733.
[828] Zie bijv. RB Noord-Nederland 3-2-2022, ECLI:NL:RBNNE:2022:232, RB Midden-Nederland 30-6-2021, ECLI:NL:RBMNE:2021:2767 en RB Midden-Nederland 1-10-2021, ECLI:NL:RBMNE:2021:5510. Soms is sprake van een nog hogere frequentie; zie bijv. Hof 's-Hertogenbosch 9-8-2022, ECLI:NL:GHSHE:2022:2741 (max. 4 keer per jaar).
[829] Zie bijv. RB Noord-Nederland 3-1-2023, ECLI:NL:RBNNE:2023:112 en RB Noord-Nederland 3-11-2022, ECLI:NL:RBNNE:2022:4093.
[830] HR 4-4-2017, ECLI:NL:HR:2017:584, ECLI:NL:HR:2017:588, ECLI:NL:HR:2017:592.
[831] Zie bijv. RB Noord-Nederland 31-8-2021, ECLI:NL:RBNNE:2021:3825 en RB Noord-Nederland 29-4-2021, ECLI:NL:RBNNE:2021:1826.
[832] Zie bijv. RB Rotterdam 26-1-2023, ECLI:NL:RBROT:2023:568.

- "De verdachte moet de reclasseringswerker dan wel de door de reclassering uitgenodigde medewerker van de digitale recherche toegang verschaffen tot alle aanwezige geautomatiseerde werken en elektronische dan wel digitale gegevensdragers".[833] Dit roept de vraag op waarom dit niet is beperkt tot aan de verdachte toebehorende apparaten. Het gaat immers om het toezicht op zijn gedrag. Daar kan tegen worden ingebracht dat dat gedrag op ieder apparaat kan plaatsvinden, maar dan zouden bijvoorbeeld ook computers in de lokale bibliotheek of het internetcafé onderzocht moeten kunnen worden. De gebruikte formulering leidt er in ieder geval toe dat de verdachte ook toegang moet verstrekken tot apparaten van zijn gezinsleden, visite, etc. Naast het praktische probleem van het doorbreken van de beveiliging van die apparaten (hoe te handelen als die derden hun wachtwoord of toegangscode niet willen afgeven?) lijkt de inbreuk op de persoonlijke levenssfeer van die derden die het onderzoek van hun apparaten zou veroorzaken, bepaald te ver te gaan.
- "Daarnaast mag er in de gegevensdragers enkel worden gezocht met een daarvoor geschikt zoekprogramma en enkel met gebruikmaking van de daartoe bij de opsporingsinstanties in gebruik zijnde en daartoe geëigende op de opsporing van kinderporno gerichte zoektermen."[834] In de praktijk wordt de inhoud van gegevensdragers niet door middel van kinderpornogerelateerde zoektermen onderzocht, maar worden de op de gegevensdrager(s) aanwezige afbeeldingen door middel van hashwaardevergelijking op geautomatiseerde wijze vergeleken met (een) verzameling(en) van reeds bekende kinderpornografische afbeeldingen.[835]
- "De controle strekt er niet toe een beeld te krijgen van het persoonlijke leven van veroordeelde."[836] Dit lijkt meer een vorm van juridische exoneratie dan een concrete grens aan de wijze waarop het toezicht mag worden uitgeoefend. Relevanter lijkt te zijn hoe te voorkomen dat een dergelijk beeld de facto ontstaat of om de stelselmatigheid van de inbreuk op de persoonlijke levenssfeer zoveel mogelijk te beperken.

8.4.2.4. Storting geldbedrag op rekening NGO

Zoals hiervoor al aangegeven komt het in art. 240b-zaken slechts zeer sporadisch voor dat slachtoffers zich als benadeelde partij stellen of dat anderszins schadevergoeding wordt gevorderd.[837] Toekenning van schadevergoeding aan individuele personen komt derhalve in dit kader slechts zeer zelden voor.

In een aantal uitspraken[838] werd echter in het kader van een veroordeling wegens overtreding van art. 240b Sr de bijzondere voorwaarde opgelegd van storting van een geldbedrag op de rekening van kinderrechtenorganisaties als Defence for Children/ECPAT en Terre des Hommes en recentelijk Stop it Now. Hoewel oplegging van een dergelijke bijzondere voorwaarde ingevolge art. 14c, tweede lid, onder 4, Sr wettelijk lijkt te zijn toegestaan, is de

---

[833] Zie bijv. RB Midden-Nederland 1-10-2021, ECLI:NL:RBMNE:2021:5510.
[834] Zie bijv. RB Zeeland-West-Brabant, 1 juli 2022, ECLI:NL:RBZWB:2022:3520.
[835] Zie: Controle van gegevensdragers: toezicht of opsporing? J.W. van den Hurk en S.J. de Vries, *NJB* 2020/571.
[836] Zie bijv. RB Rotterdam, 3-6-2022, ECLI:NL:RBROT:2022:4375, RB Noord-Nederland 15-11-2021, ECLI:NL:RBNNE:2021:4974 en RB Noord-Holland 11-11-2021, ECLI:NL:RBNHO:2021:10190.
[837] Zie hiervoor onder 7.8.
[838] RB Gelderland, 22-06-2021 ECLI:NL:RBGEL:2021:3130 (€ 500 voor Stop it Now); RB Midden-Nederland 1-9-2014, ECLI:NL:RBMNE:2014:3827 (€ 5.000 voor Terre des Hommes), Hof Den Haag 4-12-2015, ECLI:NL:GHDHA:2015:3995 (€ 7.500 voor Defence for Children) en RB Gelderland 10-4-2018, ECLI:NL:RBGEL:2018:1680 (gedurende de proeftijd € 50,- per maand voor hulplijn "Stop It Now" (kennelijk na suggestie verdediging)).

toepassing daarvan niet onproblematisch. Met name de keuze door de rechter van de instelling waaraan het geldbedrag moet worden voldaan, kan tot discussie leiden, nu daardoor ook mogelijk de financiële belangen van dergelijke instellingen, en de persoonlijke voorkeuren van de rechter een rol kunnen gaan spelen bij de besluitvorming. In dit licht verrast het niet dat deze uitspraken – voor zover bekend – weinig navolging hebben gevonden.

8.4.3. Bevel directe uitvoerbaarheid ex art. 14e Sr van bijzondere voorwaarden
In het kader van de straftoemeting in art. 240b Sr-zaken komt ook regelmatig de vraag aan de orde of opgelegde bijzondere voorwaarden ook "dadelijk uitvoerbaar", als bedoeld in art. 14e Sr kunnen en/of moeten worden verklaard. Deze vraag speelt met name als vanuit het oogpunt van de voorkoming van recidive spoedige aanvang met een behandeling of van toezichtmaatregelen wenselijk wordt geacht.

Oplegging van een bevel tot dadelijke uitvoerbaarheid is ingevolge art. 14e Sr alleen mogelijk indien er "*ernstig rekening mee moet worden gehouden dat de veroordeelde wederom een misdrijf zal begaan dat gericht is tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen*." Een wellicht niet onbelangrijk gegeven hierbij is dat uit de wetsgeschiedenis blijkt dat in ieder geval de toenmalige staatssecretaris Teeven aangaf dat bij toepassing van art. 14e Sr vooral gedacht moest worden aan gevallen van veroordeling wegens (ernstige) zedenmisdrijven.[839]

Naast de vraag van de in concreto in te schatten en in de uitspraak te onderbouwen recidivekans, zal de strafrechter hier tevens de vraag moeten beantwoorden in hoeverre het delict van art. 240b Sr kan worden beschouwd als "te zijn gericht tegen of gevaar veroorzaakt voor de onaantastbaarheid van het lichaam van een of meer personen". Zoals hiervoor onder 8.4.1. reeds beschreven (en waarnaar hier kortheidshalve verder wordt verwezen) was de rechtspraak geruime tijd verdeeld over de beantwoording van deze vraag.

Op 28 maart 2017 heeft de Hoge Raad echter met verwijzing naar de wetsgeschiedenis geoordeeld dat (in ieder geval) de gedragingen "in bezit hebben van" en "verwerven van", respectievelijk het "zich toegang verschaffen tot" kinderporno geen gedragingen zijn "*die onmiskenbaar zijn gericht tegen of gevaar veroorzaken voor de onaantastbaarheid van het lichaam van een of meer personen*" in de zin van art. 14b, tweede lid, Sr en dat deze gedragingen ook niet zonder meer kunnen worden gekarakteriseerd als misdrijven die dergelijke gedragingen omvatten.[840] Aannemelijk is derhalve dat in ieder geval bij veroordeling voor (alleen) deze gedragingen geen bevel tot directe uitvoerbaarheid van bijzondere voorwaarden kan worden gegeven.[841]

///

---

[839] In de Nota naar aanleiding van het verslag (p. 29, onder 5.3) bij wetsvoorstel 32319, (nr. 7, 2011) stelt de toenmalige staatssecretaris dat bij de toepassing van art. 14e Sr met name gedacht moest worden aan gevallen waarin ernstig recidivegevaar bestond voor een zeden- of geweldsmisdrijf c.q. aan veroordeling wegens een ernstig zedendelict, aangezien dat de gevallen waren waarin veelal ook bijvoorbeeld een verlengde proeftijd door de rechtspraak werd opgelegd.
[840] HR 28-3-2017, ECLI:NL:HR:2017:524, r.o. 2.5.3.
[841] Over andere gedragingen met betrekking tot kinderporno (zoals vervaardigen en verspreiden) heeft de Hoge Raad zich dus nog niet uitgesproken, terwijl ook bij die gedragingen de risico's op lichamelijke schade voor jeugdigen aanmerkelijk reëler lijken te zijn. Bepaald niet uitgesloten kan derhalve worden dat bij veroordeling voor dergelijke gedragingen wel een bevel directe uitvoerbaarheid kan worden gegeven, evenals in het geval dat naast de feiten met kinderpornografie ook sprake is van veroordeling voor zedendelicten met een meer fysieke dimensie.

Nawoord

Bij de vijfde editie
Om dit boek een bruikbaar naslagwerk te laten blijven is het, gezien met name de hoeveelheid nieuwe rechtspraak, nodig om regelmatig een geactualiseerde versie hiervan uit te brengen. Nieuwe rechtspraak is toegevoegd en voor zover verantwoord zijn verwijzingen naar oudere uitspraken verwijderd teneinde de toegankelijkheid te behouden. Toegevoegd zijn nieuwe technische lemma's over 'thumbnails' en 'backup's en het lemma over 'unallocated clusters/"deleted files"' is bewerkt. Verder zijn snelkoppelingen gecontroleerd op geldigheid en is feitelijke informatie zoveel mogelijk geactualiseerd.

In overleg met Aldo Kuijer is besloten zijn naam niet meer op de voorpagina te vermelden. Dat neemt niet weg dat hij nog steeds de geestelijke vader van een belangrijk deel van de teksten in dit boek is. Wij hebben de eer om hieraan verder te mogen werken en de uitdaging om het door Aldo gerealiseerde niveau op zijn minst te handhaven.

J.W. van den Hurk/R.J.A. Klaar/J.J. Mossink
Den Haag, maart 2023

Bij de derde en vierde editie
Na het vertrek van Aldo Kuijer bij het Kenniscentrum Cybercrime is nagedacht over de toekomst van dit boek, dat toch als zijn geesteskind beschouwd moet worden. Gezien de enorme hoeveelheid informatie die het bevat, de niet aflatende stroom van zaken op het gebied van kinderporno en het ontbreken van een alternatief is besloten tot een grondige update. Vanzelfsprekend zijn de verwijzingen naar jurisprudentie geactualiseerd. Ten behoeve van de leesbaarheid zijn waar mogelijk verwijzingen naar oudere jurisprudentie geschrapt. Diverse onderwerpen vroegen om grondiger herziening of aanvulling, we noemen het onderzoek aan gegevensdragers als uitvloeisel van de Smartphone-arresten, de biometrische ontgrendeling van devices, de ontoegankelijkmaking van gegevens en de teruggave van bestanden afkomstig van in beslag genomen gegevensdragers.

Met deze bewerking komt de verantwoordelijk voor de inhoud van dit boek bij ons te liggen. Wij zijn Aldo Kuijer bijzonder veel dank verschuldigd voor de immense hoeveelheid werk die hij heeft verricht om dit boek tot stand te brengen; daarzonder was dit nimmer van de grond gekomen.

J.W. van den Hurk/S.J. de Vries/R.J.A. Klaar/J.J. Mossink
Den Haag, januari 2022

Bij de tweede editie
Veel dank aan:
Sander de Vries, Rieneke van den Bosch en Christiaan Baardman van het Kenniscentrum Cybercrime voor de Rechtspraak, Jan-Willem van den Hurk van het Gerechtshof Den Haag, Harm van Beek, Ruud Schramp en Frank van der Neut van het Nederlands Forensisch Instituut, Dick van Dijk en Erik Kuijl van het Team Bestrijding Kinderpornografie en Kindersekstoerisme van de Landelijke Eenheid van de Nationale Politie, Irene Verheij, Michelle Spoormaker, Jasper van Berkum, Brechtje Lijnse en Danielle van der Ven – Laheij van het Landelijk Parket, en aan alle anderen die mij relevant materiaal hebben toegezonden en/of concepten en/of de eerste versie van deze uitgave van waardevol commentaar hebben voorzien en/of inhoudelijke ondersteuning hebben gegeven. Hun hulp was onmisbaar en zeer welkom.
De uiteindelijke tekst, en de keuzes die daarbij gemaakt zijn, komt echter volledig voor rekening van mij als auteur. Op eventuele onjuistheden of tekortkomingen dient u derhalve niet de hiervoor genoemden aan te kijken, maar ondergetekende. ☺

De tekst van de tweede editie is afgesloten op 9 april 2018; de voor 1 april 2018 gepubliceerde jurisprudentie is zo veel mogelijk verwerkt.

Aldo Kuijer.
Den Haag, april 2018

Changelog

Versie 2020.4 (maart 2023)
-vijfde, geheel herziene versie (jurisprudentie is tot 8 april 2023 bijgewerkt)

Versie 2020.3 (januari 2022)
-vierde, geheel herziene versie (jurisprudentie is tot 1 november 2021 bijgewerkt)

Versie 2020.2. (september 2020)
- aantal afbeeldingen ter illustratie veranderd
- een aantal “dode links” gerepareerd
- de jurisprudentie van de Hoge Raad is tot en met sluitingsdatum bijgewerkt.

Versie 2020.1 (april 2020)
- derde, geheel herziene versie (jurisprudentie is tot 30 maart 2020 bijgewerkt)

Versie 2018 (april 2018)
- tweede, geheel herziene versie

Versie 2017 (mei 2017).
- eerste editie