2 Materieel strafrecht en ICT

Bert-Jaap Koops en Jan-Jaap Oerlemans[1]

2.1 Inleiding

De ontwikkeling van informatie- en communicatietechnologie (ICT) heeft een steeds belangrijkere weerslag op het materiële strafrecht. Aan de ene kant heeft de opkomst van ICT geleid tot het ontstaan van nieuwe strafwaardige feiten gericht tegen deze technologie, zoals computervredebreuk en het verspreiden van kwaadaardige software. Dit is de computercriminaliteit in enge zin. Aan de andere kant maakt ICT het ook mogelijk om traditionele delicten, zoals oplichting, drugshandel, witwassen, of de verspreiding van kinderporno, via elektronische weg te plegen, waarbij de computer slechts een hulpmiddel of omgevingsfactor is – de computercriminaliteit in brede zin. Aangezien gegevens niet onder het strafrechtelijke begrip 'enig goed' vallen (zie paragraaf 1.5.2), is het Wetboek van Strafrecht (Sr) systematisch aangepast om strafwaardig geachte feiten met betrekking tot gegevens strafbaar te stellen; soms is daartoe een bestaande strafbepaling geherformuleerd, soms is een nieuwe strafbaarstelling ingevoerd. Daarbij heeft de wetgever gekozen voor het beginsel dat gegevens *als zodanig* niet strafrechtelijk worden beschermd tegen (onrechtmatige) toegang of kennisneming: slechts strafbaar is de wijze waarop men zich die gegevens toe-eigent, door in te breken in computers of (tele)communicatie af te luisteren. Dus niet de onstoffelijke gegevens zelf, maar het stoffelijk medium waarvan die gegevens zich bedienen wordt tegen misbruik beschermd.[2] Daarbij speelde ook het beginsel van de *free flow of information* een belangrijke rol: het uitgangspunt bij gegevens is, anders dan bij goederen die in beginsel eigendom van iemand zijn, dat zij vrijelijk moeten kunnen worden uitgewisseld. De wetgever houdt vooralsnog vast aan het uitgangspunt dat gegevens in principe niet als goederen worden aangemerkt. Om deze reden zijn ook in de Wet computercriminaliteit III nieuwe strafbepalingen geïntroduceerd, zoals het 'helen' van gegevens, voor schadelijke gedragingen met gegevens die niet als goederen worden beschouwd. Daar-

1 Bert-Jaap Koops is hoogleraar regulering van technologie bij TILT – Tilburg Institute for Law, Technology, and Society van Tilburg University. Jan-Jaap Oerlemans is als onderzoeker verbonden aan eLaw, het centrum voor Recht en Digitale Technologie van de Universiteit Leiden. Dit hoofdstuk bouwt voort op de versie uit de tweede druk (2007) van Bert-Jaap Koops en Theo de Roos, emeritus hoogleraar strafrecht en strafprocesrecht aan Tilburg University.

2 Zie *Kamerstukken II* 1990/91, 21551, 6, p. 9: "Het gaat om de strafrechtelijke bescherming van de huls of de verpakking, niet van de gegevens zelf".

bij lijkt de nieuwe strafbaarstelling van het wederrechtelijk overnemen van gegevens (zie paragraaf 2.3.5) wel een zekere breuk op te leveren met het eerdere uitgangspunt dat gegevens als zodanig niet worden beschermd.

De strafbepalingen betreffende computercriminaliteit in enge zin zijn nog relatief 'jong'; een analyse van deze bepalingen en bespreking van de relevante jurisprudentie heeft daarom de meeste meerwaarde. Traditionele delicten die zijn gewijzigd naar aanleiding van computercriminaliteitswetgeving, of die steeds vaker via internet worden gepleegd, worden in dit hoofdstuk korter besproken.

Hierbij willen wij benadrukken dat in de praktijk in de tenlastelegging niet altijd de nadruk wordt gelegd op de computerdelicten. Als een persoon wordt verdacht van het op afstand bespioneren van mensen via hun computer met behulp van malware, kan naast 'gegevensaantasting' bijvoorbeeld ook worden vervolgd voor het heimelijk maken van beeldopnamen (zie ook paragraaf 2.4.5).

Een vergelijkbare situatie doet zich voor als een persoon het slachtoffer wordt van 'banking malware', waarmee de internetbankiersessie van mensen wordt overgenomen.[3] Na het overnemen van inloggegevens voor de betaling wordt dan een bedrag overgemaakt naar een geldezel en wordt het geld verder witgewassen. Verdachten in dit type zaken worden ook veroordeeld voor meer traditionele delicten zoals diefstal met een valse sleutel (artikel 311 lid 1 onder 4 en 5 Sr) en oplichting (artikel 326 Sr).[4]

Soms ligt het vanuit opsporingsperspectief zelfs meer voor de hand de nadruk te leggen op een meer traditioneel delict, omdat daarvoor een hogere gevangenisstraf kan worden opgelegd. Daarbij kan gedacht worden aan 'ransomware', waarbij computersystemen gegijzeld worden en slechts na betaling van losgeld weer toegang tot het systeem of bestanden wordt verleend. In dat geval kan worden vervolgd voor gegevensaantasting of computersabotage, maar ook voor afpersing (artikel 317 lid 2 Sr), waarvoor een hogere gevangenisstraf kan worden opgelegd.[5] Gelukkig worden in de praktijk steeds vaker zowel de traditionele delicten als de computerdelicten (eventueel subsidiair) ten laste gelegd. Daardoor ontstaat meer jurisprudentie en wordt óók het belang van vertrouwelijkheid, integriteit en beschikbaarheid van computersystemen onderstreept.

Bij de bespreking in dit hoofdstuk vermelden we steeds de strafmaxima, waaronder de maximale geldboetes. In artikel 23 Sr staan de volgende zes categorieën van geldboetes:

– 1e categorie: € 415;
– 2e categorie: € 4150;
– 3e categorie: € 8300;
– 4e categorie: € 20.750;
– 5e categorie: € 83.000;

3 Zie uitgebreid Oerlemans e.a. 2016.

4 Zie bijvoorbeeld Rb. Rotterdam 2 oktober 2015, ECLI:NL:RBROT:2015:7038 (*MegaServer*), Rb. Zeeland-West-Brabant 29 juni 2016, ECLI:NL:RBZWB:2016:3877, Rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175 , nr. 5, p. 268-277, m.nt. J.J. Oerlemans (*TorRAT*-zaak) en Hof Den Haag 24 januari 2017, ECLI:NL:GHDHA:2017:81 en Rb. Rotterdam 7 april 2017, ECLI:NL:RBROT:2017:2815.

5 Zie bijvoorbeeld Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153.

– 6e categorie: € 830.000.[6]

Voordat de relevante materiaalrechtelijke bepalingen worden besproken, is het van belang de definities van 'gegevens' en 'geautomatiseerd werk' helder te hebben. De definities worden daarom in paragraaf 2.2 behandeld. Vervolgens worden de uiteenlopende strafbare feiten behandeld. Wij volgen hierbij (in grote lijnen) de volgorde van de indeling van delicten in het Cybercrimeverdrag, omdat dit een mooie opeenvolging biedt van computergerichte delicten (de computer/gegevens als object), computergerelateerde delicten (de computer/gegevens als – substantieel – instrument van klassieke delicten) en computer-relevante delicten (inhoud-gerelateerde en intellectueel-eigendomsdelicten) (vgl. paragraaf 1.2).[7] Tussendoor bespreken we delicten die systematisch bij een van deze categorieën passen, ook als ze niet als zodanig in het Cybercrimeverdrag strafbaar zijn gesteld (zoals diefstal en heling in het kader van computergerelateerde delicten, of grooming en *sextortion* in het kader van inhoud-gelerateerde delicten).
De computergerichte delicten betreffen computervredebreuk (paragraaf 2.3), onrechtmatig onderscheppen van communicatie (paragraaf 2.4, waarbij we ook het gerelateerde onderwerp van heimelijke beeldopnamen behandelen), gegevensverstoring (paragraaf 2.5), computerverstoring (paragraaf 2.6) en misbruik van hulpmiddelen (paragraaf 2.7). Vervolgens komen de computergerelateerde delicten aan bod, bestaande uit de klassieke vermogensdelicten (paragraaf 2.8, waaronder ook modernere delicten als witwassen vallen), valsheidsdelicten (paragraaf 2.9) en oplichting (paragraaf 2.10). Tot slot komen de inhoud-gerelateerde delicten aan de orde, eerst diverse computergerelateerde zedendelicten (paragraaf 2.11) en vervolgens de klassieke uitingsdelicten als belediging en discriminatie (paragraaf 2.12). We sluiten af met de auteursrechtelijke strafbepalingen (paragraaf 2.13) en een korte blik op de toekomst (paragraaf 2.14).

2.2 Definities

Gegevens
Het begrip 'gegevens' is in artikel 80quinquies Sr gedefinieerd als "iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken". Ook

6 Geldende boetes per 1 januari 2018. (Merk op dat de boetemaxima periodiek worden herijkt; toekomstige lezers wordt aangeraden de alsdan geldende boetes te raadplegen op www.wetten.nl.) Zie ook de Richtlijn voor strafvordering cybercrime, Stcrt. 2018, 3271 voor computerdelicten die vallen onder computercriminaliteit in enge zin.

7 We volgen hier het Cybercrimeverdrag als handzaam structurerend principe, niet als leidend normatief raamwerk. De meeste Nederlandse strafbepalingen waren bij de totstandkoming van het verdrag al geregeld in het Wetboek van Strafrecht; naar aanleiding van het verdrag zijn slechts op onderdelen nieuwe bepalingen ingevoerd (zoals misbruik van hulpmiddelen) of aangepast (zoals computervredebreuk).

programmatuur valt hieronder. Deze definitie is (op een theoretisch detail na[8]) onomstreden en lijkt goed te functioneren.[9]

Geautomatiseerd werk
Computers, in de terminologie van de wet aangeduid als 'geautomatiseerd werk', worden sinds de Wet computercriminaliteit III gedefinieerd in artikel 80sexies Sr: "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".[10] Deze definitie sluit aan bij de begripsomschrijving uit het Cybercrimeverdrag.[11]

GESCHIEDENIS

Voorheen luidde de definitie "een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken" respectievelijk "op te slaan, te verwerken en over te dragen".[12] Dit omvat niet "werken die uitsluitend bestemd zijn voor de opslag van gegevens of eenvoudige werken die in beginsel slechts bestemd zijn om te functioneren zonder interactie met hun omgeving, zoals een elektronisch klokje".[13] De definitie leidde vanwege de cumulatie van functies (opslaan, verwerken én overdragen) tot discussie of ook apparaten die niet alle drie functies tegelijk vervullen, zoals routers, hieronder vielen. De Hoge Raad oordeelde in 2013 dat een router als een deel van een geautomatiseerd werk moet worden beschouwd, omdat "het begrip geautomatiseerd werk niet beperkt is tot apparaten die zelfstandig aan deze drievoudige eis voldoen. Ook netwerken bestaande uit computers en/of telecommunicatievoorzieningen heeft de wetgever onder het begrip 'geautomatiseerd werk' willen brengen".[14] De uitspraak zegt daarmee niet dat een router zelf een geautomatiseerd werk is, maar wel dat deze onderdeel uitmaakt van een geautomatiseerd werk, zodat ook het hacken van een router (als binnendringen in *een deel van* een geautomatiseerd werk) strafbaar is.

De nieuwe definitie van geautomatiseerd werk is ruim en omvat in ieder geval computers, servers, modems, routers, smartphones en tablets.[15] Door de brede formulering is

8 De in de literatuur (Kaspersen 1993, p. 135) bediscussieerde cryptische clausule uit de Wet computercriminaliteit "al dan niet op overeengekomen wijze" is bij de Wet computercriminaliteit II in 2006 veranderd in (het onzes inziens nog steeds wat cryptische) "op overeengekomen wijze".
9 Zie ook Commissie-Koops 2018, p. 66-67.
10 Het begrip is gewijzigd in de Wet computercriminaliteit III, *Stb.* 2018, 322.
11 *Kamerstukken II* 2015/16, 34372, 3, p. 85.
12 *Stb*. 1993, 33. Vgl. Kaspersen 1993, p. 135 en Van Dijk & Keltjens 1995, p. 84-87. In 2006 kwam de Wet computercriminaliteit II tegemoet aan de kritiek dat de overdrachtsfunctie van computers ontbrak door opname van "en over te dragen". Het onderdeel 'elektronisch' is bekritiseerd (Koops & De Roos 2007, p. 24) omdat het toekomstige quantumcomputers en biologische computers zou uitsluiten.
13 *Kamerstukken II* 1989/90, 21551, 3, p. 6.
14 HR 26 maart 2013, ECLI:NL:HR:2013:BY9718.
15 *Kamerstukken II* 2015/16, 34372, 3, p. 86.

duidelijk dat alle apparaten die met internet en andere netwerken verbonden zijn als geautomatiseerd werk moeten worden beschouwd. Ook 'slimme' apparaten die vallen onder het Internet of Things, zoals slimme lampen, energiemeters, koelkasten en auto's, zijn dus geautomatiseerde werken.[16] Als deze apparaten door personen worden gehackt, kan sprake zijn van computervredebreuk.
Een ongelukkig element in de definitie is het begrip 'computergegevens', dat verwarring kan scheppen omdat niet gedefinieerd is wat een 'computer' of 'computergegevens' zijn. Hiermee ontstaat een zekere circulariteit: het begrip 'geautomatiseerd werk' is immers, ook door de wetgever, van oudsher bedoeld als synoniem voor 'computer', zodat het begrip niet zou moeten terugkeren in de definitie. Het zou beter zijn in de definitie te spreken van (digitale) gegevens.[17]

Criminele organisatie
Uit onderzoek blijkt dat cybercrime en gedigitaliseerde criminaliteit vaak in crimineel verband wordt gepleegd.[18] Kennis over de gebezigde definitie van een criminele organisatie en de toepasbaarheid daarvan op georganiseerde cybercriminaliteit is daarom van belang. De deelneming aan een organisatie die tot oogmerk heeft het plegen van misdrijven is strafbaar met een gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie (artikel 140 lid 1 Sr). Onder 'deelneming' wordt mede begrepen het verlenen van geldelijke of andere stoffelijke steun aan alsmede het werven van gelden of personen voor een criminele organisatie (artikel 140 lid 4 Sr). Het gaat bij 'oogmerk' om het doel van de organisatie om misdrijven te plegen. Voor het bewijs van oogmerk in dit verband heeft de Hoge Raad opgemerkt dat "onder meer betekenis [zal] kunnen toekomen aan misdrijven die in het kader van de organisatie reeds zijn gepleegd, aan het meer duurzame of gestructureerde karakter van de samenwerking". Dat kan blijken uit de onderlinge verdeling van werkzaamheden of onderlinge afstemming van activiteiten van deelnemers binnen de organisatie ter verwezenlijking van het gemeenschappelijke doel.[19] Aanwijzingen voor het bestaan van een dergelijk samenwerkingsverband kunnen zijn: gemeenschappelijke regels, het voeren van overleg, gezamenlijke besluitvorming, een bepaalde hiërarchie of een bepaalde taakverdeling.[20]
Voor de bewijsverklaring voor deelname aan een criminele organisatie is niet vereist dat een verdachte aan enig concreet misdrijf heeft deelgenomen. Ook is niet nodig dat verdachte heeft samengewerkt met alle personen die deel uitmaken van de organisatie. Elke bijdrage aan een organisatie kan strafbaar zijn, waaronder handelingen die op zichzelf niet strafbaar zijn, zolang van bovenbedoeld aandeel of ondersteuning kan

16 *Kamerstukken II* 2015/16, 34372, 3, p. 86.
17 Zie Koops, Conings & Verbruggen 2016, p. 11 (voorkeur voor 'gegevens') en Commissie-Koops 2018, p. 74-75 (voorkeur voor 'digitale gegevens').
18 Zie onder andere Kruisbergen e.a. 2018 en Leukfeldt 2016.
19 HR 15 mei 2007, ECLI:NL:HR:2007:BA0502, *NJ* 2008/559, m.nt. P.A.M. Mevis. Zie ook Aanwijzing opsporingsbevoegdheden, *Stcrt.* 2014, 24442.
20 Zie Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5610. Zie ook J.J. Oerlemans, 'Veroordeling voor deelname aan een criminele organisatie bij piratenforum', *Computerrecht* 2013/107.

worden gesproken.[21] Zo heeft de Rechtbank Den Haag in 2018 bijvoorbeeld een verdachte veroordeeld die deelnam aan de criminele organisatie 'Lizard Squad', die bekend is vanwege het platleggen van de populaire gaming-platforms PlayStation Network en Xbox Live in 2014. De bijdrage van de verdachte bestond, kort gezegd, in de dienstverlening van het bijhouden en onderhouden van de server voor een website via welke verstikkingsaanvallen (zie paragraaf 2.6) werden gepleegd door de organisatie. Daarmee heeft de verdachte volgens de rechtbank deelgenomen aan de criminele organisatie.[22]

2.3 Computervredebreuk en wederrechtelijk overnemen van gegevens

2.3.1 *Computervredebreuk algemeen (artikel 138ab Sr)*

Artikel 138ab Sr stelt computervredebreuk (hacking) strafbaar. In de kern wordt het opzettelijk en wederrechtelijk[23] binnendringen in een geautomatiseerd werk strafbaar gesteld. De bepaling werd geredigeerd naar analogie van de huisvredebreukbepaling van artikel 138 Sr. De wetgever heeft daaraan toegevoegd dat van binnendringen in elk geval sprake is de toegang tot het werk wordt verworven door enige beveiliging te doorbreken of door een technische ingreep,[24] met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid. De oude beveiligingseis (zie onder) is dus vervallen. De maximale strafbedreiging is door de implementatie van de richtlijn Aanvallen op informatiesystemen in 2015 verhoogd tot twee jaar gevangenisstraf of een geldboete van de vierde categorie.[25]

De wetgever is er bij het redigeren van de bepaling van uitgegaan dat een wachtwoord een sleutel is die de gebruiker toegang geeft tot het computersysteem of een deel daarvan. Wat betreft huissleutels is door de Hoge Raad uitgemaakt dat een sleutel ook vals is als een echte sleutel wordt gebruikt door iemand die daartoe niet gerechtigd is.[26] Er hoeven geen beveiligingsmaatregelen voor de sleutel genomen te zijn; het is voldoende dat de sleutel tegen de wil van de rechthebbende uit diens macht is geraakt. Indien deze jurisprudentie wordt getransponeerd naar de wereld van computers en wachtwoorden,

21 HR 3 juli 2012, ECLI:NL:HR:2012:BW5132.
22 Rb. Den Haag 17 mei 2018, ECLI:NL:RBDHA:2018:5775, paragraaf 4.4.5.
23 Voorheen was de formulering: "opzettelijk wederrechtelijk", zodat het opzet zich ook moest richten op de wederrechtelijkheid: de hacker moest weten dat zijn handelen wederrechtelijk is. Dit is in de Wet computercriminaliteit II aangepast: het opzet is nu alleen gericht op het binnendringen.
24 "[E]en technische ingreep veronderstelt een ingreep in c.q. het manipuleren van het technisch functioneren van het geautomatiseerde werk. Het louter intoetsen van een (al of niet vals) wachtwoord zal aldus niet als een technische ingreep kunnen worden beschouwd, omdat de afhandeling daarvan de functionaliteit van het systeem intact laat." *Kamerstukken II* 2004/05, 26671, 7, p. 33.
25 Wet van 22 april 2015, *Stb.* 2015, 165. Tijdens de behandeling van het wetsvoorstel Computercriminaliteit (bij nota van wijziging, nr. 8) werd het oorspronkelijk voorgestelde strafmaximum van drie maanden verhoogd naar zes maanden, wat in de Wet computercriminaliteit II vervolgens werd verhoogd naar één jaar gevangenisstraf. De strafverhogingen illustreren wellicht hoe de maatschappij computervredebreuk als een steeds ernstiger delict beschouwt.
26 HR 20 mei 1986, *NJ* 1987/130.

zal de hacker ook strafbaar zijn als hij een wachtwoord van een website afhaalt zonder daartoe bevoegd te zijn en daarmee een computer kraakt.[27]
Hieraan gerelateerd is de vraag of het manipuleren van URL's (adressen van webpagina's) tot computervredebreuk kan leiden. Het Hof Den Haag beantwoordde de vraag bevestigend.[28] Het (opzettelijk) manipuleren van URL's om toegang te krijgen tot niet-toegankelijk bedoelde delen van een website kan dus tot computervredebreuk leiden. Dit kan betekenen dat ook het zich met een simpele truc (zoals een jaartal veranderen in een URL) toegang verschaffen tot een nog niet bekend gemaakt document – vergelijkbaar met de manier waarop de kersttoespraak van toenmalig Koningin Beatrix in 2012 uitlekte[29] – onder computervredebreuk valt; dit is geen technische ingreep, maar zou wel kunnen worden gezien als gebruik van een valse sleutel.
Regelmatig komt het voor dat werknemers weliswaar zijn geautoriseerd tot toegang tot bepaalde delen van een computersysteem maar niet tot gebruik van het gehele systeem. Om ervoor te zorgen dat ook diegenen strafbaar zijn die doordringen in beveiligde delen van een systeem waartoe zij niet geautoriseerd zijn, is expliciet in de wettekst opgenomen dat ook het wederrechtelijk binnendringen in een deel van een geautomatiseerd werk strafbaar is. Dit heeft betrekking op het wederrechtelijk binnendringen van delen van de computer zowel met voor de mens leesbare gegevens, als met programmatuur.
Nederland heeft niet het onrechtmatig *aanwezig blijven* in een computer strafbaar gesteld. Diverse andere landen stellen niet alleen het binnendringen strafbaar, maar ook het, na rechtmatig te zijn binnengekomen, langer verblijven in het computersysteem dan de autorisatieperiode toestaat.[30] Met een creatieve interpretatie zou men kunnen betogen dat indien iemand die rechtmatig toegang had tot een computer, maar langer verblijft dan toegestaan was, vanaf het moment dat de autorisatie is afgelopen toegang heeft tot de computer met behulp van een valse sleutel of valse hoedanigheid, zodat deze vorm van onrechtmatig verblijf in een computer ook onder 'binnendringen' wordt verstaan. Zo'n interpretatie is teleologisch verdedigbaar, maar vindt geen aanknopingspunt in de wetsgeschiedenis.
Een andere vraag die zich in de praktijk voordoet, is of een poortscan opgevat zou kunnen worden als een poging tot hacken. Tijdens een poortscan worden de poorten van een computer gecontroleerd waarmee de computer met andere computers communiceert. Daarmee kunnen kwetsbaarheden via bepaalde ingangen worden geconstateerd, waarna een hacker de computer kan binnendringen. In 2014 heeft de Recht-

27 Vgl. Hof Den Haag 8 juni 2004, ECLI:NL:GHSGR:2004:AP7974: het onbevoegd gebruik van een wachtwoord vormt computervredebreuk met behulp van een valse sleutel. Zie ook Rb. Oost-Brabant 13 juli 2015, ECLI:NL:RBOBR:2015:3980.

28 Zie Hof Den Haag 3 februari 2012, ECLI:NL:GHSGR:2012:BV3397: "De omstandigheid dat een server niet dermate is beveiligd dat dergelijk binnendringen onmogelijk wordt gemaakt, doet aan dit oordeel niet af".

29 Zie Elsevier, 'RVD onderzoekt uitlekken kersttoespraak Beatrix', 25 december 2012. Zie ook de tweet van de 'hacker': *"@annejan88: BREAKING: Zojuist kersttoespraak van morgen gevonden met beetje datum ophogen in url. Echt bizar. http://vruc.ht/kersttoespraak-2012…"*.

30 Zie bijvoorbeeld in de respectievelijke wetboeken van strafrecht artikel 615-ter (Italië), artikel 197bis lid 1 (Spanje), artikel 243 lid 1 (Turkije), artikel 153bis (Argentinië) en artikel 5 Cybercrimes Act (Tanzania).

bank Rotterdam geoordeeld dat het enkel scannen van een website op kwetsbaarheden niet zonder meer binnendringen in de zin van computervredebreuk oplevert.[31] Wel werd 'poging tot computervredebreuk' bewezen. De reden was dat door 'de uiterlijke verschijningsvormen' van het gebruik van de software en het 'scannen op zwakheden', de gedraging niet anders kan worden gezien dan het proberen binnen te dringen in computersystemen. Indien het scannen naar kwetsbaarheden plaatsvindt met toestemming van de rechthebbende, bijvoorbeeld om de beveiliging van computers en netwerken te testen tijdens een penetratietest door een IT-beveiligingsbedrijf, is er echter geen sprake van wederrechtelijkheid en is de poortscan eveneens niet strafbaar.[32]

2.3.2 *Beveiligingseis*

Bij de invoering van artikel 138a Sr (oud) in 1993 werd als eis gesteld dat een beveiliging moest worden doorbroken. Hoewel de eis in 2006 is vervallen, is de discussie daarover nog steeds relevant om de achtergrond van de strafbaarstelling van hacken te begrijpen.

De beveiligingseis is destijds onderwerp geweest van veel discussie. Wat moest worden verstaan onder het doorbreken van enige beveiliging? Aanvankelijk had de wetgever, in navolging van de Commissie computercriminaliteit,[33] voorgesteld dat het inbreken in een "daartegen beveiligd" werk strafbaar was,[34] wat vervolgens is gewijzigd in de uiteindelijke formulering "indien hij a) daarbij enige beveiliging doorbreekt of b) de toegang verwerft door een technische ingreep" enzovoort.[35] De wetgever maakte daarbij in de memorie van toelichting[36] een onderscheid tussen absolute, maximale, adequate, minimale en pro-formabeveiliging. De wetgever constateerde vervolgens dat absolute beveiliging een utopie is en dat maximale beveiliging niet verlangd kan worden, omdat "het onzinnig is een gulden te beveiligen met een rijksdaalder". Ook adequate beveiliging, die de wetgever omschrijft als "een evenwicht tussen het te beveiligen belang en de mate waarop beveiligingsmaatregelen zijn aangebracht", zou voor strafbaarheid niet nodig zijn. Strafbaarheid zou al aan de orde zijn als werd binnengedrongen in een systeem dat minimaal, maar wel daadwerkelijk, beveiligd is. Enkel een pro-formabeveiliging (zoals een mededeling 'verboden toegang') was dus onvoldoende. Het grote voordeel van een beveiligingseis is dat deze mogelijk als stimulans werkt om computers en netwerken daadwerkelijk te beveiligen.[37]

De wetgever heeft besloten de beveiligingseis in artikel 138a Sr (oud) te laten vervallen, als uitvloeisel van het Cybercrimeverdrag en het EU-Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen. Het doorbreken van een beveiliging en de varianten

31 Rb. Rotterdam 11 december 2014, ECLI:NL:RBROT:2014:10047.
32 Zie ook *Kamerstukken II* 2005/06, 26671, 7, p. 36.
33 *Informatietechniek & Strafrecht* 1987, voorstel nr. 15, p. 118.
34 *Kamerstukken II* 1989/90, 21551, 1-2, p. 2.
35 *Kamerstukken II* 1990/91, 21551, 8.
36 *Kamerstukken II* 1989/90, 21551, 3, p. 16.
37 Zo ook senator Franken, *Handelingen I* 30 mei 2006, 30-1352. Zie ook het betoog van Wiemans 2004b.

daarvan worden nu als voorbeelden genoemd van binnendringen. Hoewel het Cybercrimeverdrag een beveiligingseis toelaat en ook het Kaderbesluit een beperking tot "doorbreken van een beveiliging" toestaat, achtte de minister dit laatste te beperkt, aangezien dan de varianten van technische ingreep, valse sleutel en valse hoedanigheid zouden vervallen en daardoor de reikwijdte te beperkt zou worden. De nadere invulling van het begrip 'binnendringen' moet door de rechter gebeuren.[38] Volgens ons heeft de minister hiermee miskend dat in de wetsgeschiedenis deze varianten zijn opgenomen als varianten op het doorbreken van een beveiliging.[39] Het was volgens ons dus wel mogelijk om de beveiligingseis te handhaven, en daarmee een signaal aan computergebruikers te behouden dat het wenselijk is dat zij enige vorm van beveiliging hanteren.

2.3.3 *Gekwalificeerde vormen*

Het tweede en derde lid van artikel 138ab bevatten gekwalificeerde vormen van computervredebreuk.[40] De hacker die na wederrechtelijk binnengedrongen te zijn in een computersysteem en vervolgens opgeslagen gegevens overneemt en voor zichzelf of een ander vastlegt, wordt volgens het tweede lid met een maximumstraf van vier jaren of een geldboete van de vierde categorie bedreigd. Met de Wet computercriminaliteit II valt ook het overnemen van 'stromende' gegevens (zoals een e-mail die binnenkomt in de computer waar de hacker verblijft) onder deze gekwalificeerde vorm.
Ingevolge het derde lid wordt met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie gestraft, computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk indien de dader vervolgens (a) met het oogmerk zichzelf of een ander wederrechtelijk te bevoordelen gebruikmaakt van verwerkingscapaciteit van een geautomatiseerd werk of (b) door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde. Het derde lid onder a doelt op een situatie dat iemand in een computer die niet gratis ter beschikking staat van het publiek, na het hacken gebruikmaakt van diensten (systeemfuncties of aanwezige applicatieprogrammatuur)

38 *Kamerstukken II* 2004/05, 26671, 7, p. 31-32. Enigszins bevreemdend is de redactie: "Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven a. door het doorbreken van een beveiliging (...)". Het al dan niet doorbreken van een beveiliging enzovoort maakt niet uit voor de vraag of wordt binnengedrongen – het is het verwerven van de toegang zelf dat binnendringen oplevert. Grammaticaal is de bepaling dus een zinloze toevoeging. Het doorbreken van een beveiliging zal eerder moeten worden gezien als een indicatie van wederrechtelijkheid.

39 Zie *Kamerstukken II* 1990/91, 21551, 6, p. 9-10, waarin de minister aangeeft de formulering in het gewijzigd voorstel van wet (zie noot 35) te wijzigen, waarbij hij blijft benadrukken dat er een beveiligingseis geldt. Hieruit volgt dat de toevoeging van de technische ingreep, valse signalen, valse sleutel en valse hoedanigheid alleen ziet op situaties waarin via deze trucs een beveiliging wordt omzeild in plaats van (min of meer letterlijk) doorbroken. Vgl. p. 11: "Indien dus een beheerder van een persoonsregistratie *in het geheel geen beveiligingsmaatregelen heeft getroffen, kan de hacker niet worden vervolgd*, omdat hij niets heeft doorbroken" (cursivering toegevoegd). In de wetsgeschiedenis wordt het omzeilen van een beveiliging via technische ingrepen enzovoort aldus (impliciet) behandeld onder de algemene noemer van het doorbreken van een beveiliging.

40 Tijdens de behandeling van het wetsvoorstel computercriminaliteit zijn de gekwalificeerde vormen toegevoegd, zie *Kamerstukken II* 1991/92, 21551, 12 en 15.

waarvoor elders normaliter zou moeten worden betaald. Het is een vorm van 'diefstal van gebruik'. Dit onderdeel kan mede worden verklaard door de totstandkomingsgeschiedenis. Begin jaren negentig van de vorige eeuw waren verwerkingen door computers relatief kostbaar vergeleken met het heden. Met betrekking tot deze strafbare gedraging is dan ook weinig jurisprudentie beschikbaar. Wel is er één uitspraak waarbij een hacker gebruikmaakte van de hoge uploadsnelheid van servers van een universiteit, om auteursrechtelijk beschermde werken op een forum beschikbaar te stellen.[41] In dat geval is sprake van de gekwalificeerde vorm van computervredebreuk in de zin van artikel 138ab lid 3 onder a Sr.
Volgens de toelichting op de Wet computercriminaliteit II[42] heeft het bepaalde in lid 3 onder b betrekking op de toegang tot de computer van een derde na een geslaagde hack. Computers die zijn aangesloten op een netwerk kunnen ook toegang geven tot netwerken van weer andere beheerders. Het binnendringen in een andere computer van dezelfde beheerder valt niet onder dit artikellid. In de rechtspraak is het derde lid toegepast op het opzetten van een botnet, waarbij malware ('Toxbot' genaamd) tienduizenden tot miljoenen computers had besmet.[43] Het was daarbij niet nodig om een specifieke computer aan te wijzen die als eerste was gehackt en vanwaar de malware was doorgesprongen naar andere computers; doordat de malware zich steeds verder verspreidde, was er feitelijk continu sprake van 'doorhacken'. De rechtbank oordeelde in eerste instantie dat de verspreider van de Toxbot-malware binnendringt in de (zombie)computers door het enkele besmetten van die computers. De Hoge Raad bevestigde deze interpretatie.[44] Het is wat ons betreft echter geen evidente interpretatie van het begrip 'binnendringen'.[45] Malware kan weliswaar gezien worden als een verlengstuk van de verspreider, maar door de ongerichte verspreidingsvorm kan volgens ons niet per se gezegd worden dat met het virus ook de verspreider in een computer binnendringt.[46] Om besmetting van computers als computervredebreuk te kwalificeren, moeten daarvoor volgens ons via het botnet commando's worden gegevens aan de zombiecomputers. De Hoge Raad heeft echter in zijn arrest aangegeven dat bij de installatie van malware en verbinding met een botnet ook sprake is van artikel 138ab lid 3 onder b Sr. Het verdient opmerking dat hierbij ook kan worden vervolgd op basis van artikel 350a lid 2 of lid 3 Sr jo. artikel 138b lid 2 Sr (zie paragraaf 2.5 en 2.6).

2.3.4 *'Ethisch hacken'*

Met 'ethisch hacken' (ook wel '*white hat hacking*' genoemd) wordt veelal het hacken met een 'nobel doel' aangeduid, te weten het vergroten van de veiligheid van informa-

41 Rb. Rotterdam 24 augustus 2011, ECLI:NL:RBROT:2011:BR5610.
42 MvA, *Kamerstukken II* 1990/91, 21551, 6, p. 32.
43 Rb. Breda 30 januari 2007, ECLI:NL:RBBRE:2007:AZ7266 en ECLI:NL:RBBRE:2007:AZ7281.
44 HR 22 februari 2011, ECLI:NL:HR:2011:BN9287.
45 Zie Oerlemans & Koops 2011.
46 Zie ook de Explanatory Memorandum bij het Cybercrimeverdrag, paragraaf 46: "'Access' (...) does not include the mere sending of an e-mail message or file to that system".

tiesystemen in den brede. Het onderliggende idee is dat door het in brede kring openbaar maken van kwetsbaarheden sneller oplossingen voor beveiligingsproblemen worden gevonden en dat dit de informatieveiligheid ten goede komt.[47] Een ethisch hacker maakt geen misbruik van de kwetsbaarheid die hij vindt in de beveiliging van een informatiesysteem, maar maakt deze openbaar op een manier dat de kwetsbaarheid kan worden opgelost voordat er misbruik van kan worden gemaakt.[48] Hoewel ethisch hacken in vrij brede kring wordt gezien als duidelijk onderscheiden van strafbaar hacken (waarmee men dan 'onethisch' hacken bedoelt), maakt ook de ethische hacker zich in principe schuldig aan computervredebreuk. De wetgever heeft in 1993 geen onderscheid willen maken tussen hackers die witte, grijze of zwarte hoeden dragen: er is geen uitzondering gemaakt voor hackers die de beheerder op de hoogte stellen van het feit dat ze zijn binnengedrongen, om hun aldus behulpzaam te zijn bij het ontdekken van mogelijke gebreken in de beveiliging. De reden daarvoor is dat de wetgever duidelijk wilde maken "dat het inbreken in een computer *onvoorwaardelijk niet is toegestaan*". Alleen het (ethisch) hacken om "*op uitdrukkelijk verzoek* van de leiding van een organisatie het gegevensverwerkend systeem [te] testen" is niet wederrechtelijk.[49]
Niettemin is er sinds 1993 wel het nodige veranderd en erkennen beleidsmakers inmiddels ook het belang van ethische hackers voor de samenleving. Voor het gecontroleerd en op verantwoorde wijze openbaren van kwetsbaarheden in de beveiliging in informatiesystemen stellen instellingen ook wel een *responsible disclosure*-beleid op. Het Nationaal Cyber Security Centrum heeft in 2012 een richtlijn voor *responsible disclosure* uitgebracht. In de richtlijn staat dat een organisatie het *responsible disclosure*-beleid publiekelijk moet uitdragen door bijvoorbeeld een formulier op een website te plaatsen. De organisatie en melder maken afspraken over de termijn waarop de kwetsbaarheid verholpen zal zijn en over de wijze waarop zij met elkaar zullen communiceren. In de leidraad wordt aangegeven dat een redelijke standaardtermijn voor kwetsbaarheden in software zestig dagen bedraagt. Bij kwetsbaarheden in hardware kan de termijn zes maanden bedragen. De organisatie en de melder maken afspraken over eventuele openbaarmaking en het verder inlichten van de 'ICT-security-community', zodat anderen lering kunnen trekken uit de kwetsbaarheid in kwestie. Eventueel kan worden afgesproken dat de hacker de eer of een beloning krijgt voor het ontdekken van de kwetsbaarheid. In het door de organisatie vastgestelde beleid van *responsible disclosure* dient de organisatie zich uit te spreken over het niet doen van aangifte indien conform de richtlijn wordt gehandeld. In principe mag de hacker dus verwachten dat de organisatie geen aangifte doet indien de hacker zich aan de regels houdt.[50]
Toch laat de leidraad de geldende strafrechtelijke kaders onverlet en beperkt deze *niet* de bevoegdheid van het Openbaar Ministerie om in bepaalde gevallen ambtshalve te

47 Zie Falot & Schermer 2016.
48 Falot & Schermer 2016, p. 94.
49 *Kamerstukken II* 1989/90, 21551, 3, p. 17 (cursivering toegevoegd).
50 Falot & Schermer 2016 wijzen erop dat er geen *internationaal responsible disclosure*-beleid bestaat. Hackers moeten er dus rekening mee houden dat indien een hack extraterritoriale effecten heeft, zij vervolgd kunnen worden voor computervredebreuk door buitenlandse opsporingsautoriteiten.

vervolgen. Het OM zal echter onderzoeken of er sprake is van omstandigheden bij het vinden en melden van het beveiligingslek die kunnen rechtvaardigen dat strafvervolging uitblijft.[51] In december 2014 schreef de toenmalige minister van Veiligheid en Justitie dat het OM geen vervolging heeft ingesteld van melders die conform het *responsible disclosure*-beleid van de desbetreffende organisaties handelden.[52]
In de jurisprudentie wordt tevens aangenomen dat het delict computervredebreuk onder omstandigheden gerechtvaardigd kan worden door het algemeen belang. Deze rechtvaardigingsgrond wordt binnen het strafrecht niet vaak aangenomen, maar de Rechtbanken Oost-Brabant en Den Haag hebben hem uitgebreid in hun beoordeling meegenomen in zaken waarin de verdachte het ethisch hacken in verband met een algemeen belang als verdediging aanvoerde.[53] De rechtbanken overwegen daarbij dat wederrechtelijkheid een bestanddeel is van de delictsomschrijving van computervredebreuk. Het handelen kan noodzakelijk zijn binnen een democratische samenleving vanwege een zwaarwegend belang en kan op die grond als niet-wederrechtelijk worden gezien. Daarbij wordt bekeken of het handelen van de verdachte proportioneel en subsidiair is, zoals de 'Henk Krol'-zaak illustreert. Politicus Henk Krol (50Plus) had gebruikgemaakt van verstrekte inloggegevens om aan te tonen dat een databank met gevoelige medische gegevens niet voldoende werd beveiligd. De Rechtbank Den Haag overwoog dat "het aantonen van gebreken bij de bescherming van vertrouwelijke, medische gegevens een wezenlijk maatschappelijk belang kan dienen" en het inloggen op de website en het vervolgens raadplegen van enkele dossiers dan ook niet wederrechtelijk is. Echter, omdat de verdachte meer dan eenmaal heeft ingelogd op het systeem en de gegevens heeft uitgeprint en direct naar de media is gestapt, acht de rechtbank het handelen niet proportioneel en subsidiair. De verdachte kreeg een geldboete opgelegd van € 750.[54]

2.3.5 *Wederrechtelijk overnemen van niet-openbare gegevens (artikel 138c Sr)*

De wetgever heeft het nodig geacht de bescherming die artikel 138ab Sr biedt tegen wederrechtelijke kennisneming en gebruik van gegevens, uit te breiden met een nieuwe strafbepaling die als vangnet dient voor situaties waarin geen sprake is van (of onvoldoende bewijs is voor) computervredebreuk.
Met de Wet computercriminaliteit III is in artikel 138c strafbaar gesteld het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk, voor zichzelf of voor een ander. De maximumstraf is een jaar gevangenisstraf of een geldboete van de vierde categorie. Met niet-openbare gegevens bedoelt de wetgever gegevens die niet voor het publiek beschikbaar zijn.

51 Brief van het College van procureur-generaals betreffende 'Responsible Disclosure (hoe te handelen bij "ethische hackers?")', 18 maart 2013.
52 *Kamerstukken II* 2014/15, 26643, 342, p. 2.
53 Zie Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1157 en Rb. Den Haag 17 december 2014, ECLI:NL:RBDHA:2014:15611.
54 Rb. Oost-Brabant 15 februari 2013, ECLI:NL:RBOBR:2013:BZ1157.

Gegevens die op internet zijn geplaatst, zijn openbaar, mits het publiek toegang heeft tot de internetpagina waar de teksten zijn weergegeven.[55] Van wederrechtelijkheid is geen sprake als (mag worden aangenomen dat) de rechthebbende toestemming heeft gegeven of als het overnemen geschiedt ter uitvoering van een wettelijke bevoegdheid. De wetgever verwijst verder naar de *Henk Krol*-zaak (zie paragraaf 2.3.4) om duidelijk te maken dat het overnemen van niet-openbare gegevens niet wederrechtelijk is, indien hogere belangen een dergelijke inbreuk kunnen rechtvaardigen en het handelen proportioneel en subsidiair is.[56]

Met de strafbaarstelling beoogt de wetgever de strafrechtelijke bescherming van gegevens die door middel van een geautomatiseerd werk zijn opgeslagen verder te verbeteren.[57] Het artikel is vergelijkbaar met computervredebreuk, zij het dat het bestanddeel van 'binnendringen' is weggevallen.[58] In sommige gevallen kan computervredebreuk niet worden bewezen, omdat niet kan worden aangetoond dat de verdachte opzettelijk en wederrechtelijk een computersysteem is binnengedrongen. Indien wel helder is dat zonder toestemming gegevens uit een geautomatiseerd werk zijn overgenomen die niet openbaar mogen worden gemaakt, dan kan artikel 138c Sr ten laste worden gelegd.
De strafbaarstelling is kennelijk geïnspireerd door de *Manon Thomas*-zaak uit 2007.[59] In deze zaak werden naaktfoto's van de voormalig presentatrice overgenomen en via internet openbaar gemaakt. Vermoedelijk zijn deze foto's van een gedeelde map uit het lokale wifi-netwerk bij haar thuis gekopieerd en verder verspreid, waarbij het lastig was de dader te vervolgen voor computervredebreuk.[60] Deze zaak staat natuurlijk niet op zichzelf. In de loop der jaren zijn meer mensen het slachtoffer geworden van het verspreiden van vertrouwelijke gegevens op internet waardoor hun persoonlijke levenssfeer werd geschaad.[61]
Ook is het met de strafbaarstelling mogelijk personen te vervolgen die "gegevens van een computer waartoe zij rechtmatige toegang hebben, bijvoorbeeld vanwege hun functie bij een overheidsinstelling, zonder daartoe gerechtigd te zijn voor zichzelf of voor een ander overnemen".[62] De wetgever geeft aan dat hier "als het ware sprake is van 'verduistering' van gegevens, met dien verstande dat de rechthebbende de beschikkingsmacht over de gegevens behoudt, in welk geval strafvervolging op grond van artikel 321 Sr niet mogelijk is omdat in dergelijk geval van een goed geen sprake is".[63]

55 *Kamerstukken II* 2015/16, 34372, 3, p. 61 met verwijzing naar Hof Amsterdam 23 november 2009, ECLI:NL:GHAMS:2009:BK4139.
56 *Kamerstukken II* 2015/16, 34372, 3, p. 66.
57 *Kamerstukken II* 2015/16, 34372, 3, p. 61.
58 *Kamerstukken II* 2015/16, 34372, 3, p. 64.
59 *Handelingen I* 19 juni 2018, 34-5-10, juncto *Aanhangsel Handelingen II* 2007/08, 888 (Kamervragen van Gerkens over heling van een door computervredebreuk verkregen goed, waarin de minister aankondigt de wet te willen aanpassen).
60 Zie Oerlemans 2010. Zie ook Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 62 voor een meer impliciete verwijzing naar deze zaak.
61 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 62.
62 *Kamerstukken II* 2015/16, 34372, 3, p. 64.
63 *Kamerstukken II* 2015/16, 34372, 3, p. 64.

Hoewel de achtergrond van deze strafbaarstelling begrijpelijk is, gaat de strafrechtelijke aansprakelijkheid wel erg ver. Elk wederrechtelijk overnemen van gegevens waar iemand rechtmatig toegang toe heeft, is in beginsel strafbaar. De werknemer die in het kader van het thuiswerken gegevens uit een computer van het werk mee naar huis neemt op een usb-stick is niet strafbaar als "dit gebeurt met toestemming van de werkgever en/of voldoet aan door de werkgever gestelde regels",[64] maar dus wel strafbaar als dit gebeurt zonder toestemming. Dat roept vragen op hoe expliciet de toestemming van de werkgever moet zijn – is de werknemer nu wel of niet strafbaar als de werkgever niets over het meenemen van stukken in het kader van thuiswerken heeft bepaald? Het betekent ook dat elke werknemer die in strijd met de interne regels een keer digitale documenten meeneemt (iets wat naar wij vermoeden dagelijks veelvuldig gebeurt door Nederlandse werknemers, ambtenaren van politie en justitie niet uitgezonderd), strafbaar is. Onzes inziens zijn we hier ver verwijderd van het strafrecht als ultimum remedium; dit soort situaties zouden alleen in de privaat- of arbeidsrechtelijke sfeer moeten worden aangepakt. Voor strafwaardige gevallen van het overnemen van bedrijfsgegevens is de strafbaarstelling betreffende beroeps- en bedrijfsgeheimen (artikelen 272 en 273 Sr) aangewezen; mocht deze ontoereikend worden geacht, dan ligt het eerder voor de hand deze bepaling aan te passen dan een generieke en vérgaande strafbaarstelling in te voeren.

Soortgelijke bedenkingen kunnen immers ook worden gegeven voor andere contexten die nu onder artikel 138c Sr vallen. Zijn echtgenoten die rechtmatig toegang hebben tot elkaars (of één en dezelfde) computer, strafbaar als ze (bijvoorbeeld bij huwelijksproblemen) gegevens van de ander overnemen zonder diens toestemming? Is degene die de telefoon van een vriend leent om het nummer van een gezamenlijke kennis te noteren, en daarbij (zonder toestemming te vragen) ook het nummer van de in stilte aanbeden zus van de vriend noteert, strafrechtelijk aansprakelijk onder artikel 138c Sr? We mogen hopen dat het OM niet voor dit soort triviale gevallen zal vervolgen, zoals dat ook niet voor triviale gevallen van hacken gebeurt, maar in beginsel vallen dit soort voorvallen wel onder het bereik van de nieuwe strafbaarstelling.

Waar de strafbaarstelling volgens ons vooral is doorgeslagen, is de keuze voor het moment van *overnemen*. De belangrijkste reden voor strafbaarstelling – ook vanuit de *Manon Thomas*-zaak – is de ongewenste *verspreiding* en vooral de *openbaarmaking* van gegevens. Het oprekken van de strafrechtelijke aansprakelijkheid had voorkomen kunnen worden door artikel 138c Sr te beperken tot het opzettelijk en wederrechtelijk openbaar maken van gegevens overgenomen uit een geautomatiseerd werk. Een dergelijke beperktere strafbaarstelling zou meer recht hebben gedaan aan de ultimum remedium-gedachte, en ook de aanzienlijke rechtsonzekerheid hebben voorkomen die nu ontstaan is door het ruime en zeer contextafhankelijke begrip van 'wederrechtelijk overnemen'.

64 *Kamerstukken II* 2015/16, 34372, 3, p. 66.

2.4 Afluisteren, aftappen en opnemen van communicatie

Diverse strafbepalingen waarborgen de bescherming van (tele)communicatie, als onderdeel van de bescherming van de persoonlijke levenssfeer. In 1971 werden bepalingen ingevoerd die het afluisteren van gesprekken en van telecommunicatie, alsmede enkele voorbereidingshandelingen, strafbaar stelden.[65] De artikelen 139a tot en met 139e Sr zagen met name op het strafbaar stellen van diverse vormen van afluisteren van (telefoon)gesprekken. Ook de artikelen 374bis, 441 en 441a Sr waren daarop gericht. Bij de implementatie van de Wet computercriminaliteit is met het oog op de technische ontwikkelingen de strafbaarheid uitgebreid tot afluisteren en aftappen van alle soorten gegevens.[66] De kern van de afluister- en aftapbepalingen wordt gevormd door de artikelen 139a tot en met 139c.

2.4.1 *Direct afluisteren van gesprekken (artikel 139a-b Sr)*

Allereerst is strafbaar het 'direct afluisteren' of opnemen van gesprekken die in een besloten sfeer plaatsvinden: binnen een woning, besloten lokaal of erf, voor zover dit met een technisch hulpmiddel plaatsvindt. Artikel 139a lid 1 Sr stelt het afluisteren of opnemen strafbaar met hoogstens zes maanden gevangenisstraf of geldboete van de vierde categorie. Lid 2 geeft uitzonderingen aan, als het afluisteren of opnemen gebeurt door of in opdracht van een gespreksdeelnemer, door een technisch hulpmiddel dat de gebruiker – behoudens kennelijk misbruik – van de besloten plaats niet heimelijk aanwezig heeft (zoals camera's in een diefstalgevoelig bedrijf), of ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten 2017. Maar ook gesprekken buiten de besloten sfeer, dus die in het vrije veld, op straat of in publieke gebouwen plaatsvinden, zijn beschermd tegen afluisteren en opnemen, als dat tenminste gebeurt door iemand die heimelijk een technisch hulpmiddel gebruikt (zoals een richtmicrofoon) met het oogmerk om het gesprek af te luisteren of op te nemen (artikel 139b Sr, maximaal drie maanden gevangenisstraf of geldboete van de derde categorie). Ook hier gelden volgens lid 2 uitzonderingen voor gespreksdeelnemers en voor de AIVD en MIVD. Wat betreft het opnemen van gesprekken door een gespreksdeelnemer kan men de vraag stellen of de strafuitsluiting nog op zijn plaats is. Bij de Wet BOB heeft de wetgever bepaald dat ook het direct afluisteren door justitie met toestemming van een gespreksdeelnemer onder de wettelijke bevoegdheid valt (artikel 126l Sv) omdat het een inbreuk op de privacy is. Het gewijzigde privacy-inzicht zou kunnen leiden tot het schrappen van de uitsluiting voor gespreksdeelnemers in artikelen 139a-b Sr.

65 *Stb.* 1971, 180.
66 Mede in het licht van het Internationale Telecommunicatieverdrag, *Trb.* 1983, 164.

2.4.2 *Aftappen of opnemen van gegevens (artikel 139c Sr)*

Artikel 139c is de centrale bepaling voor het aftappen van gegevens. Tot 2006 was het aftappen van niet-telecommunicatieve gegevensoverdracht geregeld in de artikelen 139a-b Sr, maar bij de Wet computercriminaliteit II is dit overgeheveld naar artikel 139c, dat van oudsher het aftappen van openbare telecommunicatie strafbaar stelde. Nu stelt artikel 139c alle vormen van het aftappen of opnemen van gegevens die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk strafbaar, voor zover deze niet voor de aftapper bestemd zijn. Alle telecommunicatie, waaronder mobiele telefonie, internetverkeer en andere vormen van gegevensverkeer, valt onder dit artikel, evenals de overdracht van gegevens binnen en tussen computers, zoals de overdracht tussen toetsenbord, computer en beeldscherm, en ook de zogenoemde residustraling die beeldscherm en kabels uitzenden. De straf is ten hoogste twee jaar gevangenisstraf of geldboete van de vierde categorie.[67]
Artikel 139c Sr kan ook ten laste worden gelegd, indien gegevens worden vastgelegd met behulp van malware ten behoeve van het plegen van oplichting.[68] Voor oplichting moeten daders immers veelal inloggegevens of financiële gegevens van computergebruikers verkrijgen. De kwaadaardige software kan op een zodanige wijze worden geconfigureerd dat als de computergebruiker zich op websites bevindt waarbij in de URL woorden als 'bank', login', eBay' en 'PayPal' voorkomen, de malware in werking treedt en gegevens probeert vast te leggen.[69] Met behulp van de keylogfunctie in malware of de 'web inject'-techniek (waarbij een extra beeldscherm bij het tonen van een bepaalde website in een webbrowser wordt ingeschoten, zodat de gebruiker niet ziet dat hij gegevens in een verkeerd venster invoert) kunnen deze gegevens worden vastgelegd en doorgestuurd naar een derde. Ook is het aftappen van bankpasgegevens en pincodes met skimapparatuur strafbaar op grond van artikel 139c Sr.[70]

In artikel 139c lid 2 Sr zijn drie uitzonderingen geformuleerd.[71] De eerste is dat het tappen of opnemen van gegevens die met een radio-ontvangapparaat zijn ontvangen niet strafbaar is, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt. Signalen in de ether zijn in beginsel vrij. Men mag gegevens met een radioontvangapparaat echter alleen vrijelijk uit de ether plukken indien daarvoor geen bijzondere inspanning wordt geleverd. Zo is het afluisteren van draadloze telefonie niet strafbaar zolang dit plaatsvindt

67 Dit was één jaar gevangenisstraf, maar het maximum is verhoogd bij Wet van 22 april 2015, *Stb.* 2015, 165.
68 Zie bijvoorbeeld Rb. Rotterdam 20 juli 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016, nr. 5, p. 268-277, m.nt. J.J. Oerlemans (*TorRAT*-zaak). Zie ook Rb. Rotterdam 16 april 2014, ECLI:NL:RBROT:2014:7370.
69 Rb. Breda 30 januari 2007, ECLI:NL:RBBRE:2007:AZ7281.
70 Rb. Rotterdam 28 november 2011, ECLI:NL:RBROT:2011:BU6142.
71 Zie ook Richtlijn voor strafvordering telecommunicatiewet, *Stcrt.* 2018, nr. 18592.

met een normale ontvanginrichting.[72] Indien iemand door een heel stelsel van ontvanginrichtingen die op elkaar zijn afgestemd stelselmatig telefoongesprekken afluistert, is dit een bijzondere inspanning en dus niet toegestaan. Het aan elkaar koppelen van een drietal semafoonontvangers om het gehele Nederlandse verkeer te kunnen opvangen is een voorbeeld van zo'n bijzondere inspanning.[73] Actuelere voorbeelden zijn het uitlezen van onbeveiligde RFID-chips, wat geen bijzondere inspanning vergt en dus niet strafbaar is,[74] en het gebruik van een radardetector om politiesnelheidscontroles te signaleren. Dat laatste is weliswaar mogelijk op basis van artikel 139c Sr, maar, tot teleurstelling van snelheidsduivels, zelfstandig strafbaar gesteld in de verkeerswetgeving.[75]
Een tweede uitzondering geldt voor het aftappen door of in opdracht van de rechthebbende op een aansluiting voor telecommunicatie (zoals een telefoon of netwerkcomputer), behoudens in geval van kennelijk misbruik. Zo kan een abonnee de gesprekken opnemen die met zijn telefoons worden gevoerd, bijvoorbeeld om te kunnen nagaan wie er van zijn telefoon gebruikmaakt. Bij een bedrijf mag dus de bedrijfsleiding in beginsel de telecommunicatie van werknemers aftappen en opnemen, althans volgens artikel 139c Sr.[76] Een omissie in de wet lijkt te zijn dat er geen uitzondering bestaat voor rechthebbenden op een computer die de gegevensoverdracht in de computer aftappen; bij het overhevelen van computeraftappen van artikelen 139a-b naar 139c lid 1 heeft de wetgever artikel 139c lid 2 niet aangepast, zodat de uitzondering beperkt is tot 'telecommunicatie'.
Ten derde geldt een uitzondering voor telecomaanbieders die gegevens aftappen of opnemen voor "de goede werking van een openbaar telecommunicatienetwerk", bijvoorbeeld voor onderhoud of het oplossen van storingen.[77] En tot slot mogen ook justitie en de inlichtingen- en veiligheidsdiensten aftappen in verband met opsporing van misdrijven en nationale veiligheid. Tot de inwerkingtreding van de Wiv 2002[78] creëerde de strafuitsluitingsgrond van artikel 139c lid 2 voor de toenmalige BVD tegelijk de bevoegdheid tot aftappen (waarbij destijds machtiging nodig was van vier ministers);

72 Het gevolg van het principe van vrij ontvangbaar etherverkeer is dat aanbieders van (mobiele) telecommunicatie ervoor moeten zorgen dat ze hun dienst beveiligen, om te voorkomen dat derden zomaar kennis kunnen nemen van de gegevensoverdracht van hun abonnees door de ether; vgl. de beveiligingsverplichting vastgelegd in artikel 11.3 Telecommunicatiewet.
73 HR 12 januari 1999, *NJ* 1999/277; vgl. ook HR 19 december 1995, *Computerrecht* 1996, p. 235-241, m.nt. Chr.H. van Dijk.
74 Schermer 2005, p. 85 en 88. Hij beveelt gebruikers van RFID aan om de gegevensoverdracht bij RFID-systemen te versleutelen.
75 Artikel 3 Besluit voertuigen. Het verbod (destijds artikel 5.1.6 Voertuigreglement) is volgens HR 8 april 2008, ECLI:NL:HR:2008:BC4284, niet in strijd met het recht op vrije ontvangst in verband met vrijheid van meningsuiting, omdat de elektromagnetische golven van radardetectoren geen "inlichtingen of denkbeelden" bevatten.
76 Vgl. artikel 273d lid 2 Sr, zie paragraaf 2.4.4.
77 Zie ook artikel 11.2a Tw.
78 *Stb.* 2002, 148.

de bevoegdheid is vervolgens zelfstandig geregeld in artikel 25 Wiv 2002 en de artikelen 47-48 Wiv 2017.[79]

2.4.3 *Voor- en nabereidingshandelingen (artikel 139d, 139e, 441 en 441a Sr)*

Naast afluisteren en aftappen zelf, zijn ook diverse voor- en nabereidingshandelingen strafbaar gesteld.[80] Artikel 139d lid 1 Sr stelt het plaatsen ('aanwezig doen zijn') van een afluisterapparaat strafbaar. Voor strafbaarheid is het noodzakelijk dat de dader de bedoeling had dat met het afluisterapparaat wederrechtelijk gesprekken afgeluisterd zouden worden. Waar in de oude tekst werd gesproken van 'gesprek', is na de invoering van de Wet computercriminaliteit "telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk" toegevoegd, en bij de Wet computercriminaliteit II nog "of andere gegevensverwerking" door een computer. Voorts is naast afluisteren en opnemen het woord 'aftappen' in de wet opgenomen.
Een voorbeeld van toepassing van deze bepaling betreft een veroordeling van de Rechtbank Noord-Nederland in 2014 voor artikel 139d lid 1 Sr en artikel 139c Sr. In casu was er sprake van opzettelijk en wederrechtelijk aftappen, omdat een simkaart in een heimelijk geplaatst *track & trace*-systeem onder een auto werd bevestigd, waardoor het mogelijk was (via meegeleverde software) door middel van een geautomatiseerd werk oproepen van alle door dat systeem opgevangen signalen van GSM-masten te ontvangen.[81] In een *banking* malware-zaak (kwaadaardige software teneinde frauduleuze online betalingen te plegen, zie paragraaf 2.5.1) zijn verdachten veroordeeld voor het voorhanden hebben van software die specifiek ontworpen is met het oogmerk om deze te plaatsen in de computer van een ING-klant tot wiens computer zij zich reeds via derden wederrechtelijk toegang hadden verschaft. Met behulp van de software konden de verdachten frauduleuze betalingen doen. Het vereiste oogmerk werd bewezen geacht, omdat de software hoofdzakelijk geschikt is gemaakt om een gekwalificeerde vorm van computervredebreuk te plegen.[82]
Opmerkelijk aan artikel 139d lid 1 Sr is de strafmaat. Deze was, met een maximumstraf van één jaar of geldboete van de vierde categorie, al aan de hoge kant – even hoog als voor het aftappen van gegevens zelf, terwijl de straf op voorbereiding normaliter lager

79 Curieus is dat artikel 139c lid 2 een uitsluitingsgrond voor de strafvordering bevat (voor het justitieel aftappen), terwijl de vergelijkbare artikelen 139a-b geen uitzondering voor de strafvordering bevatten (voor justitieel direct afluisteren), terwijl beide uitzonderingen voor uitvoering van de Wiv bevatten. Het is sowieso ongebruikelijk om te expliciteren dat een (bevoegde) handeling in het kader van de strafvordering of nationale veiligheid niet strafbaar is; de wederrechtelijkheid ontbreekt dan immers. Nu kan verwarring ontstaan wanneer strafbepalingen de ene keer wel en de andere keer niet een uitzondering voor justitie of ivd's bevatten. Het zou systematischer zijn om de uitzonderingen voor strafvordering en voor uitvoering van de Wiv uit artikel 139a en 139c Sr te schrappen.

80 Zie ook paragraaf 2.2.6 over misbruik van hulpmiddelen.

81 Zie Rb. Noord-Nederland 18 april 2014, ECLI:NL:RBNNE:2014:2018.

82 Hof Den Haag 24 januari 2017, ECLI:NL:GHDHA:2017:81. Vergelijk bijvoorbeeld met Rb. Rotterdam 3 mei 2018, ECLI:NL:RBROT:2018:5141, waarbij de Rechtbank Rotterdam het oogmerk voor het bewijzen van het voorhanden hebben van software ('Metasploit' en 'Zenmap') voor het plegen van computerdelicten niet bewezen achtte. Deze software wordt vaak door ethische hackers gebruikt voor het uitvoeren van rechtmatige beveiligingstesten.

ligt dan bij het gronddelict (vgl. artikel 46 lid 2 Sr). Het maximum is met de implementatie van Richtlijn 2013/40/EU zelfs opgehoogd naar twee jaar.[83] De reden daarvan is ons niet duidelijk; de Richtlijn beperkt de strafbaarstelling tot het aftappen zelf (inclusief medeplichtigheid, uitlokking en poging) en tot bepaalde voorbereidingshandelingen (die onder andere in artikel 139d lid 2 en 3 Sr strafbaar zijn gesteld, zie paragraaf 2.7), maar zegt niets over het bestraffen van het doen plaatsen van aftapmiddelen. Wetstechnisch had de implementatie zich kunnen beperken tot het wel door de Richtlijn vereiste verhogen van de straf in artikel 139d lid 2 Sr.
De consequentie van de keuze het maximum in het eerste lid op te hogen, is niet alleen dat de straf op voorbereiding van aftappen van gegevens even hoog blijft als die op het gronddelict, maar ook dat deze veel hoger is dan die voor het gronddelict van wederrechtelijk afluisteren van gesprekken. Artikel 139d lid 1 Sr ziet immers niet alleen op de voorbereiding van 139c maar ook op de voorbereiding van 139a en 139b. De curieuze consequentie is dat het onrechtmatig afluisteren van gesprekken met hoogstens zes maanden gevangenisstraf wordt gesanctioneerd, terwijl het plaatsen van een microfoontje om gesprekken af te luisteren tot twee jaar gevangenisstraf kan leiden, ongeacht of er daadwerkelijk mee wordt afgeluisterd. De maximumstraf is zelfs acht keer hoger voor de voorbereiding van het afluisteren in de openbare ruimte dan de straf voor het uitvoeren daarvan (24 tegenover drie maanden). Hier klopt iets niet in de wetgevingssystematiek.

Artikel 139e Sr stelt onder 1° strafbaar degene die de beschikking heeft over een voorwerp waarvan hij weet of redelijkerwijze moet vermoeden dat daarop gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen (denk aan overtreding van de artikelen 139a tot en met 139c of 273d Sr) zijn verkregen.[84] Het is ook strafbaar om deze voorwerpen aan een ander ter beschikking te stellen (3°). De term 'voorwerp' is met opzet zeer ruim en omvat zowel analoge gegevensdragers (bandopnamen) als digitale gegevensdragers (zoals usb-sticks en cd-roms). Volgens 2° is tevens diegene strafbaar die gegevens die door wederrechtelijk afluisteren, aftappen of opnemen zijn verkregen, opzettelijk aan een ander bekendmaakt. Dit geldt niet alleen als hijzelf de gegevens door wederrechtelijk afluisteren heeft verkregen, maar eveneens als hij weet of redelijkerwijs had moeten vermoeden dat zij door zulk afluisteren, aftappen of opnemen te zijner kennis zijn gekomen. De maximumstraf voor al deze gedragingen is zes maanden gevangenisstraf of geldboete van de vierde categorie.
Volgens artikel 441 Sr mag iemand die niet voor hem bestemde gegevens heeft opgevangen met een radio-elektrische ontvanginrichting, zoals een scanner die portofoons opvangt, deze gegevens niet openlijk bekendmaken, en evenmin aan iemand doorvertellen als hij zou moeten vermoeden dat ze dan publiek bekend worden gemaakt en dat

83 *Stb*. 2015, 165.
84 Hoewel dit delict vooral de vertrouwelijkheid van communicatie en daarmee de communicatieve privacy beschermt, kan het ook worden ten laste gelegd om vermogensdelicten te bestrijden, bijvoorbeeld het voorhanden hebben van een lijst met duizend creditkaartgegevens. Zie Rb. Rotterdam 14 april 2010, ECLI:NL:RBROT:2010: BM1172 en Ten Voorde 2018, p. 639.

ook inderdaad gebeurt, op straffe van maximaal drie maanden gevangenisstraf of geldboete van de derde categorie.[85]
In artikel 441a Sr ten slotte is het reclame maken voor afluisterapparatuur strafbaar gesteld met een maximumstraf van twee maanden of geldboete van de derde categorie. We nemen aan dat "verspreiding van enig geschrift" in dit verband ook betekent het verzenden van e-mailberichten. Het tonen van (geautomatiseerd geselecteerde of gepersonaliseerde) advertenties op webpagina's lijkt niet direct een vorm van 'verspreiding', maar is wel een functioneel equivalent van het aloude rondbrengen van folders in brievenbussen, en zou in die zin wellicht ook onder de strafbaarstelling kunnen vallen.

2.4.4 *Schending van geheimen door communicatieaanbieders (artikel 273d Sr)*

Artikel 273d Sr (artikel 374bis-oud, bij de Wet computercriminaliteit II overgeheveld uit de titel 'Ambtsmisdrijven' naar de titel 'Schending van geheimen'),[86] ziet op het aftappen door werknemers van communicatieaanbieders.[87] Deze bepaling bedreigt de werknemer van een communicatieaanbieder met een gevangenisstraf van ten hoogste achttien maanden of geldboete van de vierde categorie, indien hij:

- opzettelijk en wederrechtelijk kennisneemt van door deze aanbieder verzorgde, niet (mede) voor hem bestemde gegevens, of zulke gegevens overneemt, aftapt of opneemt;
- de beschikking heeft over een voorwerp waaraan, naar hij weet of redelijkerwijs moet vermoeden, een gegeven kan worden ontleend, dat door wederrechtelijk overnemen, aftappen of opnemen van zodanige gegevens is verkregen;
- opzettelijk en wederrechtelijk de inhoud van zodanige gegevens aan een ander bekendmaakt; of
- opzettelijk en wederrechtelijk een voorwerp waaraan een gegeven omtrent de inhoud van zodanige gegevens kan worden ontleend, ter beschikking stelt van een ander.

Dezelfde strafbedreiging geldt voor een werknemer die opzettelijk toelaat dat een ander deze feiten pleegt (artikel 273e). Het gaat overigens wel steeds om wederrechtelijke

85 Vroeger was ook het aantekening houden of gebruiken van aldus opgevangen gegevens strafbaar onder artikel 441 Sr, maar dit is in 1995 (*Stb*. 1995, 227) vervallen. Van gebruik van de gegevens was bijvoorbeeld sprake als iemand op basis van het beluisteren van een politiemobilofoon naar een bepaalde plaats ging.

86 Daarbij is tegelijk een lacune in de wet opgevuld: voorheen kon een internetaanbieder zelf in principe ongestraft kennisnemen van ongeopende e-mailberichten die bij hem lagen opgeslagen; de strafbepaling van artikel 374bis-oud zag alleen op berichten in transport, waar e-mailberichten in afwachting van opening door de geadresseerde volgens de logica van de wetgever niet onder vallen. Deze lacune was onwenselijk, omdat – vooruitlopend op de mogelijke herziening van het post-, telefoon- en telegraafgeheim in artikel 13 Gw – e-mail dezelfde bescherming verdient als gewone post, waarvoor wel een strafbepaling (artikel 273a (372-oud)) bestaat die postbeambten verbiedt gesloten post die aan hen is toevertrouwd te openen en te lezen.

87 Bij de Wet computercriminaliteit III is de verouderde terminologie van 'telecommunicatienetwerk of -dienst' in lijn gebracht met de sinds de Wet computercriminaliteit II gebruikelijke terminologie van 'communicatienetwerk of -dienst'.

kennisname, dus een aanbieder mag bijvoorbeeld wel e-mailberichten openen als de autoriteiten dat vorderen of als de abonnee hem daartoe heeft gemachtigd.
Sinds 2007[88] is artikel 273d niet alleen van toepassing op werknemers bij aanbieders van *openbare* communicatie (lid 1), maar ook op werknemers bij aanbieders van *niet-openbare* communicatie (lid 2). Daaronder vallen bijvoorbeeld bedrijfsnetwerken. Dit is gebeurd op advies van het toenmalige College Bescherming Persoonsgegevens, "ter bescherming van het telecommunicatiegeheim van de gebruikers van [het interne] netwerk", mede gelet op de "omvangrijke private netwerken waarin vele duizenden personen plegen te communiceren in verschillende posities en onderlinge verhoudingen en met uiteenlopende redelijke verwachtingen ten aanzien van de bescherming van de vertrouwelijkheid van de communicatie".[89] Indien de werkgever communicatie van werknemers afluistert of aftapt in overeenstemming met het (aan de wettelijke regels voldoende) interne beleid ten aanzien van controle op e-mail en internetgebruik, zal dit echter in beginsel niet strafbaar zijn onder artikel 273d lid 2 Sr.[90] Bedrijven die werknemers monitoren kunnen in dit verband niet langer vertrouwen op de strafuitsluitingsgrond van artikel 139c lid 2 Sr. Zij dienen ten minste een beleid te hebben in de lijn van de richtlijnen van de Autoriteit Persoonsgegevens om rechtmatig te kunnen monitoren.

2.4.5 *Heimelijk maken van beeldopnamen (artikel 139f en 441b Sr)*

Waar het auditief monitoren (afluisteren en aftappen) traditioneel tot de computercriminaliteit wordt gerekend, wordt het wederrechtelijk visueel monitoren meestal niet behandeld onder de noemer computercriminaliteit. Computers spelen echter een steeds belangrijkere rol bij visueel monitoren, bijvoorbeeld door met behulp van kwaadaardige software op afstand heimelijk beeldopnamen te maken, zodat bespreking in dit hoofdstuk op zijn plaats is.
Het heimelijk maken van beeldopnamen is strafbaar gesteld voor zover het gebeurt met een technisch hulpmiddel waarvan de aanwezigheid niet duidelijk is kenbaar gemaakt. Het opzettelijk en wederrechtelijk maken van foto's of video's van iemand is strafbaar met één jaar gevangenisstraf of geldboete van de vierde categorie als die persoon zich bevindt in een woning of een andere niet voor het publiek toegankelijke plaats (artikel 139f Sr)[91] en met twee maanden gevangenisstraf of geldboete van de

88 Dit onderdeel van de Wet computercriminaliteit II trad op 1 september 2007 – een jaar later dan de rest van de wet – in werking, om bedrijven de tijd te geven zich op deze nieuwe strafbaarstelling voor te bereiden.
89 *Kamerstukken II* 2004/05, 26671, 7, p. 38.
90 *Ibid.*
91 Met de Wet computercriminaliteit III is de maximale gevangenisstraf verhoogd van zes maanden naar één jaar. Volgens de wetgever zijn de strafmaxima nu beter in evenwicht, omdat ook voor het helen van gegevens maximaal een jaar gevangenisstraf geldt (*Kamerstukken II* 2015/16, 34372, 3, p. 87-88). Artikel 139f Sr kende onder 2° ook een strafbaarstelling voor het bezit van een onder 1° onrechtmatig gemaakte afbeelding; dit is bij de Wet computercriminaliteit III geïntegreerd in de nieuwe, algemene helingsbepaling (zie paragraaf 2.8.2).

derde categorie als de persoon zich op een voor het publiek toegankelijke plaats[92] bevindt (artikel 441b Sr). Oorspronkelijk werd met een 'technisch hulpmiddel' voornamelijk een (vaste) camera(opstelling) bedoeld. Uit jurisprudentie wordt helder dat ook het heimelijk maken van beeldopnamen met een mobiele telefoon strafbaar kan zijn onder artikel 139f Sr.[93] Hoewel de tekst spreekt van het vervaardigen van een afbeelding (wat het *vastleggen* van een beeld lijkt te suggereren), kan ook het 'live' uitkijken van camerabeelden (zoals het op de computer bekijken van beelden uitgezonden door een camera verborgen in een lamp in des stiefzoons slaapkamer) onder artikel 139f Sr vallen.[94] Artikel 139f Sr wordt veelvuldig gebruikt voor het bestrijden van het heimelijk fotograferen of filmen in kleedhokjes, badkamers en dergelijke.
Het is echter ook mogelijk dat het heimelijk maken van beeldopnamen plaatsvindt *in combinatie* met een computergericht delict.[95] Een spyware-zaak van de Rechtbank Rotterdam uit 2014 is daarbij illustratief.[96] In deze zaak werd een persoon veroordeeld voor het op afstand bespioneren van slachtoffers met behulp van malware; hij had de webcams van slachtoffers aangezet, nadat de malware op ongeveer tweeduizend computers was geïnstalleerd. Vervolgens werden de binnengehaalde beelden gecategoriseerd, waaronder veel beelden van jonge meisjes die naakt waren en met zichzelf of anderen seksuele handelingen verrichtten. De verdachte is in casu veroordeeld voor computervredebreuk, bezit van kinderpornografie, smaad en gegevensbeschadiging; in deze zaak had ook artikel 139c Sr ten laste kunnen worden gelegd.[97]
Voor de volledigheid wijzen we ook nog op de overtreding van het portretrecht als geregeld in artikel 35 Auteurswet: het zonder daartoe gerechtigd te zijn openbaar maken of in het openbaar tentoonstellen van een portret, is strafbaar met een geldboete van de vierde categorie. Bij in opdracht gemaakte portretten gaat het daarbij om openbaarmaking zonder toestemming van de geportretteerde of diens nabestaanden; bij niet in opdracht gemaakte portretten hangt de rechtmatigheid af van een afweging tussen het belang van openbaarmaking en het redelijk belang van de geportretteerde of diens nabestaanden tegen openbaarmaking.[98] Onder omstandigheden zou hiermee ook wraakporno kunnen worden aangepakt, mits op de op internet zonder toestem-

92 Oorspronkelijk was deze strafbaarstelling beperkt tot het maken van beeldopnamen in "een voor het publiek toegankelijke besloten ruimte, waarin spijzen, dranken of andere waren aan particulieren worden geleverd", maar dit is met de Wet uitbreiding strafbaarstelling heimelijk cameratoezicht, *Stb*. 2003, 198, uitgebreid tot alle publiek toegankelijke plaatsen.
93 Rb. Noord-Holland 25 november 2016, ECLI:NL:RBNHO:2016:9771. Daarbij nam de rechtbank ook in aanmerking dat de verdachte het intieme filmpje heeft geopenbaard via het chatprogramma 'Snapchat'.
94 Rb. Gelderland 29 augustus 2016, ECLI:NL:RBGEL:2016:4801.
95 Zie ook het antwoord van minister Opstelten (Veiligheid en Justitie) van 23 december 2014 op vragen van lid Rebel over het strafbaar stellen van 'wraakporno', *Aanhangsel Handelingen II* 2014/15, 933.
96 Rb. Rotterdam 4 september 2014, ECLI:NL:RBROT:2014:7379.
97 Rb. Rotterdam 4 september 2014, ECLI:NL:RBROT:2014:7379. Vgl. ook Rb. Haarlem 19 juli 2006, ECLI:NL:RBHAA:2006:AY4778 (veroordeling voor wederrechtelijk aftappen, artikel 139c Sr, van heimelijk gemaakte camerabeelden).
98 Verkade, *T&C Intellectueel Eigendom*, artikel 35 Aw, aant. 2b.

ming gepubliceerde naaktfoto of video het gelaat zichtbaar is, of anderszins uit de afbeelding de identiteit blijkt.[99]

2.5 Verstoring van computergegevens

Met de keuze van de wetgever om 'gegevens' niet onder het begrip 'goed' te brengen stond vast dat artikel 350 Sr (zaakbeschadiging) in het algemeen geen bescherming zou kunnen bieden bij gegevensaantasting. Deze bepaling verbiedt immers het vernielen, beschadigen en dergelijke van een goed dat aan een ander toebehoort. Vanwege het grote belang van de integriteit en beschikbaarheid van computergegevens in de huidige maatschappij, heeft de wetgever besloten gegevens dezelfde bescherming te bieden als goederen.
Om deze reden zijn bij de Wet computercriminaliteit twee bepalingen in de wetgeving opgenomen over gegevensbeschadiging, oftewel 'verstoring van computergegevens', zoals de officiële vertaling van *data interference* uit artikel 4 Cybercrimeverdrag luidt. Artikel 350a Sr bevat de opzetvariant en 350b Sr de schuldvariant. Deze bepalingen zijn vanwege het vergelijkbare beschermingsbelang gemodelleerd naar artikel 350 Sr.[100]

2.5.1 *Gegevensmanipulatie (artikel 350a lid 1 en 2 Sr)*

In het eerste lid van artikel 350a Sr wordt het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens strafbaar gesteld, alsmede het daaraan toevoegen van andere gegevens. Daarbij moet het gaan om gegevens die door middel van een geautomatiseerd werk of telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen. Het toevoegen van gegevens lijkt een vreemde eend in de bijt en de wetgever overwoog dan ook dit bestanddeel te schrappen. Bij nader inzien achtte hij dit echter wel een toegevoegde waarde te hebben, "bijvoorbeeld met het oog op de strafbaarheid van het opzettelijk en wederrechtelijk (bijvoorbeeld zonder toestemming van de geadresseerde) meezenden van (verborgen) gegevens over de e-mail".[101] Hier lijkt een opening geboden te worden voor het bestraffen van spam, maar dat wordt als zodanig niet strafwaardig geacht (zie paragraaf 2.6.2), dus wellicht moet hier de nadruk liggen op "(verborgen)" en heeft de wetgever vooral onzichtbaar meegestuurde spyware of andere malware voor ogen gehad. Dat blijkt in de praktijk in elk geval zo te werken: artikel 350a Sr wordt in de praktijk ten laste gelegd voor het

99 Vgl. HR 2 mei 2003, ECLI:NL:HR:2003:AF3416: "het geheel of gedeeltelijk onherkenbaar maken van het gelaat van de afgebeelde persoon, behoeft er niet aan af te doen dat er sprake is van portret (...), nu ook uit hetgeen die afbeelding overigens toont, de identiteit van die persoon kan blijken".

100 Een belangrijk verschil tussen artikel 350 en 350a Sr is dat het voor de strafbaarheid van vernieling van een goed noodzakelijk is dat dit "geheel of ten dele aan een ander toebehoort". Deze eis wordt voor gegevens niet gesteld, omdat de 'eigendom' van gegevens een dogmatisch discutabel begrip is.

101 *Kamerstukken II* 2004/05, 26671, 7, p. 38-39.

zonder toestemming toevoegen van 'remote administration tools' (RAT's), waarmee op afstand computers kunnen worden overgenomen.[102]
De maximumstraf is twee jaren gevangenisstraf of een geldboete van de vierde categorie. Het betreft hier een niet alleen op het oog zeer ruime strafbepaling.[103] Het delict spreekt van 'geautomatiseerd werk', hetgeen alle soorten computers omvat, inclusief smartphones en andere slimme apparaten. Ook vallen gewone gebruikshandelingen met een computer onder de delictsomschrijving, dus niet alleen het wissen van bestanden, maar ook het intikken en corrigeren van teksten in een tekstverwerker. 'Wederrechtelijk' is hier dus een cruciaal bestanddeel in de bepaling. Dat bleek bijvoorbeeld in een zaak voor de Rechtbank Maastricht, waarin de rechter bepaalde dat het veranderen van een simlock in een mobiele telefoon niet wederrechtelijk is.[104]
Artikel 350a Sr kan ook worden ten laste gelegd bij *defacement,*[105] dat wil zeggen dat de homepage van een website wordt vervangen met een andere webpagina, vaak ter propaganda van een ideologische boodschap of simpelweg 'voor de lol'. Het exploiteren van *ransomware* door misdadigers is een actueel voorbeeld van een cyberdelict dat de laatste jaren een grote vlucht heeft genomen, dat onder artikel 350a Sr kan vallen.[106] Bij ransomware wordt een computersysteem gegijzeld en losgeld geëist. Daarbij wordt vaak (een deel van) de harde schijf van een computer versleuteld en losgeld geëist in de vorm van virtuele valuta of betaling met een waardekaart.[107] Het opzettelijk en wederrechtelijk ontoegankelijk maken van gegevens op een computer met behulp van ransomware valt onder de delictsomschrijving van artikel 350a lid 1 Sr. Ook kan onder omstandigheden het delict dwang (artikel 284 Sr), afpersing (artikel 317 Sr) of oplichting (artikel 326 Sr) ten laste worden gelegd.[108] In de 'CoinVault'-ransomwarezaak stelde de rechtbank het ontoegankelijk maken van bestanden gelijk aan het begrip geweld als bedoeld in artikel 317 Sr, gelet op lid 2 van dat artikel (zie paragraaf 2.10.1).[109]

Het tweede lid van artikel 350a bevatte oorspronkelijk een gekwalificeerde vorm van gegevensbeschadiging, als dit plaatsvond na hacken via openbare telecommunicatie en "ernstige schade" met betrekking tot de gegevens werd veroorzaakt.[110] Bij de implementatie van Richtlijn 2013/40/EU is dit vervangen door een kruisverwijzing naar de

102 Rb. Rotterdam 4 september 2014, ECLI:NL:RBROT:2014:7379, Rb. Rotterdam 26 oktober 2016, ECLI:NL:RBROT:2016:8263.
103 Kaspersen 1990, p. 316-317 en Kaspersen 1987, p. 177; Charbon & Kaspersen 1990, p. 66; Vandenberghe 1987, p. 173; Wiemans 1991, p. 46-47.
104 Rb. Maastricht 12 maart 2002, ECLI:NL:RBMAA:2002:AE0125.
105 Zie de Richtlijn voor strafvordering cybercrime, *Stcrt.* 2018, 3271.
106 In 2014 werd in het Nationaal Cyber Security Beeld gewaarschuwd dat het gebruik van ransomware als type malware zal groeien. In 2016 werd door Europol in haar 'Internet Organised Crime Threat Assessment' (IOCTA)-rapport geconcludeerd dat ransomware, in zijn meer specifieke vorm van cryptoware, inmiddels het favoriete type malware van cybercriminelen is.
107 Zie bijvoorbeeld Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153. Zie uitgebreid Oerlemans e.a. 2016.
108 Zie ook de Richtlijn voor strafvordering cybercrime, *Stcrt.* 2018, 3271. Bij ransomware zal echter niet altijd sprake zijn van een 'listige kunstgreep' teneinde wederrechtelijk financieel voordeel te verkrijgen.
109 Rb. Rotterdam 26 juli 2018, ECLI:NL:RBROT:2018:6153.
110 Zie Koops & De Roos 2007, p. 41-42 voor een bespreking.

strafverzwarende omstandigheden van artikel 138b lid 2 en lid 3 Sr. Indien de gegevensbeschadiging plaatsvindt door een "aanzienlijk aantal" computers die zijn besmet met malware (wat vooral neerkomt op het gebruik van een botnet[111]), staat daar maximaal drie jaar gevangenisstraf tegenover of een geldboete van de vierde categorie (artikel 138b lid 2 Sr). Indien de gegevensbeschadiging "ernstige schade" veroorzaakt of als zij wordt gepleegd in computers die behoren tot de vitale infrastructuur,[112] geldt een strafverzwaring naar maximaal vijf jaar gevangenisstraf (artikel 138b lid 3 Sr).
In de nota naar aanleiding van het verslag wordt aangegeven dat onder 'ernstige schade' onder andere wordt verstaan: de ontregeling van systeemdiensten van (groot) openbaar nut, het ontstaan van aanzienlijke financiële schade, en het wissen of openbaar maken van persoonsgegevens of gevoelige informatie.[113] Voor wat betreft aanzienlijke financiële schade kan vermoedelijk worden aangeknoopt bij de wetsgeschiedenis van artikel 350a lid 2 Sr, waarbij de minister aangaf dat als het functioneren van een informatiesysteem gedurende geruime tijd ("toch zeker (...) enige uren") geheel of nagenoeg geheel is uitgesloten, er sprake is van ernstige schade, evenals de situatie waarin de schade tot een aanwijsbare verandering in de jaarcijfers leidt.[114] In navolging hiervan bepaalde de Hoge Raad dat het gedurende twaalf uur niet beschikbaar zijn van een informatiesysteem als ernstige schade aan te merken was.[115] Tevens heeft de Rechtbank Rotterdam een persoon voor artikel 350a lid 3 Sr veroordeeld vanwege het op grote schaal besmetten van computers met *banking* malware om daarmee frauduleuze transacties uit te voeren, waarmee ernstige schade is veroorzaakt.[116] Wij kunnen ons voorstellen dat het op grote schaal (in de duizenden) besmetten van computers met *banking* malware of ransomware wordt gezien als een handelen dat ernstige schade in de zin van artikel 350a lid 2 jo. 138b lid 3 Sr met zich meebrengt.
Opmerking verdient wel dat de nieuwe strafverzwarende omstandigheid ruimer lijkt: voorheen sprak de wet van ernstige schade "met betrekking tot die [te weten de onder lid 1 aangetaste] gegevens", wat vooral lijkt te duiden op directe schade en niet op gevolgschade. De bepaling spreekt nu algemener van het veroorzaken van ernstige schade, wat ook (causaal aanwijsbare) gevolgschade zal omvatten. Opmerkelijk is bovendien dat niet alleen financiële schade wordt bedoeld, maar mogelijk ook immateriële schade, gezien het voorbeeld van "het wissen of openbaar maken van persoonsgegevens of gevoelige informatie". In dit verband nemen we aan dat de wetgever niet *elke* aantasting van persoonsgegevens zal hebben bedoeld als "ernstige schade"; het wissen van een familiefoto of het openbaar maken van iemands geboortedatum kan bijzonder storend zijn, maar is niet echt van dezelfde orde als een bedrijfsstoring die in de jaar-

111 *Kamerstukken II* 2014/15, 34034, 3, p. 8.
112 Zie noot 140 voor een omschrijving van 'vitale infrastructuur'.
113 Zie *Kamerstukken II* 2014/15, 34034, 5, p. 11.
114 *Handelingen II* 24 juni 1992, 93-5869.
115 HR 19 januari 1999, *NJ* 1999/251.
116 Rb. Rotterdam 26 oktober 2016, ECLI:NL:RBROT:2016:8263. In 2011 liet de advocaat-generaal nog in het midden of het feit dat na besmetting van *banking* malware niet meer veilig kan worden getelebankierd als dergelijke ernstige schade kan worden aangemerkt (Concl. A-G bij HR 22 februari 2011, ECLI:NL:PHR:2011:BN9287, § 32).

cijfers zichtbaar moet zijn of de ontregeling van nutsdiensten. Vermoedelijk is vooral gedacht aan grootschalige inbreuken, zoals datalekken die leiden tot openbaarmaking van persoonsgegevens van duizenden personen, of het verspreiden van cryptoware die de persoonsgegevens van een aanzienlijk aantal individuen ontoegankelijk maakt.

2.5.2 *Kwaadaardige software (artikel 350a lid 3 en 4 Sr)*

Een van de motieven voor het ontwerpen van artikel 350a Sr was destijds de bestrijding van de zich steeds meer verspreidende computervirussen. Vroeger werd een strikt onderscheid gemaakt tussen virussen, wormen en Trojaanse paarden, maar tegenwoordig heeft kwaadaardige software vaak kenmerken van al deze typen: de kwaadaardige software (een virus) kan zichzelf verspreiden op andere computers (kenmerkend voor wormen) en doet zich vaak voor als onschuldig lijkend programma (Trojaans paard). Daarom wordt tegenwoordig meestal de verzamelterm 'kwaadaardige software' gebruikt, kortweg 'malware'. Daar sluiten wij bij aan, tenzij het voor de strafbaarstelling van belang is de meer specifieke benaming te gebruiken.
Het derde lid stelt het verspreiden van kwaadaardige software strafbaar, met een maximumstraf van vier jaren of een geldboete van de vijfde categorie. Door de regie van het derde lid is reeds het verspreiden of ter beschikking stellen van kwaadaardige software strafbaar, los van het feit of de malware daadwerkelijk in actie komt en schade aanricht.[117]
De tekst van het derde lid zoals ingevoerd door de Wet computercriminaliteit in 1993 was ongelukkig: strafbaar was het opzettelijk en wederrechtelijk gegevens ter beschikking stellen of verspreiden "die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk". De meeste kwaadaardige software, zoals een virus, valt hier strikt genomen niet onder, omdat dat geen schade aanricht door zichzelf te vermenigvuldigen, maar door een bepaald commando uit te voeren (bijvoorbeeld: 'wis de harde schijf'). Strikt genomen vielen alleen wormen onder de strafbepaling: programmaatjes die, door zichzelf steeds weer te vermenigvuldigen, een computer uiteindelijk blokkeren en daardoor schade aanrichten. Volgens ons was echter wel een wetshistorische interpretatie (het is de bedoeling van de wetgever geweest om alle soorten kwaadaardige software strafbaar te stellen, zoals men in de parlementaire stukken kan lezen) toegestaan.
In elk geval is de tekst nu verduidelijkt: sinds de invoering van de Wet computercriminaliteit II luidt dit bestanddeel: gegevens "die zijn bestemd om schade aan te richten in een geautomatiseerd werk", waardoor duidelijk is dat zowel wormen als computervirussen eronder vallen. Hoewel strikt genomen Trojaanse paarden niet bestemd hoeven te zijn om schade aan te richten *in* een geautomatiseerd werk (ze kunnen bijvoorbeeld

117 Vgl. HR 28 september 2004, *NJ* 2004/642 (*Kournikova*-worm), waarin de Hoge Raad verduidelijkte dat het bestanddeel "gegevens die bedoeld/bestemd zijn om schade aan te richten" niet betekent dat de schade daadwerkelijk optreedt, onder verwijzing naar *Kamerstukken II* 1990/91, 21551, 7, p. 5. Zie ook Rb. Leeuwarden 27 september 2001, ECLI:NL:RBLEE:2001:AD3861.

schade aanrichten door stiekem gegevens door te geven), vallen dergelijke programma's blijkens de toelichting ook onmiskenbaar onder de strafbepaling.[118]
Het opzet van de verdachte moet er mede op gericht zijn dat de verspreide gegevens bestemd zijn om schade aan te richten. De Hoge Raad bevestigde dit op basis van de tekst van de wet: het begrip 'opzettelijk' gaat vooraf aan het (toenmalige) bestanddeel "bedoeld om schade aan te richten".[119] Dat gegevens 'bestemd' zijn om schade aan te richten duidt daarbij niet alleen op de bedoeling van de dader (schade aanrichten) maar ook op de geschiktheid van het middel: malware die weliswaar bedoeld is om schade aan te richten maar daartoe volstrekt niet in staat is, zou daarom straffeloos mogen worden verspreid.
Lid 4 van artikel 350a Sr bevat een strafuitsluitingsgrond: degene die een virus verspreidt met de bedoeling schade als gevolg van dat virus te voorkomen, is niet strafbaar. Hiermee wordt gedoeld op situaties waarin iemand een virus verspreidt ter 'inenting' van nog niet besmette computers, bijvoorbeeld door een onschuldige variant van een net ontdekt virus te verspreiden. Een onschuldige variant is een virus met dezelfde signatuur maar zonder de schadelijke activiteit die het oorspronkelijke virus zou uitvoeren. Als deze onschuldige variant computers van potentiële slachtoffers eerder bereikt dan de schadelijke variant en zich daarin nestelt, zal deze laatste niet meer deze computer infecteren, omdat het schadelijke virus denkt dat de computer reeds besmet is.

2.5.3 *Culpose gegevensbeschadiging (artikel 350b Sr)*

In het eerste lid van artikel 350b Sr is de culpose variant van het eerste lid van artikel 350a Sr (gegevensbeschadiging) opgenomen. Toegevoegd is echter dat *ernstige schade* met betrekking tot de gegevens moet zijn veroorzaakt door het nalatig handelen. De delictsomschrijving zal derhalve niet snel vervuld zijn. Er moet sprake zijn van een grote veronachtzaming van een belangrijke zorgplicht én van ernstige schade. Als bijvoorbeeld een systeembeheerder van een groot netwerk, gemeten naar de maatstaf van haar deskundigheid en de stand der techniek, verwijtbaar nalatig is geweest met de beveiliging van het systeem, waardoor ernstige schade aan gegevens ontstaat,[120] zou zij strafbaar kunnen zijn. De sanctie die op vervulling van het eerste lid staat is een maand gevangenisstraf of een geldboete van de tweede categorie.
Dezelfde straf geldt voor het tweede lid van artikel 350b Sr, de culpose evenknie van het derde lid van artikel 350a Sr (malwareverspreiding). Hieronder valt waarschijnlijk niet de werknemer die een USB-stick van huis meeneemt waarin zich malware heeft genesteld en waarmee deze werknemer het bedrijfssysteem besmet (wat wel nalatig is, maar vermoedelijk niet verwijtbaar nalatig in strafrechtelijke zin), maar mogelijk wel

118 *Kamerstukken II* 1998/99, 26671, 3, p. 48.
119 HR 28 september 2004, *NJ* 2004/642 (*Kournikova*-worm).
120 Merk op dat artikel 350b lid 1 Sr nog wel spreekt van ernstige schade "met betrekking tot die gegevens", zodat het begrip 'ernstige schade' hier een andere (beperktere) betekenis heeft dan het begrip in artikel 350a lid 2 jo. 138b lid 3 Sr (zie paragraaf 2.5.1).

de systeembeheerder die verzuimt enige anti-virusprogrammatuur op een systeem te draaien. Dit culpose delict zou gebruikt kunnen worden als prikkel om de personen die binnen organisaties verantwoordelijk zijn voor informatiebeveiliging maar hun taak aanmerkelijk nalatig nakomen, scherp te houden en zodoende het niveau van informatiebeveiliging in de maatschappij te verhogen.[121] Het artikel lijkt echter een slapend bestaan te leiden; in de loop der jaren zijn er geen veroordelingen op rechtspraak.nl gepubliceerd met betrekking tot deze culpose variant.

2.6 Verstoring van computersystemen

Artikel 5 Cybercrimeverdrag stelt "verstoring van computersystemen" strafbaar, oftewel computerbeschadiging. Vaak zal dit gepaard gaan met gegevensbeschadiging, maar niet altijd. Ook geeft het zelfstandig strafbaar stellen van computerbeschadiging aan dat het beschermde rechtsgoed anders is: niet de integriteit of beschikbaarheid van gegevens staat voorop, maar de integriteit en beschikbaarheid van het computersysteem zelf, wat vooral bij kritische systemen (denk aan vitale infrastructuur) van groot maatschappelijk belang is.

2.6.1 *Computersabotage (artikel 161sexies en 351 Sr)*

Titel VII van boek 2 Wetboek van Strafrecht ziet op "Misdrijven waardoor de algemene veiligheid van personen of goederen wordt in gevaar gebracht". Deze titel bevat bepalingen over gedragingen die 'gemeen', dat wil zeggen algemeen of publiek, gevaar veroorzaken voor personen of goederen. Er zijn bijvoorbeeld artikelen opgenomen omtrent aantasting van de elektriciteitsvoorziening en de verstoring van het weg-, scheepvaart- of luchtverkeer. Gezien de rol van computers en telecommunicatiewerken in onze samenleving is bij vernieling en dergelijke daarvan mogelijk gemeen gevaar voor goederen of mensen te vrezen. Daarom zijn er aparte bepalingen gecreëerd voor geautomatiseerde werken die voor het algemeen nut van belang zijn.
Ingevolge artikel 161sexies Sr is strafbaar hij die "opzettelijk enig geautomatiseerd werk of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt", mits daarbij een zeker gevolg optreedt. Het gaat hier bijvoorbeeld om het storen van computers van een openbare telecomaanbieder of van de Belastingdienst waardoor deze niet meer functioneren, of het knoeien met de geautomatiseerde beveiliging van een kerncentrale waardoor een lek ontstaat. De dader hoeft niet opzettelijk het gevolg te hebben gewild (het onbruikbaar maken van alle belastingaangiftes), hij hoeft alleen opzettelijk de gedraging te hebben gepleegd (het inbreken op de centrale computers van de Belastingdienst). Bij deze delicten van computersabotage moet men bedenken dat het opzettelijk plegen ook voorwaardelijk opzet omvat (dat wil zeggen dat iemand zich blootstelt aan de

121 Vgl. Tjong Tjin Tai & Koops 2015, p. 1070.

geenszins als denkbeeldig te verwaarlozen kans dat iets gebeurt). Wie denkt: "Ik wil weliswaar niet dat het netwerk plat gaat, maar als het gebeurt, kan me dat eigenlijk niet schelen", handelt opzettelijk. De systeembeheerder van een openbare telecomaanbieder die een nieuw programma installeert, waarbij de werking van het netwerk gestoord kan worden, heeft daardoor een grotere verantwoordelijkheid. Als hij onder tijdsdruk een installatie doorvoert waarbij hij op de koop toeneemt dat het netwerk platgaat, zou hij zich schuldig kunnen maken aan opzettelijke computersabotage.

De toepasbaarheid en strafmaat zijn afhankelijk van het gevolg.[122] Indien gemeen gevaar voor goederen of voor de verlening van diensten te duchten is, is de maximumstraf zes jaren of een geldboete van de vijfde categorie (1°). Het gebruik van een botnet, waarbij computergebruikers die hun bank wilden bezoeken werden omgeleid naar een valse (phishing-)pagina en hun financiële gegevens heimelijk werden doorgestuurd, is door de Hoge Raad in een arrest aangemerkt als computersabotage, omdat hierdoor een gemeen gevaar voor diensten bestond.[123] De interpretatie is in dit geval aanvechtbaar, omdat de Hoge Raad redeneerde dat ook het manipuleren van een substantieel aantal computers van *eindgebruikers* (dus niet van nutsdienstverleners zelf) gemeen gevaar voor dienstverlening oplevert. Dat miskent dat artikel 161sexies spreekt van gevaar voor dienst*verlening*, niet van gevaar voor dienst*gebruik*. Artikel 161sexies moet volgens ons dan ook beperkt blijven tot aanvallen op computers van (nuts)dienstverleners.[124] Daarbij brengt ook niet elke aanval op de website van een bank de verlening van hun belangrijkste dienst op internet – het faciliteren van elektronisch betalingsverkeer – in gevaar; het platleggen van een voorlichtingspagina van een bank over verzekeringen is bijvoorbeeld niet bedreigend voor het elektronisch betalingsverkeer.[125]
Uit jurisprudentie blijkt ook dat een verstikkingsaanval (zie paragraaf 2.6.2) op overheidswebpagina's, internetaanbieders en banken als een gemeen gevaar voor diensten wordt beschouwd.[126] Een verstikkingsaanval op de webpagina van een webwinkel werd niet aangemerkt als een aanval die een gemeen gevaar voor diensten oplevert.[127]
Indien van een aanval levensgevaar voor een ander te duchten is, is de maximumstraf negen jaren of geldboete van de vijfde categorie. In het geval de aanval daarbij bovendien iemands dood ten gevolge heeft, is de gevangenisstraf ten hoogste vijftien jaren of een geldboete van de vijfde categorie. Gelukkig worden deze laatste twee feiten tot nu toe nog niet of nauwelijks door cybercriminelen gepleegd, althans voor zover de rechtspraak laat zien. Het is echter wel denkbaar dat het saboteren van computersystemen

122 Bij de implementatie van de Richtlijn aanvallen op informatiesystemen is het eerste onderdeel van artikel 161sexies Sr verplaatst naar het nieuwe artikel 350c Sr (zie paragraaf 2.6.3). Zie *Kamerstukken II* 2014/15, 34034, 3, p. 6.
123 HR 22 februari 2011, ECLI:NL:HR:2011:BN9287 (*Toxbot*-arrest).
124 Oerlemans & Koops 2011, p. 1183-1184.
125 *Ibid*.
126 Rb. Den Haag 14 maart 2005, ECLI:NL:RBSGR:2005:AT0249. Zie ook Rb. Zeeland-West-Brabant, 2 september 2014, ECLI:NL:RBZWB:2014:6659 (in casu konden klanten voor één uur geldzaken niet meer regelen via internetbankieren en iDeal).
127 Hof 's-Hertogenbosch 12 februari 2007, ECLI:NL:GHSHE:2007:BA1891.

in vitale infrastructuren of bepaalde slimme apparaten – zoals voertuigen of medische apparaten – het leven van mensen in gevaar kan brengen en dat met de opkomst van het Internet of Things (en zeker met het Internet of People) computeraanvallen vaker een gemeengevaarlijk karakter zullen krijgen.[128]

Met de Wet computercriminaliteit is voorts de tekst van artikel 351 Sr, dat het beschadigen, vernielen en onbruikbaar maken van een aantal werken ten algemene nutte met een straf bedreigt van drie jaar gevangenisstraf of een geldboete van de vierde categorie, gemoderniseerd. "Spoorweg, telegraaf, telefoon of elektriciteitswerken" is in dat artikel vervangen door "spoorweg of elektriciteitswerken, geautomatiseerde werken of werken voor telecommunicatie". Voor zover computers voor het publiek belang worden ingezet, vormt sabotage hiervan een apart delict. Het "algemene nut" duidt op computers die openstaan voor gebruik van eenieder, al dan niet na betaling, zoals computers in een openbare bibliotheek. Het verschil met het hiervoor behandelde 161sexies is dat die strafbepaling vereist dat een bepaald gevolg intreedt; artikel 351 is ook van toepassing als er geen gemeengevaarlijk gevolg optreedt.

2.6.2 *Verstikkingsaanvallen (ddos-aanvallen, artikel 138b Sr)*

De wetgever heeft, in navolging van een aanbeveling van Schellekens,[129] in de Wet computercriminaliteit II een nieuw artikel 138b Sr opgenomen. Pas sinds 2006 zijn daarmee ook verstikkingsaanvallen (*distributed denial-of-service-* of ddos-aanvallen[130]) strafbaar gesteld. Dit was niet als zodanig strafbaar in Nederland, terwijl artikel 5 Cybercrimeverdrag alsmede artikel 4 van het Europese Kaderbesluit aanvallen op informatiesystemen dat wel verplicht stelden. Oorspronkelijk luidde het voorstel om het opzettelijk via openbare telecommunicatie aan iemand toezenden van gegevens "die bestemd zijn om *diens* toegang" tot het telecomnetwerk of de telecomdienst te belemmeren strafbaar te stellen.[131] Aangezien hier echter geen ddos-aanvallen onder vallen (daarbij wordt immers meestal niet de toegang van de computergebruiker belemmerd, maar van derden die een weblocatie bezoeken), is de tekst aangepast.[132] Strafbaar is nu degene die "opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden". Op overtreding van artikel 138b lid 1 Sr staat sinds de Richtlijnimplementatie een maximumstraf van twee jaar gevangenisstraf (dit was één jaar) of een geldboete van de vierde categorie.

---

128 Vgl. Gasson & Koops 2013. Zie ook A. Greenberg, 'Hackers Remotely Kill a Jeep on the Highway—With Me in It', *Wired* 21 juli 2015.

129 Schellekens 1999, p. 16-17 en 75.

130 Een verstikkingsaanval kan ook plaatsvinden met een dos-aanval (*denial of service*), die niet, zoals bij ddos, gedistribueerd (dus vanuit verschillende computers tegelijk) plaatsvindt, maar vanuit één computer. Ook dit is strafbaar onder artikel 138b Sr. Aangezien in de praktijk ddos verreweg het meeste voorkomt, hanteren we die term in dit hoofdstuk.

131 *Kamerstukken II* 1998/99, 26671, 2 (cursivering toegevoegd).

132 Zie *Kamerstukken II* 2004/05, 26671, 7, p. 33-34.

Ook 'e-mail *bombing*', het elektronisch 'bombarderen' van een e-mailaccount, valt onder artikel 138b Sr. Een dergelijke e-bom verhindert de beschikbaarheid van de e-mail voor de gebruiker, en mogelijk wordt ook de internetverbinding zelf erdoor bemoeilijkt of geblokkeerd. Onder toegangsbelemmering valt echter niet 'gewone' spam (ongevraagde elektronische (massa)berichten, vaak met handelsreclame). Anders dan een e-bom maakt spam volgens de wetgever geen inbreuk op een elementair rechtsgoed. In de Memorie van Toelichting bij het wetsvoorstel Computercriminaliteit II zegt de minister dat hij het niet opportuun acht om spammen strafbaar te stellen, hoe hinderlijk het ook is.[133] Dat betekent dat spammers niet strafrechtelijk kunnen worden aangepakt. Zij kunnen overigens wel stevige bestuurlijke boetes krijgen van de ACM op basis van artikel 11.7 Telecommunicatiewet.[134]

De term 'bestemd' geeft aan dat de gegevens (objectief gezien) bedoeld én geschikt moeten zijn om de toegang of het gebruik te belemmeren. Of de toegang ook daadwerkelijk wordt geblokkeerd is niet van belang: het is voldoende als de reële mogelijkheid bestaat dat de toegang wordt geblokkeerd. Wanneer dat zo is, zal dus mede afhangen van de stand van de techniek. Naast artikel 138b kunnen in bepaalde gevallen ook andere bepalingen van toepassing zijn op verstikkingsaanvallen. Hierbij kan gedacht worden aan computersabotage (zie paragraaf 2.6.1), het wederrechtelijk toevoegen van gegevens (artikel 350a Sr)[135], of computervredebreuk (artikel 138ab Sr) als – zoals bij botnets – wederrechtelijk wordt binnengedrongen in een computer.[136] Merk op dat de wetgever toegangsbelemmering in het Wetboek van Strafrecht heeft geplaatst bij hacken (artikel 138ab Sr) en niet bij misbruik van kwaadaardige software (artikel 350a lid 3 Sr). Dat komt vermoedelijk door het beschermde rechtsgoed: artikel 138ab Sr beschermt vooral de vertrouwelijkheid en integriteit van computersystemen (en niet van de gegevens zelf), en artikel 138b Sr beschermt de beschikbaarheid van computersystemen. Tezamen beschermen ze dus de drie hoofdbelangen van informatiebeveiliging (vertrouwelijkheid, integriteit en beschikbaarheid) ten aanzien van computers.

Verstikkingsaanvallen worden in de regel uitgevoerd met behulp van een botnet, oftewel netwerk van geïnfecteerde computers ('zombiecomputers') die door een derde op afstand worden aangestuurd. Met behulp van een botnet kan een grote hoeveelheid computers worden aangestuurd om allemaal tegelijk een website te bezoeken. De server van de aangevallen website kan dan mogelijk de grote hoeveelheid verkeer niet meer aan, waardoor de website niet meer toegankelijk is. Dit verklaart ook het voorvoegsel van de Engelse benaming – 'denial-of-service' – van de aanval, waarbij 'distributed' aanduidt dat het een gecoördineerde aanval van meerdere computers betreft.

In navolging van Richtlijn 2013/40/EU is het gebruik van een groot aantal geautomatiseerde werken om een denial-of-service-aanval uit te voeren – oftewel het uitvoeren

133 *Kamerstukken II* 1998/99, 26671, 3, p. 40. Zie ook *Kamerstukken II* 2004/05, 26671, 10, p. 28.

134 Zie ook Boetebeleidsregel ACM 2014, *Stcrt.* 2014, 19776 (die onder andere het oudere Handhavingsbeleid spam (*Stcrt.* 2010, 660) vervangt). Zie in dit kader ook Zwenne & Van Hooidonk 2012.

135 Maar niet het wederrechtelijk aantasten van gegevens, zie Hof 's-Hertogenbosch 12 februari 2007, ECLI:NL:GHSHE:2007:BA1891.

136 Zie bijvoorbeeld Rb. Rotterdam 7 juni 2013, ECLI:NL:RBROT:2013:11278.

van een ddos-aanval met een botnet – strafbaar gesteld als een gekwalificeerde vorm van artikel 138b Sr, waarop een maximumgevangenisstraf staat van drie jaren of een geldboete van de vierde categorie. Tekstueel is niet direct duidelijk dat het om botnets gaat, maar de formulering "een aanzienlijk aantal geautomatiseerde werken die getroffen zijn door het gebruik van een middel als bedoeld in artikel 139d, tweede lid, dat hoofdzakelijk daarvoor geschikt is gemaakt of ontworpen" ziet volgens de toelichting op botnets.[137] Wij nemen aan dat "daarvoor" hierbij slaat op het feit uit het eerste lid, dat wil zeggen verstikkingsaanvallen. Bij de formulering moet dan wel de kanttekening worden geplaatst dat een botnet vele toepassingsmogelijkheden heeft en niet per se "hoofdzakelijk" geschikt is gemaakt of ontworpen voor verstikkingsaanvallen; evengoed kan een botnet bedoeld zijn om grootschalig spam te versturen of bijvoorbeeld click-fraude (zie paragraaf 2.10) te plegen.[138] De verdediging zou dus als verweer kunnen aanvoeren dat het botnet waarmee een verstikkingsaanval was gepleegd, niet hoofdzakelijk *daarvoor* geschikt was gemaakt, maar voor andere functionaliteiten.
Op een aanval die ernstige schade veroorzaakt of wordt gepleegd tegen een werk behorende tot de vitale infrastructuur, staat een maximumgevangenisstraf van ten hoogste vijf jaren of geldboete van de vierde categorie. Het begrip 'ernstige schade' is alleen kort toegelicht en wordt vooral aan rechterlijke interpretatie overgelaten[139] (zie verder de bespreking in paragraaf 2.5.1). Het begrip 'vitale infrastructuur' wordt in de toelichting omschreven als een "voorziening, systeem of een deel daarvan op het grondgebied van een lidstaat, dat van essentieel belang is voor bijvoorbeeld het behoud van vitale maatschappelijke functies, de gezondheid, de veiligheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, zoals energiecentrales, vervoersnetwerken, of overheidsnetwerken, en waarvan de verstoring of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken".[140]

2.6.3 *Computerverstoring (artikel 350c Sr)*

Bij de implementatie van de richtlijn Aanvallen op informatiesystemen is artikel 350c Sr in het Wetboek van Strafrecht geïntroduceerd.[141] De bepaling is met enige aanpassingen overgeheveld uit artikel 161sexies Sr en stelt het opzettelijk aantasten[142] van een computer of telecommunicatiewerk strafbaar, als daardoor wederrechtelijke verhindering of bemoeilijking van de opslag, verwerking of overdracht van gegevens ontstaat, of wederrechtelijke stoornis in een telecommunicatienetwerk of in de uitvoering van een telecommunicatiedienst. Waar het opzet ziet op het middel – de computeraanval – ziet de wederrechtelijkheid dus op het gevolg – de feitelijke verstoring. De aanvaller

137 *Kamerstukken II* 2014/15, 34034, 3, p. 8 in combinatie met Richtlijn 2013/40/EU.
138 Vgl. Hogben 2011.
139 *Kamerstukken II* 2014/15, 34034, 5, p. 11.
140 Zie *Kamerstukken II* 2014/15, 34034, 3, p. 9.
141 *Stb.* 2015, 165.
142 Aantasten kan bestaan uit vernielen, beschadigen, onbruikbaar maken, stoornis in de gang of werking veroorzaken of een beveiligingsmaatregel van het werk verijdelen.

hoeft dus geen opzet op een computerstoring te hebben gehad, alleen op het beschadigen van een computer of telecommunicatiewerk. Wetssystematisch had de bepaling wellicht beter kunnen worden geplaatst direct na artikel 138b Sr, waarmee het verwantschap heeft doordat beide delicten zien op vormen van computerverstoring. Het onderbrengen bij de bepalingen ten aanzien van gegevensaantasting (artikel 350a e.v. Sr) suggereert onzes inziens ten onrechte dat het delict primair de integriteit of beschikbaarheid van *gegevens* beschermt, terwijl het toch vooral bedoeld is om de integriteit en beschikbaarheid van *computersystemen* te beschermen.[143]
De maximumstraf is twee jaar gevangenisstraf of een geldboete van de vierde categorie. Waar artikel 161sexies gericht is op gemeengevaarlijke delicten en de computer- of telecommunicatieverstoring in dit verband voorheen dus alleen strafbaar was als deze stoornis veroorzaakte bij gegevens *ten algemene nutte* of *openbare* telecommunicatie, geldt de strafbaarstelling nu voor elke computerstoring. In dat verband is ook de maximumstrafmaat aangepast, meer in lijn met de overige computerdelicten sinds de Richtlijnimplementatie, met een zwaardere gevangenisstraf (twee jaar in plaats van één jaar) maar een lagere boete (vierde in plaats van vijfde categorie).
Volgens lid 2 van artikel 350c Sr zijn de strafverzwarende omstandigheden uit artikel 138b lid 2 en lid 3 Sr – indien gebruik is gemaakt van een botnet, de aanval ernstige schade veroorzaakt of is gericht tegen vitale infrastructuur – van overeenkomstige toepassing.

2.6.4 *Culpose delicten (artikel 161septies en 351bis Sr)*

Evenals gegevensbeschadiging kent ook computerverstoring een culpose variant. Artikel 161septies Sr bevat de schuldvariant van computersabotage als strafbaar gesteld in artikel 161sexies Sr. Bij storing van gegevens ten algemene nutte of in openbare telecommunicatie, alsook bij gemeen gevaar voor goederen of voor de verlening van diensten is de maximumgevangenisstraf zes maanden, bij levensgevaar voor een ander ten hoogste een jaar gevangenisstraf en indien het feit iemands dood ten gevolge heeft twee jaren gevangenisstraf; in alle gevallen geldt een maximumboete van de vierde categorie. Opmerkelijk is dat de wetgever de storing van gegevens ten algemenen nutte of in openbare telecommunicatie in artikel 161septies onder 1° Sr heeft laten staan, terwijl het daarmee corresponderende onderdeel uit artikel 161sexies is overgeheveld naar artikel 350c Sr (zie paragraaf 2.6.3). Hierdoor is een wat ongelukkige asymmetrie ontstaan tussen de doleuze en de culpose vorm van computersabotage.

143 De toelichting op de plaatsing na artikel 350b is weinig onderbouwd: de minister geeft aan dat het artikel "inhoudelijk meer aansluit bij de artikelen 350a e.v. en 351 en 351bis Sr" (*Kamerstukken II* 2014/15, 34034, 3, p. 6), daarbij over het hoofd ziend dat artikel 351 en 351bis Sr beide zien op verstoring van computers of gegevensverwerking met een publiek belang, terwijl de reden van verplaatsing juist was het vervallen van het vereiste van publiek belang in artikel 350c Sr (aldus ook Ten Voorde 2018, p. 637). Over de logischer mogelijkheid van aansluiting bij artikel 138ab en 138b Sr wordt niets gezegd.

Verder kent ook de opzettelijke computersabotage van artikel 351 Sr een culpose variant, artikel 351bis Sr, met een maximumstraf van een maand gevangenis of geldboete van de tweede categorie.

Schuld omvat in deze culpose delicten niet iedere mate van onachtzaamheid, maar alleen een min of meer grove of aanmerkelijke onvoorzichtigheid, onachtzaamheid of nalatigheid.[144] Het betekent dat ook als iemand niet een computerstoring op de koop toeneemt (wat onder voorwaardelijk opzet zou vallen), maar wel verwijtbaar slordig is met voorzorgsmaatregelen, waardoor de werking van een publiek systeem of netwerk ontregeld wordt, hij nalatige computersabotage kan plegen (artikel 161septies of artikel 351bis Sr). Wat hierbij als aanmerkelijk nalatig geldt, hangt af van de context: hoe belangrijk is het systeem, welke verantwoordelijkheden heeft de systeembeheerder, hoe ervaren is hij, installeerde hij een programma waarvan een belangrijke systeemfout in alle vaktijdschriften uitvoerig was beschreven, of gebruikte hij juist een verouderde beveiliging die een collega was vergeten te vervangen?[145] Merk op dat zelfs nietsdoen onder omstandigheden computersabotage kan opleveren, bijvoorbeeld als de systeembeheerder van een ziekenhuis niets gedaan had aan het millenniumprobleem en daardoor patiënten verkeerde medicijnen zouden hebben kregen.
Evenals bij culpose gegevensbeschadiging zijn met betrekking tot deze culpose strafbaarstellingen nog geen gepubliceerde uitspraken beschikbaar.

2.7 Misbruik van technische hulpmiddelen (artikel 139d leden 2 en 3 en artikel 350d Sr)

Artikel 6 van het Cybercrimeverdrag stelt misbruik van technische hulpmiddelen[146] strafbaar. Volgens het verdrag moeten, kort gezegd, tal van voorbereidingshandelingen strafbaar worden gesteld die worden gepleegd met het doel om een van de voorgaande cyberdelicten te plegen. Het gaat om bijvoorbeeld het ontwikkelen, verspreiden of voorhanden hebben van apparatuur of programmatuur voor hacken, malwareverspreiding of gegevensonderschepping. Ook het voorhanden hebben van wachtwoorden of toegangscodes waarmee toegang tot een computer(systeem) kan worden verkregen, is strafbaar als men van plan is om daarmee bijvoorbeeld computervredebreuk te plegen. Voorheen kende Nederland het strafbare 'misbruik van hulpmiddelen' alleen bij apparatuur voor het kraken van telecomdiensten (waarmee iemand zonder te betalen gebruik kan maken van bijvoorbeeld betaal-tv of telefonie) (artikel 326c lid 2 Sr), voorwerpen voor waardepapiervervalsing (artikel 234 Sr), middelen voor het omzeilen van technische beveiliging van computerprogrammatuur (artikel 32a Auteurswet) en het reclame maken voor afluisterapparatuur (artikel 441a Sr). Ter implementatie van de veel algemenere strafbaarstelling van voorbereidingshandelingen in artikel 6 Cyber-

144 *Kamerstukken II* 1989/90, 21551, 3, p. 19.
145 Vgl. ook Tjong Tjin Tai & Koops 2015.
146 De Engelse term uit het verdrag, 'technical devices', omvat zowel apparatuur als programmatuur; de Nederlandse vertaling van *device* luidt dan ook 'hulpmiddel' in plaats van de gebruikelijker vertaling 'apparaat'.

crimeverdrag zijn bij de Wet computercriminaliteit II twee bepalingen ingevoerd. De belangrijkste is artikel 139d leden 2 en 3 Sr:

ARTIKEL

2. Met dezelfde straf[147] *wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138ab, eerste lid, 138b of 139c wordt gepleegd:*

a) *een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of*

b) *een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden gekregen tot een geautomatiseerd werk of een deel daarvan, vervaardigt verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft*

3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt terwijl zijn oogmerk is gericht op een misdrijf als bedoeld in artikel 138ab, tweede of derde lid.

De andere bepaling was artikel 161sexies lid 2 Sr, met een vergelijkbare strafbaarstelling van misbruik van technische hulpmiddelen met het oogmerk van computersabotage (artikel 161sexies lid 1 Sr).[148] In 2015 is artikel 161sexies lid 2 Sr vervallen en vervangen door artikel 350d Sr (zie onder).

Door het scala aan verboden handelingen (verwerven, voorhanden hebben, enzovoort) en de opneming niet alleen van hulpmiddelen maar ook van wachtwoorden, bevat artikel 139d leden 2 en 3 Sr een potentieel zeer ruime strafbaarstelling. Cruciale elementen hierin zijn dan hulpmiddelen die "*hoofdzakelijk geschikt gemaakt of ontworpen*" zijn en "*met het oogmerk dat daarmee*" een bepaald misdrijf wordt gepleegd. Het voorhanden hebben van bijvoorbeeld hackprogrammatuur die alleen gebruikt wordt om de beveiliging van de eigen computer te testen, is niet strafbaar.[149] Over de hoofdzakelijkheidseis geeft de wetgever aan:

147 Als in artikel 139d lid 1 Sr, oftewel ten hoogste twee jaren gevangenisstraf of geldboete van de vierde categorie (voetnoot toegevoegd aan citaat).

148 Anders dan bij hacken werd daarbij de voorbereiding van de zwaardere vormen van computer (zoals bij levensgevaar of dood als gevolg) niet zwaarder gestraft. De toelichting gaf aan dat de vormen waar acht jaren of meer gevangenisstraf op stond onder de algemene strafbaarstelling van voorbereiding (artikel 46 Sr) kunnen vallen, zie *Kamerstukken II* 2004/05, 26671, 7, p. 36. Bij artikel 46 Sr is de maximumstraf echter niet even hoog maar de helft van het gronddelict.

149 *Kamerstukken II* 2004/05, 26671, 7, p. 36. Zie ook overweging 16 van Richtlijn 2013/40/EU over aanvallen op informatiesystemen. Vgl. in dit verband ook artikel 32a Auteurswet, dat zich beperkt tot hulpmiddelen die *uitsluitend* bestemd zijn voor de te bestrijden onrechtmatigheden, en artikel 29a lid 3 Auteurswet met een strafbaarstelling van middelen (voor het omzeilen van anti-kopieerbeveiliging) die "slechts een commercieel *beperkt* doel of nut hebben anders dan het omzeilen" of die "*vooral* ontworpen, vervaardigd of aangepast worden met het doel het omzeilen" (onze cursivering).

CITAAT

> *"Uit de inrichting en de eigenschappen van het middel dient te blijken dat dit door de producent ook bedoeld is om een delict als omschreven in de artikelen 2 tot en met 5 te begaan. (...) De term 'hoofdzakelijk' sluit niet uit dat ander al dan niet legitiem gebruik mogelijk is, maar impliceert dat zodanig gebruik als ondergeschikt moet worden beschouwd ten aanzien van de naar objectieve maatstaven vast te stellen gebruiksmogelijkheden, nl. als hulpmiddel tot het begaan van een der in de artikelen 2 tot en met 5 genoemde delicten."*[150]

Hiermee kun je in principe veel kanten op: de hoofdzakelijke geschiktheid kan zowel blijken uit de (kennelijke) bedoeling van de producent, als uit 'objectief vaststelbare' misbruikmogelijkheden die bovengeschikt zijn aan legitiem nevengebruik. Jurisprudentie heeft hier enigszins richting aan gegeven.[151] Een voorbeeld is een veroordeling van de Rechtbank Den Haag voor het voorhanden hebben van 'phishingprogrammatuur' die gericht was op het plegen van computervredebreuk, waarbij op een valse webpagina ingevoerde gegevens werden verwerkt en overgedragen om deze voor verdachte op te nemen. Het phishingprogramma werd daarbij gekwalificeerd als een hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen was voor het plegen van hacken. Daarbij heeft de verdachte ook onrechtmatig verworven DigiD-gegevens[152] voorhanden gehad, met het oogmerk om daarmee onrechtmatig te kunnen inloggen. Beide vormen van artikel 139d lid 2 waren dus van toepassing.[153] Met het verwerven van gegevens via het lokken van mensen naar gehackte webservers en het overnemen van de DigiD-gegevens was tevens sprake van een gekwalificeerde vorm van hacken (artikel 138ab lid 2 Sr).

De voorbereiding van gekwalificeerd hacken (artikel 138a lid 2-3 Sr) wordt in lid 3 aanzienlijk zwaarder bestraft. Het lijkt ons echter voor de praktijk lastig om bij een voorbereidingshandeling te bewijzen dat iemand het oogmerk heeft een *gekwalificeerde* vorm van computervredebreuk te plegen.[154] De minister geeft als voorbeeld een hackprogramma dat tevens ontworpen is om gegevens over te nemen en vast te leggen, waarmee het bewijs voor voorbereiding van artikel 138a lid 2 Sr in beginsel te leveren is.[155]

---

150 *Kamerstukken II* 2004/05, 30036 (R 1784), 3, p. 19.

151 Zie bijvoorbeeld ten aanzien van *banking* malware Hof Den Haag 24 januari 2017, ECLI:NL:GHDHA:2017:81 en Rb. Rotterdam 7 april 2017, ECLI:NL:RBROT:2017:2815, waarin verdachten zijn veroordeeld voor het voorhanden hebben van malware met het oogmerk om computervredebreuk te plegen.

152 Met DigiD kunnen burgers beveiligd (vertrouwelijk en geauthenticeerd) communiceren met de overheid.

153 Rb. Den Haag 13 mei 2015, ECLI:NL:RBDHA:2015:5525. In casu heeft de verdachte via lokmails (e-mails die lijken op valide berichten van de overheid) personen ertoe bewogen naar een DigiD-website te surfen met het uiteindelijke doel om onrechtmatig over gegevens te beschikken (zie ook paragraaf 2.10.1 over phishing). Om dit mogelijk te maken heeft de verdachte een script gebruikt dat is ondergebracht op een gehackte website. Deze scripts bevatten computerinstructies die zorgden voor de weergave van de nagemaakte phishingsite en instructies voor het ondervangen en doorsturen van vertrouwelijke gegevens naar een bepaalde persoon.

154 Zie ook Wiemans 2004b, p. 203, die sceptisch is over de gekwalificeerde vorm ("in de praktijk (vrijwel) nooit te bewijzen en daarmee overbodig geregeld").

155 *Kamerstukken I* 2005/06, 26671 en 30036, D, p. 14.

De strafmaat is (evenals bij artikel 139d lid 1 Sr, zie paragraaf 2.4.3) opmerkelijk: de *voorbereiding* van een computerdelict kan even zwaar worden bestraft als het computerdelict zelf, terwijl bij de algemene voorbereidingsstrafbaarstelling (artikel 46 Sr) de helft van het strafmaximum van het gronddelict geldt. De wetgever motiveert dit met de opmerking dat de computermisdrijfvoorbereiding op specifieke delicten slaat, terwijl artikel 46 Sr algemeen is, en dat hier oogmerk in plaats van het in artikel 46 Sr genoemde opzet (waaronder voorwaardelijk opzet) vereist is.[156]

De implementatie van artikel 6 Cybercrimeverdrag was enigszins onvolledig, omdat het misbruik van hulpmiddelen strafbaar stelde ten aanzien van hacken, verstikkingsaanvallen, aftappen en computersabotage, maar niet ten aanzien van verstoring van gegevens (artikel 350a Sr), terwijl dit wel onder de reikwijdte van artikel 6 Cybercrimeverdrag valt. De toelichting was op dit punt niet bijzonder overtuigend.[157] Bij de Richtlijnimplementatie in 2015 is dit deels gerepareerd, door invoering van artikel 350d Sr.[158] Dit artikel bevat een vergelijkbare bepaling als artikel 139d lid 2 Sr, maar dan met het oogmerk dat met de technische hulpmiddelen of wachtwoorden gegevensaantasting (artikel 350a lid 1 Sr) of computerverstoring (artikel 350c Sr) wordt gepleegd. Dit laatste onderdeel vervangt artikel 161sexies lid 2-oud Sr, dat meeverhuisd is met de verplaatsing van het eerste onderdeel van artikel 161sexies naar artikel 350c Sr. Het eerste onderdeel is echter opmerkelijk, in de zin dat het zich beperkt tot gegevensaantasting als bedoeld in artikel 350a lid 1 Sr en zich dus (nog steeds) niet uitstrekt ten aanzien van het ter beschikking stellen of verspreiden van kwaadaardige software. In de wetsgeschiedenis hebben wij voor deze beperking geen motivering kunnen vinden. Vermoedelijk is deze ingegeven door dezelfde gedachte als bij de Wet computercriminaliteit II, namelijk dat de strafbaarstelling van kwaadaardige software zelf al een voorbereidingshandeling betreft, te weten het beschikbaar stellen of verspreiden van zulke software, ongeacht of deze daadwerkelijk een computer infecteert of schade aanricht.[159] Maar aangezien artikel 350a lid 3 Sr beperkt is tot verspreiden en beschikbaar stellen, is het maken, verkrijgen voor gebruik, invoeren of het bezit van een programma om kwaadaardige software te maken (zoals een virus-*toolkit*), niet als zodanig strafbaar; het valt noch onder artikel 350a lid 3 Sr, noch onder artikel 350d Sr.[160] Het zou hooguit onder artikel 350d Sr kunnen vallen indien het oogmerk niet (alleen) het maken van een virus ter verspreiding is, maar (ook) het feitelijk aantasten van gegevens. Dat bete-

156 *Ibid*. In de visie van de minister (*ibid*.) is het maken van een hackprogramma, indien het oogmerk bestaat dit ook te gebruiken voor computervredebreuk, even strafwaardig als het plegen van computervredebreuk zelf.

157 De toelichting gaf aan dat artikel 350a lid 3 Sr (virusverspreiding) al een voorbereidingshandeling betreft, namelijk het verspreiden of beschikbaar stellen van virussen; *Kamerstukken II* 2004/05, 26671, 7, p. 36. Daarbij werd kennelijk gemakshalve voorbijgegaan aan het feit dat artikel 6 Cybercrimeverdrag ook de verkoop, het vervaardigen en andere voorbereidingshandelingen dan verspreiden of beschikbaar stellen omvat.

158 *Stb*. 2015, 165.

159 Zie noot 157.

160 Betoogd kan worden dat het valt onder artikel 139d lid 2 jo. artikel 138ab Sr, nu de rechtspraak het verspreiden van een virus ook wel als computervredebreuk kwalificeert; wij plaatsen echter vraagtekens bij deze interpretatie, zie noten 44-46 en bijbehorende tekst.

kent dat bewezen zal moeten worden dat iemand die een toolkit maakt of bezit, ook willens en wetens beoogt dat een daarmee gemaakt virus daadwerkelijk onrechtmatig een computer infecteert. Daarbij is dan ook de maximumstraf op deze voorbereiding (twee jaren gevangenis, artikel 350d Sr) de helft van de maximumstraf op de verspreiding van computervirussen (vier jaren gevangenis, artikel 350c lid 3 Sr); dat is weliswaar in lijn met de algemene lagere strafbedreiging voor voorbereiding, maar het wijkt af van de gehanteerde systematiek bij de strafbaarstelling van cybercrime-voorbereiding, waarbij dezelfde straf op voorbereiding als op het gronddelict staat. Hoewel wij niet willen pleiten voor een verdere uitbreiding van de strafbaarstelling van voorbereidingshandelingen, achten wij de beperking in artikel 350d Sr tot artikel 350a lid 1 Sr weinig systematisch.

2.8 Klassieke vermogensdelicten

2.8.1 *Diefstal en verduistering*

In de doctrine en wetsgeschiedenis is veel gediscussieerd over de vraag of (elektronische) gegevens kunnen worden beschouwd als een goed in de zin van de klassieke vermogensdelicten als diefstal (artikel 310 e.v. Sr) en verduistering (artikel 321 e.v. Sr). Hoewel een uitspraak van het Arnhemse Hof van 27 oktober 1983 dit wel aannam,[161] hebben wetsgeschiedenis en rechtspraak afdoende vastgesteld dat dit niet het geval is.[162]

Gegevens kunnen niet aan iemand toebehoren op de wijze waarop stoffelijke dingen dat wel kunnen, en daarom kunnen de delictsbestanddelen van de commune vermogensdelicten niet worden vervuld als gegevens worden gekopieerd. Gegevens kunnen slechts dan object van goederendelicten zijn wanneer sprake is van een twee-eenheid van de materiële drager en de daarmee verbonden inhoud of waarde; zo kan het aantasten van een bepaalde gegevensvastlegging zaakbeschadiging opleveren. Maar de gegevens als zodanig kunnen in beginsel geen voorwerp van vermogensdelicten zijn.

De Hoge Raad heeft dit beginsel bevestigd in zijn arrest van 3 december 1996,[163] conform de conclusie van A-G Fokkens. Hij overwoog dat computergegevens niet als 'enig goed' kunnen worden 'toegeëigend' in de zin van de Arubaanse verduisteringsbepalingen, die met ons artikel 321 Sr overeenkomen: "Immers, van een 'goed' als bedoeld in de hiervoor genoemde wettelijke bepalingen moet als een wezenlijke eigenschap worden beschouwd dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht erover verschaft. Computerge-

161 *NJ* 1984/80. In de casus werd een systeemanalist-programmeur die bij zijn werkgever programmatuur had gekopieerd en vervolgens daarmee op eigen houtje aan de slag ging, veroordeeld wegens verduistering. Het hof legde het begrip 'goed' in artikel 321 Sr zodanig uit dat het de gekopieerde gegevens omvatte. Het onrechtmatig kopiëren vervulde het bestanddeel van de wederrechtelijke toe-eigening. Zie daarover zeer kritisch Kaspersen 1990, p. 81, en Van Dijk & Keltjens 1995, p. 28 e.v.

162 Zie daarover nader paragraaf 1.4.2. Het arrest Hof Arnhem 31 maart 1994, *Computerrecht* 1994, p. 124-127, m.nt. Kaspersen, dat gewezen werd na de duidelijke keuze van de wetgever, is in dit licht onbegrijpelijk.

163 *NJ* 1997/574, m.nt. 't H.

gevens ontberen deze eigenschap". Dit behoefde overigens niet tot cassatie te leiden, omdat de Hoge Raad de bewezenverklaring buitengewoon welwillend las: aangezien bewezen was dat de verdachte zonder toestemming gegevens*dragers* van zijn baas had gebruikt, kon het hof de tenlastelegging aldus verstaan dat de verdachte zich opzettelijk wederrechtelijk een aantal dragers van computergegevens had toegeëigend. Terecht noemt annotator 't Hart deze redenering een kunststukje: "Naar mijn bescheiden mening is het de vraag of de bewezenverklaring op deze wijze niet minstens net zo ver wordt opgerekt als het begrip 'goed' indien men daaronder tevens computergegevens zou laten vallen". 't Hart plaatst ook een interessante rechtspolitieke kanttekening: "Indien de systeembeheerder (...) dragers van zijn werkgever gebruikt, zoals in de onderhavige zaak, kan als vluchtweg verduistering van die dragers gebezigd worden, ook al gaat het in feite om de gegevens zelf (...). Men krijgt zo een figuur die enige gelijkenis vertoont met vroegere vervolgingen voor joyriding, die – toen er nog geen specifieke strafbepaling in de Wegenverkeerswet was opgenomen – plaats vonden op grond van diefstal van benzine". Een oneigenlijke constructie, zo meent 't Hart terecht.
In het algemeen, behoudens dergelijke kunstgrepen, kan iemand die gegevens kopieert dus niet worden vervolgd voor verduistering of diefstal. Hoogstens kan er sprake zijn van schending van auteurs- of databankrechten of van geschriftenbescherming, of eventueel van een onrechtmatige daad.

Op deze regel bestaan echter twee uitzonderingen. De eerste is weinig omstreden: gegevens die wel onvoorwaardelijk voldoen aan de eigenschappen van uniciteit en directe geldelijke waardeerbaarheid, zoals giraal geld,[164] gelden wel als vermogensobject en kunnen dus worden gestolen of verduisterd. Het ligt voor de hand dat deze lijn wordt doorgetrokken naar elektronisch geld, waaronder cryptovaluta als bitcoins,[165] en elektronische waardepapieren zoals cognossementen.[166]
De tweede uitzondering is minder simpel. De Hoge Raad heeft in het *Runescape*-arrest van 2012 bepaald dat gegevens in de vorm van een virtueel amulet en masker in een online spel onder omstandigheden toch als goed kunnen worden aangemerkt en daarmee ook gestolen kunnen worden.[167] Indien de gegevens uniek zijn en een waardeerbare waarde vertegenwoordigen, kunnen de gegevens als goederen worden beschouwd

164 HR 11 mei 1982, *NJ* 1982/583, m.nt. 't H. Zie daarover Kaspersen 1990, p. 50-51. Deze auteur maakt wel bezwaar tegen de (impliciete) interpretatie van de Hoge Raad in een uitspraak over een vordering in een faillissement (HR 7 mei 1985, *NJ* 1986/198, m.nt. GEM), zie p. 60-61. Vgl. ook Groenhuijsen & Wiemans 1989, p. 68 e.v.

165 Op rechtspraak.nl zijn nog geen veroordelingen voor diefstal of verduistering van bitcoins gepubliceerd. Bitcoins worden echter in jurisprudentie eenvoudig behandeld als inbeslaggenomen voorwerpen in het kader van beslissingen in het kader van verbeurdverklaring of onttrekking aan het verkeer. Zie bijvoorbeeld Rb. Rotterdam 5 oktober 2016, ECLI:NL:RBROT:2016:7596 en Rb. Den Haag 22 december 2017, ECLI:NL:RBDHA:2017:15274. Het ligt dan ook voor de hand dat bitcoins en andere cryptovaluta zonder meer als goederen in de zin van de vermogensdelicten kunnen worden gekwalificeerd.

166 Een cognossement is een verhandelbaar waardepapier in het transport dat recht geeft op afgifte van een lading (zie artikel 8:916 e.v. BW). Dergelijke waardepapieren kunnen ook een elektronische vorm aannemen, zie Van Esch 2001.

167 HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (*Runescape*).

en daarmee worden 'weggenomen'; in casu was er sprake van diefstal met geweld, omdat de daders met fysiek geweld het slachtoffer hadden gedwongen in te loggen op zijn account en zij vervolgens het amulet en het masker overhevelden naar hun eigen account. Die 'waardeerbare waarde' hoeft niet economisch te zijn, maar kan ook subjectief zijn, zoals in casu het virtuele amulet en masker veel betekenden voor het jonge slachtoffer.[168]

Een bekritiseerd onderdeel van het arrest is de visie van de Hoge Raad dat de gegevens uniciteit kenden, in de zin van enkelvoudige beschikkingsmacht ('feitelijke en exclusieve heerschappij'). Het hof maakte de vergelijking met een paspoort, dat eigendom van de Staat maar in bezit van de burger is, en dat kan worden gestolen door het uit de beschikkingsmacht van de bezitter te halen; zo had het slachtoffer geen eigendom van het virtuele amulet of masker, maar raakte hij wel de beschikkingsmacht kwijt. Een verschil met het paspoort is echter dat de Staat niet rechtstreeks kan beschikken over het fysieke exemplaar, terwijl de aanbieder van een online spel wel direct kan beschikken over virtuele objecten; in die zin kent het paspoort wel 'exclusieve heerschappij', maar virtuele objecten die onderdeel zijn van een digitale (spel)omgeving niet – zowel de aanbieder als de speler kunnen tegelijkertijd direct over hetzelfde object beschikken, zodat het virtuele amulet zich meer als gegevens dan als goed gedraagt.[169] Ook zijn kanttekeningen geplaatst in verband met de spelcontext: de virtuele objecten zijn alleen gebruikt binnen de context van het spel en kunnen niet in een andere context worden gebruikt of verhandeld, wat ze anders van aard maakt dan elektriciteit of giraal geld.[170] Om deze reden wordt in de literatuur wel betoogd dat casusposities als de onderhavige beter bestreden kunnen worden door computervredebreuk of gegevensaantasting ten laste te leggen dan een vermogensdelict.[171]

Tegelijk met het *Runescape*-arrest is ook het zogenoemde 'belminuten-arrest' gewezen, waarin de verdachte een simkaart van iemand anders had gebruikt om daarmee te telefoneren. Het hof had de verdachte veroordeeld voor diefstal van belminuten en sms-berichten (waarbij we aannemen dat bedoeld is: diefstal van *het tegoed voor* sms-berichten). De Hoge Raad liet deze veroordeling in stand, omdat het hof de in de tenlastelegging gebruikte termen belminuten en sms-berichten mocht verstaan "in de economische betekenis die daaraan in het normale spraakgebruik wordt toegekend, te weten als gebruikseenheid om de daarmee aangeduide vormen van telecommunicatie-

168 Zie B.J. Koops, 'Virtuele en reële delicten. Een beschouwing over het *RuneScape*-arrest en computercriminaliteitswetgeving', *Computerrecht* 2013/4.

169 Koops 2013 en (over de uitspraak in eerste aanleg maar met dezelfde redenering) Moszkowicz 2009, p. 500-501. Hierbij moet wel worden aangetekend dat de gelijktijdige feitelijke beschikkingsmacht ook voor giraal geld geldt: zowel de bank als de rekeninghouder kan rechtstreeks over het geld beschikken. Een verschil met de online spelomgeving is dan weer dat de spelaanbieder rechtmatig van alles mag doen met het object (inclusief vernietigen), terwijl de bank niet rechtmatig in alle opzichten over het giraal geld mag beschikken. Zie ook Lodder 2013, die instemt met het oordeel van de Hoge Raad.

170 Koops 2013, Rozemond 2013 en Moszkowicz 2009.

171 *Ibid*. Zie ook Lastowka & Hunter 2005. Anders: Lodder 2013. In het 'belminuten-arrest' merkte de Hoge Raad ook "ten overvloede" op dat de casus ook viel onder artikel 326c Sr (r.o. 3.6), als subtiele hint dat voortaan dit type misbruik van telecommunicatie ook (of wellicht beter) met de daarop specifiek toegesneden bepaling ten laste gelegd kan worden.

dienstverlening te kunnen kwantificeren en in rekening te kunnen brengen".[172] Annotator Keijzer verheldert de uitspraak door onderscheid te maken tussen feitelijk gebelde minuten (G), in rekening gebrachte kosten voor gevoerde gesprekken (R) en beltegoed of vrije belminuten (V); alleen V-belminuten kunnen gelden als 'enig goed' in de zin van artikel 310 Sr, en deze kunnen ook worden 'weggenomen' door toe-eigening van een simkaart waardoor het vermogen tot bellen binnen de feitelijke macht van de verdachte en buiten de feitelijke macht van de rechthebbende komt.[173] Hoewel dit goed te volgen valt, en ook teleologisch wel verdedigbaar is, moet ook bij de *belminuten*-zaak de kanttekening worden geplaatst dat zowel rechter als annotator het begrip 'gegevens' (de *weergave* van feiten enzovoort) lijken te vereenzelvigen met de betekenis die aan de gegevens worden toegekend. Keijzer maakt een fraaie vergelijking door te zeggen dat belminuten "gegevens van een hogere orde [zijn]; zij verhouden zich tot computergegevens als bedoeld in dat arrest [HR 3 december 1996] als een schilderij tot verf".[174] Met andere woorden, het schilderij vertegenwoordigt een bepaalde economische waarde die verschilt van die van de gebruikte verf, en het is het toe-eigenen van deze economische waarde dat bestraft wordt. De vergelijking miskent echter dat bij diefstal van een schilderij nog steeds het toe-eigenen van het materiële object ten laste gelegd wordt (niet de fysieke verf maar wel het fysieke schilderij), evenals bij diefstal van een auto niet de wederrechtelijke toe-eigening van een hoeveelheid metaal, glas en stof ten laste gelegd wordt, maar diefstal van een auto. Het is niet de betekenis die in het maatschappelijk verkeer aan de auto of het schilderij wordt toegekend, dat de dief zich toe-eigent, maar het object zelf. In die zin kan alleen de *representatie* van beltegoed het object zijn van diefstal, niet het beltegoed zelf als abstract begrip. In dat licht vormt het *belminuten*-arrest juist een omkering van het *computergegevens*-arrest, waarin de Hoge Raad bepaalde dat gegevens niet, maar in casu de dragers wel, object konden zijn van verduistering; hier bepaalt de Hoge Raad dat het niet om de toe-eigening van de drager (de simkaart) gaat, maar om de toe-eigening van de gegevens die met behulp van de kaart worden gerepresenteerd.

Het Hof Den Haag rekte echter in zijn uitspraak[175] van 3 december 2015 volgens de Hoge Raad het begrip 'enig goed' te ver op, door te oordelen dat een kopie van een eindexamen als goed kan worden beschouwd. Het hof oordeelde daar dat een eindexamen, "zowel in stoffelijke vorm (afgedrukt op papier) als gefotografeerd en op een USB-stick geladen", individualiseerbaar is, een zekere economische waarde in het maatschappelijke verkeer vertegenwoordigt en kan worden overgedragen. De economische waarde zou blijken uit de omstandigheid dat de eindexamenopgaven daadwerkelijk zijn aangeboden, gekocht en via e-mail en USB-sticks zijn overgedragen. De Hoge Raad gaat hier niet in mee en stelt dat de digitale afbeeldingen van eindexamens geen goederen zijn die gestolen kunnen worden. Het is niet begrijpelijk dat het hof op de enkele grond dat de gefotografeerde examens "in het maatschappelijk verkeer een ze-

172 HR 31 januari 2012, ECLI:NL:HR:2012:BQ6575 (*belminuten*-arrest).
173 HR 31 januari 2012, ECLI:NL:HR:2012:BQ6575, *NJ* 2012/535, m.nt. Keijzer, § 4.
174 *Ibid*., § 9.
175 Hof Den Haag 3 december 2015, ECLI:NL:GHDHA:2015:3355.

kere economische waarde tot het moment van het examen" vertegenwoordigen, heeft geoordeeld dat sprake was van goederen ex artikel 416 Sr (opzetheling), mede gelet op de wetsgeschiedenis en het voornemen van de wetgever om te voorzien in een op gegevens toegespitste strafbepaling.[176]

Wanneer we – naast de duidelijke gevallen waarin gegevens volledige equivalenten zijn van (stoffelijk) geld, zoals giraal geld en bitcoins – proberen in al deze arresten een lijn te ontwaren, dan valt in elk geval te concluderen dat (elektronische) gegevens meestal niet, maar soms wel, een goed kunnen zijn in de zin van de vermogensdelicten. Dat is alleen het geval als ze een zekere waarde vertegenwoordigen in het maatschappelijk verkeer (in beginsel economisch, maar mogelijk ook gevoelswaarde) en vooral als ze uit de feitelijke beschikkingsmacht worden gehaald van de eerdere houder. Unieke feitelijke beschikkingsmacht lijkt niet vereist, wel dat degene uit wiens feitelijke macht de gegevens worden toegeëigend, de beschikkingsmacht verliest (wat bij het amulet en de belminuten het geval was, maar niet bij het examen).

Met deze conclusie valt een deel van Ten Voorde's wetssystematische kritiek te pareren op de zijns inziens onsystematische manier waarop de wetgever met de digitale vermogensdelicten is omgegaan. Deze kritiek betreft de benadering van de wetgever om bij oplichting, afpersing en afdreiging wel, maar bij diefstal en verduistering niet, gegevens en goederen gelijk te stellen. Dit leidt er onder andere toe dat bij oplichting en afpersing hetzelfde strafmaximum geldt ten aanzien van gegevens en goederen (zie daarover paragraaf 2.10.1), terwijl de wederrechtelijke toe-eigening van gegevens onder andere bepalingen moet worden gekwalificeerd (zoals artikel 138c of 139g Sr) met lagere strafmaxima dan diefstal of verduistering. "Hoe valt aan slachtoffers uit te leggen dat diefstal, heling en verduistering van gegevens die tot (groot) financieel nadeel hebben geleid worden beschouwd als misdrijven tegen de openbare orde die met een lager strafmaximum worden bedreigd dan hun 'equivalenten' in artikel 310, 416 en 321 Sr?"[177] Hoewel Ten Voorde een uitstekend overzicht biedt van de verschillende vermogensgerelateerde strafbaarstellingen, miskent hij in deze conclusie dat "diefstal (...) en verduistering van gegevens" wetstechnisch gezien alleen onder artikelen 310 en 321 Sr kunnen vallen, en dus hetzelfde strafmaximum kennen als diefstal en verduistering van goederen; voor zover de handelingen onder gegevens-gerelateerde delicten vallen, is er geen sprake van diefstal of verduistering van gegevens, maar van het wederrechtelijk aftappen of overnemen van gegevens. Dat bij dat laatste ook financieel nadeel kan ontstaan, is waar, maar één of twee jaar gevangenisstraf is een niet onaanzienlijke strafdreiging. Wat de conclusie van Ten Voorde echter vooral miskent, is dat als handelingen ten aanzien van gegevens groot financieel nadeel opleveren (vergelijkbaar met diefstal van vermogen), dit vrijwel alleen zo zal zijn in gevallen waarin de wederrechtelijk verkregen gegevens zelf geldswaarde vertegenwoordigen en de gegevens uit de beschikkingsmacht van het slachtoffer geraken. Zoals onze conclusie uit de rechtspraak

176 HR 10 oktober 2017, ECLI:NL:HR:2017:2573. Zie in deze zin ook Rb. Rotterdam 13 februari 2014, ECLI:NL:RBROT:2014:976, *Tijdschrift voor Internetrecht* 2014, nr. 3, p. 83-86, m.nt. J.S. Nan & B.W. Schermer.

177 Ten Voorde 2018, p. 641.

laat zien, zullen in die gevallen altijd (ook) de klassieke vermogensdelicten van toepassing zijn.[178] Ten aanzien van 'heling' van gegevens geldt dezelfde redenering: weliswaar kennen we nu feitelijk de figuur van 'heling van gegevens' (hoewel de wet zelf niet een zinsnede 'als schuldig aan gegevensheling' bevat) in artikel 139g Sr met een lager strafmaximum dan heling van goederen, maar als de handeling een vergelijkbare strafwaardigheid kent als heling van goederen waardoor een hogere gevangenisstraf dan één jaar op zijn plaats zou zijn, zal het vrijwel altijd gegevens betreffen die zelf als goed kunnen worden gekwalificeerd en waarbij dus artikel 416 e.v. Sr kan worden toegepast.
In deze zin lijkt er in de wettelijke benadering wellicht meer systeem te zitten dan in eerste instantie het geval lijkt, door de diverse manieren waarop gegevens en goederen al dan niet worden gelijkgesteld. Het uitgangspunt blijft dat gegevens en goederen verschillende concepten betreffen, maar dit beginsel sluit niet uit dat er een overlappend gebied is waarin gegevens voldoende vergelijkbare eigenschappen hebben als goederen om ze als goederen te kunnen behandelen. Hoewel dit overlappende gebied ten koste gaat van de eenvoud van een tweedeling, sluit het wel aan op de realiteit van de informatiemaatschappij waarin gegevens een steeds belangrijkere – ook vermogensrechtelijke – rol vervullen. Het overlapgebied maakt het mogelijk voor de rechtspraktijk om strafbepalingen te gebruiken die het meest recht doen aan de belangen die primair door een strafwaardige handeling zijn geschaad. Als gegevens zich gedragen als goederen en vooral een vermogensbelang is geschaad, kunnen de klassieke vermogensdelicten worden gehanteerd. Als echter vooral andere belangen – zoals de integriteit van computersystemen of de vertrouwelijkheid van gegevens – zijn geschaad, kunnen beter de gegevensgeoriënteerde bepalingen worden ingeroepen.

Los van deze discussie heeft de rechtspraak overigens nog bepaald dat het opnemen van geld bij een geldautomaat met behulp van een ontvreemde bankpas en bijbehorende pincode valt onder diefstal;[179] als de pincode ontbreekt, is er sprake van een poging tot diefstal – het gebruik van de bankpas door iemand die daartoe geen recht heeft, geldt als gebruik van een valse sleutel, ook zonder pincode.[180] Voorts valt ook het bedreigen met geweld van iemand die bij de geldautomaat staat om zijn pincode in te toetsen en het vervolgens wegnemen van het verschenen geld, onder diefstal met bedreiging met geweld.[181]

178 Vanzelfsprekend zijn er situaties denkbaar waarin groot financieel nadeel ontstaat door wederrechtelijke toe-eigening van gegevens zonder dat het gaat om gegevens die zich als goederen gedragen, maar dat geldt evengoed voor veel andere strafbepalingen waarbij groot financieel verlies kan ontstaan terwijl het strafmaximum lager is dan voor diefstal (bijvoorbeeld het culpoos vernielen van een Ming-vaas). Men kan in dat licht niet elke vorm van groot financieel verlies vergelijken met diefstal of verduistering.
179 HR 8 december 1992, *NJ* 1993/323.
180 HR 7 oktober 2003, nr. 2799.02, *Nieuwsbrief Strafrecht* 2003, 414.
181 HR 28 april 1992, *NJ* 1992/657.

2.8.2 *Heling van gegevens en bekendmaking van geheimen (artikel 139g, 273, 98 e.v. Sr)*

Omdat het helingsdelict in artikel 416 Sr is toegespitst op het helen van goederen en niet van gegevens, was een aparte strafbaarstelling van het helen van gegevens noodzakelijk. Bij de Wet computercriminaliteit III is in artikel 139g Sr tevens het 'helen' van gegevens strafbaar gesteld.[182] Strafbaar is a) het verwerven of voorhanden hebben en b) het aan een ander ter beschikking stellen, aan een ander bekend maken of uit winstbejag voorhanden hebben of gebruiken van niet-openbare gegevens, als men weet of redelijkerwijs moet vermoeden dat de gegevens door misdrijf zijn verkregen. De gedragingen onder a) zijn alleen strafbaar als men ten tijde van het verkrijgen van de gegevens had moeten vermoeden dat ze uit misdrijf afkomstig waren; als de verkrijger dit later verneemt, is deze niet strafbaar als deze de gegevens blijft bezitten. Dat is het wel het geval als hij ze vervolgens aan anderen doorgeeft, wat de gedraging onder b) oplevert. Op het helen van gegevens staat maximaal één jaar gevangenisstraf of een geldboete van de vierde categorie.
Het gaat hier bijvoorbeeld om cybermisdadigers die waardevolle gegevens voorhanden hebben of verder beschikbaar stellen, zoals bankrekeningnummers of wachtwoorden die eerder door misdrijf zijn verkregen.[183] Degene die door het misdrijf verkregen gegevens via internet openbaar maakt is op grond van deze bepaling strafbaar, maar niet de persoon die via internet openbaar gemaakte gegevens downloadt – in dat geval gaat het immers om openbare gegevens.
Met de strafbaarstelling wordt een voorziening getroffen voor de gevallen waarin iemand gegevens voorhanden heeft die zijn verkregen uit een misdrijf dat door een ander is begaan of waarin niet kan worden bewezen dat degene die de gegevens voorhanden heeft deze zelf door misdrijf heeft verkregen.[184] Wij verwachten overigens dat artikel 139g Sr, evenals de traditionele helingsartikelen, vaak aanzienlijke bewijsmoeilijkheden zal opleveren. Zo zal het niet gemakkelijk zijn om te bewijzen dat de verdachte ervan op de hoogte was of redelijkerwijs had moeten zijn dat de gegevens door misdrijf verkregen waren.[185]
In lid 2 van artikel 139g Sr wordt expliciet gemaakt dat degene niet strafbaar is die te goeder trouw heeft kunnen aannemen dat het algemeen belang de gedraging van het eerste lid vereiste. Daarmee wil de wetgever tot uiting brengen dat een hoger belang (bijvoorbeeld klokkenluiden) het delict kan rechtvaardigen. Bij de beslissing voor het vervolgen van het helen van niet-openbare gegevens moet dus expliciet rekening worden gehouden met conflicterende belangen: aan de ene kant het recht op een vrije

182 In 2009 had de wetgever al aan de Tweede Kamer toegezegd gegevensheling strafbaar te stellen (*Kamerstukken II* 2008/09, 28684, 232, p. 4).
183 *Kamerstukken II* 2015/16, 34372, 3, p. 62.
184 *Kamerstukken II* 2015/16, 34372, 3, p. 65.
185 Zie ook Koops 2010.

nieuwsgaring en aan de andere kant het recht op bescherming van gegevens.[186] Als richtsnoer voor het algemeen belang van de bekendmaking kunnen daarbij de civiele arresten omtrent onrechtmatige publicaties dienen, waarin criteria worden gegeven voor de afweging van enerzijds het belang van de samenleving bij de openbaarmaking van wantoestanden en anderzijds het belang van de particulier bij geheimhouding van hem betreffende gegevens.[187]

Bij de Wet computercriminaliteit was overigens al een bijzondere helingsbepaling ingevoerd ten aanzien van bedrijfsgegevens, in artikel 273 lid 1 onder 2 Sr. Strafbaar is het bekendmaken of uit winstbejag gebruiken van gegevens die door misdrijf (bijvoorbeeld hacken) zijn verkregen uit een geautomatiseerd werk van een onderneming van handel, nijverheid of dienstverlening. Voorwaarde is wel dat de gegevens betrekking hebben op de onderneming zelf, dat zij bij bekendmaking of gebruik nog niet algemeen bekend waren en dat uit het bekendmaken of gebruik enig nadeel kan ontstaan. De sanctie is maximaal zes maanden gevangenisstraf of een geldboete van de vierde categorie, even hoog als voor het bekendmaken van bedrijfsgegevens ten aanzien waarvan geheimhouding is opgelegd[188] (artikel 273 lid 1 onder 1° Sr). Evenals bij gegevensheling is het bekendmaken van bedrijfsgegevens niet strafbaar als iemand te goeder trouw kon aannemen dat dit in het algemeen belang was (artikel 273 lid 2 Sr). Artikel 273 Sr is sinds de Wet computercriminaliteit III ook van toepassing op de (ex-) werknemer die gegevensverzamelingen, zoals klantenbestanden, van zijn (ex-)werkgever meeneemt om daarmee zelfstandig een concurrerend bedrijf te beginnen, omdat hij de gegevens onrechtmatig heeft overgenomen en dus door misdrijf (artikel 138c Sr) heeft verkregen. Opvallenderwijs is de strafmaat op het wederrechtelijk overnemen (maximaal een jaar gevangenisstraf, artikel 138c Sr) echter hoger dan het uit winstbejag gebruiken van deze gegevens (artikel 273 lid 1 onder 2° Sr).

In artikel 273 Sr is al zichtbaar dat de strafbaarstelling van gegevensheling verwantschap vertoont met strafbaarstellingen van het publiceren van geheime gegevens. Terwijl heling van oudsher een klassiek vermogensdelict is (als complement van diefstal en verduistering), is gegevensheling eigenlijk meer een delict in de sfeer van de bescherming van geheimen: het beschermde rechtsgoed bij de artikelen 139g en 273 is niet zozeer (als bij heling) het eigendomsrecht, maar de vertrouwelijkheid van gegevens.[189] Aan die vertrouwelijkheid zit een zekere vermogenscomponent – niet-openba-

186 *Kamerstukken II* 2015/16, 34372, 3, p. 66-67. Daarbij wordt tevens verwezen naar HR 26 maart 2013, ECLI:NL:HR:2013:BY3752.

187 Zie bijvoorbeeld het standaardarrest HR 23 juni 1983, *NJ* 1984/801.

188 Geheimhouding behoeft niet te zijn overeengekomen, maar kan eenzijdig door de onderneming worden opgelegd. HR 14 januari 1935, p. 430 e.v. Bij bedrijfsgeheimen kan onder meer worden gedacht aan verkoopmethoden, cliëntenbestanden en productiewijzen.

189 Dat blijkt ook uit het feit dat artikel 139g Sr voorheen een strafbaarstelling bevatte van het openbaar maken van wederrechtelijk in besloten plaatsen gemaakte afbeeldingen; deze bepaling is bij de Wet computercriminaliteit III opgegaan in de algemenere strafbaarstelling van gegevensheling.

re gegevens kunnen immers geld waard zijn – maar het gaat toch primair om het beschermen van de vertrouwelijkheid van persoons- of bedrijfsgegevens als zodanig.
In dit verband past het hier ook om kort de strafbaarstelling van staatsgeheimen te noemen. De artikelen 98-98c Sr stellen een straf van maximaal zes tot vijftien jaren (of zelfs levenslang, artikel 98a lid 2 Sr) of geldboete van de vijfde categorie op het opzettelijk doorgeven aan ongerechtigden, het openbaar maken of het bemachtigen van inlichtingen of gegevens waarvan het staatsbelang (of dat van een bondgenoot) de geheimhouding vordert. Hetzelfde geldt voor voorwerpen waaraan zodanige inlichtingen kunnen worden ontleend. Onder de bepalingen vallen bijvoorbeeld ook computerprogramma's waarvan het staatsbelang de geheimhouding vordert, zoals beveiligingsprogrammatuur die voor defensie wordt gebruikt. Het niet-opzettelijk maar nalatig (culpoos) verspreiden van staatsgeheimen is strafbaar met hoogstens een jaar gevangenisstraf of geldboete van de derde categorie (artikel 98b Sr).

2.8.3 *Ondergrondse marktplaatsen, cryptovaluta en witwassen (artikel 420bis e.v. Sr)*

In 2011 gaf de eigenaar van het online drugsplatform 'Silk Road' een brutaal interview aan een Amerikaanse journalist. Hij schepte op over hoe drugs eenvoudig gekocht en verkocht konden worden via de virtuele munt bitcoin.[190] Het interview leidde tot wereldwijde aandacht voor het internetforum. Silk Road maakte een grote groei door, totdat de verdachte – tot dusver slechts bekend onder zijn nickname 'Dread Pirate Roberts' – door de FBI in 2013 werd aangehouden. De eigenaar, geïdentificeerd als Ross Ulbricht, ontving een klein percentage voor elke drugstransactie in bitcoins. In de 2,5 jaar dat het forum online was, heeft het forum volgens de Amerikaanse officier van justitie honderden miljoenen dollars aan omzet gehaald. De laptop van de verdachte bevatte 144.336 bitcoins met een toenmalige waarde van 28 miljoen dollar.[191] Ross Ulbricht werd tot een levenslange gevangenisstraf veroordeeld.
Sinds de opkomst en ondergang van Silk Road zijn er vele andere online marktplaatsen verschenen waarop drugs en andere illegale goederen en diensten worden aangeboden en verspreid.[192] Volgens een RAND-onderzoek waren er in 2016 ongeveer vijftig online marktplaatsen op het *dark web* beschikbaar.[193] Het *dark web* is dat gedeelte van internet waarvan de IP-adressen zijn verhuld, bijvoorbeeld door gebruik van het Tor-systeem (zie paragraaf 3.7.1). Via deze online marktplaatsen worden vooral drugs aangeboden, maar ook wapens en medicijnen. Uit het onderzoek bleek dat Nederlanders meer dan

190 Adrian Chen, 'The Underground Website Where You Can Buy Any Drug Imaginable', 1 juni 2011, http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 (laatst geraadpleegd 1 juli 2018).
191 U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 januari 2014, http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php (laatst geraadpleegd 1 juli 2018).
192 Zie bijvoorbeeld Europol, 'Exploring tomorrow's organised crime' (2015a) en het 'World Drug Report 2014'-rapport van de United Nations Office on Drugs and Crime.
193 Zie Kruithof e.a. 2016.

andere wereldburgers actief waren op deze *dark web*-forums en vooral handelden in XTC. Hierbij moet online drugshandel en witwassen wel in perspectief worden geplaatst:[194] de omvang van drugshandel en witwassen via internet lijkt nog steeds beperkt vergeleken met de omvang van drugshandel en witwassen in de fysieke wereld. In het RAND-onderzoek wordt bijvoorbeeld gesteld dat in 2016 de online drugshandel wereldwijd een omzet had van enkele honderden miljoenen euro's, terwijl de omvang van drugshandel in de fysieke wereld ongeveer € 24 miljard bedroeg.[195] Wel is in de gepubliceerde jurisprudentie een gestage stijging te vinden van veroordelingen voor drugshandel via online marktplaatsen op het *dark web*.[196]

Handel in illegale goederen is in Nederland strafbaar gesteld via de Opiumwet, de Wet wapens en munitie en andere bijzondere wetgeving. Daarop wordt hier verder niet ingegaan. Wat wel relevant is, is de strafbaarstelling van witwassen, in het bijzonder in combinatie met cryptovaluta zoals bitcoins. Net als bij drugshandel in de fysieke wereld, wordt bij online drugshandel ook opvallend vaak veroordeeld voor deelname aan een criminele organisatie en witwassen (artikel 420bis e.v. Sr).
Bij opzetwitwassen (artikel 420bis Sr) worden de versluierhandelingen (het verbergen of verhullen van de oorsprong), de plaatsingshandelingen (verwerven, voorhanden hebben, overdragen of omzetten) en de omzettingshandelingen (omzetten en gebruikmaken) van een voorwerp uit misdrijf verkregen, strafbaar gesteld. Op deze vorm van witwassen staat een maximumstraf van ten hoogste zes jaren of een geldboete van de vijfde categorie.
Een virtuele munt kan tevens als 'voorwerp' van witwassen worden beschouwd. In 2006 heeft de Hoge Raad ook wel aangenomen dat met valse Bahreinse dinars kan worden witgewassen, omdat de biljetten met reguliere gelden waren gekocht.[197] Daarom kan ook worden aangenomen dat met virtuele valuta als bitcoin kan worden witgewassen, omdat die tevens op geld waardeerbaar zijn en met reguliere valuta kunnen worden aangekocht.
Bij schuldwitwassen (artikel 420quater Sr, maximaal twee jaren gevangenisstraf) gaat het om de versluierhandelingen en verplaatsingshandelingen van een voorwerp, waarbij de verdachte redelijkerwijs moet vermoeden dat het voorwerp uit misdrijf afkomstig is. Bij gewoontewitwassen (artikel 420ter Sr) worden zwaardere strafmaxima van acht jaren gesteld voor degene die een gewoonte maakt van het plegen van witwas-

194 Zie bijvoorbeeld Europol 2015, 'Why is cash still king?', Den Haag, Europol 2016, 'An analysis of payment mechanisms used within cybercrime in the EU', Den Haag: Europol en het UNODC 2016, 'World Drug Report'.
195 Kruithof e.a. 2016, p. 44.
196 Zie bijvoorbeeld Rb. Noord-Nederland 15 oktober 2013, ECLI:NL:RBNNE:2013:6924, Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504, Rb. Midden-Nederland 22 oktober 2013, ECLI:NL:RBMNE:2014:4790 en ECLI:NL:RBMNE:2014:4792, Gerechtshof Arnhem-Leeuwarden 7 juli 2016, ECLI:NL:GHARL:2016:5563, Rb. Midden-Nederland 17 oktober 2017 ECLI:NL:RBMNE:2017:5217, Rb. Rotterdam 8 november 2017, ECLI:NL:RBROT:2017:8988 en Rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234.
197 HR 11 april 2006, ECLI:NL:HR:2006:AV2349.

sen.[198] Van belang is dat een veroordeling voor witwassen gepaard kan gaan met verbeurdverklaring (artikel 33 Sr). Dit betekent in concrete termen dat bijvoorbeeld een computer of andere gegevensdrager die virtueel geld bevat uit het bezit van de verdachte kan worden ontnomen, als witwassen kan worden bewezen.[199]
Voor witwassen in de zin van artikel 420bis Sr is in deze context vereist dat iemand de werkelijke aard, de herkomst, de vindplaats, de vervreemding of de verplaatsing van het (virtuele) geld verbergt of verhult, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf. Ook hij die een voorwerp verwerft, voorhanden heeft, overdraagt of omzet of van een voorwerp gebruikmaakt, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf, maakt zich schuldig aan opzetwitwassen in de zin van artikel 420bis Sr.

De vereiste verhullingshandeling bij witwassen leidde in het verleden wel eens tot problemen. Een zaak van de Rechtbank Rotterdam op 8 mei 2014 is daarvoor illustratief. Tijdens de huiszoeking bij de verdachte van drugshandel in XTC via internet werd een contant geldbedrag van € 82.900 aangetroffen, waarvoor de verdachte voor witwassen is veroordeeld. Ontslag van alle rechtsvervolging volgde echter voor een hoeveelheid van ongeveer 325 bitcoins op de bitcoinportemonnee op een USB-stick in het bezit van de verdachte. De desbetreffende officier van justitie schatte in dat de verdachte ongeveer € 160.000 had verdiend aan de handel van XTC op internet tegen betaling in bitcoins. Echter, omdat de USB-stick te vinden was op de eettafel van de verdachte en verder "niet gebleken [is] dat verdachte handelingen heeft verricht die erop neerkomen dat hij de aard, herkomst of vindplaats van de bitcoins heeft verhuld" (omdat hij ze moeilijk ergens anders kon bewaren dan in een bitcoin*wallet*) kon de rechtbank niet komen tot de kwalificatie van witwassen.[200]
De wetgever heeft in 2016 de witwaswetgeving aangepast teneinde het voorhanden hebben van uit misdaad verkregen gelden beter te kunnen bestraffen.[201] In artikel 420bis.1 Sr is enkel het verwerven of voorhanden hebben van een voorwerp dat onmiddellijk afkomstig is uit enig eigen misdrijf gekwalificeerd als eenvoudig witwassen, op straffe van een gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie. Als we de bovenstaande casus in aanmerking nemen, dan zou de verdachte vervolgd kunnen worden voor artikel 420bis.1 Sr.
Voor het vereiste dat de (virtuele) gelden afkomstig zijn uit illegale bron blijkt uit jurisprudentie dat met behulp van software zoals 'ChainAnalysis' kan worden bewezen dat de bitcoins afkomstig zijn uit online drugsmarktplaatsen.[202] Ook kunnen uit de jurisprudentie 'witwastypologieën' worden onderscheiden die van nut zijn voor de bewijs-

198 Zie Oerlemans e.a. 2016, p. 38-39.
199 Zie bijvoorbeeld Gerechtshof Arnhem-Leeuwarden 7 juli 2016, ECLI:NL:GHARL:2016:5563 en Rb. Noord-Holland 10 maart 2017, ECLI:NL:RBNHO:2017:1940.
200 Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504.
201 Wet van 23 augustus 2016, *Stb.* 2016, 313. Zie ook HR 13 december 2016, ECLI:NL:HR:2016:2842 en ECLI:NL:PHR:2016:1244 (Overzichtsarrest witwassen in verband met de Wet aanpassing witwasregeling).
202 Zie bijvoorbeeld Rb. Rotterdam 29 december 2017, ECLI:NL:RBROT:2017:10225 en Rb. Midden-Nederland, 24 januari 2018, ECLI:NL:RBMNE:2018:234.

voering voor witwassen. Denk daarbij aan een onredelijk hoge commissie[203] voor het omzetten van bitcoins in euro's, het bieden van absolute anonimiteit[204] aan klanten door bitcoinhandelaars en het gebruik van 'bitcoin mixers'[205] die de herkomst van de bitcoins verhullen. Ook kan een 'bitcoin-verweer' ter verklaring van het bezit van een grote hoeveelheid geld (namelijk dat de bitcoins gekocht waren toen de koers nog laag was en de koers sindsdien is geëxplodeerd) worden verworpen als de verdachte niet enigszins weet te staven dat hij de bitcoins destijds heeft aangekocht (bijvoorbeeld door duidelijk te maken in welke periode en bij welk bedrijf ze zijn gekocht, of inzage te geven in zijn *wallets*).[206]

2.9 Valsheid in geschrifte

2.9.1 *Valsheid in geschrifte met computers (artikel 225 e.v. Sr)*

Bij de computergerelateerde delicten is valsheid in geschrifte (artikel 225 Sr) van belang. Het bestanddeel 'geschrift' uit artikel 225 Sr komt ook voor in de delictsomschrijvingen van diverse uitingsdelicten. In een belangrijk arrest uit 1991 heeft de Hoge Raad uitgemaakt dat een weggeschreven computerbestand moet worden aangemerkt als een geschrift met bewijsbestemming in de zin van artikel 225 Sr.[207] In deze zaak ging het om fraude met een geautomatiseerde betalingenadministratie, in gebruik bij de gemeente Rotterdam.[208] De verdachte had het voor elkaar gekregen betalingsopdrachten te zijnen gunste aan een tussenbestand toe te voegen, met het gevolg dat deze als door de gemeente geautoriseerd werden uitgevoerd. Om ontdekking te voorkomen knoeide hij bovendien in het bestand van journaalposten, en bracht hij een deel van het gefraudeerde bedrag ten laste van een slapende rekening. De Hoge Raad moest de vraag beantwoorden of het genoemde tussenbestand, dat slechts een korte levensduur had en na verloop van tijd opging in andere bestanden, een geschrift met bewijsbestemming was in de zin van artikel 225 Sr. De Hoge Raad overwoog dat het hof mocht aannemen dat het bestand in kwestie bestond uit met voldoende duurzaamheid op een magneetschijf vastgelegde gegevens omtrent betalingsopdrachten die op tamelijk eenvoudige wijze leesbaar kunnen worden gemaakt. Dat het bestand een vluchtig karakter bezit en naar één of meer andere bestanden wordt weggeschreven, staat daaraan niet in de weg. Gezien het karakter van onmisbare schakel in het geheel van de geautomatiseerde ad-

203 Zie onder andere Rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234 en Rb. Midden-Nederland 10 april 2018 ECLI:NL:RBMNE:2018:1184.

204 Zie onder andere Rb. Rotterdam 8 november 2017, ECLI:NL:RBROT:2017:8988, Rb. Rotterdam 29 december 2017, ECLI:NL:RBROT:2017:10225 en Rb. Midden-Nederland 10 april 2018 ECLI:NL:RBMNE:2018:1184.

205 Zie over de werking van deze *mixing services* Van Wegberg, Oerlemans & Van Deventer 2017 en Rb. Noord-Holland 10 maart 2017, ECLI:NL:RBNHO:2017:1940, Rb. Midden-Nederland 17 oktober 2017, ECLI:NL:RBMNE:2017:5716, Rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234 en Rb. Midden-Nederland 10 april 2018, ECLI:NL:RBMNE:2018:1184.

206 Rb. Midden-Nederland 24 januari 2018, ECLI:NL:RBMNE:2018:234.

207 HR 15 januari 1991, *NJ* 1991/668, m.nt. C (*Rotterdamse computerfraude*).

208 Zie uitgebreid over deze zaak Kaspersen 1990, p. 126, en Van Dijk & Keltjens 1995, p. 129-133.

ministratie had het hof volgens de Hoge Raad eveneens de bewijsbestemming van het onderhavige geschrift kunnen aannemen.[209] Deze benadering past in de functionele rechtspraak van de cassatierechter over de bedrijfsadministratie: deze is in haar geheel te beschouwen als bestemd om te dienen tot bewijs van de daarin opgenomen gegevens, ook al valt niet aan ieder onderdeel daarvan afzonderlijk die bestemming toe te kennen.[210]
Verder valt ook het valselijk invullen van (bijvoorbeeld) een elektronisch aangifteformulier voor douaneheffingen in het kader van import van groenten binnen de Europese Unie (mede) onder artikel 225 Sr, ook als het elektronische formulier enige bewerkingen ondergaat voordat het in de administratie van de douane wordt opgenomen en zelfs als het in zijn oorspronkelijke vorm niet meer reproduceerbaar is. Het is voldoende dat blijkt dat het ooit heeft bestaan, al is het maar voor korte tijd, en dat het bestand (toen het bestond) eenvoudig toegankelijk te maken was.[211] Ook het onbevoegd gebruik van een elektronische handtekening zal valsheid in geschrifte opleveren, indien het ondertekende document een bewijsbestemming heeft (wat meestal het geval zal zijn bij elektronisch ondertekende documenten).[212]
Uit de rechtspraak valt af te leiden dat artikel 225 Sr even goed toepasbaar is op elektronische als op papieren bestanden: de vereisten dat het document leesbaar gemaakt moet kunnen worden en enige duurzaamheid moet hebben, zijn eenvoudig te vervullen bij de meeste elektronische bestanden. De belangrijkste vraag voor kwalificatie zal dan ook zijn of het onderhavige elektronische bestand een bewijsbestemming had; die vraag is contextafhankelijk en verschilt evenmin fundamenteel van de bewijsvraag bij fysieke documenten.

Tot slot zijn er diverse gekwalificeerde vormen van valsheid in geschrifte, met name voor geld-gerelateerde geschriften, zie artikel 226 Sr. Denkbaar is dat elektronisch geld en elektronische waardepapieren – die uit de aard der zaak ook uniciteit moeten hebben – hieronder kunnen vallen. Een specifieke strafbaarstelling is ook ingevoerd voor valsheid met gegevens: het, anders dan door valsheid in geschrifte, opzettelijk verstrekken van onware gegevens in het kader van subsidieverlening is strafbaar met ten hoogste vier jaren gevangenisstraf of geldboete van de vijfde categorie (artikel 227a Sr). Een vergelijkbare strafbaarstelling geldt voor het opzettelijk niet tijdig verstrekken van ge-

209 Kaspersen heeft dit onderdeel van het arrest bekritiseerd. Hij acht het 'gevaarlijk' dat een bestand waaraan in het maatschappelijk verkeer zelf geen bewijsbestemming wordt toegekend, niettemin dezelfde juridische bescherming krijgt. Terecht wijst hij er echter ook op dat het bestand ten behoeve van de interne controle wel degelijk een bewijsbestemming had. Zie H.W.K. Kaspersen, noot onder het besproken arrest in *Computerrecht* 1991, p. 206 e.v.

210 HR 29 mei 1984, *NJ* 1985/6. Zie voor een gespiegelde casus HR 10 april 2007, ECLI:NL:HR:2007:AZ6130 (de groslijsten waaraan gegevens op het computerscherm door de kasbeheerder behoren te worden gecontroleerd, hebben een bewijsbestemming).

211 HR 24 maart 1998, *Nieuwsbrief Strafrecht* 1998/5, nr. 67, p. 92.

212 Zie *Kamerstukken II* 2000/01, 27743, 3, p. 5: "Wat het strafrecht betreft kan worden opgemerkt dat het onbevoegd gebruik maken van een elektronische handtekening niet afzonderlijk is strafbaar gesteld. Onder omstandigheden is het echter denkbaar dat onbevoegd gebruik van een handtekening het delict valsheid in geschrifte op kan leveren".

gevens die men verplicht is te verstrekken in de context van subsidieverlening (artikel 227b Sr).[213]
Belangrijk is ook dat de wetgever, als uitvloeisel van het Europese kaderbesluit voor niet-chartaal geld, de strafbare voorbereidingshandelingen in artikel 234 Sr heeft uitgebreid (zie ook paragraaf 2.9.2), waarbij 'gegevens' zijn ingevoegd als strafbaar hulpmiddel. Daardoor is ook bijvoorbeeld strafbaar het vervaardigen, voorhanden hebben en overdragen van computerprogramma's waarvan men weet dat die bestemd zijn voor het namaken van reischeques, betaalcheques, wissels of aandelen.[214]

2.9.2 *Valsheid in geschrifte met (betaal)passen (artikel 232 en 234 Sr)*

Een speciaal geval van valsheid in geschrifte is het vervalsen van betaalpassen of waardekaarten (artikel 232 Sr). Hoewel het vervalsen van betaalpassen of waardekaarten in principe onder valsheid in geschrifte valt (een betaalpas dient meestal tot bewijs van bepaalde feiten en is ook voldoende duurzaam), heeft de wetgever er in 1993 voor gekozen om hiervoor een aparte strafbepaling in het leven te roepen. Dit maakt ondubbelzinnig duidelijk dat elk vervalsen van een pas of kaart waarmee kan worden betaald strafbaar is (artikel 232 lid 1 Sr, maximaal zes jaren gevangenisstraf of geldboete van de vijfde categorie). Net als bij valsheid in geschrifte is ook het opzettelijk gebruiken en, sinds 2000,[215] het opzettelijk afleveren of voorhanden hebben van een valse pas of kaart strafbaar (lid 2).
Met 'betaalpas' wordt bedoeld een persoonsgebonden pas voor het verrichten van betalingen langs elektronische weg, zoals een bankpas of een kredietkaart. Een 'waardekaart' is niet persoonsgebonden en kan door iedereen worden gebruikt, zoals een kopieerkaart, chipknip of anonieme OV-chipkaart.[216] Het vervalsen van passen om tankpunten of Airmiles te sparen is door de Hoge Raad en door lagere rechtbanken aangemerkt als de vervalsing met een betaalpas of waardekaart.[217]
De Wet computercriminaliteit II heeft de strafbaarstelling uitgebreid tot allerlei magneet- en chipkaarten, ter bescherming van het maatschappelijk vertrouwen in dit soort kaarten. Het gaat dan om betaalpassen, waardekaarten "of enige andere voor het pu-

213 Wet concentratie strafbaarstelling frauduleuze gedragingen, *Stb.* 2000, 40. De niet-opzettelijke varianten van deze delicten zijn strafbaar als overtreding (artikel 447c en 447d Sr).
214 *Stb.* 2004, 180.
215 *Stb.* 2000, 40.
216 Zie *Kamerstukken II* 1989/90, 21551, 3, p. 20-21: "Onder betaalpassen wordt verstaan elk voorwerp dat op naam van een bepaalde persoon is gesteld en is ingericht om uitsluitend door hem te kunnen worden gebruikt voor financiële transacties langs geautomatiseerde weg. (...) Onder waardekaarten wordt verstaan elk voorwerp waarvan langs geautomatiseerde weg een zeker geldsbedrag kan worden afgeschreven, evenwel zonder dat deze kaart aan een bepaalde persoon is gebonden".
217 HR 20 april 1999, *NJ* 1999/471 en Rb. Zutphen 1 juli 2003, ECLI:NL:RBZUT:2003:AH9507.

bliek beschikbare[218] kaart of een voor het publiek beschikbare drager van identificerende persoonsgegevens, bestemd voor het verrichten of verkrijgen van betalingen of andere prestaties langs geautomatiseerde weg".[219] Ook bijvoorbeeld zorgpassen met medische gegevens vallen onder de strafbaarstelling. Verder is nu ook het opzettelijk afleveren of voorhanden hebben van valse kaarten strafbaar, als men weet (of moet vermoeden) dat deze bestemd zijn voor misbruik.

Anders dan bij valsheid in geschrifte is echter sinds 2004 ook via artikel 232 lid 2 Sr niet alleen het gebruiken of ter misbruik afleveren of voorhanden hebben, maar ook het ontvangen, zich verschaffen, vervoeren, verkopen en overdragen van valse kaarten strafbaar, als uitvloeisel van het Europese kaderbesluit betaalmiddelenfraude.[220] In lijn met de tendens van strafbaarstelling van voorbereiding zijn daarbij ook voorbereidingshandelingen tot het vervalsen van kaarten zelf strafbaar gesteld in artikel 234 Sr.[221] Daardoor is ook bijvoorbeeld strafbaar het vervaardigen, voorhanden hebben en overdragen van computerprogramma's waarvan men weet dat die bestemd zijn voor het namaken van betaalpassen.

Beide artikelen zijn in de jurisprudentie regelmatig van toepassing verklaard op het 'skimmen' van betaalkaarten. Met het plaatsen van speciale apparatuur (skimapparatuur) is het mogelijk om rekeninggegevens van een betaalpas (en met aanvullende apparatuur of programmatuur ook pincodes) over te nemen. Deze gegevens kunnen later worden gebruikt om geld van de rekening van een ander op te nemen. De Rechtbank Haarlem overwoog daarbij dat het plaatsen van skimapparatuur reeds een uitvoeringshandeling is van het vervalsen van betaalpassen, en dus niet een voorbereidingshandeling onder artikel 234 Sr is maar een (poging tot) vervalsing onder artikel 232 Sr.[222] Dat geldt ook voor het losschroeven van een pinautomaat in een Ikea-filiaal en het branden van een gat in de behuizing daarvan; naar hun uiterlijke verschijningsvorm zijn deze

218 In de literatuur is kritiek geuit op de beperking tot "voor het publiek beschikbare" passen, omdat ook passen die in besloten kring worden gebruikt (zoals toegangspassen voor werknemers van een groot bedrijf) uitgerust kunnen worden met bijvoorbeeld een chipknip waarmee ook buiten het bedrijf kan worden betaald, waardoor het maatschappelijk vertrouwen in chipkaarten evenzeer in het geding kan zijn. Koops & Schellekens 1999, p. 1768-1769. De minister vindt echter in een dergelijke casus het maatschappelijk vertrouwen minder in het geding; het is de verantwoordelijkheid van de werkgever ervoor te zorgen dat vervalsing niet loont, bijvoorbeeld door het laadbare bedrag beperkt te houden, zie *Kamerstukken II* 2004/05, 26671,10, p. 31 (onze voetnoot).

219 De tekst uit *Stb.* 2006, 300 is verbeterd in de Reparatiewet II Justitie, *Stb.* 2006, 24. De vroegere term 'identiteitsgegevens' is bij Wet van 12 maart 2014, *Stb.* 2014, 125 vervangen door 'identificerende persoonsgegevens'.

220 *Stb.* 2004, 180. Kaderbesluit: *PbEG* 2001, L 149.

221 *Stb.* 2004, 180. Opmerkelijk is overigens dat het kaderbesluit een beveiligingseis stelt, als aanmoediging voor aanbieders om betaalinstrumenten te beveiligen (vergelijkbaar met de vroegere keuze van de Nederlandse wetgever bij computervredebreuk, zie paragraaf 2.3.2); de Nederlandse wetgever heeft aangegeven dit niet te willen overnemen, zodat ook onbeveiligde betaalkaarten strafrechtelijk beschermd blijven tegen namaken en bedrieglijk gebruik (*Kamerstukken II* 2002/03, 29025, 3, p. 4).

222 Rb. Haarlem 3 november 2010, ECLI:NL:RBHAA:2010:BO2789: "Het aanwenden van dergelijke apparatuur met het oog op het verkrijgen van de pincode en de op een valse betaalkaart te plaatsen gegevens vormt evenwel een handeling die aan de verwerving en het voorhanden hebben ervan voorbijgaat en moet dan ook worden aangemerkt als een – begin van – uitvoering van het proces dat strekt tot het valselijk opmaken van betaalpassen".

handelingen kennelijk gericht op de voltooiing van het vervalsen van betaalpassen en dus een strafbare poging.[223]

2.9.3 *Identiteitsfraude (artikel 231a en 231b Sr)*

Naast valsheid in geschrifte en valsheid met gegevens is ook valsheid met biometrische kenmerken strafbaar gesteld. In 2014 zijn de artikelen 231a en 231b Sr ingevoerd.[224] Artikel 231a Sr stelt strafbaar, in gevallen waarin biometrie wordt gebruikt voor identiteitsvaststelling, de vervalsing (lid 1) of het vals gebruik (lid 2) van biometrische kenmerken of biometrische persoonsgegevens om de eigen identiteit te verhelen of de identiteit van een ander te verhelen of misbruiken, met een maximumgevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie. Dit betreft bijvoorbeeld het vervalsen van de in een paspoort opgenomen vingerafdrukken, of het gebruik van een vliesje om de vinger met iemands nagemaakte vingerafdruk, om toegang te krijgen tot een beveiligd deel van een gebouw of computersysteem. (Afhankelijk van de scherpte en controlemechanismen van de sensor kunnen nagemaakte biometrische kenmerken er wel of niet in slagen het systeem te foppen; als het systeem toegang weigert omdat een nepvinger wordt gesignaleerd, zal een strafbare poging ten laste gelegd kunnen worden.) Ook het laten uitvoeren van plastische chirurgie om het gezicht op dat van een ander te doen lijken en zodoende met een gestolen paspoort van een lookalike te kunnen rondreizen, zal strafbaar zijn onder artikel 231a Sr, evenals het laten veranderen van de vingers om bij biometrische controles niet herkend te worden als een eerder geregistreerd persoon. Gelukkig heeft de wetgever wel verzekerd dat het lichamelijke zelfbeschikkingsrecht belangrijk is en plastisch chirurgische ingrepen 'op zichzelf' niet strafbaar worden; dat is alleen het geval indien de ingrepen een biometrie-omzeilend doel hebben.[225]
Dit is niet alleen van toepassing op financiële identiteitsfraude, maar ook op zogenoemde criminele identiteitsfraude, dat wil zeggen het gebruik van biometrie van een ander "met het oogmerk om de verdenking van een strafbaar feit op de ander of niet op hem te doen ontstaan". Dit kan het geval zijn als een werknemer zich toegang verschaft tot een biometrisch beveiligd deel van het computersysteem van een bedrijf om een bedrijfsgeheim te verkrijgen, en daarbij de vingerafdruk van een collega gebruikt om de verdenking op die collega te laden. Ook het rondstrooien van iemands haren of bloeddruppels bij een inbraak om de verdenking te laden op een andere, in de DNA-databank bekende, inbreker, valt hieronder, zo blijkt uit de toelichting.[226] Kennelijk is de wetgever van mening dat dan sprake is van een geval waarin biometrie wordt gebruikt ter identiteitsvaststelling, ook al hebben lichaamssporen op een bepaalde plaats niet als zodanig een functie ter identiteitsvaststelling.

223 HR 26 april 2013, ECLI:NL:HR:2013:BZ8635.
224 *Stb*. 2014, 125.
225 *Kamerstukken II* 2011/12, 33352, 3, p. 22.
226 *Kamerstukken II* 2011/12, 33352, 3, p. 24.

Artikel 231b Sr stelt op vergelijkbare wijze strafbaar het wederrechtelijke gebruik van iemands identificerende, niet-biometrische persoonsgegevens, met het oogmerk van identiteitsverhulling of misbruik, waardoor uit dat gebruik enig nadeel kan ontstaan. In de toelichting wordt als voorbeeld van misbruik van de identiteit van een ander in een online context genoemd het geval dat iemand op naam van een ander en zonder diens instemming een account aanmaakt en vervolgens op dat account die ander in een kwaad daglicht stelt waardoor deze reputatieschade lijdt.[227] De maximumstraf is met vijf jaren iets lager dan bij biometrische identiteitsfraude.
Met betrekking tot computercriminaliteit zijn de strafbaarstellingen relevant voor het misbruik van biometrische of identificerende gegevens van anderen voor de registratie voor online diensten. In 2017 werd bijvoorbeeld een verdachte veroordeeld voor oplichting en identiteitsfraude onder artikel 231b Sr, omdat deze de frauduleus verkregen paspoortgegevens van een persoon had gebruikt om een account aan te maken op marktplaats.nl om via deze online handelsplaats toegangskaartjes te kopen.[228]
Door het noemen van artikelen 231a en 231b in artikel 234 Sr zijn ook voorbereidingshandelingen strafbaar, zoals het voorhanden hebben van hulpmiddelen om biometrie na te maken in de wetenschap dat deze middelen bestemd zijn om identiteitsfraude te plegen.

2.10 Oplichting

2.10.1 *Oplichting, afpersing en afdreiging (artikel 326, 317 en 318 Sr)*

Oplichting is, eenvoudig gezegd, het iemand door valse middelen bewegen om iets af te staan. Wanneer iemand door dwang wordt bewogen iets af te staan, bijvoorbeeld door middel van dreiging (bijvoorbeeld met geweld), is er sprake van afpersing of afdreiging. Het verschil tussen deze twee delicten is dat afpersing gebeurt door geweld of dreiging met geweld, terwijl afdreiging plaatsvindt door dreiging met smaad of het bekendmaken van een geheim. Deze handelingen zijn strafbaar gesteld in verschillende strafbepalingen, die over het algemeen onafhankelijk zijn van de techniek. Veel situaties waarin oplichting of afpersing met behulp van computers plaatsvindt vallen dan ook onder de traditionele strafbepalingen.
Internetoplichting komt veel voor. Bij het Landelijk Meldpunt Internetoplichting (LMIO) van de politie zijn in 2015 meer dan 35.000 aangiftes van internetoplichting binnengekomen. Daaruit bleek dat de gedupeerden gemiddeld voor € 200 werden opgelicht. Het meldpunt geeft aan dat een verschuiving waarneembaar is van internetop-

227 *Kamerstukken II* 2013/14, 33352, C, p. 4-5.
228 Rb. Midden-Nederland 24 februari 2017, ECLI:NL:RBMNE:2017:904. Zie ook Rb. Overijssel 20 oktober 2016, ECLI:NL:RBOVE:2016:4065 en Rb. Rotterdam 28 oktober 2016, ECLI:NL:RBROT:2016:10262 en Rb. Den Haag 8 februari 2018, ECLI:NL:RBDHA:2018:1355.

lichting via online handelsplaatsen, zoals Marktplaats, naar fraude via sociale media, zoals Facebook.[229]

Internetoplichting is vaak strafbaar op grond van de algemene strafbepaling voor oplichting in artikel 326 Sr. Bij oplichting moet iemand – met het oogmerk om zichzelf of een ander wederrechtelijk te bevoordelen – door het aannemen van een valse naam of een valse hoedanigheid, of door "listige kunstgrepen" of door een "samenweefsel van verdichtsels", worden bewogen tot het afgeven van een goed of het ter beschikking stellen van gegevens, tot het aangaan van een schuld, of tot het kwijtschelden van een schuld van iemand anders.[230] Het delict wordt met een maximumstraf van vier jaren[231] of een geldboete van de vijfde categorie gesanctioneerd. Volgens rechtspraak valt ook het onbevoegd opnemen van geld met een bankpas en pincode onder "bewegen tot afgifte".[232]

Daarnaast is sinds 2009 door de clausule "het ter beschikking stellen van gegevens" ook het door nep-e-mails of -websites listig aftroggelen van financiële gegevens – phishing – als oplichting strafbaar.

GESCHIEDENIS

Omdat gegevens niet onder het begrip 'goed' vallen, werd aan artikel 326 Sr bij de Wet computercriminaliteit toegevoegd het afgeven van "gegevens met geldswaarde in het handelsverkeer". Dezelfde toevoeging is gedaan bij afpersing (artikel 317 Sr) en afdreiging (artikel 318 Sr). Met dit begrip wordt bedoeld gegevens die verhandelbaar zijn op de (legale) markt, zoals adressenbestanden of programmatuur. Gegevens die alleen op de zwarte markt verhandelbaar zijn, zoals via phishing ontfutselde pincodes, wachtwoorden of kredietkaartnummers, vallen echter niet onder dit begrip. Het onvrijwillig (na dreiging met geweld) noemen van een pincode kon volgens de Hoge Raad dan ook niet worden gezien als afgifte in de zin van artikel 317.[233] In 2004 is de zinsnede "met geldswaarde in het handelsverkeer" komen te vervallen in artikel 317 Sr.[234] De reden hiervoor was dat, "hoewel het kaderbesluit op zichzelf niet vereist dat afpersing van een pincode strafbaar wordt gesteld," het past, gelet op de ratio van het kaderbesluit van fraudebestrijding, "de strafbepaling betreffende afpersing zodanig te wijzigen, dat ook

229 Zie Politie.nl, 'Internetoplichter schuift naar social media', 27 mei 2016, https://www.politie.nl/nieuws/2016/mei/26/internetoplichter-schuift-naar-social-media.html (laatst geraadpleegd 1 juli 2018).

230 Zie HR 20 december 2016, ECLI:NL:HR:2016:2892, *NJ* 2017/158, m.nt. N. Keijzer voor een overzichtsarrest over oplichting; in het op dezelfde dag gewezen overzichtsarrest ECLI:NL:HR:2016:2889 werden de algemene beschouwingen toegepast op online handelsfraude in de vorm van het onder valse naam en hoedanigheid aanbieden maar niet leveren van iPhones via marktplaats.nl.

231 De maximumstraf is in 2006 verhoogd van drie naar vier jaren, *Stb.* 2006, 11.

232 HR 19 november 1991, *NJ* 1992/124. Overigens kan de gedraging ook worden gekwalificeerd als diefstal door middel van valse sleutels, HR 8 december 1992, *NJ* 1993/323. Het geld ontlokken aan een speelautomaat door telkens een munt aan een draad langs een schakelaar in het apparaat te bewegen, valt evenwel niet onder oplichting, zie HR 24 september 1991, *NJ* 1992/123; de gedraging zou volgens de conclusie van Meijers gekwalificeerd moeten worden als diefstal.

233 HR 13 juni 1995, *NJ* 1995/635.

234 *Stb.* 2004, 180.

het onder bedreiging van geweld iemand te dwingen een pincode te noemen, strafbaar wordt".[235] De wijziging beperkte zich echter om onduidelijke redenen tot afpersing (artikel 317 Sr).[236] Pas in 2009 werd (en passant in een antiterrorismewet) de zinsnede "met geldswaarde in het handelsverkeer" ook geschrapt in de artikelen 318 Sr (afdreiging) en 326 Sr (oplichting); sindsdien is phishing als zodanig strafbaar.[237]

Ten Voorde heeft kritiek geuit op de gelijkschakeling van gegevens en goederen in de oplichtingsdelicten. Hierdoor worden de beschermde belangen diffuser, omdat bij de bescherming van gegevens niet primair het vermogensbelang maar eerder belangen van privacy en informatiebeveiliging spelen. Deze pluraliteit van belangen roept vragen op over de duidelijkheid en toepasbaarheid van de artikelen.[238]
De kritiek van Ten Voorde snijdt hout waar het de mogelijke vervaging van de beschermde belangen betreft. Door het laten vervallen van de zinsnede "met geldswaarde in het handelsverkeer" is het vermogensbelang uit het zicht verdwenen ten faveure van meer algemene belangen van vertrouwelijkheid van gegevens. De wetswijziging betekent dat bijvoorbeeld ook het met listige kunstgrepen verleiden van een medestudent tijdens een tentamen tot het ter beschikking stellen van het antwoord op vraag 3, oplichting oplevert. Zelfs het slinks verleiden van een vriend om het telefoonnummer van zijn in stilte aanbeden zus door te geven, kan als oplichting worden gekwalificeerd, als we aannemen dat het oogmerk om deze zus vervolgens te kunnen bellen wederrechtelijk voordeel oplevert (bijvoorbeeld ten opzichte van andere stille aanbidders die haar niet kunnen bereiken omdat ze haar nummer geheim houdt). Voor dergelijke ontfutselingen van geheime informatie zijn de oplichtingsdelicten volgens ons – en naar wij aannemen Ten Voorde – niet bedoeld. Onzes inziens is het daarom van belang om bij de interpretatie van oplichting, afpersing en afdreiging vooral de wetsgeschiedenis voor ogen te blijven houden: de wetgever heeft specifiek bedoeld om phishing te bestrijden en vergelijkbare vormen van het wederrechtelijk in handen krijgen van pincodes en andere vooral financieel gerelateerde gegevens. De artikelen moeten dan ook met name worden ingezet ter bestrijding van financiële identiteitsfraude, waardoor het vermogensbelang in deze strafbaarstellingen onverkort op de voorgrond kan blijven staan.

In de praktijk wordt regelmatig voor phishing vervolgd.[239] Het verspreiden van phishing-berichten of pagina's zelf kan, ook zonder dat mensen erin trappen, worden

235 *Kamerstukken II* 2002/03, 29025, 3, p. 7.
236 Zie Koops & Wiemans 2005, wijzend op de omissie in artikel 326 Sr ten aanzien van phishing.
237 *Stb.* 2009, 245.
238 Ten Voorde 2018, p. 642.
239 Zie bijvoorbeeld Rb. Amsterdam 3 mei 2013, ECLI:NL:RBAMS:2013:CA2296, Rb. Noord-Holland 21 oktober 2013, ECLI:NL:RBNHO:2013:9735, Rb. Amsterdam 6 februari 2014, ECLI:NL:RBAMS:2014:1445, Rb. Amsterdam 24 januari 2017, ECLI:NL:RBAMS:2017:392, Hof Den Haag 21 februari 2017, ECLI:NL:GHDHA:2017:384. Phishing kan zowel elektronisch, telefonisch als per post plaatsvinden. Zie uitgebreid Leukfeldt & Jansen 2016.

vervolgd als poging tot oplichting.[240] Indien de financiële of persoonsgegevens niet worden verkregen door listen maar door (dreiging met) geweld of het bekendmaken van een geheim, kan dit vallen onder afpersing (artikel 317 Sr, maximaal negen jaren gevangenisstraf of geldboete van de vijfde categorie) respectievelijk afdreiging (artikel 318 Sr, maximaal vier jaren gevangenisstraf of geldboete van de vijfde categorie). Bij de Wet computercriminaliteit is nog een tweede lid aan artikel 317 Sr toegevoegd, waarin ook afpersing strafbaar wordt gesteld die plaatsvindt door dreiging dat opgeslagen computergegevens worden vernietigd of ontoegankelijk worden gemaakt. Dit maakt ondubbelzinnig duidelijk dat de dwang van afpersing ook kan plaatsvinden door dreiging met gegevensbeschadiging.[241]
Een andere verschijningsvorm van online fraude is de zogenoemde *click fraud*, waarbij botnets worden gebruikt om de besmette computers massaal internetadvertenties te laten bezoeken en deze advertenties (die in eigen beheer zijn opgezet) voor het aantal 'clicks' te laten uitbetalen.[242] Ons zijn geen gevallen bekend waarin daders zijn veroordeeld onder artikel 326 Sr voor click-fraude.[243]

2.10.2 *Oplichting met telecommunicatiediensten (artikel 326c Sr)*

Bij de Wet computercriminaliteit is een vorm van oplichting strafbaar gesteld die specifiek betrekking heeft op telecommunicatiediensten: artikel 326c lid 1 Sr. Op het delict staat een maximumstraf van vier jaren gevangenisstraf of geldboete van de vijfde categorie. Dit betreft het gebruiken van een publiek beschikbare telecomdienst door een technische ingreep of met valse signalen, met het oogmerk om daarvoor niet (volledig) te betalen. Hierbij kan gedacht worden aan het kraken van betaal-tv,[244] of aan *phone freaking*, waarbij iemand door een technische ingreep kan bellen zonder gesprekskosten of op rekening van iemand anders. In jurisprudentie is zelfs het enkele bellen met iemands toestel zonder diens toestemming gekwalificeerd onder artikel 326c Sr als het gebruikmaken van een vals signaal, wellicht omdat het in casu om dure 0909-nummers ging, en de wetgever met de strafbepaling niet alleen telecomaanbieders maar ook nietsvermoedende derden heeft willen beschermen.[245]
In lid 2 en 3 van dit artikel zijn ook voorbereidingshandelingen strafbaar gesteld. Dit betreft het openlijk ter verspreiding aanbieden, ter verspreiding voorhanden hebben of uit winstbejag maken of bewaren van middelen die het misdrijf uit het eerste lid mo-

240 Zie ook Koops & Wiemans 2005.
241 Opmerkelijk in dit licht is dat in Rb. Breda 30 januari 2007, ECLI:NL:RBBRE:2007:AZ7266 de dreiging met een ddos-aanval gekwalificeerd is als poging tot afpersing door bedreiging met geweld in plaats van (de ook in de tenlastelegging genoemde) bedreiging dat gegevens ontoegankelijk zouden worden gemaakt.
242 Zie uitgebreid Hogben 2011.
243 Wel zijn personen veroordeeld voor het ophogen van de 'cost per click' in gehackte accounts van online adverteerders, om de via die gehackte accounts verspreide advertenties voor hun eigen namaakwebshops zichtbaarder te maken; dit leverde strafbare gegevensaantasting (artikel 350a Sr) op. Zie Rb. Den Haag 22 december 2017, ECLI:NL:RBDHA:2017:15272, 15274 en 15275.
244 Zie HR 8 juli 2008, ECLI:NL:HR:2008:BC9192 met betrekking tot het kraken van het betaal-tv-kanaal Canal+.
245 Rb. Zutphen 1 maart 2010, ECLI:NL:RBZUT:2010:BL6030.

gelijk maken – denk aan het aanbieden op internet van programma's of decoders die betaal-tv kraken.
In de rechtspraak werd het uit winstbejag bewaren van apparatuur om telefoonkaarten op te waarderen bestraft op basis van artikel 326c lid 2 Sr, ook al is de apparatuur niet rechtstreeks een hulpmiddel voor het plegen van het feit van lid 1 maar slechts indirect via – eenvoudig te maken – valse telefoonkaarten.[246] Het publiceren van een artikel met een stappenplan voor het plegen van telecomfraude werd eveneens bestraft op basis van artikel 326c lid 2: de Hoge Raad vernietigde een vrijsprekend arrest van het Hof, onder verwijzing naar de ratio van de strafbaarstelling zoals hij die eerder[247] had opgevat en weergegeven. Het hof had het begrip 'gegevens' gezien die ratio te beperkt uitgelegd.[248]

2.10.3 *Online handelsfraude (artikel 326d Sr)*

Met de Wet computercriminaliteit III is artikel 326d Sr ingevoerd. Met deze bepaling moet het eenvoudig worden om op te treden tegen online handelsfraude, ook wel 'marktplaatsoplichting' of 'marktplaatsfraude' genoemd, naar de meest voorkomende vorm. Volgens de wetgever is het slechts beperkt mogelijk om tegen deze vorm van oplichting op te treden met het delict oplichting of flessentrekkerij.[249] Het aanbieden van goederen of diensten via internet zonder de intentie om te leveren, is niet zonder meer strafbaar als oplichting. Daarvoor is vereist het aannemen van een valse naam of hoedanigheid, listige kunstgrepen of een samenweefsel van verdichtsels. In 2014 heeft de Hoge Raad geoordeeld dat het zich in strijd met de waarheid voordoen als bonafide verkoper in combinatie met het verstrekken van onbruikbare contactgegevens aan een wederpartij het aannemen van een valse hoedanigheid en oplichting oplevert. Maar de enkele omstandigheid dat iemand in strijd met de waarheid zich voordoet als bonafide verkoper, en wel in staat is en voornemens is om te leveren maar dit vervolgens niet doet, levert op zichzelf geen valse hoedanigheid in de zin van artikel 326 Sr op. Daarvoor is méér nodig, zoals het opzettelijk hanteren van foute namen en e-mailadressen om de mogelijkheden tot verhaal te bemoeilijken.[250]

246 HR 15 april 2003, ECLI:NL:HR:2003:AF3372, *Computerrecht* 2003/5, p. 318-323, m.nt. Kaspersen.
247 *Ibid.*
248 HR 29 maart 2005, ECLI:NL:HR:2005:AS4663. Vgl. de conclusie van A-G Machielse, die verwijst naar de wetsgeschiedenis, artikel 80quinquies, het Europees Verdrag inzake de wettelijke bescherming van diensten die op voorwaarde toegankelijk zijn (Raad van Europa 24 januari 2001), alsmede naar de bijna identieke Richtlijn 98/84/EG. Al deze regelingen indiceren een ruime uitleg van artikel 326c lid 2 Sr. Zie echter ook het tegengestelde oordeel van Kaspersen in zijn noot bij de uitspraak in eerste aanleg, Rb. Haarlem (politierechter) 16 januari 2003, *Computerrecht* 2003/2, p. 154-156, m.nt. Kaspersen. Volgens hem gaat het vooral om computergegevens en -codes, niet om papieren tekst (waarvoor de wetgever liever het begrip 'inlichtingen' gebruikt). In deze interpretatie wordt de reikwijdte van de strafbare voorbereidingshandeling wel érg ver opgerekt.
249 Flessentrekkerij is het zich bij herhaling schuldig maken aan het kopen van goederen zonder van plan te zijn daarvoor te betalen (artikel 326a Sr).
250 HR 11 november 2014, ECLI:NL:HR:2014:3144.

Met artikel 326d Sr wordt strafbaar gesteld het maken van een beroep of gewoonte van het door middel van een geautomatiseerd werk verkopen van goederen of verlenen van diensten tegen betaling, met het oogmerk om die goederen of diensten niet (volledig) te leveren maar wel zichzelf of een ander te verzekeren van betaling. Voor dit delict moet bewezen worden dat een beroep of gewoonte wordt gemaakt van het leveringsloos verkopen van goederen of diensten. Hiervoor is gekozen om tot uitdrukking te brengen dat niet tegen ieder geval van internetfraude strafrechtelijk moet worden opgetreden, maar vooral tegen grootschalige vormen ervan. In de praktijk zullen private partijen in de eerste plaats fraude bestrijden; waar het echt noodzakelijk is, zal het Openbaar Ministerie optreden.[251] Daarbij kan gebruikt worden gemaakt van gebundelde aangiften van private partijen.
Voor een gewoonte is vereist het meermalen verrichten van gelijksoortige feiten, waarbij de pluraliteit niet slechts toevallig is maar de feiten onderling in zeker verband staan qua aard van de feiten en psychische gerichtheid van de dader. Dit kan ook aan de orde zijn wanneer gedurende een korte tijd een groot aantal afzonderlijke transacties via een website of meerdere websites plaatsvindt, zonder de intentie om het aangeboden goed of dienst te leveren. Eenmalig te koop aanbieden valt er (vanzelfsprekend) niet onder.[252]

2.10.4 *Koersmanipulatie (artikel 334 Sr)*

Verder zijn ook speciale vormen van oplichting denkbaar met ICT als hulpmiddel. In 2003 werd een relatief weinig gebruikte bepaling – het verspreiden van leugenachtige berichten om aandelenkoersen te beïnvloeden (artikel 334 Sr) – toegepast op iemand die geprobeerd had via een discussieforum op een webpagina koersen te manipuleren; aangezien de forumdeelnemers zich hier niets van aantrokken, bleef het bij een strafbare poging.[253] Tot in cassatie voerde de verdachte het verweer dat de berichten feitelijk juist en dus niet leugenachtig waren; het hof en de Hoge Raad concludeerden echter, onzes inziens terecht, dat het verzwijgen van cruciale informatie (namelijk dat de verdachte zelf verantwoordelijk was voor de grote aan- en verkopen waarop hij wees in zijn bericht als indicatie van een aanstaande koersstijging) leugenachtigheid opleverde.[254] In die zin ziet artikel 334 dus niet alleen op het belang van 'nothing but the truth', maar ook op 'the whole truth', in het kader van koersgevoelige informatie.
In 2014 heeft het Hof Den Haag overwogen dat – in verband met de Libor-fraude van de Rabobank waarvoor een boete werd opgelegd van € 70 miljoen – de valse vermelding van rentetarieven in spreadsheets moet worden opgevat als gedaan met het oog-

251 *Kamerstukken II* 2015/16, 34372, 3, p. 75.
252 *Kamerstukken II* 2015/16, 34372, 3, p. 92.
253 Rb. Amsterdam 3 juli 2003, ECLI:NL:RBAMS:2003:AH9509, *Computerrecht* 2003/5, m.nt. Kaspersen, p. 316-318.
254 HR 6 februari 2007, ECLI:NL:HR:2007:AY6713.

merk om de trader te bevoordelen in de zin van artikel 334 Sr.[255] De advocaat-generaal betoogde dat de spreadsheet is aan te merken als het leugenachtige bericht, waardoor er valse Liborfixings tot stand kwamen. Verder had de handeling tot oogmerk dat de prijzen van fondsen en geldswaardig papier zouden stijgen of dalen. Het hof was het eens met de advocaat-generaal op dit punt.

2.11 Computergerelateerde zedenmisdrijven

Vóór het grootschalig gebruik van internet vonden zedenmisdrijven *offline* plaats en werd het vastgelegd materiaal, zoals kinderporno, voornamelijk in blaadjes via de post verspreid. Internet heeft nieuwe vormen van zedenmisdrijven mogelijk gemaakt en faciliteert de verspreiding van afbeeldingen en video's op een grote schaal. Ook maakt internet rechtstreeks (seksueel) contact op afstand mogelijk. De wetgever heeft hier eerder op ingespeeld door aanpassingen van het delict inzake kinderporno en de introductie van het delict grooming, terwijl rechters vormen van webcamseks soms als bepaalde bestaande zedenmisdrijven hebben gekwalificeerd. De wetgever is tevens voornemens een nieuwe titel 'seksuele misdrijven' in het Wetboek van Strafrecht te introduceren, waarbij nadrukkelijk aandacht zal zijn voor "nieuwe onlinefenomenen", zoals grooming, sexting en *sexchatting*.[256]
In deze paragraaf worden de huidige zedenmisdrijven in relatie tot ICT besproken. Dit zijn respectievelijk: kinderpornografie (paragraaf 2.11.1), grooming (paragraaf 2.11.2), webcamseks met minderjarigen (paragraaf 2.11.3), *sextortion* (paragraaf 2.11.4) en wraakporno (paragraaf 2.11.5).

2.11.1 *Kinderpornografie (artikel 240b Sr)*

Strafbaarstelling algemeen
Kinderpornografie is één van de meest voorkomende vormen van cybercrime in Nederland als naar het aantal gepubliceerde zaken wordt gekeken. De wijdverbreide beschikbaarheid van kinderporno uit zich ook in het grote aantal afbeeldingen dat verdachten in hun bezit hebben. Het bezit van honderdduizenden en zelfs een enkele keer miljoenen kinderpornografische afbeeldingen komt geregeld voor in de jurisprudentie.[257]
In artikel 240b Sr is strafbaar gesteld degene die een afbeelding – of een gegevensdrager, bevattende een afbeelding – van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van 18 jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrok-

255 Hof Den Haag 19 mei 2015, ECLI:NL:GHDHA:2015:1204. Het ging hier om een artikel 12-procedure, waarbij Rabobankklanten hadden geklaagd over de manier waarop het OM de zaak had afgedaan; het hof wees deze klacht af.
256 Zie Ten Voorde 2017 voor een overzicht van alle mogelijke strafbepalingen.
257 Rb. Rotterdam 9 december 2009, ECLI:NL:RBROT:2009:BK6022, Rb. Den Haag 13 maart 2013, ECLI:NL:RBDHA:2013:2872, Hof Den Haag 22 april 2012, ECLI:NL:GHSGR:2012:BW0675, Rb. Oost-Brabant 4 januari 2017, ECLI:NL:RBOBR:2017:71 en Rb. Rotterdam 31 maart 2017, ECLI:NL:RBROT:2017:2445.

ken, 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. Daarbij kan een maximumstraf worden opgelegd van vier jaren of geldboete van de vijfde categorie. Indien daarvan een beroep of gewoonte wordt gemaakt, is de maximumstraf ten hoogste acht jaren (lid 2).
Bij een 'seksuele gedraging' kan het ook gaan om een afbeelding die op zichzelf niet expliciet seksueel van aard is, maar die gelet op de wijze waarop de afbeelding tot stand is gekomen in het concrete geval onmiskenbaar strekt tot het opwekken van seksuele prikkeling.[258] Het kan daarbij gaan om een bepaalde houding of pose van de jeugdigen, maar ook om het inzoomen op de genitaliën van minderjarigen.[259]
De leeftijdsgrens is in 2002 verhoogd van 16 naar 18 jaar, mede gelet op de norm die wordt gehanteerd in het Cybercrimeverdrag.[260] Het begrip 'kennelijk' in "kennelijk de leeftijd van 18 jaar nog niet heeft bereikt" heeft een belangrijke functie in bewijstechnische zin: het bewijs van de leeftijd van de afgebeelde minderjarige zal vaak moeilijk of niet te leveren zijn, zeker als de identiteit niet bekend is. De leeftijd behoeft door de opneming van het woord 'kennelijk' niet te worden bewezen; zij moet worden geschat. Dat kan betekenen dat veroordeeld kan worden terwijl de afgebeelde persoon in feite 18 jaar of ouder is.[261]

Verspreiding
Het bestanddeel 'verspreiden' wordt in de rechtspraak ruim uitgelegd. Voor verspreiding is ten minste voorwaardelijk opzet vereist. Het enkele doorgeven van een digitale afbeelding via e-mail aan één persoon is verspreiden, "nu onder verspreiden ook zeer wel kan worden verstaan het vergroten van de kring van degenen, die kennisnemen van deze afbeeldingen. Dat geldt in de visie van het Hof zeker als het gaat om het downloaden van bepaalde afbeeldingen van – het min of meer vrij toegankelijke – internet en het via diezelfde weg doorsturen naar een andere persoon".[262] Ook het ter beschikking stellen van URL's die doorzenden naar een internetpagina met daarop kinderpornografisch materiaal wordt gekwalificeerd als de verspreiding van kinderpornografie.[263]
Lastiger is de vraag of het enkele aanbieden van kinderporno in bijvoorbeeld een *peer-to-peer* netwerk valt onder verspreiden. De Rechtbank Den Haag besliste in 2006 dat het enkele feit dat de mogelijkheid bestond dat anderen via internet kinderpornografi-

258 HR 7 december 2010, ECLI:NL:HR:2010:BO6446.
259 *Kamerstukken II* 1994/95, 23682, 5, p. 9-11. Zie ook HR 10 juni 2014, ECLI:NL:HR:2014:1359. Zie uitgebreid Aanwijzing kinderpornografie (artikel 240b), *Stcrt.* 2016, 19415.
260 Wet partiële wijziging zedelijkheidswetgeving, *Stb.* 2002, 388.
261 Ook het omgekeerde geval kan zich voordoen. Zie hierover de nota 'Bestrijding seksueel misbruik van en seksueel geweld tegen kinderen', *Kamerstukken II* 1998/99, 26690, 2, p. 28-29.
262 Hof 's-Hertogenbosch 23 november 2001, *Nieuwsbrief Strafrecht* 2002, nr. 19.
263 Rb. Amsterdam 23 juli 2012, ECLI:NL:RBAMS:2012:BX2325, r.o. 4.4.8. De rechtbank oordeelde daarnaast ook dat het feit dat "[d]e URLs zijn aangetroffen in de chatlog die verdachte bewaarde op de VMware van zijn computer" eveneens tot het bezit van kinderporno van de onderliggende afbeeldingen leidt.

sche bestanden van verdachtes computer zouden kunnen binnenhalen nog niet het voltooide delict van verspreiden van kinderporno oplevert.[264] Volgens de rechtbank moet daarbij komen dat anderen daadwerkelijk gebruik hebben gemaakt van de mogelijkheid (waarvan de verdachte zich bewust was) om uit de gedeelde, niet afgeschermde map op verdachtes computer afbeeldingen te downloaden. Wanneer dat niet is gebeurd, is er geen sprake van 'verspreiden'. Wel is er sprake van voorwaardelijk opzet gericht op poging. Andere rechtbanken toetsen echter niet of het materiaal daadwerkelijk door anderen is gedownload.[265] Het is duidelijker dat van verspreiding sprake is indien het gaat om een gesloten *peer-to-peer* netwerk (ook wel 'friend-to-friend'-netwerk genoemd). Zo achtte de Rechtbank Haarlem bijvoorbeeld de verspreiding van kinderporno bewezen, omdat de verdachte gebruikmaakte van een gesloten *peer-to-peer filesharing*-netwerk, waarbij bestanden aan door hem zelf gekozen en toegevoegde contactpersonen werden verspreid. De verdachte had daarvan op de hoogte moeten zijn, nu hij een account heeft aangemaakt op [netwerk] en via dit computerprogramma bestanden heeft gedownload.[266]

In bezit hebben

In het verleden was niet het bezit (voor zichzelf) als zodanig strafbaar, maar enkel het "in voorraad hebben" van kinderpornografie, wat suggereerde dat het gaat om bezit met het oog op verspreiding aan anderen. De Hoge Raad heeft echter eind jaren negentig van de vorige eeuw uitgemaakt dat het bestanddeel 'in voorraad hebben' mede bestrijkt het bezit van een enkele afbeelding, ook als het gaat om één of meer afbeeldingen voor privégebruik.[267] Er behoefde dus geen sprake te zijn van een bestemming tot verspreiding. Bij de wet van 13 juli 2002 is dit geëxpliciteerd in de wettekst door "in voorraad heeft" te vervangen door "in bezit heeft".

Toch gaat veel jurisprudentie over de vraag of een computergebruiker opzet heeft gehad op het bezit van kinderpornografie.[268] Het in bezit hebben dient daarbij opzettelijk te geschieden, op zijn minst in voorwaardelijke zin. Voor voorwaardelijk opzet is in deze context vereist dat de verdachte zich willens en wetens heeft blootgesteld aan de aanmerkelijke kans kinderpornografisch materiaal in zijn bezit te krijgen en te hebben.[269] Dat is niet (per se) het geval bij een computer die aantoonbaar buiten de beschikkingsmacht van de verdachte is geweest (bijvoorbeeld als deze ook in gebruik is

264 Rb. 's-Gravenhage 17 november 2006, *NJFS* 2007, 24.

265 Zie bijvoorbeeld Hof 's-Hertogenbosch 5 oktober 2005, ECLI:NL:GHSHE:2005:AU4032 en Rb. Den Haag 13 maart 2013, ECLI:NL:RBDHA:2013:2872.

266 Rb. Noord-Holland 6 november 2014, ECLI:NL:RBNNE:2014:5488.

267 HR 21 april 1998, *NJ* 1998/782, m.nt. 't H.

268 Zie bijvoorbeeld Rb. Den Haag 4 april 2011, ECLI:NL:RBSGR:2011:BR4524, Rb. Zeeland-West-Brabant 24 juni 2013, ECLI:NL:RBZWB:2013:6323, Rb. Oost-Brabant 24 december 2013, ECLI:NL:RBOBR:2013:7088, Rb. Noord-Holland 23 april 2014, ECLI:NL:RBNHO:2014:3705, Rb. Noord-Holland 23 oktober 2015, ECLI:NL:RBNNE:2015:6139, Hof Den Haag 22 november 2016, ECLI:NL:GHDHA:2016:3702, Rb. Amsterdam 26 januari 2017, ECLI:NL:RBAMS:2017:537.

269 Zie bijvoorbeeld Rb. Zwolle-Lelystad 9 februari 2010, ECLI:NL:RBZLY:2010:BM0070.

bij personeel en echtgenote) en de link tussen de verdachte en het materiaal op de computer niet kan worden bewezen.[270]

De vraag of er sprake is van opzet op het bezit is in het bijzonder aan de orde als, bij computers die wel duidelijk toewijsbaar zijn aan de verdachte, uit digitaal forensisch onderzoek blijkt dat de afbeeldingen zijn verwijderd van de harde schijf van de verdachte, maar met forensische software daar toch sporen van worden gevonden. De sporen zelf constitueren niet per definitie opzet op het bezit van kinderpornografie, maar zijn wel als een aanwijzing te beschouwen dat iemand zich bezig heeft gehouden met kinderporno. Slechts als het maar om enkele plaatjes met kinderporno gaat en er geen enkele aanwijzing is dat de verdachte actief heeft gezocht naar kinderporno, is er geen sprake van bezit wegens het ontbreken van het element opzet.[271] In de kern komt het erop neer dat opzet moet blijken uit de *actieve bemoeienis* met kinderporno van de computergebruiker.[272] Indien er bewust op zoek is gegaan naar kinderpornografie, dan wordt het bezit daarvan doorgaans aangenomen.[273] Is er incidenteel of per ongeluk geklikt op een link en kwam men op een kinderpornowebsite terecht, dan wordt opzet door de computergebruiker niet aangenomen. Voor deze groep geldt volgens Stevens en Koops 'niet strafbaar, tenzij'. Zodra de verdachte meer bemoeienis met kinderporno lijkt te hebben dan incidenteel, slaat de standaard al snel om naar 'strafbaar, tenzij'.[274]

Stevens en Koops geven in hun overzichtsartikel over het opzettelijk bezit van kinderpornografie een aantal factoren weer waarmee rechters rekening kunnen houden: de computerkennis van de verdachte, het aanwezig zijn van speciale programmatuur voor het wissen en tevoorschijn halen van bestanden, het aantal kinderpornobestanden op de harde schijf en de tijdsduur tussen het downloaden, bekijken en weggooien van de bestanden.

In veel zaken is echter duidelijk dat er opzet op bezit is, vanwege het hoge aantal afbeeldingen. Dat levert een ander probleem op in verband met de belasting voor de opsporingsinstanties om alle afbeeldingen te beschrijven. In de praktijk wordt de gegevensdrager daarom ook wel met automatische software doorzocht en gematcht met reeds bekende kinderporno.[275] In de tenlastelegging wordt vervolgens steeds vaker gewerkt met een 'collectiescan' die een representatief beeld geeft van de totaal onderzochte collectie beeldmateriaal. Het Openbaar Ministerie verwerkt deze strafbare elementen vervolgens in de tenlastelegging. De tenlastelegging dient een voldoende concrete beschrijving te bevatten van de collectiescan of de vindplaats van die beschrijving moet in het dossier worden vermeld. Daarnaast wordt in een zogenoemde 'toonmap' een beperkte maar representatieve hoeveelheid strafbaar materiaal aan de procesdeelne-

270 Hof Den Bosch 25 april 2017, ECLI:NL:GHSHE:2017:1786.

271 Zie Stevens & Koops 2009, p. 684.

272 Stevens & Koops 2009, p. 695. Zie ook Hof Den Haag 18 januari, ECLI:NL:GHDHA:2013:BZ9494, *Computerrecht* 2013, nr. 5, p. 265-268, m.nt. J.J. Oerlemans.

273 Zie bijvoorbeeld HR 11 september 2007, ECLI:NL:HR:2007:BA6316, Rb. Groningen 28 januari 2008, ECLI:NL:RBGRO:2008:BC3529 en HR 30 september 2008, ECLI:NL:HR:2008:BD4872 en Rb. Rotterdam 22 maart 2016, ECLI:NL:RBROT:2016:2166.

274 Stevens & Koops 2009, p. 691.

275 Zie ook Aanwijzing kinderpornografie (artikel 240b), *Stcrt.* 2016, 19415.

mers beschikbaar gesteld om eventueel in te zien.[276] De Hoge Raad heeft de geldigheid van deze manier van werken in enkele overzichtsarresten bevestigd.[277]

Toegang verschaffen

Met de toenemende mogelijkheden van (breedband)internet om real-time video's te bekijken, heeft een zekere verschuiving plaatsgevonden in de markt voor kinderpornografie: in plaats van het downloaden en op de eigen computer bekijken, werd steeds meer kinderpornografie online bekeken. Het online bekijken van kinderpornografie valt echter niet onder in bezit hebben (voor zover de bekeken afbeeldingen niet ook worden opgeslagen in bijvoorbeeld de map *temporary Internet files*). Omdat het online bekijken van kinderpornografie echter evenzeer de markt voor kinderporno in stand houdt als het downloaden ervan, is het van belang ook deze gedraging strafbaar te stellen.

In 2009 is door de implementatie van het verdrag van Lanzarote[278] artikel 240b Sr aangepast met de toevoeging dat ook (eenvoudig gezegd) het toegang verschaffen tot kinderporno door middel van een computer of via internet strafbaar is.[279] Sinds deze uitbreiding is dus ook het *realtime* naar kinderporno kijken op internet zonder sporen achter te laten op de harde schijf, strafbaar. Vereist is daarbij wel dat er een actieve handeling is gevoerd gericht op het verkrijgen van toegang, waarmee het opzet op de toegangsverschaffing bewezen kan worden geacht.[280] De actieve handeling uit zich bijvoorbeeld in de betaling voor een website waar kinderporno op te vinden is, maar ook door te klikken op een link waarvan de naam een indicatie geeft dat het om kinderporno gaat.[281]

Sexting

Bij kinderpornografie maakt het niet uit of het materiaal door de afgebeelde minderjarige zelf of door een ander is vervaardigd.[282] Dit betekent dat in beginsel ook gevallen van *sexting*, het doorsturen van naaktfoto's van zichzelf naar een ander, onder de strafbaarstelling van artikel 240b Sr vallen. Dit werpt de vraag op of het wel wenselijk is om jongeren te vervolgen in de context van sexting. Het Openbaar Ministerie vindt een vervolging voor kinderpornografie in die gevallen vaak te zwaar. In 2016 is daarom gestart met het doorsturen van pubers naar bureau Halt voor dit gedrag.[283]

276 Zie Aanwijzing kinderpornografie (artikel 240b Sr), *Stcrt.* 2016, 19415.
277 HR 20 december 2011, ECLI:NL:HR:2011:BS1739, *NJ* 2012/147, HR 24 juni 2014, ECLI:NL:HR:2014:1497, *NJ* 2014/339 en HR 17 november 2015, ECLI:NL:HR:2015:3322.
278 Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, Lanzarote, 25 oktober 2007, *Trb.* 2008, 58.
279 *Stb.* 2009, 544.
280 *Kamerstukken II* 2008/09, 31810, 3, p. 4.
281 *Kamerstukken II* 2008/09, 31810, 3, p. 4.
282 Zie Rb. Den Haag 30 juni 2015, ECLI:NL:RBDHA:2015:7428 en Hof Den Haag 14 oktober 2014, ECLI:NL:GHDHA:2014:4627.
283 Kristel van Teeffelen, '"Sexting" is geen kinderporno. Justitie stuurt jonge verspreiders van blootfoto's daarom vaker naar stichting Halt', *Trouw*, 13 april 2017.

Toch zal, in gevallen waarin de naaktbeelden zonder toestemming verder zijn verspreid (bijvoorbeeld als grap of uit wraak), het delict wel ten laste worden gelegd, afhankelijk van de schade die is berokkend aan de afgebeelde minderjarige en het belang van deze minderjarige (en eventuele andere betrokkenen).[284] Daarbij kan gedacht worden aan situaties waarbij ook nog sprake is van andere delicten, zoals afpersing of bedreiging.[285]

Virtuele kinderpornografie

Vooruitlopend op de implementatie van het Cybercrimeverdrag is in 2002 ook virtuele kinderpornografie in Nederland strafbaar gesteld.[286] Van oudsher viel dit niet onder artikel 240b Sr: wanneer de afgebeelde persoon niet bij de totstandkoming van de afbeelding betrokken is, is immers de ratio van de strafbaarstelling, de bescherming van kinderen tegen voor hen schadelijke praktijken, niet aan de orde.[287] Beslissend was de schade die in werkelijkheid op het moment van de totstandkoming van de afbeelding werd toegebracht. Onder omstandigheden kon er in het geval van virtuele en gemanipuleerde afbeeldingen overigens wel uit hoofde van andere bepalingen sprake zijn van strafbare feiten (artikel 240 Sr, de Auteurswet). Volgens artikel 9 van het Cybercrimeverdrag is evenwel ook het virtueel afbeelden van kinderen in een seksuele context strafwaardig, omdat deze afbeeldingen kunnen worden gebruikt voor het aanmoedigen of verleiden van kinderen tot seksuele handelingen; daarom zijn ze onderdeel van de subcultuur van kindermisbruik.[288]

Daarmee zijn dus ook ratio's voor strafbaarstelling het voorkomen van verdere verspreiding van eenmaal gemaakt materiaal en het voorkomen dat afbeeldingen worden gebruikt om jeugdigen te verleiden tot seksuele handelingen.[289] Na de implementatie van het Verdrag van Lanzarote[290] in 2007 is daar de algemene ratio bijgekomen dat met de strafbaarstelling van kinderporno ook wordt voorkomen dat gedrag deel kan gaan uitmaken van een subcultuur die seksueel misbruik van kinderen bevordert.[291]

De Nederlandse wetgever heeft artikel 240b Sr naar aanleiding van het Cybercrimeverdrag aangepast door daar "of schijnbaar is betrokken" in te voegen. Het begrip 'schijnbaar' is wat ons betreft wat ongelukkig, want dit laat veel ruimte open voor interpreta-

284 Zie bijvoorbeeld Rechtbank Rotterdam 18 mei 2017, ECLI:NL:RBROT:2017:4260: de 22-jarige verdachte wordt veroordeeld op basis van artikel 240b Sr, ook al betrof het met wederzijds goedvinden gemaakte seksfoto's en een -filmpje met een 17-jarig meisje. De rechtbank overwoog dat het geringe leeftijdsverschil niet "in het nadeel" van verdachte werkte, maar dat "met de verspreiding van de afbeeldingen en het filmpje door de verdachte aan anderen dan de betrokkene, het risico op verspreiding van de foto's en het filmpje daadwerkelijk is verwezenlijkt", waardoor het geheel van handelingen strafbare vervaardiging, verwerving en bezit van kinderporno opleverde.

285 Zie ook Aanwijzing kinderpornografie (artikel 240b Sr), *Stcrt*. 2016, 19415.

286 Wet partiële wijziging zedelijkheidswetgeving, *Stb.* 2002, 388. Zie artikel 9 lid 2 onder c Cybercrimeverdrag; de strafbaarstelling is volgens artikel 9 lid 4 overigens optioneel voor de verdragsstaten.

287 In die zin de minister van Justitie, *Kamerstukken II* 1994/95, 23682, 5, p. 10.

288 Explanatory Report, paragraaf 102, beschikbaar via https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

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

290 *Trb*. 2008, nr. 58.

291 Aanwijzing kinderpornografie 2007, p. 8.

tie. Het lijkt beter een beperktere aanduiding te hanteren die aangeeft waar het echt om gaat: "realistische afbeeldingen" (zoals het Cybercrimeverdrag het noemt) of liever nog afbeeldingen "die niet van echt te onderscheiden zijn", zoals de Amerikaanse wetgeving hanteert.[292] Door de opneming van 'schijnbaar' in de wettekst, hoeft "het openbaar ministerie niet [meer] de daadwerkelijke betrokkenheid van een echt kind te bewijzen. Voldoende is dat aannemelijk wordt gemaakt dat de afgebeelde persoon op een echt kind lijkt".[293]

Uit de jurisprudentie blijkt dat verschillende keren voor bezit van virtuele kinderporno is vervolgd. In 2008 veroordeelde de Rechtbank 's-Hertogenbosch voor het eerst een verdachte voor virtuele kinderpornografie. Het ging daar om een cartoonfilmpje met seks tussen een volwassene en een jong meisje. De rechtbank overwoog daarbij ook dat de verdachte het filmpje aan minderjarigen liet zien met mogelijk de bedoeling om seks met meerderjarigen als normaal gedrag aan te moedigen.[294] Daarbij overwoog de rechtbank ook "dat het gebeuren, incl. de afgebeelde personen, weliswaar voor volwassenen van echt is te onderscheiden, maar niet voor het gemiddelde kind".[295] Twee jaar later kwalificeerde dezelfde rechtbank een seksfilmpje met getekende minderjarigen niet als kinderpornografie, omdat "het voor de gemiddelde kijker onmiddellijk duidelijk is dat het gebeuren niet echt is en dat het gaat om gemanipuleerde afbeeldingen die niet realistisch zijn. Daarom kan het bestanddeel 'schijnbaar was/waren betrokken' niet bewezen worden".[296]

In de jurisprudentie zijn verder twee veroordelingen te vinden voor het bezit van kinderporno in de vorm van de erotische vorm van Manga-cartoons, 'Hentai' genoemd. Het Hof Arnhem en de Rechtbank Zutphen kwalificeerden bepaalde Hentai-afbeeldingen wel als (strafbare virtuele) kinderporno en andere afbeeldingen niet; de laatste waren, in tegenstelling tot de eerste, niet voldoende realistisch, dat wil zeggen dat "het voor de gemiddelde kijker onmiddellijk duidelijk is dat het gebeuren niet echt is en dat het gaat om gemanipuleerde afbeeldingen".[297] Daarentegen achtte het Hof 's-Hertogenbosch in 2011 dat het bezit van Hentai-afbeeldingen niet als kinderporno moet worden gekwalificeerd, omdat "voor de gemiddelde kijker (en ook kinderen) het bij de virtuele afbeeldingen (...) aanstonds blijkt dat het gaat om gemanipuleerde afbeeldingen die niet realistisch zijn. Het morele gehalte van deze afbeeldingen kan hieraan niet afdoen".[298]

De wetgever zou volgens het hof bedoelen dat het gewijzigde artikel sinds de toevoeging van 'schijnbaar' ziet op drie gevallen: (1) een afbeelding van een echt kind; (2) een

292 18 U.S. Code § 2256(8)(B), ingevoerd door de Protect Act 2003.
293 *Kamerstukken II* 2001/02, 27745, 6, p. 8.
294 De titel van het filmpje 'Sex Lessons for young girls' en de aankondiging 'Lessons jerking and facial' zijn in dat opzicht veelzeggend.
295 Rb. 's-Hertogenbosch 4 februari 2008, ECLI:NL:RBSHE:2008:BC3225.
296 Rb. 's-Hertogenbosch 30 maart 2010, ECLI:NL:RBSHE:2010:BL8876.
297 Rb. Zutphen 21 december 2010, ECLI:NL:RBZUT:2010:BO8152; evenzo Hof Arnhem 12 april 2012, ECLI:NL:GHARN:2012:BW3415.
298 Hof 's-Hertogenbosch 14 april 2011, ECLI:NL:GHSHE:2011:BQ1179. Zie ook Rb. Groningen 27 september 2012, ECLI:NL:RBGRO:2012:BX8917.

afbeelding van een echt persoon die eruitziet als een kind; (3) een realistische afbeelding van een niet bestaand kind. Volgens het hof ging het hier niet om een "realistische afbeelding van een niet-bestaand kind".[299] Daarom kan de afbeelding niet als kinderpornografie worden gekwalificeerd. Deze overweging is door de Hoge Raad in 2013 bevestigd.[300]
Schilderijen met kinderpornografische afbeeldingen kunnen volgens de Hoge Raad wel onder de delictsomschrijving van artikel 240b Sr vallen en als virtuele kinderpornografie worden gekwalificeerd, als ze voldoende realistisch zijn, wat ook het geval kan zijn als aanstonds duidelijk is dat het niet om foto's maar om realistische schilderijen gaat (zelfs als het schilderij op ondergeschikte onderdelen niet werkelijkheidsgetrouw is, zoals in casu de aanwezigheid van engelenvleugels op de rug van de afgebeelde kinderen).[301] In dit verband moet worden opgemerkt dat de wetgever het niet wenselijk vond om een uitzondering te maken voor "artistieke virtuele kinderporno". De artisticiteit die zou kleven aan een realistische virtuele pornografische afbeelding, ontneemt niet het strafwaardige karakter daaraan.[302]

Voor de volledigheid wijzen wij hier nog op het feit dat, toen de wetgever in 2010 dierenporno strafbaar stelde (artikel 254 Sr), ook *virtuele dierenporno* strafbaar is gesteld, oftewel het bezit (enzovoort) van een afbeelding "van een ontuchtige handeling, waarbij een mens en een dier zijn betrokken *of schijnbaar zijn betrokken*" (artikel 254a Sr), met een maximumstraf van zes maanden gevangenis of geldboete van de derde categorie (of, bij gewoonte of beroep, een jaar resp. vierde categorie).[303] Hoewel de nodige veroordelingen hebben plaatsgevonden voor het bezit van dierenporno (veelal in combinatie met kinderporno), hebben wij geen uitspraken kunnen vinden betreffende virtuele dierenporno.

2.11.2 *Grooming (artikel 248e Sr)*

Grooming kan worden omschreven als het door gebruikmaking van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst voorstellen tot een ontmoeting met een persoon van minder dan 16 jaar met het oogmerk ontuchtige handelingen te plegen of kinderporno te vervaardigen (artikel 248e Sr). Het oogmerk van de dader bij de ontmoeting moet dus gericht zijn op het plegen van ontuchtige handelin-

299 Hof 's-Hertogenbosch 14 april 2011, ECLI:NL:GHSHE:2011:BQ1179.
300 HR 12 maart 2013, ECLI:NL:HR:2013:BY9719: "Het oordeel van het Hof dat de in de tenlastelegging onder de gedachtestreepjes 5 tot en met 8 omschreven afbeeldingen niet als realistisch in deze zin zijn aan te merken, is feitelijk van aard. Gelet ook op de – niet door het middel bestreden – vaststellingen van het Hof dat de afgebeelde personen 'geen echte kinderen' zijn en dat voor 'de gemiddelde kijker (en ook kinderen) (...) aanstonds blijkt dat het gaat om gemanipuleerde afbeeldingen', is dit oordeel voorts niet onbegrijpelijk".
301 Zie HR 8 december 2015, ECLI:NL:HR:2015:348, *NJ* 2013/403, m.nt. Borgers.
302 *Kamerstukken II* 2001/02, 27745, 6, p. 8-9.
303 Wet van 4 maart 2010, *Stb*. 2010, 111.

gen of het vervaardigen van kinderpornografie.[304] Op het delict staat een gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. Het artikel is in 2010 ingevoerd naar aanleiding van de ratificatie van het Verdrag van Lanzarote.[305] Ook minderjarigen kunnen het delict grooming plegen, omdat er in artikel 248e Sr geen leeftijdsbeperking betreffende de dader staat.
Uit de delictsomschrijving volgt dat het louter communiceren met een minderjarige, ongeacht de ontuchtige toonzetting, niet strafbaar is.[306] De Hoge Raad heeft duidelijk gemaakt dat voor strafbaarheid van grooming vereist is dat de verdachte "een ontmoeting voorstelt" én "hij enige handeling onderneemt gericht op het verwezenlijken van ontmoeting".[307] Die uitvoeringshandeling uit zich al snel in de richting van een concreet voorstel voor een bepaalde datum, tijd en plaats,[308] bijvoorbeeld door het toesturen van een reisschema, plattegrond of route-instructies. Daarbij hoeft de ontmoeting niet daadwerkelijk plaats te vinden.[309] Grooming is immers in feite een voorbereidingshandeling.[310]
In de rechtspraak is niet uitgekristalliseerd of poging tot grooming strafbaar is.[311] De wetgever heeft echter aangegeven dat, mede in het licht van het Verdrag van Lanzarote, strafbare poging tot grooming mogelijk is. Dat is bijvoorbeeld mogelijk als een ontmoeting is voorgesteld (met ontuchtig oogmerk), maar nog geen verwezenlijkingshandeling is ondernomen. Dat kan het geval zijn in de situatie dat de minderjarige (of degene die zich voordoet als minderjarige) niet op het voorstel ingaat of waarbij een ouder bijtijds heeft ingegrepen; het voorstel is in dat geval het begin van de uitvoering van grooming.[312]

Met de Wet computercriminaliteit III is artikel 248e Sr gewijzigd, waardoor een persoon ook strafbaar is als een (echte of virtuele) 'lokpuber' wordt ingezet, oftewel het groomen van "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". Door de wijziging is een persoon ook strafbaar als deze meent te communiceren met

304 *Kamerstukken II* 2008/09, 31810, 3, p. 9. Zie ook Hof Arnhem 15 september 2011, ECLI:NL:GHARN:2011:BT1553.
305 *Trb*. 2008, 58. *Stb*. 2009, 544, inwerkingtreding 1 januari 2010. Zie artikel 23 van het verdrag voor de omschrijving van grooming.
306 Zie ook *Kamerstukken II* 2008/09, 31810, 7, p. 4. Zie ook Rb. Oost-Brabant op 9 december 2014, ECLI:NL:RBOBR:2014:7494.
307 HR 11 november 2014, ECLI:NL:HR:2014:3140.
308 Zie R.S.B. Kool, *Tekst & Commentaar Sr* (2016) bij artikel 240b Sr met verwijzing naar HR 11 november 2014, ECLI:NL:HR:2014:3140, Rb. Oost-Brabant 18 november 2016, ECLI:NL:RBOBR:2016:6439 en Rb. Overijssel 23 september 2016, ECLI:NL:RBOVE:2016:3227.
309 Zie ook *Kamerstukken II* 2015/16, 34372, 3, p. 90.
310 Zie ook *Kamerstukken II* 2008/09, 31810, 3, p. 9.
311 Zie R.S.B. Kool, *Tekst & Commentaar Sr* (2016) bij artikel 240b Sr en Lindenberg 2016.
312 *Kamerstukken II* 2015/16, 34372, 3, p. 91.

een persoon beneden de 16 jaar, maar die persoon in werkelijkheid ouder is.[313] Het is zelfs mogelijk dat een persoon zich schuldig maakt aan grooming als het gesprek en het voorstel tot een ontmoeting plaatsvinden met een virtueel persoon, zoals een avatar van een jong meisje in combinatie met een chatbot.[314]
De wijziging is ingegeven door een zaak in Leiden, waarbij een man had getracht een minderjarige in een chatbox te verleiden tot een ontmoeting, terwijl het in werkelijkheid een meerderjarige politieagente was. Destijds werd volgens de Rechtbank Den Haag niet voldaan aan de delictsomschrijving.[315] Met de toevoeging is er geen twijfel meer mogelijk dat een dergelijke handeling strafbaar kan zijn. In de literatuur wordt benadrukt dat de scheidslijn met uitlokking in online conversaties dun is en dat 'lokpubers' het Tallon-criterium (zie paragraaf 3.9.1) in acht moeten nemen.[316]

2.11.3 *Webcamseks met minderjarigen (onder andere artikel 239, 248a en 248d Sr)*

Webcamseks tussen twee volwassen is (in Nederland) niet strafbaar. Uiteenlopende vormen van webcamseks met een minderjarige kunnen echter onder diverse strafbepalingen vallen.[317]
Indien iemand een minderjarige verleidt of dwingt om geslachtsdelen te laten zien of te masturberen voor de webcam, kan dit vallen onder artikel 247 Sr (ontucht) als de minderjarige onder de zestien is, artikel 246 Sr (aanranding van de eerbaarheid) als er dwang (bedreiging met geweld of een feitelijkheid) wordt gebruikt of artikel 248a Sr (ontucht) als er verleiding (giften, beloften, misleiding of misbruik van overwicht) wordt gebruikt, artikel 248f Sr (kinderprostitutie) als de minderjarige voor de webcam onder dwang seks heeft met een derde of artikel 248b Sr (ontucht met een 16- of 17-jarige prostitué(e)). Ook zou een dergelijke handeling wellicht gekwalificeerd kunnen worden als opzettelijke toegangsverschaffing tot kinderpornografie (artikel 240b Sr).
Ook de omgekeerde situatie kan zich voordoen, waarbij iemand zijn geslachtsdelen toont of masturbeert voor de webcam in communicatie met een minderjarige. Onder omstandigheden zou dit gekwalificeerd kunnen worden als oneerbaarheid op een niet-publieke plaats waarbij een ander zijns ondanks aanwezig is (artikel 239 Sr), het aan iemand, anders dan op diens verzoek, toesturen van een aanstootgevende afbeel-

313 Voorheen was hier onduidelijkheid over. Zie Rb. Amsterdam 11 april 2011, ECLI:NL:RBAMS:2011:BQ0961. De procureur-generaal heeft in 2014 betoogd dat het niet uitmaakt als het slachtoffer een fictief 10-jarig meisje is en voorbereide misdrijven niet konden worden voltooid; voldoende is dat uit de bewijsvoering kan worden afgeleid dat de bewezenverklaarde gedragingen strekten ter voorbereiding van feiten als in de bewezenverklaring bedoeld en dat het opzet van verdachte op het begaan daarvan was gericht (HR 11 februari 2014, ECLI:NL:PHR:2014:427 concl. P-G).
314 Dit onderdeel is bij amendement ingevoerd, *Kamerstukken II* 2016/17, 34372, 15. Zie over de problematiek van virtuele creaties (in het bijzonder het voorbeeld van 'Sweetie 2.0') Schermer e.a. 2016, De Hingh 2018 en Schermer, Koops & Van der Hof 2019. Zie voor kritiek op deze wijziging en strafbaarstelling onder andere De Hingh 2018.
315 Hof Den Haag 25 juni 2013, ECLI:NL:GHDHA:2013:2302.
316 Zie onder andere Ölçer 2014 en Schermer e.a. 2016, p. 57-61.
317 Zie Schermer, Koops & Van der Hof 2019 voor een overzicht.

ding (artikel 240 Sr), het aanbieden of vertonen aan iemand onder de zestien van een afbeelding die schadelijk is voor personen onder de zestien (artikel 240a Sr) of het met ontuchtig oogmerk bewegen van iemand onder de zestien om getuige te zijn van seksuele handelingen (artikel 248d Sr).
De maximumstraffen voor deze delicten variëren van laag (twee of drie maanden gevangenisstraf, artikel 240a en 239 Sr) tot hoog (zes tot tien jaren gevangenisstraf, artikel 247, 246, 248f Sr). In artikel 248 Sr zijn bovendien strafverzwarende omstandigheden geformuleerd[318] bij het plegen van delicten met betrekking tot onder andere kinderpornografie, ontucht en aanranding. De meeste bepalingen waarin de minderjarige wordt verleid of gedwongen tot seks voor de webcam, kennen relatief hoge straffen. De straffen zijn veelal lager voor het ongevraagd door de dader verzenden van seksuele beelden, maar omdat artikel 248d Sr apart staat genoemd in artikel 67, eerste lid Sv, kunnen ook bij verdenking van dit delict de benodigde bijzondere opsporingsbevoegdheden worden ingezet.

Hoewel deze zedendelicten van oudsher bedoeld zijn voor fysieke situaties, is het niet uitgesloten dat het misbruik op afstand, via online verbindingen, plaatsvindt. Webcamseks levert meestal geen fysiek misbruik op, maar kan wel aanzienlijke psychische schade veroorzaken en de seksuele integriteit van de minderjarige aantasten; de ratio van strafbaarstelling verzet zich dus niet tegen toepassing van deze bepalingen in online contexten.[319]
Diverse van deze bepalingen worden dan ook in de jurisprudentie toegepast op webcamseks. Zo veroordeelde de Rechtbank Haarlem iemand op basis van artikel 239 Sr, omdat hij zijn geslachtsdeel aan een negenjarig meisje via de webcam had getoond; volgens de rechtbank is dit schennis van de eerbaarheid op een niet-openbare plaats, waarbij een ander (het meisje) haars ondanks (oftewel tegen haar wil) tegenwoordig is. Het verweer dat het geslachtsdeel niet reëel maar slechts virtueel 'tegenwoordig' was, verwierp de rechtbank, nu het gaat om "het versturen van 'live' beelden. Hierbij is in het algemeen het effect van overrompeling en indringendheid van de waarneming groter. Daar komt nog bij dat in het onderhavige geval de beelden werden begeleid door direct contact tussen de verdachte en zijn slachtoffer middels het chatten". Evenmin werd het verweer gehonoreerd dat het meisje de webcambeelden gewoon had kunnen wegklikken – ze was te jong om vrijelijk haar wil te kunnen bepalen, zodat ze tegen

318 Aangepast bij Wet van 12 februari 2014, *Stb*. 2014, 74 ter implementatie van Richtlijn 2011/93/EU.
319 Een expliciete uitzondering bij de zedendelicten is artikel 240c Sr, dat het opzettelijk aanwezig zijn bij een seksshow met een minderjarige strafbaar stelt. Uit de wetsgeschiedenis blijkt dat onder 'aanwezig zijn' wordt begrepen het lijfelijk aanwezig zijn of in hetzelfde gebouw aanwezig zijn terwijl de voorstelling via een gesloten circuit wordt bekeken; een amendement om het door middel van een webcam bijwonen van een dergelijke voorstelling onder het begrip 'aanwezig zijn' te brengen, werd door de minister van Justitie ontraden en is daarna ingetrokken. Daarom is het artikel niet van toepassing op online seksshows. Zie Rb. Breda 10 februari 2006, ECLI:NL:RBBRE:2006:AV1470.

haar wil aanwezig moest worden geacht.[320] Artikel 240a Sr is eveneens toegepast op het via de webcam laten zien van een geslachtsdeel aan iemand onder de zestien.[321]
Artikel 246 Sr is toegepast op webcambeelden van zich ontkledende meisjes, waarbij de rechtbank expliciet overwoog dat de uitleg van strafbepalingen die strekken tot bescherming van bepaalde rechten dient in te spelen op nieuwe technische mogelijkheden. De rechtbank oordeelde in casu dat het om afgedwongen ontuchtige handelingen als bedoeld in artikel 246 Sr ging, aangezien de meisjes niet wisten dat hun webcam gehackt was en hun recht op seksuele zelfbeschikking was aangetast nu zij zich uitkleedden en naakt waren terwijl ze niet wisten dat zij begluurd werden.[322] Dat oordeel gaat vermoedelijk te ver, aangezien de Hoge Raad heeft bepaald dat artikel 246 Sr enige interactie vereist en niet passieve registratie omvat.[323]
Een andere vergaande uitspraak is die van de Rechtbank Rotterdam, waarbij het via chat/internetgesprekken bewegen van meisjes tussen de 12 en 16 jaar tot het voor de webcam inbrengen van hun vingers in de vagina is gekwalificeerd als het plegen van ontuchtige handelingen die mede bestaan uit het seksueel binnendringen van het lichaam (artikel 245 Sr).[324]
Volgens de Hoge Raad is voor ontucht als bedoeld in artikel 247 Sr geen lichamelijke aanraking nodig; het is afhankelijk van de omstandigheden van het geval of een bewezenverklaarde gedraging het plegen van ontucht 'met' een minderjarige oplevert.[325] Webcam-gerelateerde ontucht lijkt in dat verband niet uitgesloten. Ook artikel 248a Sr (ontucht) wordt toegepast om iemand te vervolgen die een minderjarige door giften, misbruik van overwicht of misleiding beweegt tot het plegen van ontuchtige handelingen.[326] Het misbruik van uit feitelijke verhoudingen voortvloeiend overwicht kan bijvoorbeeld bestaan uit het misbruiken van zijn geestelijk overwicht als meerderjarige ten opzichte van een minderjarige en het dreigen expliciete foto's van het slachtoffer te verspreiden.[327] Uit bewijsmiddelen zal moeten blijken dat er tussen de verdachte en de (echte of zich als zodanig voordoende) minderjarige voor het plegen van ontucht interactie is geweest. Hierbij kan gedacht worden aan zich naakt voor de webcam tonen of het verrichten van ontuchtige handelingen voor de camera.[328]

---

320 Rb. Haarlem 24 december 2004, ECLI:NL:RBHAA:2004:AR8212. Volgens HR 9 december 2003, ECLI:NL:HR:2003:AL8452 kan bij een telefoongesprek (in casu van een 'hijger') echter niet worden gesproken van aanwezigheid in de zin van artikel 239 Sr, zodat werd ontslagen van rechtsvervolging; vervolging op basis van belaging (artikel 285b Sr) zou eventueel wel mogelijk zijn, mits de 'hijger' vaker belt. Volgens Van Laanen was in deze laatste zaak een andere uitkomst mogelijk geweest, aangezien artikel 239 volgens de wetgeschiedenis ook betrekking kan hebben op schennis door middel van het gesproken woord.

321 Rb. Leeuwarden 23 april 2009, ECLI:NL:RBLEE:2009:BI2330 en Rb. Leeuwarden 10 mei 2011, ECLI:NL:RBLEE:2011:BQ4176.

322 Rb. Haarlem 24 juli 2008, ECLI:NL:RBHAA:2008:BD8449.

323 HR 21 februari 2012, ECLI:NL:HR:2012:BU5254.

324 Rb. Rotterdam 15 maart 2016, ECLI:NL:RBROT:2016:1928.

325 HR 30 november 2004, ECLI:NL:HR:2004:AQ0950.

326 Rb. Haarlem 24 december 2004, ECLI:NL:RBHAA:2004:AR8212; in casu ging het om een strafbare poging, nu het meisje niet inging op de vraag. Zie ook Rb. Zutphen 1 maart 2006, ECLI:NL:RBZUT:2006:AV3246.

327 Hof 's-Gravenhage 30 september 2013, ECLI:NL:GHDHA:2013:3706.

328 *Kamerstukken II* 2015/16, 34372, 3, p. 90. Zie bijvoorbeeld Rb. Rotterdam 15 november 2017, ECLI:NL:RBROT:2017:8965.

Met de Wet computercriminaliteit III is, vergelijkbaar met de wijziging bij grooming (paragraaf 2.11.2), ook artikel 248a Sr gewijzigd om het seksueel misbruiken van kinderen via internet beter strafbaar te stellen.[329] Volgens de wetgever komt het steeds vaker voor dat groomers, waaronder 'loverboys', meisjes proberen te verleiden om zich voor de webcam uit te kleden en seksuele handelingen te verrichten. Het beeldmateriaal wordt vervolgens gebruikt om het slachtoffer onder druk te zetten om steeds opnieuw voor de camera te komen of verdergaande seksuele handelingen te verrichten.[330] Met de wijziging wordt ook de verleiding van iemand die zich voordoet als een minderjarige of "een virtuele creatie van een persoon die de leeftijd van achttien jaren nog niet heeft bereikt" als ontucht strafbaar.

De wijziging is beperkt tot artikel 248a Sr. Oorspronkelijk was ook een wijziging van artikel 248d Sr voorzien, maar volgens de wetgever bleek uit de adviezen dat lokpubers in de praktijk niet worden ingezet voor opsporing van dit feit, en dat het verrichten van seksuele handelingen voor de webcam door de verdachte zelf al onder artikelen 239 en 240a Sr kan worden gebracht.[331] De minister gaat echter niet in op het feit dat de strafmaat van artikelen 239 en 240a Sr lager is dan die voor artikel 248d, en dat, anders dan bij 248d, geen voorlopige hechtenis is toegelaten, zodat bijvoorbeeld geen internettap of vordering van verkeersgegevens mogelijk is voor de opsporing. Daar komt bij dat later bij amendement ook het seksuele contact met virtuele creaties, zoals chatbots, strafbaar is gesteld in artikel 248a (evenals artikel 248e) Sr; het is echter de vraag of het verrichten van seksuele handelingen voor de webcam strafbaar is onder artikel 239 of 240a Sr, indien de webcam in verbinding staat met een virtuele persoon – de artikelen spreken immers van "een ander" en "personen", waarmee echte personen worden bedoeld. Vermoedelijk kan ook geen strafbare poging worden ten laste gelegd, omdat het gaat om een absoluut ondeugdelijke poging (de virtuele creatie kan immers nooit een persoon zijn).[332]

Aangezien artikel 248a zeker niet het enige zedendelict is dat wordt toegepast in de context van webcamseks met minderjarigen, lijkt het ons weinig systematisch dat (echte en virtuele) lokpubers wel kunnen worden ingezet in het kader van de artikelen 248a en 248e Sr, maar niet bij andere delicten. Er valt in dat licht ook iets voor te zeggen om in plaats van aanpassing van deze twee artikelen, een meer algemene bepaling op te nemen in titel XIV (zedenmisdrijven) met de strekking dat onder personen als bedoeld in deze titel ook virtuele creaties worden verstaan, en dat onder minderjarigen ook personen (en virtuele creaties) die zich voordoen als minderjarigen worden verstaan.

329 *Kamerstukken II* 2015/16, 34372, 3, p. 67; *Kamerstukken II* 2016/17, 34372,15.

330 *Kamerstukken II* 2015/16, 34372, 3, p. 68.

331 *Kamerstukken II* 2015/16, 34372, 3, p. 70. Artikel 239 Sr is ook van toepassing op meerderjarigen. Bij artikel 240a Sr wordt er, zo nemen wij aan, hierbij kennelijk van uitgegaan dat het versturen van oneerbare webcambeelden aan iemand die zich voordoet als minderjarige, als strafbare poging kan worden vervolgd.

332 Schermer e.a. 2016, p. 38.

2.11.4 *Sextortion*

Een bijzonder geval van webcamseksmisbruik betreft *sextortion*. Dit is niet beperkt tot minderjarigen maar treft veelal ook meerderjarigen. Van '*sextortion*' is sprake als iemand eerst wordt verleid om een relatief onschuldig naaktbeeld te tonen of te sturen (bijvoorbeeld het optillen van een T-shirt zodat de borsten even zichtbaar zijn voor de webcam) en vervolgens deze beelden of webcamopnamen worden gebruikt om de persoon te dwingen tot meer – en steeds verdergaande – seksuele handelingen voor de webcam, onder de dreiging dat de beelden via internet worden verspreid. Als vooraf-gaand aan de *sextortion* de afbeeldingen of video's zijn overgenomen uit de computer van het slachtoffer kan uiteraard ook computervredebreuk en het installeren van kwaadaardige software ten laste worden gelegd.[333]
In de jurisprudentie is deze gedraging ook aangemerkt als online aanranding (artikel 246 Sr) en afdreiging (artikel 318 Sr).[334] Het is voor aanranding dus niet vereist dat er fysiek contact is tussen de dader en het slachtoffer; aanranding kan onder deze omstandigheid ook op afstand plaatsvinden. Slachtoffers hebben vaak niet de mogelijkheid om te verhinderen dat de dader de afbeeldingen verspreidt en voelen zich daarom gedwongen toe te geven aan de dader. In dat geval is er sprake van (poging tot) aanranding op afstand. Van afdreiging (artikel 318 Sr) kan sprake zijn als de afbeeldingen of video's later tegen het slachtoffer worden gebruikt om deze te chanteren. In de *Aydin C.*-zaak werden beelden gebruikt voor chantage van masturberende mannen die aan het webcammen waren met – zo dachten ze – minderjarige jongens. Bij niet-betaling zou de verdachte de beelden verspreiden onder vrienden en familie. De ernst van het delict is zichtbaar in deze zaak waarin de verdachte (in eerste aanleg; het hoger beroep loopt nog medio 2018) werd veroordeeld tot de maximale gevangenisstraf van ruim tien jaar voor *sextortion* van 34 meisjes (naast bezit van kinderporno).[335]

2.11.5 *Wraakporno*

Van 'wraakporno' is sprake als beelden van seksuele handelingen tussen personen zonder toestemming via internet worden verspreid, bijvoorbeeld uit wraak (maar mogelijk ook om andere redenen; de benaming wraakporno (*revenge porn*) is inmiddels ingeburgerd voor het algemene fenomeen). Wraakporno kreeg wereldwijde aandacht toen op 31 augustus 2014 ongeveer vijfhonderd naaktfoto's van wereldsterren uit voornamelijk de Verenigde Staten online verschenen. De gebeurtenis werd op internet '*The Fap-*

333 Zie Rb. Zeeland-West-Brabant 16 mei 2017, ECLI:NL:RBZWB:2017:2873.
334 Rb. Dordrecht 20 oktober 2005, ECLI:NL:RBDOR:2005:AU4724; Rb. Breda 10 februari 2006, ECLI:NL:RBBRE:2006:AV1470. Rb. Gelderland 31 mei 2016, ECLI:NL:RBGEL:2016:3037, Gerechtshof Arnhem-Leeuwarden 8 december 2015, ECLI:NL:GHARL:2015:9221, m.nt. Tina van der Linden-Smit en Kea Kroeks-de Raaij in UDH:IR/13054, Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, nr. 2, p. 169-180, m.nt. J.J. Oerlemans (*Aydin C.*), en Rb. Zeeland-West-Brabant 16 mei 2017, ECLI:NL:RBZWB:2017:2873, Rb. Noord-Nederland, 17 augustus 2017, ECLI:NL:RBNNE:2017:3163.
335 Rb. Amsterdam 16 maart 2017, ECLI:NL:RBAMS:2017:1627, *Computerrecht* 2017/103, nr. 2, p. 169-180, m.nt. J.J. Oerlemans (*Aydin C.*).

pening' genoemd.[336] Nadat de wachtwoorden van de sterren op een of andere wijzen waren achterhaald, hebben hackers zich toegang verschaft tot de online kopie in de cloud van Apple (iCloud) en de foto's vervolgens verspreid. De naaktfoto's werden verspreid via het beruchte forum 4Chan.org en daarna razendsnel via nog grootschaliger websites als Reddit en Imgur.[337] Ook in Nederland werd in 2018 een verdachte veroordeeld voor het hacken van de iCloud-accounts en het zich toegang verschaffen tot de privéfoto's van Nederlandse sterren.[338]

De verspreiding van naaktfoto's zonder toestemming kan mogelijk tot strafrechtelijke vervolging leiden op grond van belediging (artikel 266 Sr), smaad (artikel 261 Sr) en, indien er feiten worden verkondigd die in strijd zijn met de waarheid, laster (artikel 262 Sr) (zie verder paragraaf 2.12 met betrekking tot deze uitingsdelicten).[339] Als de afbeeldingen of video's uit de computer van het slachtoffer worden gehaald, kan mogelijk ook computervredebreuk (artikel 138ab Sr) en het wederrechtelijk overnemen van niet-openbare gegevens (artikel 138c Sr) ten laste worden gelegd. Bij herkenbare beelden kan voor portretrechtinbreuk worden vervolgd, zij het alleen als overtreding (artikel 35 Aw, zie paragraaf 2.4.5). Langs civielrechtelijke weg kan het materiaal ook offline worden gehaald met een beroep op onrechtmatige daad of de Wet bescherming persoonsgegevens.

Hoewel de minister zich lange tijd op het standpunt stelde dat er genoeg wettelijke mogelijkheden waren om wraakporno te bestrijden en dat de wet op dit punt geen lacunes kende,[340] is de regering inmiddels van mening – zoals ook vastgelegd in het regeerakkoord – dat het zonder toestemming verspreiden van naaktfoto's strafbaar zou moeten zijn.[341] De emotionele schade bij de slachtoffers is groot. Er is een nadrukkelijke roep in de samenleving om slachtoffers tegen deze gedragingen in bescherming te nemen. Daartoe is in 2018 een conceptwetsvoorstel in consultatie gegeven met onder andere een strafbaarstelling van het aan een ander bekend maken of openbaar maken van seksueel beeldmateriaal van een persoon met het oogmerk van benadeling van die persoon (voorgesteld artikel 139h Sr, maximumstraf van twee jaren of geldboete van de vierde categorie).[342] Ten tijde van het schrijven van dit boek (medio 2018) is nog niet duidelijk hoe de uiteindelijke regeling eruit zal komen te zien.

336 The fappening is een combinatie van het werkwoord '*fap*' (een internetterm voor masturbatie) en de populaire Amerikaanse film '*The Happening*').

337 Zie onder andere Charles Arthur, 'Naked celebrity hack: security experts focus on iCloud backup theory', *The Guardian* 1 september 2014.

338 Rb. Amsterdam, 16 mei 2018, ECLI:NL:RBAMS:2018:3297.

339 Zie bijvoorbeeld Hof Amsterdam 18 oktober 2017, ECLI:NL:GHAMS:2017:4648. Zie ook Van der Hof 2016 en Ten Voorde 2017.

340 *Aanhangsel Handelingen II* 2014/15, 933; *Kamerstukken II* 2014/15, 28684, 443, p. 1.

341 Zie *Kamerstukken II* 2017/18, 29279, 441.

342 Zie https://www.rijksoverheid.nl/documenten/kamerstukken/2018/05/16/wetsvoorstel-en-memorie-van-toelichting-herwaardering-strafbaarstelling-actuele-delictsvormen-consultatieversie (laatst geraadpleegd 1 juli 2018).

2.12 Uitingsdelicten

Bij uitingsdelicten gaat het veelal om het 'zwartmaken' van personen of groepen van personen. Het is duidelijk dat internet daartoe een geschikt medium is, met een uitzonderlijk groot bereik. Uitingsdelicten op internet komen dan ook relatief vaak voor. Volgens sommige auteurs vervolgt het Openbaar Ministerie te weinig voor deze strafbepalingen.[343] In antwoord op Kamervragen legde de toenmalige minister van Justitie uit dat het verschil tussen het aantal aangiften en het aantal vervolgingen met name wordt veroorzaakt door het niet kunnen instellen van een opsporingsonderzoek in verband met het ontbreken van een daderindicatie, het niet kunnen achterhalen van de verdachte, het ontbreken van voldoende bewijs, dan wel de niet-strafbaarheid van de uiting.[344]
Wat daarvan ook zij, opgemerkt moet worden dat geschillen vaak via civielrechtelijke weg worden afgehandeld. Via een kort geding kan bijvoorbeeld het verwijderen van een bericht of rectificatie door belanghebbenden worden bedongen. Rechters zullen bij deze zogenoemde 'onrechtmatige perspublicaties' altijd een afweging moeten maken tussen het recht op bescherming van de eer en goede naam van personen en de vrijheid van meningsuiting. Ook maakt de overheid met sociale-mediadiensten afspraken over hoe wordt omgegaan met meldingen van uitingsdelicten op hun platformen. De private partijen maken zelf op verschillende wijzen gebruik van bijvoorbeeld filteringstechnieken om strafbare en ongewenste inhoud te weren van hun platformen. Naar aanleiding van meldingen wordt strafbare of onrechtmatige inhoud dikwijls verwijderd van hun platform.
In deze subparagraaf worden de strafbepalingen met betrekking tot de belangrijkste (groepen van) uitingsdelicten in een online context besproken: smaad (artikel 261 lid 1 Sr), belediging (artikel 266 Sr), discriminatie (artikelen 139c-139g Sr) en opruiing (artikel 131 en 132 Sr). Vervolgens komen de hiermee verband houdende vraagstukken van de aansprakelijkheid van internetaanbieders en *notice-and-takedown* aan bod.

2.12.1 *Smaad en laster (artikel 261, 262 Sr)*

Titel XVI van boek II van het Wetboek van Strafrecht is gewijd aan belediging. Wat deze delicten gemeen hebben is de aantasting van de eer en goede naam in het openbaar. Artikel 261 lid 1 Sr bedreigt het opzettelijk aanranden van iemands eer of goede naam door tenlastelegging van een bepaald feit, met het kennelijke doel om daaraan ruchtbaarheid te geven, met een gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie. Het tweede lid (smaadschrift) voorziet maximaal een jaar

343 Zie bijvoorbeeld Bart Custers, 'Online discriminatie vereist steviger aanpak van justitie', *Trouw* 5 oktober 2016.

344 Antwoord op Kamervragen van het lid Marcouch van 18 november 2016 over het niet behandelen van aangiften van discriminatie, *Aanhangsel Handelingen II* 2016/17, 563. Zie ook Antwoorden van minister Opstelten van 10 december 2013 over vragen van het lid Dijkhoff over het bericht 'Onderzoek nepaccount VU-studente loopt dood in Amerika', *Aanhangsel Handelingen II* 2013/14, 723.

gevangenisstraf of geldboete van de derde categorie wanneer de dader smaad bedrijft door middel van geschriften of afbeeldingen die worden verspreid, openlijk tentoongesteld of aangeslagen. Het derde lid behelst een strafuitsluitingsgrond voor degene die heeft gehandeld tot noodzakelijke verdediging dan wel die te goeder trouw heeft kunnen aannemen dat het ten laste gelegde waar was en dat het algemeen belang de tenlastelegging eiste.

Laster betreft het plegen van smaad of smaadschrift, terwijl men weet dat het ten laste gelegde gelogen is (artikel 262 Sr). Op laster staat een maximumstraf van twee jaren gevangenisstraf of geldboete van de vierde categorie.

De delictsomschrijvingen voor smaad en laster zijn ook toepasbaar in een online context. Al in 1999 oordeelde de Hoge Raad over een smaadschrift dat werd gepleegd via internet.[345] Een ontevreden universitair docent had de eer en goede naam van zijn vrouwelijke chef aangerand door een aantal berichten in de nieuwsgroep <alt.binaries.pictures.erotica.breasts> te plaatsen. Daarop werden één of meer pornografische afbeeldingen geplaatst, terwijl hij zijn afzenderadres had veranderd in een adres dat rechtstreeks in verband kon worden gebracht met zijn chef. Daarbij had hij de tekst gevoegd: "Als u meer wilt, e-mail mij dan". Aldus werd de chef neergezet als een verspreider van pornografie. Door dat via internet te doen, zo overwoog het hof, werd zij onder een groter publiek en in beginsel zelfs wereldwijd als zodanig aangemerkt. Anderen zouden de gevolgtrekking kunnen maken dat zij een grootschalige verspreider was van pornografie. Uiteraard wist de verdachte dat dit in strijd met de waarheid was. Ook was het evident dat hij de beledigende en onware boodschap(pen) had verzonden met het kennelijke doel om daaraan ruchtbaarheid te geven, zodat alle bestanddelen van artikel 262 Sr (laster) vervuld waren.

Een meer actueel voorbeeld betreft een smaadschrift over agenten op sociale-netwerkdiensten, zoals Hyves[346] (een platform dat een decennium geleden zeer populair was maar inmiddels niet meer bestaat) en Facebook.[347] De betrokken verdachten waren het niet eens met hun arrestatie door de politieagenten en plaatsen daarop foto's en identiteitsgegevens van de agenten op het platform, in combinatie met beledigende en smadelijke bijschriften. Op de Hyvespagina werd bijvoorbeeld een foto geplaatst van de agent en de uitlating gedaan dat de agent haar, de verdachte, had verkracht. Interessant zijn de overwegingen van de rechtbank over het feit of toegang tot de pagina's door de verdachten is beperkt. Dat is namelijk relevant voor het onderdeel met het doel om "ruchtbaarheid te geven" aan de tekst. In de onderhavige gevallen was de toegang niet beperkt, zodat dit onderdeel ook bewezen kon worden verklaard. Maar ook "indien een beschuldiging op een afgeschermde Hyvespagina is gepubliceerd, maar wel door

345 HR 9 maart 1999, *NJ* 1999/346. Zie voor een actueler arrest: HR 18 april 2017, ECLI:NL:HR:2017:704 over smaad via het sociale-mediaplatform Hyves.

346 Rb. Den Haag 22 april 2015, ECLI:NL:RBDHA:2015:4690.

347 Rb. Noord-Holland 3 september 2014, ECLI:NL:RBNHO:2013:7820.

twintig à vijfentwintig personen te lezen is geweest, is met het kennelijke doel van ruchtbaarheid gehandeld", aldus de rechtbank.[348]
Een andere vorm van mogelijke smaad of laster die op internet voorkomt betreft 'klaagpagina's', waarin wordt geklaagd over bijvoorbeeld een (vermeend) slecht product, een onbetrouwbaar bedrijf of een onuitstaanbaar persoon. Belangrijk hier is de strafuitsluitingsgrond van het algemeen belang (artikel 261 lid 3 Sr), waar het bij klaagpagina's nu juist om gaat. Men beoogt de gemeenschap te waarschuwen tegen een product, bedrijf of persoon. Het is evenwel aan de rechter om te beoordelen of de bewuste klaagpagina in de bewuste vorm inderdaad voldoende het algemeen belang dient – iets wat niet eenvoudig is vast te stellen. Een voorbeeld betreft de vraag of een bericht moet worden verwijderd over een vermeende oplichter, dat is verspreid via het LinkedIn- en Facebookaccount van de verdachte.[349] In casu overwoog de rechtbank dat het verwijderen een beperking is van de vrijheid van meningsuiting als bedoeld in artikel 10 EVRM. De rechtbank is van mening dat dit recht in deze omstandigheden kan worden beperkt, nu door de eiser aannemelijk is gemaakt dat de uitlatingen haar in zakelijk opzicht schade hebben berokkend dan wel zouden berokkenen.[350]

2.12.2 *Belediging, bedreiging en belaging (artikel 266 e.v., 284 e.v. Sr)*

Artikel 266 lid 1 Sr stelt de eenvoudige belediging strafbaar. De opzettelijke belediging kan onder meer plaatsvinden door een toegezonden of aangeboden geschrift of afbeelding. De maximale gevangenisstraf voor deze vorm van belediging is drie maanden of een geldboete van de tweede categorie. Ook hier geldt een bijzondere rechtvaardigingsgrond (lid 2, 'functioneel schelden'). Van belang is in dit verband ook het verspreidingsdelict van artikel 271 Sr (verspreiding, openlijk tentoonstellen of aanslaan of ter verspreiding in voorraad hebben van beledigende of voor een overledene smadelijke geschriften). De strafmaat is dezelfde als die van de eenvoudige belediging.
Een voorbeeld van belediging op internet betreft een tweet waarin een gemeenteraadslid een officier van justitie, betrokken bij de vervolging van politicus Jos van Rey, vergeleek met een SS-kampbeul. Dit resulteerde in een veroordeling wegens belediging.[351]
In deze context is het van belang op te merken dat rechtbanken in principe de nettiquette-regel onderschrijven dat "retweet is not endorsement".[352] Gebruikers van de sociale-mediadienst Twitter kunnen berichten van anderen namelijk doorsturen ('retweeten'), niet alleen omdat ze het ermee eens zijn, maar ook juist om de aandacht te vestigen op een in hun ogen verwerpelijke uiting. In 2011 leidde de vervolging van schrijver Bert Brussen in verband met de retweet van een bedreiging aan het adres van

348 Rb. Noord-Holland 3 september 2014, ECLI:NL:RBNHO:2013:7820 met verwijzing naar HR 22 januari 1965, *NJ* 1965/131.
349 Rb. Oost-Nederland, 15 januari 2013, ECLI:NL:RBONE:2013:BY8479.
350 Rb. Oost-Nederland, 15 januari 2013, ECLI:NL:RBONE:2013:BY8479, r.o. 4.2 en 4.9.
351 Rb. Limburg 22 augustus 2016, ECLI:NL:RBLIM:2016:7288.
352 Deze norm wordt ook bevestigd in Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 11.22, m.nt. J.J. Oerlemans, *Computerrecht* 2016/47, nr. 2, p. 122-124 ('Context-zaak').

Geert Wilders tot verontwaardiging.[353] De schrijver zou de bedreiging met een retweet namelijk niet per definitie onderschrijven, zo ervaarden veel internetgebruikers. Het Openbaar Ministerie zette de vervolging niet door en seponeerde de zaak.[354] De originele plaatser van het bericht werd overigens voor bedreiging (artikel 285 Sr) veroordeeld tot 130 uur werkstraf.[355]

In een arrest uit 2014 merkte de Hoge Raad met betrekking tot een andere bedreiging ten opzichte van Wilders op dat meer is vereist dan dat een verdachte een bedreiging op Twitter heeft gezet.[356] De enkele plaatsing van het bericht biedt nog niet een toereikende motivering voor het oordeel dat de verdachte bewust de aanmerkelijke kans heeft aanvaard dat bij Wilders in redelijkheid de vrees kon ontstaan dat hij het leven zou kunnen verliezen. Het vereiste opzet bij bedreiging was in deze zaak niet bewezen. Daarentegen kan zelfs het enkele zichtbaar hebben van een WhatsApp-status (waarmee iemand bepaalde informatie tijdelijk beschikbaar maakt voor al diens contacten, die vervolgens desgewenst de 'statusupdate' kunnen bekijken) al bedreiging opleveren, als deze een bedreigende inhoud heeft en de verdachte ervan uitging dat het slachtoffer deze kon en zou lezen. Dat het slachtoffer zelf een handeling verricht om kennis te nemen van de inhoud, doet aan de bedreiging niet af.[357]

Uit deze zaak (evenals uit veel andere zaken) blijkt ook dat belaging (artikel 285b Sr) even goed via internet (*cyberstalking*) als fysiek (hinderlijk volgen) kan plaatsvinden, gezien de techniekonafhankelijke formulering (wederrechtelijk stelselmatig opzettelijk inbreuk maken op iemands privacy met het oogmerk van dwang of vrees aanjagen, strafbaar met maximaal drie jaren gevangenisstraf of geldboete van de vierde categorie). In casu ging het om gedurende twee maanden regelmatig versturen van sms-berichten en WhatsApp-statussen.[358] Voor stelselmatigheid bij belaging is van belang dat het lastigvallen een bepaalde aard, indringendheid, duur en frequentie heeft; de interpretatie daarvan is zeer casus-afhankelijk: soms kunnen enkele berichten al belaging opleveren,[359] soms ook vormen 'vele bedreigingen' per sms geen belaging (als niet een bepaald effect op het slachtoffer is aangetoond).[360] Het gaat ook niet alleen om het versturen van berichten: ook bijvoorbeeld het doen van (pizza)bestellingen en het plaatsen van valse (seks)advertenties op iemands naam (waardoor deze gedurende meerde-

353 De tekst van de tweet luidde als volgt: *"Rijkelijke beloning voor diegene die Wilders z'n keel doorsnijdt. Liefst van rechts naar link, maar van links naar rechts is ook ok!"*. Zie Rb. Den Haag 9 juni 2011, ECLI:NL:RBSGR:2011:BQ7588.

354 Zie 'OM seponeert zaak tegen Bert Brussen', 11 mei 2011, www.om.nl/vaste-onderdelen/zoeken/@29126/seponeert-zaak-bert/ (laatst geraadpleegd 1 juli 2018).

355 Rb. Den Haag 9 juni 2011, ECLI:NL:RBSGR:2011:BQ7588.

356 HR 7 oktober 2014, ECLI:NL:HR:2014:2916.

357 Rechtbank Zeeland-West-Brabant 30 maart 2017, ECLI:NL:RBZWB:2017:1967.

358 *Ibid*.

359 HR 12 maart 2013, ECLI:NL:HR:2013:BZ3625 (drie anonieme, gaandeweg indringender wordende sms-berichten die refereerden aan de functionele betrokkenheid van de aangeefster als politierechercheur en die feitelijk angst en sociale ontwrichting veroorzaakten).

360 HR 12 maart 2013, ECLI:NL:HR:2013:BZ3626.

re dagen en veelvuldig door derden wordt benaderd, deels ook met seksuele intenties), kan strafbare belaging opleveren.[361]

2.12.3 *Discriminatie (artikel 137 e.v. Sr)*

Belediging van bevolkingsgroepen en discriminatie zijn strafbaar gesteld in de artikelen 137c tot en met 137g en 429quater Sr. Discriminatie wordt gedefinieerd in artikel 90quater Sr als "elke vorm van onderscheid, elke uitsluiting, beperking of voorkeur, die ten doel heeft of ten gevolge kan hebben dat de erkenning, het genot of de uitoefening op voet van gelijkheid van de rechten van de mens en de fundamentele vrijheden op politiek, economisch, sociaal of cultureel terrein of op andere terreinen van het maatschappelijk leven, wordt teniet gedaan of aangetast". Bij het Cybercrimeverdrag is een aanvullend protocol opgesteld betreffende de strafbaarstelling van handelingen van racistische of xenofobische aard verricht via computersystemen.[362] Nederland heeft dit protocol op 28 januari 2003 ondertekend en op 22 juli 2010 geratificeerd. Aangezien de discriminatiebepalingen van toepassing zijn ongeacht of zij via internet of andere computersystemen worden gepleegd, voldeed de Nederlandse wetgeving reeds aan de eisen van het protocol. Nieuw was alleen de expliciete bepaling over 'negationisme', oftewel de ontkenning, vergoelijking of goedkeuring van genocide of misdrijven tegen de menselijkheid (artikel 6 Protocol). Dit is in de Nederlandse wet niet expliciet strafbaar gesteld, maar het zal in de meeste gevallen strafbaar zijn onder artikel 137e Sr (het openbaar maken van discriminerende uitlatingen). Een initiatiefwetsvoorstel van Kamerlid Voordewind tot strafbaarstelling van negationisme is in de Tweede Kamer blijven steken.[363] Bij de ratificatie van het Protocol heeft Nederland dan ook een voorbehoud gemaakt bij artikel 6, met de strekking dat negationisme alleen strafbaar is voor zover het aanzet tot haat, discriminatie of geweld op grond van ras of religie.[364]

Uitingsdelicten kunnen goed via ICT worden gepleegd, met name ook via webpagina's, waarbij de grote verspreiding van het medium de ernst van het feit sterk kan verhogen. In de rechtspraak zijn bijvoorbeeld uitlatingen als: "Dat de meeste allochtonen het nog steeds verdommen om te werken hadden wij hem wel van tevoren kunnen vertellen. (...) Met andere woorden komen de zwartjes het geld hier niet halen, dan moet Pronk het persoonlijk brengen" bestraft als aanzetten tot haat en discriminatie van mensen wegens hun ras (artikel 137d Sr).[365] Een ander voorbeeld betreft een veroordeling tot het beledigen en aanzetten tot discriminatie van en gewelddadig optreden tegen men-

361 HR 20 maart 2018, ECLI:NL:HR:2018:392.
362 *Trb.* 2003, 60 met correctie in *Trb*. 2010, 334.
363 Zie *Kamerstukken II* 2005/06, 30579, 1-3; het (vooralsnog) laatste Kamerstuk is *Handelingen II* 13 september 2011, 105-15-52.
364 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/declarations (laatst geraadpleegd 1 juli 2018).
365 Rb. Den Haag 13 juli 1999, parketnr. 09/901011-98 en 99, genoemd in Van Donselaar en Rodrigues 2001, p. 66.

sen wegens hun seksuele geaardheid (artikel 137c en 137d Sr).[366] De verdachte had in een kort tijdsbestek zes tweets geplaatst met een voor homoseksuelen zeer kwetsende, bedreigende en gewelddadige inhoud.
Het probleem van uitingsdelicten op internet moet niet worden onderschat. In 2013 berichtte de NOS dat er in Nederland dagelijks (!) ongeveer 35.000 bedreigingen via Twitter worden geuit.[367] De politie trekt ongeveer tweehonderd daarvan na. De tweets worden door middel van 'Real Time Intelligence Centers' door de politie gemonitord.[368] Als de betrokkenen kunnen worden opgespoord, krijgen ze soms een bezoek van de politie en in ernstige gevallen volgt een arrestatie. Dreigtweets kunnen ook ernstige consequenties hebben. Zo leidde de bedreiging van een jonge man op een forum dat hij zijn klasgenoten zou doodschieten tot de sluiting van scholen in Leiden voor een periode van drie dagen. Hij bleek de bedreiging vanuit een hostel in Costa Rica te hebben geplaatst, hetgeen de opsporing bemoeilijkte.[369] Ook kan worden gedacht aan bommeldingen die tot een klopjacht op de dader van de berichten kunnen leiden.[370]

2.12.4 *Opruiing (artikel 131-132 Sr)*

Vanwege de terroristische dreiging is er in toenemende mate aandacht voor het delict opruiing (artikel 131 en 132 Sr, maximaal vijf respectievelijk drie jaren gevangenisstraf of geldboete van de vierde categorie). In de rechtspraak veroordelen rechters mensen regelmatig voor het plaatsen van opruiende filmpjes op YouTube. In 2013 werd door de Rechtbank Amsterdam bijvoorbeeld een verdachte veroordeeld voor het verspreiden van afbeeldingen en een geschrift ter opruiing, door op internetsites films en een tekst te plaatsen die oproepen tot de gewapende jihad, alsook door daaromtrent op het forum van die websites een discussie te starten.[371] Daarmee heeft de verdachte getracht "mensen aan te zetten tot het begaan van strafbare feiten of van agressie tegen het openbaar gezag", aldus de rechtbank. Ook bij opruiing leidt een retweet van een op zichzelf opruiend bericht echter niet altijd tot strafbaarheid. In 2015 overwoog de Rechtbank Den Haag bijvoorbeeld in een terrorismezaak dat het "retweeten van een bericht dat op zich als opruiend wordt beoordeeld in beginsel niet strafbaar is ingevolge artikel 131 Sr". Dat kan anders zijn wanneer uit "het commentaar van verdachte bij de retweet blijkt dat hij de inhoud onderschrijft, of wanneer het geretweete bericht past

366 Rb. Amsterdam 30 januari 2013, ECLI:NL:RBAMS:2013:BZ0575. Zie voor een vergelijkbare zaak ten opzichte van joden Rb. Den Haag 17 september 2015, ECLI:NL:RBDHA:2015:12631.
367 Nos.nl, '200 ernstige dreigtweets per dag', 31 oktober 2013, http://nos.nl/artikel/569183-200-ernstige-dreigtweets-per-dag.html (laatst geraadpleegd 1 juli 2018).
368 Politie.nl, 'Opsporing succesvoller dankzij RTIC', 14 augustus 2015. Beschikbaar op: https://www.politie.nl/nieuws/2015/augustus/14/04-opsporing-succesvoller-dankzij-rtic.html (laatst geraadpleegd 1 juli 2018).
369 Rb. Den Haag 19 november 2013, ECLI:NL:RBDHA:2013:15617.
370 Zie bijvoorbeeld Rb. Den Haag 5 maart 2013, ECLI:NL:RBDHA:2013:BZ3281, Rb. Noord-Holland 11 februari 2016, ECLI:NL:RBNHO:2016:1023 (de 'V&D-dreiger') en Hof Arnhem-Leeuwarden 20 april 2018, ECLI:NL:GHARL:2018:3737 (de 'Jumbo-dreiger').
371 Rb. Amsterdam 23 oktober 2013, ECLI:NL:RBROT:2013:8266. Zie voor opruiende tweets met een jihadistische boodschap ook Hof Den Haag 20 mei 2017, ECLI:NL:GHDHA:2017:1224.

binnen een reeks van berichten van verdachte van dezelfde aard en/of strekking, binnen een bepaalde periode. Hetzelfde geldt ook voor het delen van een hyperlink", aldus de rechtbank.[372]
Uitingen die beschrijven hoe (bijvoorbeeld terroristische) aanslagen (kunnen) worden gepleegd maar niet duidelijk oproepen dat ook te doen, vallen niet onder opruiing. Kort na de aanslagen van 11 september 2001 ontstond commotie over een handboek terrorisme dat te vinden was op internet. Het ging om een soort receptenboek dat aangaf hoe bepaalde terroristische handelingen kunnen worden verricht. In antwoord op Kamervragen gaf de minister aan dat dergelijke informatie niet kan worden beschouwd als opruiing of verspreiding tot opruiing (artikel 131-132 Sr), noch als uitlokking (artikel 47 lid 1 onder 2 Sr) of als poging tot uitlokking daarvan (artikel 46a Sr), en dat hij vooralsnog geen mogelijkheden zag "om verspreiding van de informatie tegen te gaan, hoe verwerpelijk ik deze ook vind".[373]

2.12.5 *Strafrechtelijke aansprakelijkheid van internetaanbieders (artikel 54a Sr)*

Artikel 54a Sr bevat een wettelijke vervolgingsuitsluitingsgrond voor internetaanbieders die 'als zodanig' (dat wil zeggen als tussenpersoon) optreden (zie onder). Zij kunnen (vanzelfsprekend) wel aansprakelijk zijn als ze niet *als zodanig* – dus als internetaanbieder – optreden, maar anderszins betrokken zijn bij strafbare inhoud. Indien een dienstaanbieder actieve bemoeienis met de inhoud heeft, bijvoorbeeld als actieve moderator van een nieuwsgroep, discussieforum, blog of mailinglijst, waarbij hij aangeeft toe te zien op het weren van discriminerende uitingen, dan is zijn positie veeleer met die van een hoofdredacteur van een tijdschrift te vergelijken en kan hij zonder meer als medepleger of medeplichtige van eventuele uitingsdelicten worden aangemerkt.[374] Wil een internetaanbieder niet (mede)aansprakelijk zijn voor strafbare inhoud die hij faciliteert, dan moet hij zich dus niet met de inhoud 'inlaten'.[375]
Omdat tussenpersonen op internet echter veelal een andere rol hebben dan klassieke drukkers of uitgevers (die meestal alles onder ogen krijgen en veel directer toezien op de inhoud van wat zij drukken en publiceren), bestaat het gevaar van (zelf)censuur indien internetaanbieders onder dreiging van strafrechtelijke medeplichtigheid aan uitingsdelicten, al te snel zouden overgaan tot het filteren of verwijderen van omstreden uitingen. Om die reden heeft de wetgever een expliciete vervolgingsuitsluitingsgrond

372 Rb. Den Haag 10 december 2015, ECLI:NL:RBDHA:2015:14365, r.o. 11.22, *Computerrecht* 2016/47, nr. 2, m.nt. J.J. Oerlemans ('Context-zaak'). Over de strafrechtelijke aansprakelijkheid voor hyperlinks in het algemeen, zie Kentgens 2010.

373 *Aanhangsel Handelingen II* 2001/02, 465, p. 975.

374 Vgl. Harteveld & Van der Neut 1996, Van der Net 2000, p. 55 en Schellekens 2001, p. 147-152. Over de diverse mogelijke rollen van aanbieders, zie De Roos & Wissink 1996, p. 191 e.v.

375 *Kamerstukken II* 2001/02, 28197, 3, p. 64: "Dat wil in concreto zeggen dat de tussenpersoon zich dient te beperken tot zijn intermediaire, werktuigelijke rol ten aanzien van de van een ander afkomstige gegevens. De tussenpersoon mag zich niet bemoeien met ontstaan, bestemming en inhoud van de doorgegeven of opgeslagen gegevens. De dienstverlener die van een ander afkomstige gegevens opslaat, mag dat dus niet onder zijn gezag [of] toezicht doen plaatsvinden (...) De tussenpersoon moet een intermediaire rol vervullen en zich niet met de gegevens inlaten".

in het leven geroepen. Artikel 54a Sr kent echter een roerige geschiedenis; pas in de Wet computercriminaliteit III is een (grotendeels) adequate regeling getroffen.

GESCHIEDENIS

In het wetsvoorstel Computercriminaliteit II werd oorspronkelijk een nieuwe tekst van artikel 53 Sr (dat uitsluiting van aansprakelijkheid voor uitgevers regelt) voorgesteld om de aansprakelijkheid van internetaanbieders te regelen. Kort gezegd zou een tussenpersoon als zodanig niet worden vervolgd voor uitingsdelicten indien hij zijn identiteit had bekendgemaakt, de dader bekendmaakte en na aanmaning alle handelingen zou verrichten ter voorkoming van verdere verspreiding.[376] Bij nota van wijziging werd dit voorstel ingetrokken,[377] omdat het strijdig was met Richtlijn 2000/31/EG (elektronische handel).[378]

De Wet elektronische handel[379] heeft de Richtlijn grotendeels geïmplementeerd in het civiele recht (zie artikel 6:196c BW), maar voerde ook artikel 54a Sr in: "Een tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens die van een ander afkomstig zijn, wordt als zodanig niet vervolgd indien hij voldoet aan een bevel van de officier van justitie, na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris, om alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om de gegevens ontoegankelijk te maken". Onder deze bepaling vallen aanbieders van zowel transport-, *caching*- als opslagdiensten.[380]

De bepaling was echter ongelukkig, omdat de vrijwaring gekoppeld was aan een verondersteld maar niet geregeld *notice-and-takedown*-regime: de aanbieder moest het materiaal verwijderen op vordering van de officier van justitie, die daarvoor machtiging van de rechter-commissaris nodig had. De officier had echter geen bevoegdheid om de r-c om toestemming te vragen; het Wetboek van Strafrecht zelf (dus artikel 54a Sr) kan geen grondslag bieden voor opsporingsbevoegdheden, artikel 125o Sv is hier niet van toepassing[381] (zie nader paragraaf 3.2.6 en 3.2.7) en er was geen andere grondslag voor de officier om bij de r-c een machtiging te vragen.[382] Ook is in de literatuur kritiek geuit op de gebrekkige rechtsbescherming: er waren geen bepalingen voor notificatie aan de inhoudsaanbieder, en noch de inhoudsaan-

376 *Kamerstukken II* 1998/99, 26671, 1-3. Zie daarover De Roos 1998, Schuijt 1998 en Koops & Schellekens 1999.
377 *Kamerstukken II* 1999/2000, 26671, 5.
378 Richtlijn 2000/31/EG, *PbEG* 17 juli 2000, L 178/ 1-16. Zie hierover in dit verband Van der Net 2000, p. 67 e.v. en Schellekens 2001, p. 215-225. Zo was het onderdeel dat de internetaanbieder verplicht was de identiteit van de dader bekend te maken, onverenigbaar met de richtlijn, aldus *Kamerstukken II* 2001/02, 28197, 3, p. 66.
379 Aanpassingswet richtlijn inzake elektronische handel, *Stb.* 2004, 210.
380 *Kamerstukken II* 2001/02, 28197, 3, p. 62.
381 Artikel 125o Sv biedt geen basis om derden te bevelen mee te werken met ontoegankelijkmaking, zie *Kamerstukken II* 2004/05, 26671, 10, p. 16.
382 Rb. Assen 24 november 2009, ECLI:NL:RBASS:2009:BK4226. Zie ook Schellekens, Koops & Teepe 2007.

> bieder noch de internetaanbieder kon in beroep gaan tegen ontoegankelijkmaking of tegen het uitblijven van de opheffing daarvan.[383]

De Wet computercriminaliteit III voorziet wel in een sluitend(er) stelsel van *notice-and-takedown*. Artikel 54a Sr is herzien en nu gekoppeld aan de bevoegdheid van de officier om verwijdering te vorderen op basis van het nieuwe artikel 125p Sv. De regeling is ook voorzien van meer rechtswaarborgen (zie nader paragraaf 3.2.7). Er blijft echter een aanzienlijke kans bestaan dat het verwijderde materiaal nooit door een rechter ter zitting wordt getoetst op strafbaarheid, wat een gevaar inhoudt dat te snel vermeend onrechtmatig materiaal wordt weggehaald.[384] Het is dan ook van belang dat de rechter-commissaris alleen bij *onmiskenbaar* onrechtmatig materiaal een machtiging geeft voor een verwijderingsbevel.
De internetaanbieder kan de ontoegankelijkmaking uitvoeren door de gegevens te versleutelen, of ze te verwijderen met behoud van een kopie voor de strafvordering. Voorwaarde is wel dat de aanbieder hiertoe in staat is; bij een opslagaanbieder zal dat eerder het geval zijn dan bij een transport- of *caching*-aanbieder.[385] Indien de internetaanbieder weigert aan een ontoegankelijkmakingsbevel te voldoen, vervalt de uitsluitingsgrond en is hij vermoedelijk bovendien strafbaar op grond van artikel 184 Sr, het niet voldoen aan een bevoegd gegeven ambtelijk bevel.[386]
Artikel 54a Sr zou kunnen suggereren dat een internetaanbieder zich niet op de aansprakelijkheidsuitsluiting kan beroepen als er nooit een ontoegankelijkmakingsbevel is gegeven, ook al heeft hij het materiaal (bijvoorbeeld vrijwillig) verwijderd. Naar de geest van de bepaling – en als richtlijnconforme interpretatie – moet echter worden geconcludeerd dat de aanbieder ook niet, althans niet *als zodanig*, strafrechtelijk aansprakelijk kan worden gehouden voor illegale inhoud in de periode voordat de officier van justitie een bevel geeft.[387]

Artikel 54a Sr heeft dezelfde ratio als de bepalingen van artikel 53-54 Sr (de uitsluiting van aansprakelijkheid, onder bepaalde voorwaarden, voor uitgever en drukker), namelijk het beschermen van de vrijheid van meningsuiting.[388] Een belangrijk verschil met de artikelen 53-54 is echter dat deze artikelen zich beperken tot een strafuitsluitingsgrond bij drukpersdelicten, dus voornamelijk uitingsdelicten. Artikel 54a Sr biedt echter strafuitsluiting voor elk mogelijk strafbaar feit waarbij de internetaanbieder als

383 Schellekens, Koops & Teepe 2007.
384 Zie paragraaf 3.2.7. Zie ook Koops 2010 en Oerlemans 2017c.
385 *Kamerstukken II* 2001/02, 28197, 3, p. 65.
386 *Kamerstukken II* 2001/02, 28197, 3, p. 66.
387 Schellekens, Koops & Teepe 2007, p. 27.
388 *Kamerstukken II* 2001/02, 28197, 3, p. 62-63: "De ratio is de vrijheid van meningsuiting in een digitale omgeving zo veel mogelijk te ondersteunen door de neiging tot preventieve censuur weg te nemen. De tussenpersoon kan zonder angst voor een strafrechtelijke vervolging van een ander afkomstige gegevens doorgeven of al dan niet tijdelijk opslaan. Zelfs al heeft hij kennis van het strafbare karakter van de gegevens. (...) De regeling dient een onbelemmerde informatie-uitwisseling en daarmee een grondbeginsel van de democratische rechtsstaat".

tussenpersoon optreedt, dus bijvoorbeeld ook voor de verspreiding van virussen of het plegen van ddos-aanvallen. "De rechtvaardiging voor dit onderscheid is gelegen in de algemene intermediaire functie die in het huidige en toekomstige, internationale maatschappelijke verkeer wordt vervuld door de tussenpersoon die een telecommunicatiedienst verleent bestaande in de doorgifte of opslag van gegevens."[389] Bij mogelijke aansprakelijkheid voor computergerichte delicten als virusverspreiding zou de internetaanbieder immers toch het internetverkeer in de gaten moeten houden, en daarmee zou alsnog het risico van preventieve censuur optreden.

Een en ander wil niet zeggen dat internetaanbieders geen enkele verantwoordelijkheid hebben om in de gaten te houden welke inhoud zij doorgeven. De *Notice and Take-down*-gedragscode (zie paragraaf 3.2.7) is een voorbeeld van zelfregulering. Internetaanbieders filteren inmiddels standaard op (bekende) kinderpornografie.[390] Ook blijken (de populaire Amerikaanse) sociale-mediadienstaanbieders bereid om strafbare of 'onwenselijke' berichten van hun platformen te weren door filters toe te passen en zo snel mogelijk te reageren op verzoeken om materiaal ontoegankelijk te maken. Contractueel behouden internetaanbieders zich vaak het recht voor om (in hun ogen) onrechtmatige (en soms ook anderszins 'schadelijke') inhoud te weren.[391] Een en ander wordt verder gefaciliteerd door activiteiten zoals die van de 'European Union Internet Referral Unit' (EU IRU) bij Europol, die zich richt op het detecteren van extremistische propaganda op internet en daarvan melding doet bij internetaanbieders, naast het ondersteunen van lidstaten bij de aanpak hiervan.[392]

In het licht van deze zelf- en coregulering is er in toenemende mate aandacht voor het vraagstuk van zorgplichten van internetaanbieders.[393] Zowel de aanwezigheid van grote hoeveelheden schadelijke of maatschappelijk onwenselijke uitingen op internet, als de activiteiten die aanbieders zelf al op zich nemen, roepen de vraag op of internetaanbieders een (vooral privaatrechtelijke) zorgplicht hebben om activiteiten te ontwikkelen ter bestrijding van onrechtmatige inhoud. Voor internetaanbieders zijn er echter weinig aanknopingspunten een dergelijke zorgplicht te construeren,[394] en gezien het risico van overblokkering bij actieve bestrijding van schadelijke inhoud[395] lijkt ons dat een goede zaak.

Aan de andere kant hoeft volgens ons ook niet op voorhand elke zorgplicht te worden uitgesloten, met name omdat de brede reikwijdte van artikel 54a Sr zou kunnen suggereren dat internetaanbieders ook geen verantwoordelijkheid zouden hebben om computergerichte criminaliteit tegen te gaan. Bij het monitoren van internetverkeer op

389 *Kamerstukken II* 2001/02, 28197, 3, p. 63.
390 Zie reeds Stol e.a. 2008, p. 110-111.
391 Vgl. Van der Net 2000, p. 61.
392 Zie https://www.europol.europa.eu/newsroom/news/europol-internet-referral-unit-one-year (laatst geraadpleegd 1 juli 2018). De juridische basis voor het team is gecreëerd in de Europol-Verordening 2016/794, *OJ* L 135/53, 24 mei 2016.
393 Zie Van Eijk e.a. 2010 en Tjong Tjin Tai & Koops 2015.
394 Tjong Tjin Tai & Koops 2015, p. 1068-1069. Vgl. ook Van der Net 2000, p. 60. Vgl. Schellekens 2001, p. 154-156.
395 Vgl. Van der Net 2000, p. 60 en Schellekens 2001, p. 154-156.

bijvoorbeeld virussen, ransomware of ddos-aanvallen is het niet nodig kennis te nemen van de uitingen van internetgebruikers, maar volstaat het om automatisch na te gaan of bepaalde karakteristieke bitreeksen van bekende virussen of aanvallen voorkomen in gehoste of getransporteerde berichten. Een zorgplicht voor bestrijding van cybercriminaliteit in enge zin levert minder gevaar op van zelfcensuur en zou in dat licht een waardevolle bijdrage kunnen leveren aan de bestrijding van cybercriminaliteit.[396]

2.13 Auteursrechtschendingen

Artikel 10 Cybercrimeverdrag bevat een verplichting tot strafbaarstelling van bepaalde inbreuken op auteursrecht en naburige rechten. De Nederlandse wet kent wel strafbepalingen in het auteursrecht, maar het auteursrecht wordt in Nederland vrijwel alleen civielrechtelijk, en niet of nauwelijks, strafrechtelijk gehandhaafd.[397] Om die reden beperken we ons hier tot een korte aanduiding van de belangrijkste strafbepalingen.
Artikel 31 Auteurswet (Aw) bevat een algemene strafbaarstelling van opzettelijke inbreuken op het auteursrecht van een ander, met een maximum van zes maanden gevangenisstraf of geldboete van de vierde categorie. Het verspreiden van, en andere commerciële handelingen met, voorwerpen waarop inbreukmakende werken staan, kent een maximumstraf van één jaar gevangenis of geldboete van de vijfde categorie (artikel 31a Aw). Indien deze inbreuken beroeps- of bedrijfsmatig worden gepleegd, stijgt het strafmaximum naar vier jaren gevangenisstraf (artikel 31b Aw). Inbreuk op persoonlijkheidsrechten (bijvoorbeeld wederrechtelijk wijzigen van de auteursnaam) is strafbaar onder artikel 34 Aw (maximaal zes maanden gevangenisstraf of geldboete van de vierde categorie).
Het aanbieden, ter verspreiding voorhanden hebben of uit winstbejag bewaren van middelen ter omzeiling van anti-kopieerbeveiliging, is strafbaar met maximaal zes maanden gevangenisstraf of geldboete van de vierde categorie (artikel 32a Aw). Het gaat daarbij om middelen die *uitsluitend* bestemd zijn voor omzeiling van anti-kopieerbeveiliging. In de rechtspraak is dit artikel toegepast op het aanbieden van gemodificeerde chips ('mod-chips') voor Sony-spelcomputers.[398] Simlocks in mobiele telefoons zijn echter geen auteursrechtelijk beschermde werken, zodat het uitschakelen daarvan niet wederrechtelijk is.[399] Het artikel werd ook ingeroepen in een zaak waarin De Telegraaf zoekresultaten van de databank van de NVM toonde (en hierdoor bepaalde beveiligingen van de webstek van de NVM zou omzeilen), maar het hof ging

396 Vgl. Tjong Tjin Tai & Koops 2015, p. 1072.
397 Verkade, *T&C Intellectuele eigendom*, artikel 31 Aw, aant. 1, verwijzend naar de Aanwijzing intellectueleeigendomsfraude (2005A022), *Stcrt*. 2006, 6, p. 10 en Hof Den Haag 27 januari 2014, ECLI:NL:GHDHA:2014:84 (niet-onvankelijkverklaring OM bij grootschalig illegaal uploaden van 5.000 e-books op The Pirate Bay). De douane handhaaft overigens wel strafrechtelijk, zie *Kamerstukken II* 2015/16, 31934, 7, p. 2.
398 Rb. Alkmaar 30 november 2000, *Computerrecht* 2001/2, p. 157, m.nt. Koelman.
399 Rb. Maastricht 12 maart 2002, ECLI:NL:RBMAA:2002:AE0125.

hier niet op in omdat het slechts het gebruik en niet het verhandelen van eventuele kraakmiddelen betrof.[400]

2.14 Blik op de toekomst

Dit hoofdstuk bood een overzicht van strafbaarstelling van computercriminaliteit naar huidig recht. Zoals uit de vele besproken wetten – niet beperkt tot de serie-computercriminaliteit, maar ook vele wetten daarnaast – blijkt, is dit veld voortdurend in beweging. Ontwikkelingen in technologie maken vaak nieuwe gedragingen mogelijk, of leiden tot ingrijpende wijzigingen in het gedrag van mens en maatschappij, zodat vaak vragen rijzen rond de toepasbaarheid van de strafwetgeving op schadelijke of anderszins maatschappelijk onwenselijke vormen van gedrag. Het is moeilijk te voorzien welke verdere aanpassingen in het Wetboek van Strafrecht in de toekomst nodig zullen zijn in het licht van toekomstige technische ontwikkelingen.[401] Ter afsluiting van dit hoofdstuk willen we slechts wijzen op enkele ontwikkelingen waarvan wij verwachten dat die significante vragen zullen doen rijzen rond de toepasbaarheid van het huidige strafrecht. Te denken valt bijvoorbeeld aan:

- de toename van aanvallen op apparaten in het Internet of Things (IoT), en op iets langere termijn op mensen in het Internet of People. Deze aanvallen zullen strafbaar zijn onder de bestaande delicten (bijvoorbeeld artikel 138ab, 139c en 350a Sr), maar de rechtspraak zal moeten bepalen wanneer de strafverzwarende omstandigheden van artikel 138b leden 2 en 3 aan de orde is. Wat is 'ernstige' schade? Welke IoT-apparaten behoren tot de vitale infrastructuur? Welke met het lichaam verbonden apparaten zijn 'van essentieel belang' voor 'de gezondheid'?
- nieuwe vormen van criminaliteit via aanvallen op IoT-apparaten, zoals het hacken en op afstand doen bewegen van de ruitenwissers, het ontoegankelijk maken van een slimme auto, of het op afstand tijdelijk uitschakelen van de koelkast of verwarming thuis. Zulke criminaliteit valt altijd te kwalificeren onder de computergerichte delicten (hacken, gegevensbeschadiging), maar roept ook Runescape-achtige vragen op over kwalificatie onder klassieke delicten. Is het heimelijk uitzetten van de koelkast zodat melk en kliekjes bederven zonder dat de bewoner het in de gaten heeft, een poging tot het toebrengen van (zwaar) lichamelijk letsel? Is het uitzetten van de verwarming tijdens een vrieskoude nacht een poging tot doodslag?
- een toename van doxing (of doxxing): het verzamelen (veelal uit publiek toegankelijke bronnen) en vervolgens publiceren van gegevens over een bepaalde persoon of organisatie, hetzij als vorm van (burger)activisme (vergelijkbaar met het Chinese fenomeen van 'human flesh search'), maar ook als vorm van iemand lastig vallen.[402]

400 Hof 's-Gravenhage 21 december 2000, *Computerrecht* 2001/2, p. 89-93, m.nt. Struik (*ElCheapo*), in stand gehouden door HR 22 maart 2002, ECLI:NL:HR:2002:AD9138.

401 Voor enkele criminologische inschattingen van toekomstige ontwikkelingen, zie bijvoorbeeld Europol 2015a en Goodman 2016.

402 Zie https://en.wikipedia.org/wiki/Doxing (laatst geraadpleegd 1 juli 2018).

Rechtspraak zal moeten vaststellen onder welke voorwaarden dit als bijvoorbeeld smaad of belaging kan worden gekwalificeerd;

- nieuwe vormen van beeldmanipulatie, zoals *deepfake*,[403] waarbij over het gezicht van een gefilmde persoon in een video het gezicht van een ander wordt geprojecteerd. Denk bijvoorbeeld aan het vervangen van het gezicht van een actrice in een pornofilm door dat van een klasgenote, of het vervangen van het gezicht van een Wilders-aanhanger in een video over een partijbijeenkomst door dat van een collega. Dit kan uit de hand gelopen grappen betreffen, maar ook georganiseerde afpersing, en roept vragen op over bijvoorbeeld de kwalificatie van 'afbeelding van een persoon'. Ook zal mogelijk discussie ontstaan over de noodzaak van zelfstandige strafbaarstelling, vergelijkbaar met de discussie rond wraakporno;
- maatschappelijk ontwrichtende vormen van cybercrime. Denk aan het hacken en verwijderen van gegevens op computers van vitale infrastructuren, zoals energiebedrijven en de waterschappen. De 'Wannacry-aanval' uit 2017 leidde onder andere tot een onbruikbare spoorlijn tussen Duitsland en Rusland en onbruikbare benzinestations in Frankrijk. Wanneer kunnen dergelijke ontwrichtende aanvallen precies als terroristisch misdrijf bestempeld worden? En wat zijn proportionele verdedigingsacties, als een slachtoffer een aanval eigenlijk alleen effectief kan stoppen door zelf (terug) te hacken en aanvallende computers te saboteren (mede in aanmerking nemend dat aanvallen afkomstig kunnen zijn van gehackte computers van onschuldige derden)?
- de opkomst van 'fake news' in het 'post-truth'-tijdperk, met een toenemende roep om bestrijding hiervan. Moet nepnieuws (ook) langs strafrechtelijke weg worden aangepakt en wellicht zelfs – bij ernstige vormen – strafbaar worden gesteld (vergelijkbaar met bijvoorbeeld koersmanipulatie)? Of valt nepnieuws al onder bestaande strafbepalingen?
- misbruik van virtual reality, waarbij software wordt gemanipuleerd zodat iemand virtueel wordt aangevallen, in elkaar geslagen of verkracht; hoewel het hier geen fysiek geweld betreft, heeft virtual reality mogelijk psychologisch de overtuigingskracht van de fysieke werkelijkheid, zodat de grens tussen fysiek en mentaal geweld bij virtual reality zal vervagen. Dit roept vragen op over de toepasbaarheid van klassieke geweldsmisdrijven op virtuele aanvallen;
- misbruik van virtual reality in combinatie met sensoren die op het lichaam zijn aangebracht, waardoor de in het vorige punt bedoelde aanvallen wel een fysieke component hebben. Denk aan ongewenste seksuele intimiteiten bij gebruik van seksuele sensoren (teledildonics). De klassieke geweldsdelicten, waaronder verkrachting, zullen hier van toepassing zijn, maar vragen zullen rijzen rond situaties waarin de sensoren in spelsituaties en op vrijwillige basis worden gebruikt. Waar ligt de grens van onvrijwillige seks wanneer een (meerderjarig) slachtoffer zelf sensoren aanbrengt op zijn of haar geslachtsdelen en met een enkele muisklik (of wellicht een simpel spraakcommando) een eind kan maken aan een seksuele situatie?

403 Zie https://en.wikipedia.org/wiki/Deepfake (laatst geraadpleegd 1 juli 2018).

Is er sprake van poging tot verkrachting wanneer iemand via teledildonics een penetratiebeweging maakt maar de communicatiepartner (anders dan de dader denkt) geen sensor heeft aangebracht op het te penetreren lichaamsdeel?

- aanvallen op en misbruik van robots. Naarmate drones, huishoudrobots en zorgrobots meer in gebruik raken, valt te voorzien dat deze gehackt en op afstand bestuurd zullen worden, zodat fysieke aanvallen met robots kunnen worden gepleegd. Dit roept vergelijkbare vragen op als bij aanvallen op IoT-apparaten, maar ook vragen rond schuldaansprakelijkheid. Kan de eigenaar van een slecht beveiligde robotstofzuiger of drone die, tegen de algemeen bekende regels in, verzuimd heeft het standaard-wachtwoord te veranderen, worden vervolgd op basis van het culpose delict van artikel 161septies Sr, wanneer de gehackte stofzuiger of drone levensgevaar oplevert voor in de woonkamer kruipende baby's of in de tuin spelende peuters? Ook zullen complexe toerekeningsvraagstukken ontstaan, wanneer haperende robots ernstig lichamelijk letsel of iemands dood veroorzaken. Valt deze verwijtbaar toe te rekenen aan de gebruiker of producent, in culpose zin of zelfs als voorwaardelijk opzet? En als er aanwijzingen zijn dat de hapering opzettelijk is veroorzaakt (en het dus om een bewuste aanval kan gaan), kan de gebruiker van de robot dan succesvol een 'hacker-verweer' (ik heb niets gedaan, het moet een hacker geweest zijn) inroepen?