Cybercriminaliteit

Koops, E.J.

Published in:
Recht en compuer, zesde druk

Document version:
Peer reviewed version

Publication date:
2014

B.J. Koops, 'Cybercriminaliteit',
in: Van der Hof, Lodder & Zwenne (red.), *Recht & Computer*, 6e druk, Deventer: Kluwer, p. 213-241

9. Cybercriminaliteit

Bert-Jaap Koops

1. Inleiding

De informatiemaatschappij is kwetsbaar. Individuen, bedrijven en de overheid worden steeds afhankelijker van computers en informatie, niet in het minst omdat vrijwel alle computers tegenwoordig verbonden zijn met netwerken waardoor het risico van aanvallen op informatiesystemen significant toeneemt. Fysieke en offline processen worden in toenemende mate vervangen door digitale en online processen. De noodzaak van adequate beveiliging van computers en informatie is daardoor alleen maar groter geworden. Adequate informatiebeveiliging is echter een enorme uitdaging die niet door alle computergebruikers even goed wordt opgepakt. Beveiliging kan ook nooit volledig zijn, zeker niet in een dynamische Internetomgeving waarin cybercriminelen wereldwijd de nieuwste kwetsbaarheden opsporen en uitbuiten. Er ligt daarom ook een belangrijke rol voor het strafrecht om aanvallen op computers en informatie te bestrijden. Daarvoor is materiële en procedurele wetgeving nodig die zo goed mogelijk dekkend en actueel is. De opdracht voor de wetgever is om de wet voldoende abstract – zo men wil techniek-neutraal – te maken zodat nieuwe ontwikkelingen in ICT en cybercriminaliteit opgevangen kunnen worden met bestaande bepalingen, en tegelijkertijd dusdanig specifiek te formuleren dat het voldoende duidelijk is voor burgers en politie wat zij wel en niet mogen doen. Een goede balans tussen toekomstbestendigheid en rechtszekerheid is geen gemakkelijk opgave,[1] maar Nederland heeft inmiddels een behoorlijke traditie opgebouwd in cybercriminaliteitswetgeving die tijdig inspeelt op ICT-ontwikkelingen. In dit hoofdstuk wordt een overzicht gegeven van deze wetgeving, met als hoofdbestanddelen een bespreking op hoofdlijnen van het materiële (par. 9.3) en procedurele strafrecht (par. 9.4).[2] Deze kern wordt geflankeerd door een schets van de context en geschiedenis van cybercriminaliteit en de wetgeving (par. 9.2) en een korte reflectie over de rol van het strafrecht en een blik op de toekomst (par. 9.5).

2. Achtergronden

2.1. Begripsbepaling

Cybercriminaliteit kan worden omschreven als strafbare feiten[3] 'gepleegd door gebruikmaking van elektronische communicatienetwerken en informatiesystemen of tegen dergelijke netwerken en systemen'.[4] De nadruk ligt hierbij op met netwerken verbonden computers. De Nederlandse wetgeving gebruikt van oudsher de term computercriminaliteit, wat kan worden omschreven als criminaliteit waarbij computers of computergegevens een substantiële rol spelen. In de jaren '80 en '90 lag de nadruk op computers zelf, terwijl inmiddels de nadruk ligt op computernetwerken. Omdat de meeste computers aangesloten zijn op een netwerk – meestal het Internet, of anders op interne netwerken – is het verschil niet echt wezenlijk meer. Een aanval op een losstaande computer valt wel onder computercriminaliteit maar, formeel gesproken, niet onder cybercriminaliteit. De begrippen worden echter in de praktijk vaak als synoniemen gehanteerd, en het ligt voor de hand het tegenwoordig frequenter gebruikte begrip 'cybercriminaliteit' als

[1] Zie Koops 2006.
[2] Voor een meer gedetailleerde bespreking van de wetgeving, zie Koops 2007a.
[3] De Nederlandse versie van de Mededeling gebruikt de ongelukkige vertaling 'misdrijven' voor het Engelse 'criminal acts'; men kan beter spreken van strafbare feiten omdat cybercriminaliteit in principe ook overtredingen kan betreffen.
[4] Europese Commissie 2007, p. 2.

kernbegrip te gebruiken maar daar een brede invulling aan te geven door ook niet-netwerkgerelateerde computercriminaliteit hieronder te laten vallen.

Cybercriminaliteit kan worden onderscheiden in drie typen:[5]

1. computergerichte delicten: strafbare feiten gepleegd tegen computers, computernetwerken of computergegevens; hierbij fungeren computers of gegevens als doel;

2. computer-gerelateerde delicten: strafbare feiten gepleegd met gebruikmaking van computers, computernetwerken of computergegevens; hierbij fungeren computers of gegevens als substantieel hulpmiddel, wat wil zeggen dat de deze een relevante rol speelt bij het plegen van het delict;

3. computer-relevante delicten: strafbare feiten waarbij computers, computernetwerken of gegevens op de een of andere manier relevant zijn, als omgevingsfactor; hierbij fungeren computers of gegevens als een niet-substantieel hulpmiddel, bijvoorbeeld voor het opslaan van kinderpornografie of het versturen van een email bij de voorbereiding van een bankoverval; deze categorie omvat vooral uitingsdelicten, maar ook alle klassieke delicten (zoals moord of verkrachting) waarbij mogelijk bewijsmateriaal opgeslagen ligt in computers en waarbij de computer dus voor de opsporing een relevante factor is.

2.2. Criminologische context

Computers en vooral computernetwerken vormen een vruchtbare bodem voor criminaliteit. Het Internet kent vele aspecten die het makkelijk(er) of aantrekkelijk(er) maken voor potentiële misdadigers om hun slag te slaan. Op basis van criminologische literatuur over cybercriminaliteit kunnen als relevante criminogene factoren worden genoemd dat het Internet wereldwijd is, er sprake is van deterritorialisering, er flexibele netwerken gevormd worden tussen daders of dadergroepen, de interactie tussen dader en slachtoffer op afstand plaatsvindt en dat er maar beperkt sprake is van 'capable guardianship' in de sociale omgeving van potentiële daders; verder is er sprake van anonimiteit, manipuleerbaarheid van programmatuur en data, automatisering van aanvallen, een veel grotere schaal om misdrijven te plegen, gekoppeld aan de mogelijkheid om grote winst te behalen door aggregatie van kleine winsten van veel slachtoffers, een informatie-economie waarin gegevens geld waard zijn, en snelle ICT-innovatiecycli.[6] Al met al betekent dit dat het Internet een 'opportunity structure' schept voor het plegen van criminaliteit op wereldwijde schaal, waardoor criminaliteit langzamerhand transformeert van fysieke, locale misdaad naar digitale netwerkmisdaad.[7] Cybercriminaliteit gaat lang niet meer alleen om hackers die hun reputatie binnen hun referentiegroep willen verstevigen, maar er is ook toenemend sprake van criminaliteit met winstoogmerk, met een ondergrondse markt van hackermiddelen en buitgemaakte (financiële) gegevens,[8] en mogelijk ook van verwevenheid van criminaliteit met andere soorten cyberaanvallen (door terroristen of buitenlandse mogendheden)[9].

Daarbij moet wel worden aangetekend dat de empirische kennis over de omvang van cybercriminaliteit nog niet bijzonder groot is. Er bestaat van oudsher een hoog 'dark number' omdat slachtoffers – zowel individuen als bedrijven – vaak geen aangifte doen,[10] terwijl gepubliceerde cijfers over schade die aangericht is door cyberaanvallen vaak met een korrel zout moeten worden genomen omdat ze gerapporteerd worden door (beveiligings)bedrijven die er belang bij hebben om de risico's van cyberaanvallen uit te vergroten. De meest betrouwbare indicatie van de omvang van cybercriminaliteit kan worden gevonden in slachtofferstudies, maar ook deze zijn beperkt omdat ze of onder individuen of onder bedrijven (maar niet onder beide tegelijk) worden gehouden en omdat slachtoffers zelf niet altijd goed kunnen aangeven of en hoe

[5] Deze typologie komt overeen met de driedeling van Donn Parker (1973) en wordt ook gevolgd in het Cybercrime-Verdrag (zie par. 2.3.1).
[6] Koops 2010a, met literatuurverwijzingen.
[7] Wall 2007.
[8] Glenny 2012.
[9] Brenner 2009; Lodder & Boer 2012.
[10] Kaspersen 2007, p. 17-18.

ze slachtoffer zijn van cybercriminaliteit. Recente slachtofferstudies in Nederland laten wel zien dat cybercriminaliteit een veelvoorkomende vorm van criminaliteit is, even prevalent als fietsendiefstal. Een in 2011 uitgevoerd onderzoek geeft aan dat op jaarbasis 4,3% van alle Nederlandse Internetgebruikers slachtoffer wordt van hacken en 3,5% van e-fraude. Leeftijd en Internetactiviteiten zijn de belangrijkste voorspellers van slachtofferschap: jongeren en mensen die meer Internetten lopen een hoger risico slachtoffer te worden van cybercriminaliteit.[11] Over daders is ook nog niet veel bekend. In de literatuur worden drie hackertypen onderscheiden: de jeugdige crimineel die hackt voor de lol, uit nieuwsgierigheid of om indruk te maken op zijn referentiegroep; de ideologische hacker, die veelal intelligent en soms obsessief en anti-sociaal is; en de financieel gemotiveerde hacker, die allerlei achtergronden kan hebben.[12] E-fraudeurs blijken min of meer dezelfde dadereigenschappen te hebben als klassieke fraudeurs, maar wel op jongere leeftijd te beginnen.[13]

In de hackergemeenschap wordt veel waarde gehecht aan het onderscheid tussen 'black hat hackers' of 'crackers' – kwaadwillende hackers – en 'white hat hackers' of 'ethische hackers' – de goedwillende hackers die helpen beveiligingsproblemen op te lossen. Dat onderscheid wordt in de wetgeving niet gemaakt en ook in het beleid met enige terughoudendheid benaderd[14] - de strafbaarstelling van hacken gaat uit van opzettelijk handelen, ongeacht of het 'goed' of 'kwaad' opzet is. Er bestaat een aanzienlijk cultuurverschil tussen de (brede en diverse) hackergemeenschap in Nederland, waaronder de nodige wittehoeddragers, en de (strafvorderlijke en beveiligings)autoriteiten, die vooralsnog een spanningsveld blijft opleveren rond beveiligingsincidenten.

2.3. Wetsgeschiedenis

2.3.1. Internationale context

Na twee niet-bindende aanbevelingen[15] besloot de Raad van Europa een bindend instrument op te stellen om wetgeving rond cybercriminaliteit te stimuleren en tot op zekere hoogte te harmoniseren. Dat leidde tot het Cybercrime-Verdrag (hierna: CCV), dat in 2001 in Boedapest werd ondertekend en in 2004 in werking trad.[16] Het verdrag is het belangrijkste internationale instrument op dit terrein, dat (stand van zaken mei 2013) door 39 landen is geratificeerd, niet alleen de meeste RvE-lidstaten maar ook de VS, Australië, Japan en, jawel, de Domenicaanse Republiek.[17] Daarnaast volgen ook de nodige andere landen het verdrag als voorbeeld voor hun wetgeving zonder partij te worden.

Omdat de Verenigde Staten bij de voorbereiding betrokken was met de bedoeling om partij te worden (wat in 2007 ook gebeurde), werd de strafbaarstelling van racistische uitlatingen niet in het Verdrag opgenomen (die voor de VS onaanvaardbaar zou zijn wegens het Eerste Amendement over vrije meningsuiting), maar in een Aanvullend Protocol.[18] Een ander urgent onderwerp met een belangrijke cyberdimensie – het seksueel misbruiken van minderjarigen – werd geregeld in het Verdrag van Lanzarote, dat in 2010 in werking trad.[19]

Ondertussen zat de Europese Unie niet stil. Aangezien het Cybercrime-Verdrag niet door alle EU-leden is geratificeerd, werd de behoefte gevoeld om voor de EU-lidstaten bindende regels te

---

[11] Domenie e.a. 2013. Zie ook Van Wilsem 2012 over slachtofferschap van identiteitsfraude.
[12] Van der Hulst & Neve 2008, p. 106-107.
[13] Leukfeldt & Stol 2012.
[14] Vgl. NCSC z.j.
[15] Council of Europe, *Recommendation R(89) 9 on Computer-related Crime*; *Recommendation R(95) 13 concerning problems of criminal procedural law connected with information technology*.
[16] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, *Trb.* 2002, 18. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG.
[17] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG.
[18] Aanvullend Protocol (…) betreffende de strafbaarstelling van handelingen van racistische of xenofobische aard verricht via computersystemen, *Trb.* 2005, 46. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CL=ENG.
[19] Verdrag inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, *Trb.* 2008, 58. Zie http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=201&CL=ENG.

stellen voor computercriminaliteit. Dit leidde tot drie Kaderbesluiten (inmiddels deels vervangen door Richtijnen), over fraude met niet-chartaal geld, aanvallen op computersystemen en seksuele uitbuiting van kinderen en kinderpornografie.[20] Daarnaast is er niet-bindend Europees beleid dat beoogt om lidstaten een stap verder te brengen in de strijd tegen computermisdaad en aanpalende gebieden.[21]

2.3.2. Wet computercriminaliteit en opvolgers

Nederland voerde in 1993 omvangrijke wetgeving in met de Wet computercriminaliteit.[22] Deze wet kwam tot stand op basis van aanbevelingen van de Commissie computercriminaliteit en een gedegen discussie daarover in literatuur en parlement.[23] Naast strafbaarstelling van de belangrijkste vormen van computercriminaliteit bevatte de wet ook een uitvoerige regeling van computergerelateerde opsporingsbevoegdheden.

Vanwege de ontwikkelingen in de techniek ontstond al snel behoefte aan actualisering van de wetgeving. Het wetsvoorstel Computercriminaliteit II uit 1999 werd echter ingehaald door Europese ontwikkelingen, met name het Cybercrime-Verdrag dat moest worden geïmplementeerd. Pas in 2006 trad de Wet computercriminaliteit II (hierna ook: CCII) in werking,[24] kort na de inwerkingtreding van de goedkeuringswet van het Cybercrime-Verdrag.[25] De wet CCII voerde enkele nieuwe strafbepalingen in en paste op onderdelen het materiële en procedurele strafrecht aan.

In 2010 werd vervolgens een Wetsvoorstel versterking bestrijding computercriminaliteit in consultatie gegeven dat enkele overgebleven onderwerpen zou regelen, zoals een bevel illegale inhoud van Internet te verwijderen en heling van gegevens.[26] Tegelijkertijd begonnen diverse andere dossiers, met name rond opsporingsbevoegdheden als hacken en het decryptiebevel, op te spelen. Samen met de eerdere onderwerpen werden deze dossiers opgepakt in een wetsontwerp Computercriminaliteit III (hierna: Wetsontwerp CCIII) dat in april 2013 voor consultatie werd rondgestuurd.[27] Naar verwachting zal eind 2013 het wetsvoorstel naar de Raad van State worden gestuurd, zodat het vermoedelijk in de loop van 2014 bij de Tweede Kamer kan worden ingediend. Hopelijk duurt het vervolgens niet zo lang als bij CCII voordat de wetswijziging van kracht wordt.

2.3.3. Overige wetten

Hoewel het zwaartepunt van Nederlandse cybercrimewetgeving ligt bij de Wet computercriminaliteit en zijn opvolgers, zijn ook de nodige andere wetten van belang. Sommige daarvan regelen een voor cybercriminaliteit belangrijk thema, zoals seksueel misbruik van kinderen,[28] het vorderen van verkeersgegevens en andere gegevens[29] en de bewaarplicht van verkeersgegevens.[30] Andere zijn meer algemene wetten met een of meer relevante bepalingen, zoals de strafbaarstelling van phishing (het hengelen naar, vooral financiële, gegevens) in een

---

[20] Kaderbesluit 2001/413/JBZ, Richtlijn 2013/40/EU (vervangt Kaderbesluit 2005/222/JBZ) en Richtlijn 2011/93/EU (vervangt Kaderbesluit 2004/68/JBZ).
[21] Europese Commissie 2007.
[22] *Staatsblad* 1993, 33.
[23] Commissie computercriminaliteit 1987; *Kamerstukken II* 1989/90, 21 551, nrs. 1-3; Kaspersen 1990; Wiemans 1991.
[24] *Staatsblad* 2006, 300.
[25] *Staatsblad* 2006, 299.
[26] Conceptwetsvoorstel versterking bestrijding computercriminaliteit, http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit. Zie ook Koops 2010b.
[27] Conceptwetsvoorstel in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), http://www.internetconsultatie.nl/computercriminaliteit.
[28] Wet partiële wijziging zedelijkheidswetgeving, *Stb.* 2002, 388; Wet tot uitvoering van het te Lanzarote totstandgekomen Verdrag (…), *Stb.* 2009, 544.
[29] Wet vorderen gegevens telecommunicatie, *Stb.* 2004, 105; Wet bevoegdheden vorderen gegevens, *Stb.* 2005, 390.
[30] Wet bewaarplicht telecommunicatiegegevens, *Stb.* 2009, 333, aangepast bij Wet van 6 juli 2011, *Stb.* 2011, 350.

antiterrorismewet,[31] de strafbaarstelling van virtuele dierenpornografie bij de strafbaarstelling van seks met dieren,[32] en de regeling van bijzondere opsporingsbevoegdheden.[33]

2.4. Wetssystematiek

2.4.1. Gegevens als 'goed'?

Een fundamentele keuze in de wetgeving is geweest om gegevens niet als 'goed' in strafrechtelijke zin te behandelen, maar als zelfstandig begrip met een eigen definitie (art. 80quinquies Sr: 'iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken'). Hoewel het Hof Arnhem in 1983 computergegevens had aangemerkt als 'goed' dat verduisterd kon worden,[34] is na de nodige discussie[35] uitgekristalliseerd dat gegevens andere eigenschappen hebben dan goederen. Hoewel gegevens met elektriciteit – dat wel als 'goed' wordt beschouwd[36] – gemeen hebben dat zij geld waard kunnen zijn, zijn ze 'multipel': meerdere mensen kunnen tegelijkertijd beschikken over dezelfde gegevens, wat bij elektriciteit (helaas) niet mogelijk is. Voorts zijn gegevens in beginsel het product van geestelijke arbeid, terwijl goederen (evenals elektriciteit) het product zijn van fysieke arbeid. In navolging van de Commissie computercriminaliteit koos de wetgever er in de Wet computercriminaliteit dan ook voor om parallelle of sui-generisbepalingen op te nemen ten aanzien van computergegevens, in plaats van deze onder te brengen bij bestaande delicten als zaakbeschadiging of diefstal. In de strafvordering betekent deze benadering dat gegevens niet als zodanig in beslag kunnen worden genomen, maar kunnen worden gekopieerd en eventueel ontoegankelijk gemaakt als ze moeten worden onttrokken aan de beschikkingsmacht van de verdachte. De Hoge Raad heeft deze benadering in 1996 bevestigd, met nadruk op het feit dat computergegevens niet de eigenschap hebben 'dat degene die de feitelijke macht daarover heeft deze noodzakelijkerwijze verliest indien een ander zich de feitelijke macht daarover verschaft'.[37]

Met de opkomst van objecten in virtuele omgevingen – online multispelerspellen en virtuele werelden – lijkt daar verandering in te zijn gekomen. In deze omgevingen is er immers wel sprake van uitsluitende beschikkingsmacht (althans tussen gebruikers onderling – de spelaanbieder heeft altijd ook beschikkingsmacht naast de gebruiker). In navolging van het Hof Leeuwarden heeft de Hoge Raad inmiddels bepaald dat onder omstandigheden gegevens zich wel degelijk als goed kunnen gedragen, wanneer de beschikkingsmacht door een handeling overgaat van de een naar de ander en wanneer ze een waarde vertegenwoordigen. Die waarde hoeft niet economisch te zijn maar kan ook subjectief zijn, zoals in casu een virtueel amulet en masker veel betekenden voor het jonge slachtoffer.[38] In dit geval kon het wegnemen van de gegevens daarom als diefstal worden gekwalificeerd. Er zijn kanttekeningen te plaatsen bij de redenering van de Hoge Raad,[39] onder andere omdat de deur nu open staat naar een erg casuïstische benadering van de vraag of bepaalde gegevens zich als 'goed' of als 'gegeven' gedragen. Wat mij betreft is het openen van die deur (nog) niet nodig, omdat bestaande bepalingen die de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens beschermen, voldoende zijn om feitencomplexen te bestraffen waarbij gegevens worden weggenomen of beschadigd.[40] Belangrijker is echter dat het arrest aanleiding geeft fundamenteel stil te staan bij het onderscheid tussen 'gegeven' en 'goed' en de argumentatie die wordt gehanteerd. Dommering betoogt dat het Elektriciteitsarrest meer kwaad dan goed gedaan heeft, nu het in de rechtsontwikkeling geleid heeft tot een tamelijk ad-hocargumentatie die de ene keer de nadruk legt op de aard van het object (wel of niet bepaalbaar

[31] Wet in verband met de strafbaarstelling van het deelnemen en meewerken aan training voor terrorisme (...) en enkele andere wijzigingen, *Stb.* 2009, 245; deze wet wijzigde art. 326 Sr (oplichting).
[32] Wet verbod seks met dieren, *Stb*. 2010, 111.
[33] Wet bijzondere opsporingsbevoegdheden, *Stb*. 1999, 245.
[34] Hof Arnhem 27 oktober 1983, *NJ* 1984, 80.
[35] Zie Kaspersen 2007, met literatuurverwijzingen.
[36] HR 23 mei 1921, *NJ* 1921, p. 564 e.v.
[37] HR 3 december 1996, *NJ* 1997, 574 m.nt. 'tH.
[38] HR 31 januari 2012, LJN BQ9251, *NJ* 2012/536, m.nt. Keijzer.
[39] Zie Koops 2013; Rozemond 2013.
[40] Koops 2013.

en uniek) en de andere keer op de maatschappelijke functie (zoals bij giraal geld en belminuten[41]). Volgens Dommering had het strafrecht in plaats van een onderscheid te maken tussen een drager en niet-tastbare maar mogelijk wel economisch waardeerbare gegevens (of elektronen), beter kunnen aansluiten bij het onderscheid in het civiele recht tussen materiële zaken en (immateriële) rechten of aanspraken.[42] Dat lijkt mij een waardevolle suggestie om een steekhoudender systematiek aan te brengen in de wet. Het valt echter niet te verwachten dat wetgever of rechter de lang geleden ingeslagen weg gaat verlaten en de systematiek zal omgooien. Voorlopig moeten we het dus doen met een onzekerheidsprincipe waarbij niet op voorhand valt te voorspellen of bepaalde computergegevens zich als 'gegeven' of als 'goed' gedragen in een rechtszaak.

2.4.2. Overige systematische keuzes

Een ander fundamenteel onderscheid dat gemaakt wordt in de wet, is of gegevens zijn opgeslagen of onderweg zijn. Bijvoorbeeld voor het wederrechtelijk kennisnemen van gegevens, bestaan er verschillende bepalingen: artikel 138ab Sr voor opgeslagen gegevens, artikel 139c Sr voor stromende gegevens. Vooral in de strafvordering bestaan significante systematische verschillen tussen het onderzoek van opgeslagen gegevens (art. 125i-125o Sv) en het onderzoek van stromende gegevens, oftewel communicatie (art. 126la e.v. Sv). Hiermee samenhangend (maar niet helemaal samenvallend) hanteert de strafvordering een belangrijk algemeen onderscheid tussen doorzoeking en inbeslagneming, die veelal openlijk plaatsvinden en voor de verdachte kenbaar zijn (eerste boek, titel IV Sv) en bijzondere opsporingsbevoegdheden, die vaak heimelijk plaatsvinden en niet voor de verdachte kenbaar zijn (eerste boek, titel IVA Sv). Het onderscheid is van belang omdat er systematische verschillen bestaan in rechtsbescherming; zo moeten bij een doorzoeking vastgelegde gegevens worden vernietigd zodra blijkt dat ze niet van belang zijn voor het onderzoek (art. 125n lid 1 Sv[43]), terwijl afgetapte of gevorderde gegevens pas twee maanden na afhandeling van de zaak mogen worden vernietigd (art. 126cc Sv). Hoewel het onderscheid tussen opgeslagen en stromende gegevens historisch goed verklaarbaar is, wordt het in een context van cloud computing minder relevant, omdat in de cloud gegevens 'opgeslagen' liggen die feitelijk langdurig of doorlopend onderweg zijn. Tot nu toe heeft de wetgever het onderscheid kunnen handhaven (bijvoorbeeld door een aparte bepaling in te voeren om bij een communicatieaanbieder opgeslagen gegevens te vorderen, art. 126ng Sv), maar nu de cloud vaste voet aan de grond krijgt in het Internetlandschap waardoor gegevensopslag grotendeels via communicatienetwerken geschiedt, zal de wetgever zich moeten herbezinnen op het tot nu toe gemaakte systematische onderscheid.[44]

Vanuit wetssystematisch oogpunt is ook van belang dat het Wetboek van Strafrecht en het Wetboek van Strafvordering goed op elkaar zijn afgestemd; het zijn immers communicerende vaten. In principe worden dan ook dezelfde basisbegrippen – geautomatiseerd werk, gegevens, communicatie – gebruikt. Definities in Sr gelden echter niet automatisch voor Sv; in navolging van Wiemans beoogde de wetgever dan ook de definities van gegevens en geautomatiseerd werk ook op te nemen in nieuwe artikelen 138e en 138f Sv.[45] In het wetsontwerp CCIII is dit voorstel echter, zonder toelichting, verdwenen.

Verder valt op dat de wetgeving niet geheel consistent is in het gebruik van begrippen rond communicatie. Waar vroeger de nadruk lag op aanbieders van openbare telecommunicatie, is bij de Wet computercriminaliteit II het begrip 'aanbieder van een communicatiedienst' (art. 126la Sv) ingevoerd, waardoor aftapbevoegdheden zijn uitgebreid tot niet-openbare aanbieders. Op diverse plaatsen hanteert de wetgever echter nog het 'oude' begrip van een openbaar

---

[41] HR 11 mei 1982, *NJ* 1982, 583, m.nt. 'tH (giraal geld); HR 31 januari 2012, *NJ* 2012, 535, m.nt. Keijzer (belminuten).
[42] Dommering 2013.
[43] Het is overigens onsystematisch dat deze vernietigingsplicht zich beperkt tot gegevens die zijn vastgelegd bij een doorzoeking, en niet ziet op gegevens die zijn overgenomen uit een (anders dan bij een doorzoeking, bijvoorbeeld bij een aanhouding) inbeslaggenomen computer.
[44] Koops e.a. 2012.
[45] Wiemans 2004, p. 238-240; Conceptwetsvoorstel versterking bestrijding computercriminaliteit, http://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit, p. 6.

telecommunicatienetwerk (zie vooral art. 138ab lid 3 en 350a lid 2 Sr en 125la, 126i, 126ii Sv). Het is lang niet altijd duidelijk waarom deze bepalingen alleen openbare telecommunicatie en niet ook (grote) besloten bedrijfsnetwerken betreffen, terwijl de wetgever deze wel op één lijn heeft gesteld bij andere bepalingen (zoals in art. 273d Sr en 126m Sv). Ook wordt weinig systematisch nu eens de term 'communicatiedienst' gehanteerd (bijvoorbeeld in art. 126la Sv) en dan weer 'telecommunicatiedienst' (in art. 273d lid 2 Sr), terwijl ogenschijnlijk daarmee hetzelfde wordt bedoeld. Daarbij komt dat de opkomst van cloudopslagdiensten het (uit de Europese regelgeving afkomstige) onderscheid tussen elektronische communicatieaanbieders en aanbieders van diensten van de informatiemaatschappij vertroebelt. Dat maakt het vooralsnog onduidelijk in hoeverre een aanbieder van een cloudopslagdienst valt onder de definitie van art. 126la Sv en bijvoorbeeld gebonden is aan de strafbaarstelling van wederrechtelijke inzage in bij hem opgeslagen gegevens die niet voor hem zijn bestemd (art. 273d Sr). Al met al is er genoeg aanleiding voor de wetgever om systematisch met de stofkam door zowel Sr als Sv te gaan en alle communicatiegerelateerde begrippen consistent te formuleren en definiëren.[46]

3. Materieel strafrecht[47]

3.1. Computergerichte delicten

Gegevens worden gedefinieerd als 'iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken' (art. 80quinquies Sr). Ook programmatuur valt hieronder. Computers worden door de wetgever, in een nobele poging om Nederlandse termen te gebruiken, een 'geautomatiseerd werk' genoemd, waaronder wordt verstaan 'een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen' (art. 80sexies Sr).[48] 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',[49] maar verder is het een ruime definitie. Een passieve RFID-chip zal in beginsel geen geautomatiseerd werk zijn, maar een interactieve RFID-chip wel.[50] Bovendien gaat het om een 'inrichting', wat niet alleen enkelvoudige apparaten omvat maar ook 'netwerken bestaande uit computers en/of telecommunicatievoorzieningen', zoals de combinatie van een computer, WiFi-router en Internetverbinding. Dat betekent dat het onrechtmatig toegang verschaffen tot een router onder hacken (art. 138ab Sr) kan vallen, ook al slaat de router zelf geen gegevens op, omdat het een deel is van het geautomatiseerde werk van computer+router+Internetverbinding.[51] Dit opent de mogelijkheid dat ook passieve gegevensdragers (zoals een RFID-chip) object zouden kunnen zijn van hacken of computersabotage, als zij (onlosmakelijk?) deel uitmaken van een computersysteem. Naarmate het 'Internet der dingen' zich verder ontwikkelt, zal moeten blijken hoe het begrip 'geautomatiseerd werk' verder wordt geïnterpreteerd.

Hacken – in de terminologie van de wet 'computervredebreuk' – is strafbaar gesteld in art. 138ab (138a-oud) Sr als het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan. In een curieuze formulering[52] heeft de wetgever daaraan toegevoegd dat van binnendringen in elk geval sprake is als hij daarbij enige beveiliging doorbreekt of zich de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel

---

[46] Zie ook Koops e.a. 2012. In het Conceptwetsvoorstel computercriminaliteit III, http://www.internetconsultatie.nl/computercriminaliteit, wordt alleen art. 273d Sr aangepast ('telecommunicatie' wordt vervangen door 'communicatie'), maar geen integrale consistentieslag gemaakt.
[47] Deze paragraaf bouwt voort op de bespreking in Koops & De Roos 2007. Ik dank Theo de Roos voor zijn bijdrage hieraan.
[48] Vgl. Kaspersen 1993, p. 135; Van Dijk & Keltjens 1995, p. 84-87. Merk op dat de definitie alleen elektronische computers, en dus niet bijvoorbeeld quantumcomputers en biologische computers, omvat.
[49] *Kamerstukken II* 1989/90, 21 551, nr. 3, p. 6.
[50] Vgl. Schermer 2005, p. 83-84.
[51] HR 26 maart 2013, LJN BY9718.
[52] Zie de kritiek in Koops & De Roos 2007, p. 28.

dan wel door het aannemen van een valse hoedanigheid. Voorheen gold een beveiligingseis, maar deze is in 2006 afgeschaft. Dat was niet nodig geweest en valt te betreuren, omdat hierdoor het signaal wegvalt aan computerbezitters dat zij ten minste een minimale moeite zouden moeten nemen om hun systemen te beveiligen.[53] Nu is het doorbreken van een beveiliging een voldoende maar geen noodzakelijke voorwaarde. Het onrechtmatig gebruiken van een wachtwoord kan worden gekwalificeerd als het gebruik van een valse sleutel[54] maar ook als het aannemen van een valse hoedanigheid, zoals Henk Krol ervoer toen hij werd veroordeeld voor het hacken van medische dossiers. Zijn beroep op klokkenluiderschap – om gebrekkige beveiliging aan de kaak te stellen – ging niet op, omdat hij niet-subsidiair had gehandeld door te snel de publiciteit te zoeken.[55] Onder binnendringen met valse signalen valt onder andere het gebruik van een SQL-injectie.[56]

Art. 138ab lid 2 en 3 betreft gekwalificeerde vormen van computervredebreuk. Het gaat om situaties waarin iemand bij een hack opgeslagen gegevens overneemt en voor zichzelf of een ander vastlegt (lid 2), dan wel met het oogmerk van wederrechtelijke bevoordeling gebruik maakt van verwerkingscapaciteit of verder hackt naar de computer van een derde (lid 3). Lid 3 geldt alleen wanneer de eerste hack plaatsvond via een openbaar telecommunicatienetwerk en niet via een niet-openbaar netwerk (bijvoorbeeld van een computer naar een andere computer binnen het SURF-netwerk); dit verschil in strafbaarheid laat zich moeilijk verklaren.

In de rechtspraak is het derde lid toegepast op het opzetten van een botnet[57], waarbij een virus (toxbot) grote aantallen computers had besmet.[58] Het was daarbij niet nodig om een specifieke computer aan te wijzen die als eerste was gehackt en vanwaar het virus was doorgesprongen naar andere computers, omdat het virus zich steeds verder verspreidde, zodat er feitelijk continu sprake was van 'doorhacken'. De interpretatie dat de verspreider van een virus binnendringt in de (zombie)computers door het enkele besmetten van die computers is aanvechtbaar, omdat door de ongerichte verspreidingsvorm niet per se gezegd kan worden dat met het virus ook de verspreider in een computer binnendringt. Dat is pas het geval wanneer de verspreider als botnetbeheerder een verbinding legt met de besmette computers door commando's te sturen. Het ligt meer voor de hand om het opzetten van een botnet te vervolgen als virusverspreiding en niet als (door)hacken, tenzij er voldoende bewijs is dat de botverspreider zelf contact heeft gemaakt met besmette computers en dus aldaar zelf is binnengedrongen.[59]

Naar analogie met zaakbeschadiging is ook gegevensaantasting strafbaar gesteld, in artikel 350a Sr. Zelfs culpoze (niet-opzettelijke) gegevensbeschadiging is strafbaar (art. 350b Sr), wat een interessante mogelijkheid biedt – die het OM tot nu toe niet heeft opgepakt – om aanmerkelijk nalatige gegevensbeheerders te vervolgen voor datalekken. Artikel 350a lid 1 stelt strafbaar het opzettelijk en wederrechtelijk veranderen, wissen, onbruikbaar of ontoegankelijk maken van gegevens die door middel van een geautomatiseerd werk of telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen, alsmede het toevoegen daaraan van andere gegevens. Dat laatste is opgenomen omdat ook het toevoegen van gegevens de integriteit van een gegevensbestand aantast. Het betreft een zeer ruime strafbaarstelling, zodat het element van wederrechtelijkheid hier een cruciaal bestanddeel is. Dat bleek bijvoorbeeld in een zaak voor de rechtbank Maastricht, waarin de rechter bepaalde dat het veranderen van een sim-lock niet wederrechtelijk is.[60] Lid 2 stelt een hogere straf op gegevensaantasting als deze plaatsvindt na binnendringen via openbare telecommunicatie en ernstige schade ontstaat.

---

[53] Ibid., p. 31-32.
[54] Ibid., p. 29.
[55] Rb. 's-Hertogenbosch 15 februari 2013, LJN BZ1163.
[56] Hof 's-Gravenhage 2 februari 2012, LJN BV3397. Zie over SQL-injecties http://nl.wikipedia.org/wiki/SQL-injectie.
[57] Een botnet is een netwerk van computers die door een bot (een 'software-robot') zijn besmet en die onder controle staan van een externe beheerder, veelal degene die de bot het net op heeft gestuurd. De besmette computers worden zombiecomputers of zombies genoemd.
[58] HR 22 februari 2011, LJN BN9287.
[59] Oerlemans en Koops 2011.
[60] Rb. Maastricht 12 maart 2002, LJN AE0125.

Artikel 350a lid 3 Sv stelt het verspreiden van virussen strafbaar, geformuleerd als het opzettelijk en wederrechtelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk. Hieronder vallen niet alleen wormen en virussen, maar ook Trojaanse paarden, ook al hoeven die niet per se bestemd te zijn om schade aan te richten.[61] De verspreiding is strafbaar ongeacht of schade daadwerkelijk optreedt.[62]

Een ernstiger vorm van gegevensaantasting is computersabotage, dat wil zeggen beschadiging van computers en telecommunicatiewerken waarbij gemeen gevaar voor goederen of mensen te vrezen is (art. 161sexies Sr). Ook hier bestaat een culpoze variant (art. 161septies Sr). Het gaat dan om geautomatiseerde werken die voor het algemeen nut van belang zijn, zoals het storen van computers van een telecomaanbieder, de Belastingdienst of een kerncentrale. De strafmaat neemt toe naarmate het gevolg ernstiger is, van verhindering van gegevensverwerking tot aan levensgevaar en de dood. Gemeen gevaar voor diensten ontstaat bijvoorbeeld bij DDoS-aanvallen op overheidspagina's,[63] maar niet bij DDoS-aanval op een enkel e-handelbedrijf.[64] Wel is het gebruik van een botnet voor phishing, waarbij computergebruikers die hun bank wilden bezoeken werden omgeleid naar een valse pagina en hun financiële gegevens heimelijk werden doorgestuurd, bestraft als computersabotage vanwege gemeen gevaar voor diensten.[65] Dat is een aanvechtbare interpretatie omdat artikel 161sexies Sr bedoeld is voor aanvallen op computers van dienstverleners, niet op die van gebruikers.[66]

Naast computersabotage valt onder verstoring van computersystemen (art. 5 CCV) ook de wederrechtelijke belemmering van toegang tot computers door het aanbieden of verzenden van gegevens (art. 138b Sr). Deze bepaling was oorspronkelijk bedoeld voor mailbombardementen maar is uiteindelijk ruim geformuleerd om met name ook DDoS-aanvallen te bestrijken. Of de toegang ook daadwerkelijk wordt geblokkeerd is niet van belang: het is voldoende als de reële mogelijkheid bestaat dat de toegang wordt geblokkeerd. Dat zal dus mede afhangen van de stand van de techniek. Onder toegangsbelemmering valt evenwel niet gewone spam, aangezien dit volgens de wetgever geen inbreuk maakt op een elementair rechtsgoed. Strafbaarstelling van spam wordt niet opportuun geacht;[67] de bestuursrechtelijke handhaving (art. 11.7 Telecommunicatiewet j° art. 1 onder 2 Wet op de economische delicten) volstaat.

Diverse strafbepalingen waarborgen de bescherming van (tele)communicatie, zowel het afluisteren of opnemen van gesprekken (art. 139a en 139b Sr) als het aftappen of opnemen van gegevens die worden verwerkt of overgedragen door een computer of via telecommunicatie (art. 139c Sr). Hieronder valt niet alleen alle telecommunicatie, maar ook de overdracht van gegevens binnen en tussen computers, zoals de overdracht tussen toetsenbord, computer en beeldscherm, en de zogenoemde residustraling die beeldscherm en kabels uitzenden. Wel gelden uitzonderingen voor het uit de lucht plukken van radiosignalen, voor aftappen (binnen redelijke grenzen) door rechthebbenden van de telecommunicatieaansluiting (zoals hoteleigenaars en werkgevers), en voor technische controles door telecomaanbieders (art. 139c lid 2 Sr). Daarentegen geldt het verbod voor telecomaanbieders om in inhoud van aan hen toevertrouwde communicatie te kijken (art. 273d Sr) nu ook voor niet-openbare communicatieaanbieders, waaronder werkgevers (art. 273d lid 2 Sr). Dat betekent dat werkgevers ten minste een beleid moeten hebben in de lijn van de vuistregels van het CBP om rechtmatig te kunnen monitoren.[68]

Tot nu toe geldt dat het aftappen door een gespreksdeelnemer zelf niet strafbaar is: wie gesprekken aangaat, neemt het risico dat de ander het gesprek opneemt en daar dan mogelijk iets mee doet.[69] Nu de techniek het heimelijk opnemen en wereldwijd verspreiden van opnames makkelijker maakt dan ooit, wordt het risico van ongewenste verspreiding van privégesprekken wel erg groot. In het wetsontwerp uit 2010 werd voorgesteld ook het wederrechtelijk opnemen

[61] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 48.
[62] HR 28 september 2004, *NJ* 2004, 642.
[63] Rb. 's-Gravenhage 14 maart 2005, LJN AT0249.
[64] Hof 's-Hertogenbosch 12 februari 2007, LJN BA1891.
[65] HR 22 februari 2011, LJN BN9287.
[66] Oerlemans en Koops 2011.
[67] *Kamerstukken II* 1998/99, 26 671, nr. 3, p. 40.
[68] Koops & De Roos 2007, p. 38.
[69] *Kamerstukken II* 1967/68, 9419, nr. 3, p. 5.

door communicatiepartners zelf strafbaar te stellen, maar dit voorstel is niet teruggekeerd in het wetsontwerp CCIII uit mei 2013. Het is afwachten wat de wetgever hier verder mee doet.

Naast afluisteren en aftappen zelf, zijn ook diverse voor- en nabereidingshandelingen strafbaar gesteld, van het wederrechtelijk plaatsen van afluisterapparatuur (art. 139d Sr) tot het wederrechtelijk beschikken over of bekendmaken van afgeluisterde gesprekken of afgetapte gegevens (art. 139e Sr). Dit laatste kan worden gezien als een vorm van heling, waaronder ook het bekendmaken of uit winstbejag gebruiken van gegevens die door misdrijf zijn verkregen uit een computer van een onderneming van handel, nijverheid of dienstverlening valt (art. 273 lid 1 onder 2° Sr). Voorwaarde daarbij is dat de gegevens betrekking hebben op de onderneming zelf, dat zij nog niet algemeen bekend waren en dat uit het bekendmaken of gebruik enig nadeel kan ontstaan. Vanwege de toegenomen kwetsbaarheid van gegevens, waarbij het moeilijk zo niet onmogelijk is om eenmaal op Internet gepubliceerde gegevens verwijderd te krijgen, stelt de wetgever in het wetsontwerp CCIII voor een generieke strafbaarstelling van 'heling' van gegevens in te voeren, geredigeerd naar analogie met heling van goederen (art. 416 en 417bis Sr). Ook wordt in dat ontwerp het opzettelijk en wederrechtelijk overnemen van niet-openbare gegevens uit een computer strafbaar gesteld. Dat is een vergaande strafbaarstelling, waarbij vanuit de ultimum-remediumgedachte vraagtekens zijn te plaatsen. De ruime bepalingen van hacken en gegevensaantasting bieden, zo lijkt mij, al veel mogelijkheden om wederrechtelijke overname van gegevens te bestraffen.

Artikel 6 van het Cybercrime-verdrag stelt misbruik van hulpmiddelen (zowel apparatuur als programmatuur) strafbaar. Dit is geïmplementeerd in artikel 139d leden 2 en 3 Sr en artikel 161sexies lid 2 Sr. Het is een vergaande vorm van strafbaarstelling van voorbereidingshandelingen[70] (zeker omdat er, anders dan bij de algemene strafbaarstelling in art. 46 Sr, niet de halve maar dezelfde straf op staat als het voorbereide delict). De reikwijdte wordt wel beperkt doordat het moet gaan om hulpmiddelen die 'hoofdzakelijk geschikt' zijn voor het plegen van cybercriminaliteit en door de eis dat de maker/bezitter/verspreider oogmerk moet hebben dat met het hulpmiddel een cyberdelict wordt gepleegd.

3.2. Computer-gerelateerde delicten

Het Cybercrime-verdrag regelt de strafbaarstelling van twee computer-gerelateerde delicten. Volgens artikel 7 moet valsheid in geschrifte strafbaar worden gesteld. Computer-gerelateerde valsheid valt onder de algemene bepaling van artikel 225 Sr, zoals reeds in 1991 in de Rotterdamse computerfraudezaak werd uitgemaakt.[71] Een computerbestand is een 'geschrift' als bedoeld in artikel 225 wanneer het voldoende duurzaam is (dat is al snel het geval als het ergens opgeslagen is en niet (alleen) in het werkgeheugen staat) en als het leesbaar kan worden gemaakt. Belangrijk is vooral dat het geschrift een bewijsbestemming (in rechte) moet hebben, wat het geval is bij bijvoorbeeld incasso-opdrachten, bestanden die noodzakelijk zijn voor de betalingadministratie en elektronische aangifteformulieren, maar niet voor bijvoorbeeld een gewone email of een gemiddeld tekstbestand. Manipulatie daarvan kan wel vervolgd worden op basis van gegevensmanipulatie (art. 350a Sr). De wetgever heeft voorts een specialis van valsheid geschapen in de vorm van het vervalsen van betaalpassen, waardekaarten (zoals een telefoonkaart) en andere voor het publiek beschikbare kaarten of dragers van identiteitsgegevens (zoals zorgpassen) (art. 232 Sr). Ook het opzettelijk afleveren, voorhanden hebben, ontvangen, verkopen en overdragen van een valse pas of kaart is strafbaar (lid 2). Ook voorbereidingshandelingen tot het vervalsen van kaarten is strafbaar gesteld, inclusief het voorhanden hebben of overdragen van gegevens (zoals computerprogramma's) die bestemd zijn tot pasvervalsing (art. 234 Sr). Met deze bepalingen kan skimming goed worden bestraft.

[70] Zie voor kritiekpunten Koops & De Roos 2007, p. 43-46, met literatuurverwijzingen.
[71] HR 15 januari 1991, *NJ* 1991, 668 m.nt. C.

Artikel 8 Cybercrime-verdrag ziet op computer-gerelateerde fraude. De fraudebepalingen in het Wetboek van Strafrecht – oplichting (art. 326 Sr), afpersing en afdreiging (art. 317-318 Sr) – zijn aangepast om ook het aftroggelen van gegevens strafbaar te stellen. Oorspronkelijk hanteerde de wetgever daarbij 'gegevens met geldwaarde in het handelsverkeer', waaronder alleen legaal verhandelbare gegevens (zoals programmatuur of marketingbestanden) vielen, maar dit is in 2004 (art. 317) en 2009 (art. 318, 326) veralgemeniseerd tot 'gegevens' om ook het aftroggelen van pincodes en wachtwoorden (die alleen op de zwarte markt geldswaarde hebben) te bestrijden.[72] Bij de Wet computercriminaliteit is ook de afpersingbepaling aangepast zodat niet alleen dreigen met geweld maar ook dreiging met gegevensaantasting afpersing kan opleveren, en is een specifieke strafbaarstelling van telecomfraude ingevoerd. Artikel 326c Sr bedreigt met straf het gebruiken van een publiek beschikbare telecommunicatiedienst door een technische ingreep of met valse signalen, met de bedoeling om daarvoor niet (volledig) te betalen. Hiermee kan het kraken van betaal-tv worden bestreden, of het manipuleren van telefoonkaarten om gratis of goedkoper te bellen.

Computer-gerelateerde diefstal en verduistering zijn niet geregeld in het Cybercrime-verdrag, omdat diefstal van gegevensdragers van nature onder diefstalbepalingen valt en 'diefstal' van gegevens bij de voorbereiding van het verdrag niet aan de orde was; gegevens worden immers niet als zodanig onttrokken aan de beschikkingsmacht van de houder.[73] Inmiddels lijkt dat anders te liggen voor gegevens die uniciteit hebben (en dus overgaan in beschikkingsmacht van de een naar de ander) en die een waarde vertegenwoordigen, zoals bij virtuele 'goederen' en bij belminuten, waarmee de discussie over de vraag of computergegevens een strafrechtelijke 'goed' zijn weer is heropend. Rechtspraak zal verder moeten uitwijzen in hoeverre het RuneScape-arrest navolging krijgt.[74]

3.3. Uitingsdelicten

3.3.1. Kinderpornografie

Artikel 240b Sr stelt handelingen met betrekking tot kinderpornografie strafbaar. Het bereik van de bepaling is in de afgelopen twee decennia sterk uitgebreid en de strafmaat is significant verhoogd (van drie maanden voor 1996 tot momenteel vier jaar (lid 1), of acht jaar als het uit beroep of gewoonte wordt gepleegd (lid 2)). Oorspronkelijk stond centraal het voorkomen en beperken van daadwerkelijk misbruik van jongeren om kinderpornografische afbeeldingen te maken. Vanwege het Cybercrime-verdrag heeft Nederland de wetgeving echter aangepast en daar nu ook andere ratio's aan toegevoegd: het voorkomen van verdere verspreiding van eenmaal gemaakt materiaal, en het voorkomen dat afbeeldingen worden gebruikt om jeugdigen te verleiden tot seksuele handelingen; dit alles ter bestrijding van een subcultuur die kindermisbruik bevordert.[75]

Bij de implementatie van artikel 9 Cybercrime-verdrag is de leeftijdsgrens verhoogd van 16 naar 18 jaar en is virtuele kinderpornografie strafbaar gesteld.[76] Dit laatste past bij de nieuwe ratio: virtuele kinderpornografie hangt samen met een subcultuur van kindermisbruik, en kan bovendien gebruikt worden om kinderen te verleiden, zoals het filmpje uit de eerste Nederlandse rechtszaak op dit terrein.[77] Hoewel de wetsgeschiedenis en de tekst van het Cybercrime-verdrag suggereren dat het om realistische afbeeldingen moet gaan, wat een schijn van echtheid suggereert,[78] hanteert de rechtspraak een ruimere invulling die ook cartoons en schilderijen omvat.[79] Animaties vallen echter niet onder de strafbaarstelling 'indien het voor de gemiddelde kijker onmiddellijk

---

[72] *Stb.* 2004, 180; *Stb.* 2009, 245.
[73] HR 3 december 1996, *NJ* 1997, 574 m.nt. 't H.
[74] HR 31 januari 2012, *NJ* 2012/535 (RuneScape) en NJ 2012/536 (belminuten), m.nt. Keijzer. Zie boven, noot 38 en bijbehorende tekst.
[75] Aanwijzing kinderpornografie (artikel 240b Sr), *Stcrt.* 2010, nr. 19121.
[76] Wet partiële wijziging zedelijkheidswetgeving, *Stb.* 2002, 388.
[77] Rb. 's-Hertogenbosch 2 april 2008, LJN BC3225.
[78] Zie Koops & De Roos 2007, p. 59-60.
[79] Rb. 's-Hertogenbosch 2 april 2008, LJN BC3225; Rb. Amsterdam 17 december 2010, LJN BO9296.

duidelijk is dat het gebeuren niet echt is en dat het gaat om gemanipuleerde afbeeldingen'.[80] De precieze maatstaf van het realismegehalte is in de rechtspraak nog niet helemaal uitgekristalliseerd.

Er zijn veel zaken waarin kinderporno op de harde schijf staat terwijl de verdachte het bezit ontkent, hetzij omdat hij het bestaan niet kende (in tijdelijke Internetbestanden) hetzij omdat hij de kinderporno meteen had gewist (waarna het alleen met forensische software is terug te halen). Of een dergelijk verweer stand houdt is sterk contextafhankelijk. Een jurisprudentieanalyse toont aan dat rechters beoordelen a) of verdachte wist van het bestaan, b) erover kan of kon beschikken, en c) zich niet tijdig op effectieve wijze ontdaan heeft van de afbeeldingen. De verdachte moet kortom kennen, kunnen en willen bezitten. In twijfelgevallen let de rechter op de context; doorslaggevend is vaak of de verdachte actief op zoek is geweest naar kinderporno.[81]

Ter implementatie van het Lanzarote-verdrag[82] is artikel 240b Sr uitgebreid met het zich opzettelijk toegang verschaffen tot kinderporno.[83] Tegenwoordig wordt dit materiaal op ondergrondse netwerken ook 'stromend' aangeboden, waarbij geïnteresseerden het materiaal online bekijken in plaats van het binnen te halen. Dit werkt als een vangnet voor de categorie kinderpornogebruikers die bewust vermijden kinderporno in bezit te hebben.[84] Het moet wel gaan om bewijsbaar opzettelijke toegangsverschaffing (bijvoorbeeld blijkend uit een betaling of zoektermen); onwetend of per ongeluk klikken op een link is niet strafbaar. Ook is vanaf 1 januari 2010 'grooming' strafbaar, het contact leggen met kinderen met het oogmerk om ze vervolgens seksueel te misbruiken. De strafbaarstelling (art. 248e Sr) is beperkt tot gevallen waarin het eerste contact elektronisch wordt gelegd, waarin een afspraak tot ontmoeting wordt voorgesteld met oogmerk van ontucht of kinderpornovervaardiging (bijvoorbeeld blijkend uit het meenemen van condooms of een camera) en waarin een handeling wordt getroffen ter verwezenlijking van de ontmoeting, zoals het afdrukken van een routebeschrijving. Mijns inziens moet het laatste element (een handeling ter verwezenlijking) wel iets meer inhouden dan het ontmoetingsvoorstel zelf; het kwalificeren van concrete voorstellen wat betreft tijd en plaats als een verwezenlijkingshandeling[85] lijkt mij, in elk geval qua tekstuele interpretatie, onjuist. Het uitoefenen van druk op de jongere en voorspiegelen dat seks op die leeftijd normaal is, en het geven van verdachte's mobiele nummer aan de jongere, zijn wel verwezenlijkingshandelingen die meer zijn dan het voorstellen van de ontmoeting zelf.[86]

De kwetsbaarheid van minderjarige Internetgebruikers voor seksueel misbruik bestaat niet alleen uit grooming maar ook uit andere zedenmisdrijven, zoals afgedwongen webcamseks (wat afhankelijk van de omstandigheden kan vallen onder art. 239, 240 of 246 Sr).[87] Er ligt een duidelijke rol voor het strafrecht om kwetsbare jongeren te beschermen tegen misbruik, maar er moet wel ruimte zijn voor jongeren om (onderling) te experimenteren en zich seksueel te ontplooien; de balans tussen autonomie en bescherming lijkt soms door te slaan naar overmatige bescherming.[88]

3.3.2. Overige uitingsdelicten

Het strafrecht kent de nodige andere uitingsdelicten: discriminatie (art. 137c e.v. Sr), belediging van leden van het koninklijk huis (art. 111 e.v. Sr) en bevriendestaatshoofden (art. 118 Sr), smaad (art. 261 Sr), laster (art. 262 Sr) en eenvoudige belediging (art. 266 Sr). Deze uitingsdelicten kunnen even goed via ICT als via fysieke media worden gepleegd, al kan het van de context afhangen of in een bepaald forum een bepaalde uiting discriminerend of beledigend is. Ook als het uitingsdelict het bestanddeel 'geschrift' bevat, kan het via ICT worden gepleegd,

---

[80] Rb. Zutphen 21 december 2010, LJN BO8152 en Hof Arnhem 12 april 2012, LJN BW3415.
[81] Stevens & Koops 2009.
[82] Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, CETS 201, Lanzarote, 25.X.2007, *Trb.* 2008, 58.
[83] Stb. 2009, 544.
[84] Stevens & Koops 2009.
[85] Rb. 's-Hertogenbosch 28 december 2011, LJN BU9341.
[86] Hof 's-Hertogenbosch 27 februari 2013, LJN BZ2577 (hoger beroep van LJN BU9341).
[87] Voor een overzicht, zie Koops 2009.
[88] Van der Hof 2013.

zoals al bleek bij valsheid in geschrifte. Voor smaadschrift is het voldoende als de smadelijke uiting aantoonbaar ooit vastgelegd is geweest op een duurzame drager, ook al was die vastlegging van korte duur. Wat wel vragen oproept is wanneer in een Internetcontext een uitlating 'openbaar' wordt gemaakt of 'verspreid'.[89] De drempel lijkt laag te liggen: een smadelijke uiting over de ex-man ("ik moet mijn kind meegeven aan een pedo") verstuurd op een besloten profiel met 20 à 25 'vrienden' geldt als ter kennis van het publiek brengen, omdat 'de tekst op de Hyves-pagina van de verdachte zichtbaar was voor personen die kennelijk naar eigen inzicht en zonder enige restrictie over de uitlating konden beschikken, voor de verdachte voorzienbaar en op voorhand feitelijk te verwachten was dat de geplaatste tekst verder zou worden verspreid.'[90] Het versturen van een lullig filmpje naar één persoon met de opmerking het niet verder te verspreiden geldt echter niet als openbaarmaken; de voorzienbaarheid van verdere verspreiding is dan vooralsnog (althans volgens de desbetreffende rechtbank) nog niet dusdanig dat voorwaardelijk opzet op verspreiding kan worden aangenomen.[91] Een andere relevante vraag is of een hyperlink naar strafbare informatie ook strafbaar is; de drempel voor aansprakelijkheid zal hoger liggen dan bij civiele aansprakelijkheid in bijvoorbeeld auteursrechtzaken.[92]

3.3.3. Aansprakelijkheid Internetaanbieders en Notice-and-Takedown

Bij de aanpassingswet richtlijn elektronische handel is artikel 54a Sr opgenomen, dat Internetaanbieders vrijwaart van aansprakelijkheid voor delicten gepleegd via hun netwerken of diensten, voorzover ze als zodanig (als tussenpersoon en niet als medeverantwoordelijke van de inhoud) functioneren.[93] De ratio hiervan is het voorkomen van zelfcensuur door Internetaanbieders die uit vrees voor vervolging wegens medeplichtigheid aan uitings- of andere delicten te snel materiaal zouden blokkeren dat zij doorgeven of hosten.

De bepaling is ongelukkig omdat de vrijwaring gekoppeld is aan een verondersteld maar niet geregeld notice-and-takedown-regime: de aanbieder moet het materiaal verwijderen op vordering van de officier van justitie, die daarvoor machtiging van de rechter-commissaris nodig heeft. De officier heeft echter geen bevoegdheid om de r-c om toestemming te vragen[94] (art. 125o Sv is hier niet toepasselijk) en er is gebrekkige rechtsbescherming.[95] Daarom wordt in het wetsontwerp CCIII een sluitend stelsel van notice-and-takedown voorgesteld waarbij artikel 54a Sr wordt gekoppeld aan een bevoegdheid van de officier om verwijdering te vorderen (voorgesteld art. 125p Sv), die voorzien is van meer rechtswaarborgen. Er blijft echter een grote kans bestaan dat het verwijderde materiaal nooit door een rechter ter zitting wordt getoetst op strafbaarheid,[96] zodat we zullen moeten vertrouwen op de rechter-commissaris om alleen bij onmiskenbaar onrechtmatig materiaal een machtiging te geven voor een verwijderingsbevel.

4. Procedureel strafrecht[97]

Procedureel strafrecht betreft de opsporing en vervolging van strafbare feiten, alsmede de tenuitvoerlegging van straffen. Vanuit ICT-perspectief zijn vooral ICT-gerelateerde opsporingsbevoegdheden relevant, die grofweg kunnen worden ingedeeld in klassieke doorzoeking en inbeslagneming (zeg maar de 125-serie in het Wetboek van Strafvordering (Sv)) en in bijzondere opsporingsbevoegdheden (de schier eindeloze 126-serie in Sv). Ook is digitaal

[89] Zie uitgebreid Van der Hof e.a. 2006.
[90] HR 5 juli 2011, LJN BQ2009.
[91] Rb. Almelo 25 april 2013, LJN BZ8524.
[92] Koops & De Roos 2007, p. 68. Zie ook Kentgens 2010.
[93] *Stb.* 2004, 210. Zie ook hoofdstuk 11 van Den Dekker en Van der Linden.
[94] Rb. Assen 24 november 2009, LJN BK4226.
[95] Schellekens, Koops & Teepe 2007.
[96] Zie Koops 2010b.
[97] Deze paragraaf bouwt voort op de bespreking in Koops & Buruma 2007. Ik dank Ybo Buruma voor zijn bijdrage hieraan.

bewijs van belang, waar ik kort op inga. ICT-gerelateerde tenuitvoerlegging (elektronische enkelband, computerverbod e.d.) valt buiten het bestek van dit hoofdstuk.[98]

Digitale opsporingsbevoegdheden zijn niet alleen relevant voor cybercriminaliteit in enge zin (zoals hierboven behandeld) maar voor elk strafbaar feit waarbij inlichtingen of bewijsmateriaal via ICT verwerkt is (het derde type cybercriminaliteit in par. 9.2.1).

4.1. Doorzoeking en gerelateerde bevoegdheden

De officier van justitie kan bij heterdaad of verdenking van een misdrijf waarvoor voorlopige hechtenis mogelijk is, elke plaats doorzoeken, behoudens woningen zonder toestemming en behoudens kantoren van professionele verschoningsgerechtigden (art. 96c j° 218 Sv). De rechter-commissaris kan ambtshalve of op vordering van de officier van justitie elke plaats (dus ook de zojuist uitgezonderde plaatsen) doorzoeken (art. 110 Sv). Voorts kunnen opsporingsambtenaren bij heterdaad of verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten, voertuigen (met uitzondering van woongedeelten) doorzoeken (art. 96b Sv).

Tijdens een doorzoeking zijn de autoriteiten bevoegd in de te doorzoeken ruimtes aangetroffen computers te onderzoeken: zowel eigen materiaal als bestanden of berichten van derden die aldaar bewaard worden, kunnen worden ingezien en gekopieerd. Die benadering was een uitgangspunt van de wetgever bij de Wet computercriminaliteit. De wetgever vond dat voor computeronderzoek tijdens een doorzoeking geen zelfstandige bevoegdheid nodig was: als men bevoegd is te doorzoeken, waarbij bijvoorbeeld kasten opgebroken en doorzocht mogen worden, is men daarmee ook bevoegd om een computer aan te zetten en te onderzoeken. En evenals autoriteiten kopieën van vingerafdrukken mogen maken bij een doorzoeking, mogen zij kopieën maken van aangetroffen computergegevens.

Van *inbeslagneming* van vastgelegde gegevens kan door de aard van digitaal opgeslagen gegevens echter geen sprake zijn. Er kan dus theoretisch geen doorzoeking worden aangevraagd als justitie alleen beoogt om een computer te doorzoeken en gegevens te kopiëren (al kan natuurlijk wel altijd een doorzoeking ter inbeslagneming van een gegevens*drager* plaatsvinden). Bij de Wet bevoegdheden vorderen gegevens is daarom een zelfstandige bevoegdheid in ingevoerd tot 'doorzoeken van een plaats ter vastlegging van gegevens die op deze plaats op een gegevensdrager zijn opgeslagen of vastgelegd' (art. 125i Sv). Deze doorzoeking is mogelijk onder dezelfde voorwaarden als de reguliere doorzoeking; artikel 125i Sv verwijst daartoe naar de artikelen 96b, 96c, 97 en 110. Het voorstel van Wiemans om in plaats van deze vrij ingewikkelde verwijzingsbepaling een veel simpeler bepaling in de betekenissentitel op te nemen dat onder 'doorzoeking ter inbeslagneming' ook 'doorzoeking ter vastlegging van gegevens' wordt verstaan, is helaas niet overgenomen door de wetgever.[99]

Bij een doorzoeking kan justitie gegevens dus kopiëren ten behoeve van de waarheidsvinding, maar daarbij blijven de gegevens beschikbaar voor de betrokkene. Soms kan het wenselijk zijn om de gegevens aan diens beschikkingsmacht te onttrekken, bijvoorbeeld bij digitale kinderporno of kraakprogramma's (zoals men goederen ook in beslag kan nemen ter onttrekking aan het verkeer). Hierin is voorzien door artikel 125o Sv, op basis waarvan de officier van justitie of de rechter-commissaris kan bevelen om onrechtmatige gegevens (die *corpus delicti* zijn) die in een computer zijn aangetroffen ontoegankelijk te maken en te vernietigen. Justitie kan dit zelf doen of een derde verzoeken om gegevens ontoegankelijk te maken; artikel 125o Sv impliceert echter geen medewerkingsplicht voor systeembeheerders.[100]

Bij een doorzoeking mag geen onderzoek plaatsvinden naar gegevens die zijn ingevoerd door of vanwege beroepsmatige geheimhouders, tenzij met hun toestemming (art. 125l j° 218 Sv). Verder bestaat er, als gegevens bij een doorzoeking worden vastgelegd (of ontoegankelijk gemaakt, zie onder), een notificatieplicht aan betrokkenen, dat wil zeggen de verdachte (tenzij die

[98] Digitalisering van het strafproces wordt besproken door Van den Hoogen in hoofdstuk 13. Zie ook Lodder en Oskamp 2007.
[99] Wiemans 2004, p. 236-237.
[100] *Kamerstukken II* 1998-1999, 26 671, nr. 3, p. 21; *Kamerstukken II* 2004-2005, 26 671, nr. 10, p. 16.

via de processtukken toch al op de hoogte geraakt), de verantwoordelijke voor de gegevens (in de zin van art. 1 onder d Wbp) en de rechthebbende van de plaats waar de doorzoeking plaatsvond (art. 125m Sv). Bij een doorzoeking vastgelegde gegevens moeten worden vernietigd zodra ze niet meer van belang zijn voor het onderzoek; ze kunnen wel worden bewaard voor een ander onderzoek of in een register zware criminaliteit (art. 125n Sv). Opmerkelijk is dat artikel 125n zich beperkt tot gegevens vastgelegd bij een doorzoeking, en dus niet ziet op gegevens die zijn overgenomen uit bijvoorbeeld een inbeslaggenomen computer.[101] De wetgever heeft ook enkele bepalingen opgenomen ter bescherming van het communicatiegeheim in het kader van doorzoekingen, maar deze is weinig systematisch en maakt een achterhaald onderscheid tussen fysieke en elektronische communicatievormen.[102]

De doorzoeking kan vanaf de plaats waar de doorzoeking plaatsvindt, worden voortgezet (een zogeheten 'netwerkzoeking') in een elders aanwezig computersysteem, mits de personen die op de plek van doorzoeking wonen, plegen te werken of te verblijven, met toestemming van de rechthebbende tot een dergelijke computer toegang hebben (art. 125j Sv). Er moet zowel een feitelijke band bestaan tussen de persoon en de locatie waar de doorzoeking plaatsvindt (dus niet een netwerkzoeking vanaf de smartphone van een toevallige bezoeker of de schoonmaker), als een juridische band (toestemming) tussen de persoon en de computer elders (dus geen netwerkzoeking in door de verdachte gehackte computers). De netwerkzoeking mag alleen plaatsvinden op Nederlands grondgebied. In artikel 32 Cybercrime-verdrag is bepaald dat de netwerkzoeking alleen grensoverschrijdend mag plaatsvinden bij openbare gegevens (zoals publiek toegankelijke weblocaties) en met toestemming van de rechthebbende (de 'eigenaar' van de gegevens, een dienstaanbieder of de buitenlandse staat). Dit levert in de praktijk natuurlijk veel problemen op, zeker met de opkomst van de cloud. De discussie over grensoverschrijdende netwerkzoekingen en ontoegankelijkmakingen zal de komende jaren nationaal en internationaal gevoerd moeten worden.[103]

De netwerkzoeking (een verlengde doorzoeking) moet onderscheiden worden van een doorzoeking op afstand, wat een zelfstandige doorzoeking van een computer is zonder dat (eerst) een plaats wordt doorzocht. Ook dit is een heikel discussiepunt, waar de wetgever nu een bevoegdheid voor voorstelt (art. 125ja Sv in Wetsontwerp CCIII). De bevoegdheid is vooral van belang om op afstand een Trojaans paard in verdachte's computer te kunnen plaatsen, waarbij diverse functionaliteiten kunnen worden benut (denk aan het onderscheppen van toetsaanslagen om een wachtwoord te achterhalen; het kopiëren van bestanden op de harde schijf; het aanzetten van de webcam of microfoon om in verdachte's omgeving te kunnen kijken en luisteren). Duidelijk is dat dit een zeer vergaande bevoegdheid is, waar veel haken en ogen aan zitten,[104] en dat dit in de parlementaire behandeling stevig bediscussieerd zal moeten worden. In elk geval zou de vormgeving van de bevoegdheid aangepast moeten worden; de doorzoeking op afstand vindt heimelijk en mogelijk gedurende een langere periode plaats en is daarom een bijzondere opsporingsbevoegdheid die systematisch gezien thuishoort in de 126-serie, met bijbehorende rechtswaarborgen, en niet in de titel betreffende de doorzoeking.

Bij een doorzoeking zal het regelmatig voorkomen dat een computer beveiligd is of dat bestanden op de computer versleuteld zijn. De doorzoekende autoriteit kan degene van wie redelijkerwijs kan worden vermoed dat hij kennis draagt van de beveiliging bevelen toegang te verschaffen tot de computer of bestanden, hetzij door zelf te ontsluiten hetzij door een wachtwoord te geven (art. 125k Sv). Dit is overigens alleen mogelijk bij een doorzoeking ter vastlegging van gegevens (125i) of een netwerkzoeking (125j); bij een traditionele doorzoeking ter inbeslagneming – waar evengoed beveiligde computers en gegevensdragers zullen worden aangetroffen, die niet zelden in beslag worden genomen – kan de bevoegdheid niet worden toegepast. Het is de vraag of de wetgever dat bedoeld of voorzien heeft, maar de wettekst laat moeilijk een andere lezing toe. De bevoegdheid geldt evenmin in andere situaties waarin de politie een beveiligde computer in handen krijgt, zoals wanneer iemand de verdachte aanhoudt en een smartphone in beslag neemt

[101] Wiemans 2004, p. 249.
[102] Koops 2003.
[103] Vgl. *Kamerstukken II* 2012/13, 28 684, nr. 363; Koops e.a. 2012a.
[104] Zie kritische besprekingen in Oerlemans 2011, Jacobs 2012 en Koning 2012.

(art. 95, eerste lid, Sv). Is het niet wenselijk om ook in dergelijke gevallen een toegankelijkmakingsbevel te kunnen geven?

Het bevel wordt niet aan verdachten of verschoningsgerechtigden gegeven (art. 125k lid 3 Sv). De wetgever overweegt in terrorisme- en (gewoontematige) kinderpornozaken wel een ontsleutelbevel aan verdachten te kunnen geven, vanwege de toename van het gebruik van onkraakbare encryptie binnen (met name) kinderpornonetwerken.[105] Hoewel dit inbreuk maakt op het nemo-teneturbeginsel, zou deze inbreuk aanvaardbaar kunnen zijn in het licht van artikel 6 EVRM indien de wettelijke regeling en uitvoering met voldoende waarborgen worden omkleed.[106] Of de in het wetsontwerp CCIII voorgestelde regeling daaraan voldoet, met een voorgestelde strafbedreiging van maar liefst drie jaar, valt echter sterk te betwijfelen.

4.2. Bijzondere opsporingsbevoegdheden

Als uitvloeisel van de IRT-affaire en de daaropvolgende parlementaire enquête opsporingsmethoden in de jaren '90, zijn met de Wet bijzondere opsporingsbevoegdheden[107] (hierna: Wet BOB) veel – en voor ICT de meest relevante – bevoegdheden vastgelegd in het Wetboek van Strafvordering. Daarbij kunnen naast de traditionele opsporing van gepleegde strafbare feiten, ook bevoegdheden worden toegepast in het kader van beraamde georganiseerde misdaad (zie art. 126o lid 1 Sv). Ook kunnen sinds 1 februari 2007 in het kader van terrorismebestrijding bijzondere opsporingsbevoegdheden worden toegepast bij aanwijzingen van een terroristisch misdrijf (zie art. 83 Sv), een lagere drempel dan de 'redelijke verdenking' bij traditionele strafvordering.[108] Het eerste type bevoegdheid is vastgelegd in artikelen 126g e.v. Sv, het tweede in artikelen 126o e.v. Sv, en het derde in artikelen 126za e.v. Sv. Gemakshalve verwijs ik hieronder slechts naar de eerste reeks. Veel bevoegdheden kunnen alleen toegepast worden bij voorlopigehechtenismisdrijven (art. 67, eerste lid, Sv), maar omdat in dat artikel vrijwel alle cyberdelicten specifiek zijn opgesomd, ook die waar minder dan vier jaar gevangenisstraf op staat, levert dat voor de opsporing van cybercriminaliteit geen problemen op. De meest ingrijpende bevoegdheden kunnen alleen worden ingezet als er een misdrijf is dat een ernstige inbreuk op de rechtsorde oplevert. Algemene waarborgen rond geheimhouders, notificatie, bewaring en vernietiging van gegevens en technische hulpmiddelen zijn geregeld in artikelen 126aa e.v. Sv (die volgens de logica van de wetgever na art. 126zu Sv komen).

Binnen het bestek van dit hoofdstuk kan slechts kort worden gewezen op de voornaamste ICT-opsporingsbevoegdheden. Het onderzoek van (tele)communicatie[109] omvat, in toenemende mate van ingrijpendheid:

- het opvragen van gebruikersgegevens (art. 126na Sv), om te weten wie bij welk telefoonnummer of IP-adres hoort of om te weten bij welke aanbieder men moet zijn voor het aftappen van verdachte;
- het opvragen van verkeersgegevens (art. 126n Sv), dat wil zeggen datum, tijdstip en duur van de verbinding, locatiegegevens, nummers van randapparatuur en de soorten diensten;
- het aftappen van communicatie die via een communicatieaanbieder (gedefinieerd in art. 126la Sv) wordt getransporteerd (art. 126m Sv); sinds de Wet CCII kunnen ook private communicatieaanbieders (zoals bedrijfsnetwerken) worden getapt, evenals, mits technisch vanuit Nederland mogelijk, personen die zich in het buitenland bevinden (art. 126ma Sv).

Aanbieders van openbare communicatieaanbieders hebben meewerkverplichtingen onder hoofdstuk 13 van de Telecommunicatiewet, waarin ook verplichtingen staan voor het aftapbaar maken van netwerken en diensten en voor het bewaren van verkeersgegevens (dataretentie).[110]

---

[105] Conceptwetsvoorstel in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III), http://www.internetconsultatie.nl/computercriminaliteit.
[106] Koops 2012.
[107] *Stb.* 1999, 245, inwerkingtreding 1 februari 2000.
[108] *Stb.* 2006, 580. Aanwijzingen zijn bijvoorbeeld moeilijk verifieerbare geruchten dat een aanslag wordt voorbereid of uitkomsten van dreigingsanalyses van de AIVD. *Kamerstukken II* 2004/05, 30 164, nr. 3, p. 9.
[109] Zie hierover uitgebreid Asscher en Ekker 2003; Smits 2006; Fischer 2010.

Een tweede belangrijke groep is het vorderen van gegevens (bij anderen dan communicatieaanbieders). Dit is geregeld in artikelen 126nc e.v. Sv. Politie en justitie kunnen, in volgorde van oplopende zwaarte, identificerende, 'andere' en gevoelige gegevens opvragen, alsmede toekomstige gegevens, bij allerlei personen en instanties.[111] Gevoelige gegevens zijn de gegevens genoemd in artikel 16 Wbp. Nadat de Hoge Raad foto's behorend bij OV-chipkaarten had gekwalificeerd als gevoelige gegevens[112] – uit foto's is immers ras en soms ook de gezondheid af te leiden – probeert de praktijk te omzeilen dat voor het vorderen van beeldmateriaal steeds toestemming van de rechter-commissaris moet worden gevraagd; dat is begrijpelijk, maar lijkt wel in strijd met de wet.[113]

Verder vallen te noemen direct afluisteren (art. 126l Sv), inclusief de bevoegdheid om fysiek in te breken in computers om afluisterapparaatjes of -programmaatjes te plaatsen; dekmanteloperaties, infiltratie en pseudokoop/verkoop/dienstverlening (art. 126h e.v. Sv);[114] het verkennend onderzoek (art. 126hh Sv), waarbij een gebied of maatschappelijke sector kan worden doorgelicht op mogelijke strafbare feiten door koppeling en analyse van databestanden; en stelselmatige observatie (art. 126g Sv). Dit laatste kan worden gebruikt als de politie stelselmatig open Internetbronnen onderzoekt waarbij gericht op personen wordt gezocht, zeker als daarbij platforms met ingebouwde analyse- en visualisatiemiddelen als iColumbo worden gebruikt;[115] voor incidentele zoekacties kan artikel 3 Politiewet 2012 volstaan, maar langduriger of veelomvattender zoekacties maken mijns inziens een meer dan geringe inbreuk op de privacy, zodat daarvoor een expliciete grondslag nodig is. Artikel 126g Sv ligt daartoe voor de hand, maar observatie van Internet kijkt (ook) naar het verleden en niet, zoals bij observatie in de fysieke ruimte, alleen naar het heden.[116] Dit is één voorbeeld waaruit blijkt dat de Wet BOB niet goed is toegesneden op een Internetomgeving; het Internetlandschap ziet er nu toch wel echt anders uit dan de wetgever eind jaren '90 voor ogen had. Een integrale herziening van de Wet BOB in relatie tot Internet zou welkom zijn.[117]

4.3. Bewijsaspecten

Nederland kent een betrekkelijk open bewijsstelsel. Als wettige bewijsmiddelen gelden de eigen waarneming van de rechter, verklaringen van verdachte, getuigen en deskundigen, en schriftelijke bescheiden (art. 339 Sv). Langs de weg van de 'eigen waarneming' van de rechter kunnen ook video-, geluids- en (andere) elektronische gegevens de rechter rechtstreeks bereiken. Van de schriftelijke bescheiden hebben processen-verbaal en andere door bevoegde instanties opgemaakte geschriften, alsook geschriften opgemaakt door buitenlandse ambtenaren, zelfstandige rechtskracht; alle overige geschriften kunnen ook dienen als bewijsmateriaal, maar alleen in samenhang met andere bewijsmiddelen (art. 344 Sv). Geschriften hoeven niet op papier te staan, maar kunnen ook elektronisch zijn; het gaat erom dat zij voor voorlezing vatbaar zijn.[118] Aan digitaal bewijs worden verder geen formele eisen gesteld. Het komt vooral neer op de overtuigingskracht van het bewijs, dat de rechter de innerlijke overtuiging moet geven dat de verdachte het telastgelegde feit heeft begaan (art. 338 Sv). Die overtuigingskracht hangt bij digitaal bewijs vooral samen met de betrouwbaarheid ervan. Hoewel de betrouwbaarheid van computergegevens niet bijzonder groot – ze kunnen immers makkelijk worden gemanipuleerd – levert digitaal bewijs in de rechtspraktijk tot nu toe weinig problemen of discussie op. Deels komt dat omdat politie computerbewijs normaliter op een forensisch aanvaardbare manier veiligstelt (door het maken van een één-op-één-kopie die niet-manipuleerbaar wordt opgeslagen), maar deels ook omdat de verdediging tot nu toe vaak niet digitaal bewijs ter discussie stelt. De rechter

---

[110] Telecommunicatiewet, *Stb.* 1998, 664; Wet bewaarplicht telecommunicatiegegevens, *Stb.* 2009, 333 en *Stb.* 2011, 350.
[111] *Stb.* 2005, 390.
[112] HR 23 maart 2010, LJN BK6331.
[113] Zwenne en Mommers 2010.
[114] Zie Siemerink 2000.
[115] Zie over iColumbo Koops e.a. 2012b.
[116] Oerlemans en Koops 2012.
[117] Schermer 2012.
[118] A.L. Melai, M.S. Groenhuijsen e.a. (red.), *Wetboek van Strafvordering*, losbladig commentaar, aant. 2 op art. 344.

kan er dan van uitgaan dat het bewijs integer is. Dat garandeert overigens alleen dat de opsporingsautoriteiten niet hebben geknoeid met het materiaal; het geeft nog geen zekerheid over de vraag of de eigenaar van de computer de gegevens heeft ingevoerd noch of de inhoud van de gegevens zelf correct is (ook verdachten kunnen liegen in hun dagboek of emails).

Complicaties treden misschien op bij bewijsvergaring uit de cloud, waar nog weinig ervaring mee bestaat (behalve bij webmail, die evenals netpost van een Nederlandse toegangsaanbieder gewoon als bewijs kan dienen). Omdat materiaal in de cloud verspreid en redundant wordt opgeslagen, is er niet zoals bij computeronderzoek sprake van een één-op-één-kopie, maar van een (her)samenstelling van het document dat uit de cloud wordt opgevraagd. Of dat in de praktijk aangevochten zal worden en hoe de rechter daartegenaan zal kijken, moet worden afgewacht.[119]

Relevant is verder de vraag welke invloed onregelmatigheden bij de bewijsgaring hebben op de bruikbaarheid van dat bewijs. Het kan leiden tot bewijsuitsluiting (of strafvermindering, en in extreme gevallen niet-ontvankelijkverklaring, zie art. 359a Sv), maar dat hoeft niet per se. De rechter kijkt naar het hele dossier en de procedure als geheel, waarbij onder andere gekeken wordt naar de mate waarin het omstreden materiaal betwistbaar is voor de verdediging in de rechtszaal en in welke mate het oordeel stoelt op ander bewijs dan het omstreden bewijs.[120] Bovendien wordt de nodige ruimte geboden door het leerstuk van de Schutznorm, die bepaalt dat bewijsmateriaal niet hoeft te worden uitgesloten indien de norm die is geschonden (bij onrechtmatig verkregen bewijs) een ander belang dient dan dat van de verdachte.[121] Bewijsuitsluiting is alleen aan de orde wanneer de norm waarop een beroep wordt gedaan in abstracto strekt tot bescherming van de belangen van de verdachte, terwijl ook in concreto de door die norm beschermde belangen van de verdachte moeten zijn geschaad.[122] Dat biedt mogelijkheden om toch bewijs te gebruiken waarbij bijvoorbeeld internationale normen zijn geschaad door grensoverschrijdende opsporing zonder toestemming van de buitenlandse staat, aangezien dan vooral de norm van nationale soevereiniteit en niet het privacybelang van computergebruikers geschonden is.[123]

5. Afsluiting

Cybercrimewetgeving laat zien dat een werkbare combinatie mogelijk is van internationale kaders en nationale invulling en aanvulling. De Nederlandse wet kent een breed vangnet om computercriminaliteit te bestrijden. Vrijwel alle verschijningsvormen van cybercriminaliteit kunnen onder strafbepalingen worden gebracht, mede door de ruime formulering van basisdelicten als computervredebreuk (art. 138ab WvSr) en gegevensaantasting (art. 350a WvSr). Ook de opsporing kan qua bevoegdheden goed uit de voeten met de wetgeving; de praktijk vraagt wel vaak om nieuwe bevoegdheden, zoals het via Internet kunnen plaatsen van afluisterprogrammaatjes, maar dat is inherent aan de opsporingstaak waarbij altijd grenzen van bevoegdheden worden opgezocht.

Hoewel een algemeen probleem van Internetregulering is dat techniek zich snel ontwikkelt terwijl wetgeving de nodige tijd nodig heeft, valt te constateren dat cybercrimewetgeving grosso modo goed bij de tijd is en voldoende snel kan reageren op ontwikkelingen in de misdaad. Een probleem is wel dat internationale regulering meer tijd vergt dan nationale wetgeving en dat ook de Nederlandse cybercrimewetgeving soms traag verloopt, zoals blijkt uit het Wetsvoorstel CCII uit 1999 dat pas in 2006 werd aangenomen. Maar de wetgevingspraktijk laat ook zien dat gaten in de wetgeving op zich snel kunnen worden gedicht, door opname van cybercrimebepalingen in reparatie- of omnibuswetten. Te hopen valt wel dat de huidige actualiseringsoperatie – Computercriminaliteit III – voortvarender gaat dan de voorganger.

---

[119] Zie nader over cloud-bewijs, Koops e.a. 2012a.
[120] Zie EHRM 12 juli 1988, Schenk t. Frankrijk, app.nr. 10862/84.
[121] Zie HR 30 maart 2004, LJN AM2533, par. 3.5.
[122] Aldus de conclusie van A-G Jörg bij HR 6 juli 2004, LJN AO9785.
[123] Zie hierover ook De Hert & Koops 2001.

Het is de vraag of op langere termijn nationale wetgeving die op basisniveau internationaal is geharmoniseerd, voldoende aanknopingspunten blijft bieden voor de bestrijding van cybercriminaliteit. De huidige strategie van geharmoniseerde minimumwetgeving en wederzijdse rechtshulp, waarin veel ruimte is voor nationale invulling en eigen beleidsvorming, heeft beperkte slagkracht in een mondiale cyberomgeving. Vroeg of laat zal een intensievere internationale inspanning nodig zijn waarbij lidstaten een deel van hun nationale soevereiniteit zullen moeten opgeven om internationale en nationale grensoverschrijdende acties (zoals een grensoverschrijdende netwerkzoeking en het ontmantelen van botnets) toe te staan, wil men cybercrime effectief tegenwicht kunnen blijven bieden. De Europese kaders zullen vermoedelijk meer gewicht en sturing moeten krijgen wanneer ontwikkelingen in cybercrime daartoe noodzaken.

Tot slot zij opgemerkt dat de juridische benadering die in dit hoofdstuk centraal staat, maar een deel van het verhaal is bij de bestrijding van cybercriminaliteit. Maatregelen gericht op preventie, bewustwording bij eindgebruikers, interventies door softwareontwikkelaars en Internetaanbieders en wellicht verstoringsacties zijn evenzeer van belang als een strafrechtelijke aanpak. Het recht speelt een belangrijke rol bij de bestrijding van cybercrime, maar alleen binnen de context van een integrale visie die alle mogelijke sturingsinstrumenten benut.[124]

Gebruikte afkortingen

BOB	bijzondere opsporingsbevoegdheden
CCV	Cybercrime-Verdrag
DDoS	Distributed Denial-of-Service
HR	Hoge Raad
NJ	Nederlandse Jurisprudentie
RFID	Radio Frequency Identification
OM	Openbaar Ministerie
ovj	officier van justitie
r-c	rechter-commissaris
Sr	Wetboek van Strafrecht
Sv	Wetboek van Strafvordering

Bibliografie

Asscher, L.F. en A.H. Ekker (red.) (2003), *Verkeersgegevens. Een juridische en technische inventarisatie*, Amsterdam, Otto Cramwinckel Uitgever.

Brenner, S.W. (2009), *Cyberthreats. The Emerging Fault Lines of the Nation State*, Oxford: Oxford UP.

Commissie computercriminaliteit (1987), *Informatietechniek & Strafrecht. Rapport van de Commissie Computercriminaliteit*, Staatsuitgeverij, Ministerie van Justitie 1987.

De Hert, P. & B.J. Koops (2001), 'Privacy is nog steeds een grondrecht. Pleidooi voor de uitsluiting van onrechtmatig bewijs', *Ars Aequi* 50 (12), p. 972-975.

Domenie, M.M.L. e.a. (2013), *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*, Den Haag: Boom Lemma uitgevers.

Dommering, E.J. (2013), 'De door het recht bestuurde wereld is altijd virtueel geweest', *Nederlands Juristenblad*, p. 1266-1272.

Europese Commissie (2007), *Mededeling van de Commissie. Naar een algemeen beleid voor de bestrijding van cybercriminaliteit*, COM(2007) 267 definitief, 22.5.2007.

[124] Vgl. Europese Commissie 2007 en bijvoorbeeld Katyal xxx.

Fischer, J.C. (2010), *Communications Network Traffic Data. Technical and Legal Aspects*, diss. Eindhoven, Eindhoven: TU/e.
Glenny, M. (2012), *Dark Market. How Hackers Became the New Mafia*, London: Vintage.
Groenhuijsen, M.S. & F.P.E. Wiemans (1989), *Van electriciteit naar computercriminaliteit*, Arnhem: Gouda Quint 1989.
Jacobs, B. (2012), 'Policeware', *Nederlands Juristenblad* (39), p. 2761-2764.
Kaspersen, H.W.K. (1990), *Strafbaarstelling van computermisbruik*, Antwerpen/Deventer: Kluwer 1990.
Kaspersen, H.W.K. (2007), '*Cyber crime* in historisch perspectief', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 13-22.
Katyal, N.K. (2001), 'Criminal Law in Cyberspace', *University of Pennsylvania Law Review* Vol. 149, p. 1003-1114.
Kentgens, Arno (2010), '"Verspreiden" in het digitale tijdperk. De strafrechtelijke aansprakelijkheid voor hyperlinks, *Nederlands Juristenblad*, p. 1984-89.
Koning, M.E. (2012), 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *Privacy & Informatie* (2), p. 46-52.
Koops, B.J. (2003), 'Van brieven, geschriften en onbegrijpelijke wetgeving', *Delikt & Delinkwent 33* (8), p. 850-878.
Koops, B.J. (2006), 'Should ICT Regulation Be Technology-Neutral?', in: Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 77-108
Koops, B.J. (red.) (2007), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007.
Koops, B.J. & Th. de Roos (2007), 'Materieel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 23-75.
Koops, B.J. & Y. Buruma (2007), 'Formeel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 77-121.
Koops, B.J. (2009), 'Sex, Kids, and Crime in Cyberspace: Some Reflections on Crossing Boundaries', in: A.R. Lodder & A. Oskamp (eds), *Caught in the Cyber Crime Act* (liber-Kaspersen), Deventer: Kluwer 2009, p. 63-76.
Koops, B.J. (2010a), 'The Internet and its Opportunities for Cybercrime', in: M. Herzog-Evans (ed.), *Transnational Criminology Manual*, Vol. 1, Nijmegen: WLP, p. 735-754.
Koops, B.J. (2010b), 'Tijd voor Computercriminaliteit III', *Nederlands Juristenblad*, p. 2461-2466.
Koops, B.J. (2012), *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, Meppel/Den Haag: Boom Lemma uitgevers / WODC, serie Onderzoek & Beleid 305.
Koops, B.J. e.a. (2012a), *Misdaad en opsporing in de wolken. Knelpunten en kansen van* cloud computing *voor de Nederlandse opsporing*, Tilburg/Den Haag: TILT/ WODC.
Koops, B.J. e.a. (2012b), *Juridische scan openbrononderzoek. Een analyse op hoofdlijnen van de juridische aspecten van de iRN/iColumbo-infrastructuur en HDIeF-tools*, Tilburg: TILT/TNO.
Koops, B.J. (2013), 'Virtuele en reële delicten. Een beschouwing over het RuneScape-arrest en computercriminaliteitswetgeving', *Computerrecht*, p. 14-22.
Leukfeldt, E.R. & W.Ph. Stol (2012), 'De rol van internet bij fraudedelicten. Internetfraudeurs en klassieke fraudeurs vergeleken', *Justitiële verkenningen* 38(1), p. 108-120.
Lodder, A.R. & A. Oskamp (2007), 'ICT-toepassingen in het strafrecht', in: B.J. Koops (red.), *Strafrecht en ICT*, 2e druk, Den Haag: Sdu 2007, p. 181-204.
Lodder, A.R. & L.J.M. Boer (2012), 'Cyberwar? What war? Meer in het bijzonder: welk recht?', *Justitiële verkenningen* 38(1), p. 52-67.
NCSC (z.j.), *Leidraad om te komen tot een praktijk van Responsible Disclosure*, https://www.ncsc.nl/binaries/nl/actueel/nieuwsberichten/leidraad-responsible-disclosure/2/Responsible%2BDisclosure.pdf.
Oerlemans, J.J. & B.J. Koops (2011), 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *Nederlands Juristenblad* (18), p. 1181-1185.
Oerlemans, J.J. & B.J. Koops (2012), 'Surveilleren en opsporen in een internetomgeving', *Justitiële verkenningen* 38(5), p. 35-49.
Oerlemans, J.J. (2011), 'Hacken als opsporingsbevoegdheid', *Delikt en Delinkwent* (8), p. 888-908.
Parker, D. (1973), *Computer Abuse,* Palo Alto 1973.

Rozemond, K. (2013), 'RuneScape', *Ars Aequi*, p. 294-301.
Schellekens, M.H.M., B.J. Koops & W. Teepe (2007), *Wat niet weg is, is gezien. Een analyse van art. 54a Sr in het licht van een Notice-and-Take-Down-regime*, Tilburg: TILT/Cycris.
Schermer, B. (2005), 'Criminaliteit en RFID', in: Zwenne & Schermer (red.), *Privacy en andere juridische aspecten van RFID*, Den Haag: Elsevier Juridisch 2005, p. 83-96.
Schermer, B. (2012), 'Digitale IRT-affaire of nieuwe opsporing?', *Webwereld*, 14 maart 2012, http://webwereld.nl/beveiliging/59972-digitale-irt-affaire-of-nieuwe-opsporing-opinie.
Siemerink, L. (2000), *De wenselijkheid en mogelijkheid van infiltratie en pseudokoop op het Internet,* Deventer: Kluwer 2000, ITeR-reeks deel 30.
Smits, A.H.H. (2006), *Strafvorderlijk onderzoek van telecommunicatie*, diss. Tilburg, Nijmegen: Wolf Legal Publishers.
Stevens, L. & B.J. Koops (2009), 'Opzet op de harde schijf: criteria voor opzettelijk bezit van digitale kinderporno', *Delikt & Delinkwent* (7), p. 669-696.
Van der Hof, S. e.a. (2006), *Openbaarheid in het Internettijdperk. De invloed van ICT op juridische concepten van openbaarheid*, Den Haag: Sdu uitgevers, ITeR-reeks deel 79.
Van der Hof, S. (2013), *Digitale kinderrechten: balanceren tussen autonomie en bescherming*, oratie Leiden, 1 maart 2013.
Van der Hulst, R.C. & R.J.M. Neve (2008), *High-tech crime, soorten criminaliteit en hun daders. Een literatuurinventarisatie*, Den Haag: WODC.
Van Dijk, H. & J.M.J. Keltjens (1995), *Computercriminaliteit*, Zwolle: Tjeenk Willink 1995.
Van Wilsem, J. (2012), 'Slachtofferschap van identiteitsfraude; een studie naar aard, omvang, risicofactoren en nasleep', *Justitiële verkenningen* 38(1), p. 97-107.
Wall, D.S. (2007), *Cybercrime. The Transformation of Crime in the Information Age*, Cambridge (UK): Polity Press.
Wiemans, F.P.E. (1991), *Computercriminaliteit. Commentaren op het wetsvoorstel computercriminaliteit*, Maastricht: Cipher Management 1991.
Wiemans, F.P.E. (2004), *Onderzoek van gegevens in geautomatiseerde werken*, Nijmegen: WLP.
Zwenne, G.-J. en L. Mommers (2010), 'Zijn foto's en beeldopnamen "rasgegevens" in de zin van artikel 126nd Sv en artikel 18 Wbp?', *Privacy & Informatie*, p. 237-247.