arsaequi.nl/maandblad AA20180630

Digitale vermogensdelicten in het Wetboek van Strafrecht. Een zoekplaatje met gevolgen?

Jeroen ten Voorde*

In deze bijdrage wordt bezien met behulp van welke strafbaarstellingen in het Wetboek van Strafrecht in het digitale domein gepleegde vermogenscriminaliteit kan worden bestraft en welke rechtsbelangen daarmee worden beschermd. Digitale vermogensdelicten blijken, onder meer door hun deels Europese (EU) herkomst, niet steeds dezelfde rechtsbelangen te beschermen als de vermogensdelicten, hetgeen theoretische en praktische bezwaren heeft.

1 Inleiding

Op 1 maart 2018 was het vijfentwintig jaar geleden dat de Wet computercriminaliteit in werking trad.[1] Aan de basis van die wet lag een rapport, getiteld *Informatietechniek en strafrecht*, dat was samengesteld door de commissie computercriminaliteit (ook bekend als de commissie-Franken). Deze commissie stelde dat het toen geldende strafrecht onvoldoende was toegesneden 'op de dreigingen die zijn verbonden aan het ge- en misbruik van moderne informatietechnieken', die onder meer werden geconstateerd op het terrein van de economie en de privacy van burgers en bedrijven.[2] De commissie oordeelde dat deze dreigingen dusdanig groot zijn dat strafrechtelijk ingrijpen wenselijk is. Ze zag zich voor de vraag gesteld of het bestaande strafrecht reeds voldoende bescherming bood en kwam tot een ontkennend antwoord. Dat hield verband met de reikwijdte van het bestanddeel 'goed' dat in meerdere strafbaarstellingen is opgenomen, onder andere van diefstal, afpersing en oplichting. Zouden onder dat bestanddeel ook computergegevens kunnen vallen, dan hoefde het geldende strafrecht volgens de commissie niet te worden gewijzigd. Zij oordeelde echter dat gegevens iets anders zijn dan een goed, zodat 'andere vormen van bescherming van toepassing moeten zijn dan de vormen waarmee materiële zaken [lees: goederen, JMtV] worden beschermd. Dit sluit aan bij de traditie, ook in Nederland, waarin produkten van psychische arbeid door afzonderlijke bepalingen zijn beschermd'.[3] Deze keuze noodzaakte de commissie tot het doen van voorstellen tot aanpassing van bestaande strafbaarstellingen en het invoeren van nieuwe strafbaarstellingen op het terrein van computercriminaliteit.

Deze voorstellen strekten niet tot introductie van een aparte wet of tot het invoeren van een aparte titel in het Wetboek van Strafrecht. De commissie liet in haar rapport de bestaande systematiek van het wetboek ongemoeid en stelde voor de nieuwe door haar voorgestelde delicten te plaatsen binnen de bestaande titels.[4] Die werkwijze wijst erop dat volgens de commissie met computercriminaliteit geen andere rechtsbelangen zijn gemoeid dan de rechtsbelangen die reeds door het Wetboek van Strafrecht worden beschermd.

Het voorstel van de commissie om nieuwe strafbaarstellingen op het terrein van computercriminaliteit in te passen in reeds

* Prof.mr. J.M. ten Voorde is universitair hoofddocent straf(proces)recht aan de Universiteit Leiden en bijzonder hoogleraar strafrechtsfilosofie (leerstoel Leo Polak) aan de Rijksuniversiteit Groningen.
Met dank aan Jan-Jaap Oerlemans voor zijn commentaar op een eerdere versie van dit artikel.

1 Wet van 23 december 1992, *Stb.* 1993, 33.
2 H. Franken e.a., *Informatietechniek & Strafrecht*, Den Haag: Staatsuitgeverij 1987, p. 107-108.
3 Franken e.a. 1987, p. 39.
4 Franken e.a. 1987, p. 31.

Foto en knutselwerk: Manon Heinsman | © Ars Aequi

bestaande titels van het Wetboek van Strafrecht werd door de minister van Justitie in het wetsvoorstel computercriminaliteit overgenomen.[5] Volgens de minister verschilt computercriminaliteit niet wezenlijk van bestaande vormen van criminaliteit, zodat het strafmaximum niet (wezenlijk) behoort te verschillen. Dat wordt gegarandeerd door de nieuwe strafbaarstellingen te plaatsen bij de bestaande, daarop gelijkende strafbaarstellingen. Vernieling van gegevens (art. 350a Sr) werd om die reden geplaatst na vernieling van goederen (art. 350 Sr).

Deze werkwijze, waardoor strafbaarstellingen op het terrein van computercriminaliteit verspreid over het Wetboek van Strafrecht zijn te vinden, is nadien niet verlaten[6] en vinden we ook terug in het thans bij de Eerste Kamer aanhangige wetsvoorstel computercriminaliteit III dat opnieuw tot aanpassingen in het Wetboek van Strafrecht moet leiden.[7] Verschillende van de hierin voorgestelde wijzigingen betreffen vermogenscriminaliteit. Digitale vermogenscriminaliteit is een fenomeen dat de laatste jaren in verschillende wetenschappelijke disciplines op steeds meer belangstelling mag rekenen.

In deze bijdrage wordt bezien met behulp van welke strafbaarstellingen in het Wetboek van Strafrecht in het digitale domein gepleegde vermogenscriminaliteit kan worden bestraft en welke rechtsbelangen daarmee worden beschermd

In deze bijdrage wordt bezien met behulp van welke strafbaarstellingen in het Wetboek van Strafrecht in het digitale domein gepleegde vermogenscriminaliteit kan worden bestraft en welke rechtsbelangen daarmee worden beschermd. Om die vragen te beantwoorden, bepaal ik eerst welke de vermogensdelicten zijn en welke rechtsbelangen zij beogen te beschermen (par. 2). Vervolgens geef ik een overzicht van bestaande (en toekomstige) strafbaarstellingen op het terrein van digitale vermogenscriminaliteit (par. 3). Ik geef ook antwoord op de vraag welke rechtsbelangen deze delicten beogen te beschermen. We zullen zien dat digitale vermogensdelicten niet steeds dezelfde rechtsbelangen beschermen als de vermogensdelicten, hetgeen zowel theoretische als praktische bezwaren heeft. Tevens wordt bezien in hoeverre zij als vermogensdelicten kunnen worden beschouwd, gelet op de in paragraaf 2 omschreven rechtsbelangen. Indien het antwoord op die vraag negatief is, is de vraag of de door de commissie-Franken gemaakte keuze nog kan worden gehandhaafd. Hierop wordt in de slotparagraaf ingegaan (par. 4).

2 Over vermogensdelicten en digitale vermogensdelicten

2.1 Ontwikkeling van rechtsbelangen

Het Wetboek van Strafrecht ontbeert een titel betreffende de bescherming van het vermogen. Wel kunnen we achterhalen welke titels volgens de wetgever de vermogensrechten van het individu beschermen: XXII tot en met XXVII.[8] Het opschrift van deze titels maakt duidelijk welke strafbare feiten tot de vermogensdelicten worden gerekend: diefstal en stroperij, afpersing en afdreiging, verduistering, bedrog, benadeling van schuldeisers en rechthebbenden en vernieling en beschadiging.[9] Het vermogen waarover iemand een bepaald recht uitoefent en dat met behulp van de strafwet tegen ontvreemding, vervalsing, vernieling of beschadiging, enzovoorts wordt beschermd,[10] wordt in de wettekst op uiteenlopende manieren uitgedrukt. In verschillende delictsomschrijvingen komen we ook het bestanddeel 'goed' tegen, terwijl andere bestanddelen daarvan een variant zijn, zoals 'voorwerp'. Van Bemmelen stelt dat onder goed primair voor verplaatsing vatbare voorwerpen werd verstaan.[11]

Vanaf de eerste helft van de twintigste eeuw zien we volgens Van Bemmelen met betrekking tot de vermogensdelicten twee ontwikkelingen. Allereerst is de strafrechtelijke bescherming uitgebreid naar 'ieder vermogensbestanddeel', hetgeen onder andere blijkt uit het bekende Elektriciteitsarrest.[12] Het rechtsbelang dat door de vermogensdelicten wordt beschermd is echter niet langer beperkt tot bescherming van de vermogensrechten van een specifieke eigenaar of bezitter. Ook de evenredige verdeling van goederen, het voortbestaan van belangrijke, publieke goederen en een goede kapitaalsvorming zijn door de vermogensdelicten te beschermen rechtsbelangen geworden.[13]

Deze belangen zijn meer collectieve belangen; zij reiken verder dan de bescherming van een goed van een individuele eigenaar of bezitter. De eerste twee belangen stonden

5 *Kamerstukken II* 1989/90, 31551, 3, p. 3.

6 Wet van 1 juni 2006, *Stb.* 2006, 330 (Wet computercriminaliteit II).

7 *Kamerstukken I* 2016/17, 34372, A.

8 H.J. Smidt, *Geschiedenis van het Wetboek van Strafrecht* (Tweede Deel; bewerkt door J.W. Smidt), Haarlem: Tjeenk Willink 1891, p. 3. In literatuur wordt opvallend genoeg niet naar deze passage uit de wetsgeschiedenis verwezen. Zie o.a. J.D. den Hartogh & N.S. de Wit, 'Vermogensdelicten: te ingewikkeld geregeld?', *DD* 2002, p. 857; D.H. de Jong, 'Vermogensdelicten: klassieke delictsomschrijvingen en moderne interpretatie', *DD* 1996, p. 857-850 en V.M.A. Sinnige, *De systematiek van de vermogensdelicten* (diss. Groningen), Deventer: Wolters Kluwer 2017 wier indeling van de vermogensdelicten telkens iets lijkt te wijzigen. Zie bijv. p. 2, 27, 95.

9 Dit zijn de huidige opschriften van de betreffende titels.

10 De aard van de gedragingen en het doel waarmee die gedragingen worden verricht, zijn mede bepalend voor strafbaarstelling. Op die manier wordt afbakening ten opzichte van het civiele recht gewaarborgd. Dit geldt in het bijzonder voor de strafbepalingen die vallen onder de titel bedrog, waaronder oplichting (art. 326 Sr).

11 J.M. van Bemmelen & W.F.C. van Hattum, *Hand- en leerboek van het Nederlandse strafrecht. Deel II. Bijzondere delicten* (door J.M. van Bemmelen), 's-Gravenhage/Arnhem: Martinus Nijhoff/Gouda Quint – Brouwer en Zoon 1954, p. 262. Zie t.a.v. diefstal Sinnige 2017, p. 35-41.

12 HR 23 mei 1921, *NJ* 1921, p. 564, m.nt. B.M. Taverne. Zie M.S. van Oosten, 'De strafrechtelijke bescherming van het vermogen', *Tijdschrift voor Strafrecht* 1950, p. 200-227.

13 Van Bemmelen 1954, p. 263-265.

vooral tijdens en na de beide wereldoorlogen op de voorgrond; zij hebben tegenwoordig aan praktisch belang ingeboet. Strafbaarstellingen die deze belangen beogen te beschermen vinden we nog wel in het overzicht van wetten in artikel 1 en 1a van de Wet op de Economische Delicten.[14] Het derde belang, een goede kapitaalsvorming, herkennen we in strafbaarstellingen op het terrein van het effectenverkeer en het financieel toezicht; ook de strafbaarstelling van witwassen (art. 420bis e.v. Sr) kan ermee in verband worden gebracht, indien onder dit belang mede wordt verstaan de bescherming van het financieel en economisch verkeer. Zo uitgelegd betreft het te beschermen belang van goede kapitaalsvorming niet alleen het tegengaan van het zich meer dan normaal verrijken, zoals Van Bemmelen stelde.[15] In dat geval is het belang nog tamelijk individualistisch uitgelegd en komt het neer op het spiegelbeeld van het belang de eigendom en het bezit van een persoon te beschermen. Indien het ook om een meer collectief belang gaat, dan beschermt dit belang de economie die uitgaat van eerlijke concurrentie zonder te worden besmet door uit misdrijf afkomstig vermogen of vermogen dat eerlijke concurrentie belemmert of door valse of onvolledige informatie een gezonde economische ontwikkeling in de weg staat.[16] Zo beschouwd vallen ook heling en witwassen (Titel XXX en XXXA) onder de vermogensdelicten.

2.2 Rechtsbelangen en digitale vermogensdelicten

Uit het voorgaande valt af te leiden dat vermogensdelicten meerdere belangen beschermen. We zagen ook dat het aloude belang dat door de vermogensdelicten wordt beschermd, is uitgebreid. Hiervoor wees ik al op het Elektriciteitsarrest. In deze zaak rees de vraag of elektriciteit een goed is dat kan worden weggenomen. De Hoge Raad beantwoordde deze vraag bevestigend en onderbouwde dat oordeel met de volgende argumenten: elektriciteit heeft een zelfstandig bestaan, zij kan door menselijk toedoen op een andere zaak worden overgebracht of worden geaccumuleerd, zij kan door toedoen van de mens worden opgewekt en kan van hem die haar opwekte ter beschikking blijven, zij vertegenwoordigt een bepaalde waarde, omdat de verkrijging met kosten en moeite gepaard ging en te eigen bate kan worden gebruikt of tegen vergoeding aan anderen kan worden overgebracht en zij kan uit de macht van de één en in de macht van een ander geraken.[17]

In latere arresten worden deze argumenten soms wel, soms niet herhaald terwijl de Hoge Raad ook andere argumenten introduceerde. In het Giraal geld-arrest stelde de Hoge Raad dat 'gelet op de functie van zogenaamd giraal geld in het maatschappelijk verkeer' op grond van een 'redelijke uitleg' van artikel 321 Sr (verduistering) giraal geld als goed moet worden beschouwd.[18] In het Pincode-arrest werd bepaald dat 'de in de geest van een persoon opgeslagen bekendheid met de bij zijn betaalpas behorende cijfercombinatie' niet als goed kan worden aangemerkt. Daarvan is volgens de Hoge Raad slechts sprake 'indien door die afgifte de afgever de beschikking over het afgegevene verliest'.[19]

In 2012 wees de Hoge Raad op dezelfde dag in twee zaken arrest over de betekenis van een goed: één over diefstal van belminuten en sms-berichten en één over diefstal van een virtueel amulet en een virtueel masker in het computerspel RuneScape

In 2012 wees de Hoge Raad op dezelfde dag in twee zaken arrest over de betekenis van goed: één over diefstal van belminuten en sms-berichten en één over diefstal van een virtueel amulet en een virtueel masker in het computerspel RuneScape.[20] In het arrest over belminuten en sms-berichten wijst de Hoge Raad op de economische betekenis die in het normale spraakgebruik aan belminuten en sms-berichten wordt gegeven alsmede op 'de functie die belminuten en sms-berichten in deze economische betekenis in het maatschappelijk verkeer vervullen'. Dit en andere arresten maakt duidelijk dat het maatschappelijk of economisch verkeer een steeds belangrijker te beschermen rechtsbelang is geworden. Dat belang moet ruim worden opgevat; het gaat om relaties tussen (rechts)personen die door het recht worden beheerst en die zich niet beperken tot de fysieke wereld. Relaties bestaan ook in de digitale wereld. Op het eerste gezicht lijkt er verwantschap te bestaan met het belang dat door de wetgever aan de vermogensdelicten ten grondslag werd gelegd: bescherming van het vermogen(srecht) van een andere (rechts)persoon. In het Elektriciteitsarrest wordt de relatie tussen personen nog door de

14 Bijvoorbeeld de Noodwet voedselvoorziening, de Prijzennoodwet en de Bodemproductiewet.
15 Vgl. *Kamerstukken II* 2012/13, 33685, 3, p. 1 m.b.t. financieel-economische criminaliteit.
16 Vgl. *Kamerstukken II* 2013/14, 33994, 3, p. 1 m.b.t. het faillissementsstrafrecht.
17 HR 23 mei 1921, *NJ* 1921, p. 564, m.nt. B.M. Taverne.
18 HR 11 mei 1982, *NJ* 1982/583, m.nt. A.C. 't Hart.
19 HR 13 juni 1995, *NJ* 1995/635.
20 HR 31 januari 2012, *NJ* 2012/535, respectievelijk HR 31 januari 2012, *NJ* 2012/536, m.nt. N. Keijzer.

Hoge Raad benadrukt, in het Giraal geldarrest en het Belminuten en sms-berichtenarrest krijgt de bescherming van het economisch verkeer een prominente plaats.

In het RuneScape-arrest stonden geen publieke belangen centraal, maar was de vraag hoever de bescherming van het individuele vermogen(srecht) strekt, in geval dat vermogen slechts bestaat in de context van een spel, namelijk in de vorm van een virtueel masker en een virtueel amulet. Volgens de Hoge Raad kon in het onderhavige geval om de volgende redenen van een goed dat kan worden weggenomen worden gesproken. Ten eerste hadden het virtuele masker en de virtuele amulet voor dader en slachtoffer een 'reële waarde' 'die hen kan worden afgenomen'. Ten tweede ging het 'om in de loop van het spel ontstane waarden, die door inspanning en tijdsinvestering zijn verworven of zijn te verwerven'. Ten derde had het slachtoffer 'binnen het spel over die objecten "de feitelijke en exclusieve heerschappij"'. Ten vierde had hij 'door het handelen van de verdachte en zijn mededader de beschikkingsmacht over deze objecten […] verloren'. Ik merk op dat de Hoge Raad in het RuneScape-arrest zijn oordeel enkel op individuele rechtsbelangen baseert. Daarbij is het om het even dat die belangen slechts in een spelsituatie bestaan. Wellicht houdt dat verband met het feit dat voor zowel de daders als het slachtoffer het onderscheid tussen de virtuele en reële wereld relatief was; zij namen het spel buitengewoon serieus. Van 'slechts een spelletje' was in hun ogen geen sprake.[21]

De vermenging tussen virtuele en reële wereld leidt tot een verdere verruiming van het beschermde rechtsbelang: niet alleen reële vermogensrechten, ook vermogen dat slechts in de context van een (virtueel) spel bestaat kunnen als een goed worden beschouwd

Deze vermenging tussen virtuele en reële wereld leidt tot een verdere verruiming van het beschermde rechtsbelang: niet alleen reële vermogensrechten, ook vermogen dat slechts in de context van een (virtueel) spel bestaat,[22] terwijl door de deelnemers aan dat spel veel waarde wordt gehecht, kunnen als een goed worden beschouwd. Dat het virtuele vermogen ook voor anderen dan dader en slachtoffer een reële waarde heeft, zoals blijkt uit het verhandelen ervan op verkoopsites als eBay en marktplaats, is volgens de Hoge Raad kennelijk niet van belang om van een goed te kunnen spreken. Mede daarom heeft het arrest ook minder goede pers gehad. Het beschermen van virtueel vermogen (oftewel vermogen dat slechts bestaat binnen de 'magische cirkel' van een spel), zou buiten het strafrecht moeten vallen. Dat betekent niet dat de gedragingen die in de RuneScape-zaak zijn bewezenverklaard, niet strafbaar zouden zijn. Zij moeten echter anders worden gekwalificeerd.[23]

2.3 Van goed naar gegevens

Koops en Rozemond stellen dat gevallen als die in de RuneScape-zaak met behulp van het delict computervredebreuk moeten worden aangepakt. Daarin is onder meer strafbaar gesteld het overnemen, aftappen of opnemen van gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk waarin de dader is binnengedrongen (art. 138ab lid 2 Sr). In deze strafbaarstelling lezen we het bestanddeel 'gegevens'. Gegevens verschillen van goederen doordat zij geen product zijn van 'fysieke arbeid': zij zijn 'geestesprodukten' en 'multiple', wat wil zeggen dat het erover beschikken niet uitsluit 'dat ook anderen over dezelfde gegevens kunnen beschikken'. De commissie-Franken overwoog dat overeenstemming bestaat om gedragingen die de beschikbaarheid van gegevens aantasten strafbaar te stellen. Bij gegevens kan geen 'ongedifferentieerd strafrechtelijk regime worden gecreëerd ten aanzien van diverse soorten immateriële goederen, waarvoor bijzondere regelingen zijn gegeven, die zijn onderworpen aan allerlei beperkingen en nuanceringen'.[24] Deze beperkingen en nuanceringen, die onder meer in de Auteurswet zijn te vinden, verzetten zich tegen het opnemen van één titel in het Wetboek van Strafrecht dat de bescherming van gegevens op het oog heeft, omdat daarmee meerdere doelen worden gediend, namelijk: de beschikbaarheid, de integriteit en de exclusiviteit van gegevens alsmede het exclusieve gebruik daarvan.[25]

De laatste twee doelen lijken met de rechtsbelangen die door de vermogensdelicten worden beschermd verband te houden. De exclusiviteit van (het gebruik van) gegevens verwijst naar het belang het exclusieve bezit en gebruik van gegevens te beschermen. De twee eerste doelen zien op andere belangen,

21 Zie L. Strikwerda, 'Virtuele activiteiten, echte strafbare feiten. Een rechtsfilosofische analyse van virtuele computercriminaliteit', *Strafblad* 2017/48, par. 4.3. Het hof had in zijn arrest nog opgemerkt dat de wervingshandelingen buiten de context van het spel hadden plaatsgevonden. Die omstandigheid is volgens Strikwerda van belang om van diefstal te kunnen spreken, omdat deze gedragingen buiten de 'magische cirkel' plaatsvonden. De Hoge Raad verwijst niet naar dit argument (hoogstens impliciet), zodat het mij voorkomt dat dit argument niet erg relevant is. Het buiten de context van het spel gebruikte geweld levert bewijs op van de strafverzwarende omstandigheid in art. 312 Sr. Het argument zegt nog niets over de eigenschappen van de virtuele amulet of het virtuele masker. De bewezenverklaarde gedragingen bevestigen hoe reëel de waarde ervan in de ogen van daders en slachtoffer was. Maar dat had het hof al vastgesteld, zodat het naar het uitgeoefende geweld verwijzende argument m.i. geen toegevoegde waarde heeft.

22 Of op grond van het civiele recht van een vermogensrecht kan worden gesproken, werd onder andere besproken door: E.D.C. Neppelenbroek, 'De juridische positie van de dief van toegang tot een virtuele amulet. Over de brug tussen diefstal en inbezitneming', *RMThemis* 2011, p. 263-273.

23 N. Rozemond, 'RuneScape', *Ars Aequi* 2013, p. 294-301 (AA20130294); B.J. Koops, 'Virtuele en reële delicten. Een beschouwing over het RuneScape-arrest en computercriminaliteitwetgeving', *Computerrecht* 2013/4. Zie veel positiever C. Spierings & G. Pesselse, 'Reële diefstal van een virtuele amulet: een analyse van het RuneScape-arrest vanuit strafrechtelijk en goederenrechtelijk perspectief', *NTBR* 2012/28; Strikwerda 2017.

24 Franken e.a. 1987, p. 38-39.

25 Franken e.a. 1987, p. 39-65; Koops 2013.

waaronder de algemene veiligheid van informatie- en communicatietechnologie, de privacy van personen, de vertrouwelijkheid van gegevens en dergelijke. Hoewel het in deze strafbaarstellingen telkens gaat om gegevens, verschillen de rechtsbelangen van elkaar. De wetgever heeft met het opnemen van een definitie in het wetboek (art. 80quinquies Sr) voorkomen dat die uiteenlopende rechtsbelangen tot verschillende interpretaties van het bestanddeel gegevens leiden. De strafbaarstellingen die naar verloop van tijd aan het Wetboek van Strafrecht zijn toegevoegd en een specifiek rechtsbelang beogen te beschermen, leiden een min of meer zelfstandig bestaan. Zij moeten vooral worden bezien in het licht van de strafbepalingen die hetzelfde rechtsbelang beogen te beschermen en niet als een samenhangend geheel van strafbaarstellingen op het terrein van computercriminaliteit. Dat betekent tevens, zoals weldra blijkt, dat digitale vermogensdelicten ook andere belangen beschermen dan de rechtsbelangen die in paragraaf 2.1 werden beschreven.

3 Vermogensdelicten in een gedigitaliseerde samenleving

In deze paragraaf bespreek ik verschillende vermogensdelicten die in het Wetboek van Strafrecht zijn opgenomen en die zijn aangepast aan de gedigitaliseerde samenleving. Ik bespreek achtereenvolgens afpersing, afdreiging en oplichting en vernieling en beschadiging. Tevens bespreek ik enkele elders in het wetboek voorkomende delicten die in het kader van vermogenscriminaliteit worden gebruikt. Ik houd daarbij de door deze strafbepalingen te beschermen rechtsbelangen telkens tegen het licht. Daarnaast beantwoord ik de vraag of de belangen die door de vermogensdelicten worden beschermd ook bij digitale vermogensdelicten op de voorgrond staan.

3.1 Afpersing, afdreiging en oplichting

De Wet computercriminaliteit bracht wijziging in verschillende vermogensdelicten. Allereerst werd de delictsomschrijving van afpersing en afdreiging (art. 317 en 318 Sr) en van oplichting (art. 326 Sr) gewijzigd. Toegevoegd werd het bestanddeel: '[in art. 317 en 318 Sr: hetzij tot] het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer'.[26] De aanvulling werd wenselijk geacht, omdat sommige gegevens in het handelsverkeer een vermogens- of geldswaarde hebben en bij afgifte (door dwang of leugens) een aantasting van het vermogen van een ander oplevert.[27] De delictsomschrijving was beperkt tot gegevens die een geldswaarde hebben in het handelsverkeer.

Anders dan afpersing of afdreiging of oplichting van goederen, gaat het niet om het afgeven, maar om het ter beschikking stellen daarvan. Die terminologie is nodig, omdat gegevens volgens de wetgever slechts kunnen worden gekopieerd en niet uit de beschikkingsmacht van een ander kunnen worden gehaald (gegevens zijn immers *multiple*). Bij deze vermogensdelicten zijn twee situaties denkbaar:

1 het slachtoffer had als enige de beschikking over de gegevens en verliest door het ter beschikking stellen ervan aan een ander daarover het monopolie, waardoor zijn vermogen is aangetast, en
2 het slachtoffer bezit niet als enige de gegevens en zijn vermogen wordt door het wegnemen ervan niet aangetast. In het laatste geval gaat het erom dat het vermogen van de dader op onrechtmatige wijze vermeerdert.

Deze delicten beschermen dus niet alleen het vermogen van de eigenaar of bezitter van goed of gegevens. Ook de ongerechtvaardigde verrijking ligt aan deze strafbaarstellingen ten grondslag.

De zinsnede 'met geldswaarde in het handelsverkeer' leverde in de rechtspraktijk onder andere problemen op met betrekking tot het zogenoemde *phishing* (het 'listig aftroggelen van financiële gegevens'). Dat zou niet strafbaar zijn, omdat de door afgifte verkregen gegevens als zodanig geen geldswaarde in het handelsverkeer zouden hebben.[28] Inmiddels is de zinsnede geschrapt, eerst in artikel 317 Sr, later ook in artikel 318 en artikel 326 Sr.[29] Daardoor hoeft niet langer te worden bewezen of de gegevens een geldswaarde in het handelsverkeer hebben. De wetswijzigingen beoogden het bestrijden van betaalpas- en betaalkaartfraude te vereenvoudigen. Het belang om deze fraude te bestrijden wordt onder meer benadrukt in het EU-Kaderbesluit houdende bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten dat tot de wetswijzigingen leidde.[30] Dat kaderbesluit verwijst onder meer naar de bestrijding van georganiseerde criminaliteit. De Europese Commissie stelt voor het kaderbesluit te vervangen door een richtlijn.[31] Het kaderbesluit sluit volgens haar onvoldoende aan 'bij nieuwe uitdagingen en

26 Aan art. 317 Sr werd ook een tweede lid toegevoegd, waarin strafbaar wordt gesteld afpersing door dreiging met gegevensbeschadiging. De wet introduceerde ook een nieuwe strafbaarstelling, namelijk het listiglijk gebruik maken van een telecommunicatiedienst (art. 326c Sr). Bij de Eerste Kamer wordt, als onderdeel van het wetsvoorstel computercriminaliteit III, voorgesteld online handelsfraude, voor zover daarvan een beroep of gewoonte wordt gemaakt, strafbaar te stellen (*Kamerstukken II* 2016/17, 34372, A).

27 *Kamerstukken II* 1989/90, 21551, 3, p. 8; *Kamerstukken II* 1990/91, 21551, 6, p. 19; Franken e.a. 1987, p. 68.

28 Zie B.J. Koops & Th. de Roos, 'Materieel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu 2007, p. 53.

29 Wet van 21 april 2004, *Stb*. 2004, 180; Wet van 12 juni 2009, *Stb.* 2009, 245.

30 Kaderbesluit 2001/413/JBZ van de Raad van 28 mei 2001 betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, *PbEG* L 149; *Kamerstukken II* 2002/03, 29025, 3, p. 7-8.

31 Voorstel voor een Richtlijn van het Europees Parlement en de Raad betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten en ter vervanging van Kaderbesluit 2001/413/JBZ, COM(2017) 489 final (hierna: COM(2017) 489 final).

technologische ontwikkelingen, zoals virtuele valuta en mobiele betalingen'. Ze wijst erop dat grote sommen geld worden verdiend met fraude met betaalkaarten die steeds vaker online plaatsvindt.[32] Deze fraude bedreigt de 'veiligheid', in het bijzonder omdat daarmee georganiseerde misdaad en terrorisme worden gefinancierd. Tevens staat zij aan een veilige 'digitale eengemaakte markt' in de weg. De Commissie benoemt ook economische verliezen en verlies van consumentenvertrouwen in het gebruik van betaalkaarten, omdat consumenten zouden vrezen (financieel) te worden benadeeld door cybercriminaliteit.[33] Deze volgorde van belangen is niet verbazend, gelet op de rechtsgrondslag waarop het kaderbesluit en de nieuwe richtlijn rusten (art. 83 lid 1 van het Verdrag betreffende de Werking van de Europese Unie). Dat noemt het beschermen van het vermogen immers niet als grondslag voor geharmoniseerde strafbaarstellingen. Het betekent echter wel dat, voor zover het gaat om afpersing, afdreiging en oplichting met betrekking tot gegevens, andere belangen op de voorgrond staan dan de belangen die deze vermogensdelicten oorspronkelijk beoogden te beschermen.[34]

Voor zover het gaat om afpersing, afdreiging en oplichting met betrekking tot gegevens, staan andere belangen op de voorgrond dan de belangen die deze vermogensdelicten oorspronkelijk beoogden te beschermen

3.2 Vernieling en beschadiging

De Wet computercriminaliteit bracht ook verandering aan in Titel XXVII van het Tweede Boek. Er werden twee nieuwe strafbaarstellingen toegevoegd en één werd gewijzigd. De nieuwe bepalingen stellen strafbaar het opzettelijk of door schuld door middel van een geautomatiseerd werk opgeslagen, verwerkte of overgedragen gegevens veranderen, wissen, onbruikbaar of ontoegankelijk maken dan wel andere gegevens daaraan toevoegen. De wetgever wilde met deze nieuwe strafbaarstellingen 'overspanning van het begrip "goed"' voorkomen en 'aantasting van gegevens ongeacht de wijze waarop zij zijn vastgelegd' strafbaar stellen. De strekking van deze bepalingen is volgens de wetgever het beschermen van 'de integriteit van gegevens', 'ongeacht hun functie tegenover derden'.[35] De bepalingen verschillen van artikel 350 Sr. In artikel 350a en 350b Sr wordt, net als in artikel 351 en 351bis Sr, niet gesproken van gegevens die geheel of gedeeltelijk aan een ander toebehoren. Zij hebben dus niet de strekking de vermogensrechten van derden te beschermen.[36] Het belang dat wordt beschermd is volgens de wetgever het 'ongestoord gebruik van computergegevens tegen onbevoegde wijziging, verwijdering, enz. van die gegevens'.[37] Dat belang lijkt niet direct in verband te staan met het beschermen van schaarse goederen (lees: gegevens). Het realiseren van goede kapitaalsvorming lijkt wel te worden beoogd. De economie loopt immers schade op en functioneert minder goed wanneer gegevens worden beschadigd door al dan niet grootschalige cyberaanvallen.[38] Banken en bedrijven worden door deze strafbare feiten benadeeld, hetgeen tot schending van vertrouwen in die instellingen kan leiden waardoor zij zich tijd en moeite moeten getroosten in het herstellen van vertrouwen.[39]

Het valt op dat het beschadigen van de economie niet als eerste belang wordt genoemd in Europese regelgeving. Daarin staat voorop een veiliger informatiemaatschappij die bestand is tegen aanvallen van georganiseerde criminaliteit en die niet ten behoeve van terroristische activiteiten wordt gebruikt.[40] De artikelen 350a en 350b Sr lijken eerder verband te houden met artikel 351 en 351bis Sr, dan met artikel 350 Sr. In artikel 351 Sr is strafbaar gesteld het vernielen, beschadigen, enzovoorts van werken van openbaar nut of ten behoeve van de landsverdediging. Niet de bescherming van het vermogensrecht van een ander staat centraal, maar het algemeen belang dat wordt gediend wanneer deze werken of goederen niet worden vernield, beschadigd, enzovoorts. Een verschil met dit artikel is dat in artikel 350a en 350b Sr niet bewezen hoeft te worden dat het algemeen belang wordt geschonden wanneer computergegevens worden vernield of beschadigd. Het verschil met artikel 351 en 351bis Sr is verder geaccentueerd met de komst van artikel 350c en 350d Sr, dat beschadiging, enzovoort, van een geautomatiseerd werk of een werk voor telecommunicatie en enkele specifieke voorbereidingshandelingen met betrekking tot het beschadigen, enzovoort, daarvan strafbaar stelt. Deze strafbaarstellingen stonden oorspronkelijk in artikel 161sexies Sr, een strafbepaling uit Titel VII van het Tweede Boek.[41] Ze werden in 2015 verplaatst naar hun huidige plaats,

32 Zie J.J. Oerlemans e.a., *Cybercrime en witwassen. Bitcoins, online dienstverleners en andere witwasmethoden bij banking malware en ransomware*, Den Haag: Boom criminologie/WODC 2016.

33 COM(2017) 489 final.

34 Iets waarvoor de wetgever al beducht was tijdens de totstandkoming van de Wet computercriminaliteit. Zie *Kamerstukken II* 1990/91, 21551, 6, p. 19-20.

35 *Kamerstukken II* 1989/90, 21551, 3, p. 23-24; *Kamerstukken II* 1990/91, 21551, 6, p. 41. Stol en Strikwerda spreken van 'het beschermen van gegevens tegen manipulatie': W. Stol & L. Strikwerda, *Strafrechtspleging in een digitale samenleving*, Den Haag: Boom juridisch 2017, p. 126.

36 Uiteraard kan het vermogen wel worden aangetast door deze delicten, bijvoorbeeld wanneer het gebruik van een computer onmogelijk is gemaakt en kosten moeten worden gemaakt hem opnieuw te kunnen gebruiken. Zie over het betalen van losgeld na het plaatsen van malware: B.H.M. Custers, J.J. Oerlemans & R.L.D. Pool, 'Ransomware, cryptoware en het witwassen van losgeld in bitcoins', *Strafblad* 2016/2.

37 *Kamerstukken II* 1989/90, 21551, 3, p. 23.

38 Vgl. Richtlijn 2013/40/EU van het Europees parlement en de Raad van 12 augustus 2013 over aanvallen op informatiesystemen en ter vervanging van Kaderbesluit 2005/222/JBZ van de Raad, *PbEU*, L 218/8 (hierna Richtlijn 2013/40/EU).

39 Zie Rb. Rotterdam 26 oktober 2016, ECLI:NL:RBROT:2016:8263.

40 Kaderbesluit 2005/222/JBZ van de Raad van 24 februari 2005 over aanvallen op informatiesystemen, *PbEU* L 69/67; Richtlijn 2013/40/EU.

41 De strafbepalingen in Titel VII dienen ter bescherming van de gezondheid en levens van mensen, infrastructurele werken en (andere) voorzieningen (K. Lindenberg in: *T&C Sr*, Inleidende opmerkingen Titel VII van het Tweede Boek, aant. 1).

omdat een aantal onderdelen met de implementatie van de EU-richtlijn over aanvallen op informatiesystemen (2013/40/EU) uit de strafbepaling werd geschrapt, namelijk 'ten algemenen nutte' en 'openbare' voor geautomatiseerd werk en voor telecommunicatie. Volgens de wetgever lag de verplaatsing voor de hand, omdat de aangepaste strafbepalingen beter aansluiten bij artikel 350a en 350b Sr en artikel 351 en 351bis Sr.[42]

De verwijzing naar de laatste twee artikelen begrijp ik niet, omdat zij juist wel gaan over werken ten algemenen nutte. Wel zie ik een verband met artikel 350a en 350b Sr. De gevallen waarop deze artikelen betrekking hebben betreffen het ongestoord kunnen gebruiken van een geautomatiseerd werk of telecommunicatienetwerk. Het verwijderen van een verwijzing naar het algemeen nut of openbare karakter van het geautomatiseerd werk of telecommunicatienetwerk zou de indruk kunnen wekken dat het in de nieuwe bepalingen vooral gaat om voorzieningen waarvan individuen gebruik maken en waardoor in geval van vernieling of beschadiging individuen worden geraakt. Dan zou zijn te begrijpen waarom deze delicten zijn verplaatst. Het argument wordt in de wetsgeschiedenis echter niet gebruikt, vermoedelijk omdat bescherming van het vermogen van het individu in de artikelen 350a tot en met 350d Sr niet op de eerste plaats komt. Hoewel zij daadwerkelijke schade vereisen (in de vorm van vernieling, beschadiging, ontoegankelijk maken of onbruikbaar maken), lijkt het achterliggende rechtsbelang niet zozeer met die schade in verband te staan; centraal staat het veilige gebruik van informatiesystemen ten behoeve van onze gedigitaliseerde economie en samenleving.[43] Dat roept de vraag op of deze strafbaarstellingen vermogensdelicten zijn.

3.3 Witwassen met behulp van cryptogeld[44]

Witwassen is strafbaar gesteld in artikel 420bis e.v. Sr (Titel XXXA van het Tweede Boek). Zij behoren vanwege het beschermd belang tot de vermogensdelicten. Zij beschermen de integriteit van het niet-criminele financiële en economische verkeer tegen opbrengsten van misdrijven. Dat kunnen vermogensdelicten zijn, maar dat hoeft niet. Artikel 420bis Sr onderscheidt verschillende witwashandelingen, namelijk – kort gezegd – het verbergen of verhullen en het voorhanden hebben van voorwerpen waarvan de dader weet of redelijkerwijs moet vermoeden dat deze middellijk of onmiddellijk van misdrijf afkomstig zijn. Onder voorwerpen worden volgens artikel 420bis lid 2 Sr verstaan alle zaken en vermogensrechten. Gegevens worden niet beschouwd als voorwerpen.[45]

Gelet op het RuneScape-arrest zal het niet als een verrassing klinken dat bitcoins als voorwerpen worden beschouwd: zij vertegenwoordigen een reële waarde, zijn door inspanning en tijdsinvestering te verwerven en de bezitter heeft er de feitelijke en exclusieve heerschappij over

Dat roept vragen op wanneer criminele activiteiten gepaard gaan met het gebruik van zogeheten cryptogeld als bitcoins. Daarmee kunnen betalingen worden verricht, zonder dat deze zijn gefiatteerd of worden gecontroleerd door overheden. Bitcoins worden gebruikt bij criminele activiteiten. Custers, Oerlemans & Pool wijzen erop dat voor het ongedaan maken van malware op een computer soms met bitcoins moet worden betaald. Uit rechtspraak blijkt dat bitcoins worden gebruikt in het kader van hennephandel; verlangd wordt dan dat betalingen met bitcoins plaatsvinden.[46] Bitcoins zijn gegevens en we zagen dat gegevens buiten het bereik van voorwerpen vallen. Voorwerpen en goederen werden in het Wetboek van Strafrecht, in ieder geval voor zover het gaat om de vermogensdelicten, als synoniemen gebruikt.[47] In de Wet computercriminaliteit wordt de term voorwerp gelijkgesteld met een stoffelijke zaak.[48] Dat zou betekenen dat goed en voorwerp geen synoniemen meer zijn. De literatuur en rechtspraak hebben dit standpunt van de wetgever genegeerd. De rechtspraak over goed wordt namelijk gebruikt om te bepalen of bitcoins voorwerpen zijn.[49] Gelet op het RuneScape-arrest zal het dan niet als een verrassing klinken dat bitcoins als voorwerpen worden beschouwd: zij vertegenwoordigen een reële waarde, zijn door inspanning en tijdsinvestering verworven of te verwerven en de bezitter heeft er – gelet op de opslag van bitcoins op een met een privécode versleutelde portemonnee (*bitcoinwallet*) – de feitelijke en exclusieve heerschappij over.[50] Wanneer vervolgens de herkomst wordt verhuld (wat mogelijk is met behulp van een zogenoemde bitcoinmixer) of verborgen, kan er van witwassen sprake zijn. Hetzelfde geldt wanneer iemand bitcoins alleen voorhanden heeft.[51]

42 *Kamerstukken II* 2014/15, 34034, 3, p. 6.
43 Vgl. Koops & De Roos 2007, p. 42; Koops 2013.
44 Zie J.J. Oerlemans, 'Veroordelingen voor online drugshandel en witwassen', *Computerrecht* 2018/37 voor enkele relevante recente rechterlijke uitspraken.
45 V. Mul, in: *T&C Sr*, aant. 9a bij art. 420bis.
46 Custers, Oerlemans & Pool 2016; R.J. de Jong, 'Bitcoinminers, bitcoincashers, bitcoinmixers en het strafrecht', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, p. 14; Oerlemans 2018.
47 Zie Smidt 1891, p. 487, 536-537.
48 *Kamerstukken II* 1989/90, 21551, 3, p. 8.
49 Zie naast de door Oerlemans (2018) genoemde rechtspraak, bijvoorbeeld ook Rb. Midden-Nederland 3 april 2018, ECLI:NL:RBMNE:2018:1191.
50 Zie De Jong 2017, p. 13.
51 In dat geval hangt het van bijkomende gedragingen af of sprake is van witwassen of eenvoudig witwassen (art. 420bis.1 Sr). Voor eenvoudig witwassen zijn geen handelingen vereist die zijn gericht op het verbergen of verhullen van de voorwerpen die iemand voorhanden heeft. Dat is bij witwassen wel het geval. Zie Rb. Amsterdam 13 maart 2018, ECLI:NL:RBAMS:2018:1738.

Het verbergen of verhullen/voorhanden hebben van bitcoins kan dus strafbaar witwassen opleveren. De vraag is wat die conclusie zegt over de te beschermen rechtsbelangen. Witwassen strekt volgens vaste rechtspraak van de Hoge Raad 'ter bescherming van de aantasting van de integriteit van het financieel en economisch verkeer en van de openbare orde'.[52] Het eerste rechtsbelang houdt verband met goede kapitaalsvorming, een belang waarin ook het tegengaan van ongerechtvaardigde verrijking wordt gelezen. Met financieel en economisch verkeer wordt het reguliere verkeer bedoeld, zodat het betalen met en de handel in bitcoins (die net als ander cryptogeld juridisch nauwelijks een status hebben) daarbuiten vallen, tenzij met witwassen ook de bescherming van het irreguliere financieel en economisch verkeer wordt beoogd. In dat geval zou met de strafbaarstelling van witwassen ook het criminele financieel en economische verkeer worden beschermd. Dat zal niet de bedoeling zijn.

Welk rechtsbelang wordt dan beschermd? Met cryptogeld kunnen grote sommen geld worden verdiend. Wanneer dat is verkregen ten gevolge van strafbaar handelen, is sprake van ongerechtvaardigde verrijking. Dit is een onderdeel van het belang van goede kapitaalsvorming. Ook dit belang houdt verband met de door de Hoge Raad geformuleerde strekking van witwassen. Beide belangen zijn echter niet helemaal identiek. Met de strafbaarstelling van witwassen kunnen dus kennelijk ook andere dan de door de Hoge Raad genoemde belangen zijn gemoeid, namelijk het voorkomen dat mensen wegkomen met criminele opbrengsten. Dat rechtsbelang sluit aan bij de opvatting van de wetgever over witwassen.[53] De door de Hoge Raad geformuleerde strekking van de witwasbepalingen is met andere woorden niet (langer) volledig.

3.4 Valsheidsdelicten

Hoewel zelf geen vermogensdelicten, vinden we in de valsheidsmisdrijven strafbaarstellingen die met vermogensdelicten een band kunnen hebben.[54] Vermogensdelicten worden onder andere begaan met behulp van valse of vervalste betaalpassen. Wanneer een betaalpas wordt vervalst met het oogmerk om zichzelf of een ander te bevoordelen, is dat strafbaar (art. 232 Sr).[55] Bevoordeling hoeft nog niet te hebben plaatsgevonden, zodat niet kan worden gezegd dat we hier te maken hebben met een vermogensdelict. Het misdrijf van artikel 232 Sr gaat daaraan vooraf, omdat met behulp van valse betaalpassen onder andere diefstal mogelijk is.[56]

Artikel 232 Sr werd ingevoegd met de Wet computercriminaliteit. Nadien is het Wetboek van Strafrecht nader aangevuld, mede vanwege Europese regelgeving. Het EU-Kaderbesluit betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten voorziet in strafbaarstelling van het namaken van betaalinstrumenten (art. 2).[57] De Nederlandse wetgever koos ervoor dit feit strafbaar te stellen in artikel 226 lid 1, onderdeel 5° Sr dat strafbaar stelt valsheid in geschrifte indien zij is gepleegd in krediet- en handelspapier. Daaronder worden verstaan reischeques, betaalcheques en andere cheques en wissels.[58]

Het kaderbesluit leidde tevens tot uitbreiding van artikel 234 Sr, dat oorspronkelijk strafbaar stelde het voorhanden hebben van stoffen of voorwerpen waarvan hij weet dat deze bestemd zijn tot het plegen van het misdrijf van artikel 226, lid 1, onderdeel 2-5° Sr. Als gevolg van de implementatie van het EU-Kaderbesluit werd artikel 234 Sr gewijzigd, zodat nu strafbaar is het voorhanden, enzovoort, hebben van computerprogramma's waarvan hij weet dat deze zijn bestemd tot het namaken of vervalsen van (onder andere) betaal- of reischeques. Artikel 234 Sr verwijst sinds 2004 ook naar artikel 232 Sr. Indien we artikel 232 Sr (en art. 226, onderdeel 5° Sr) beschouwen als misdrijf waarmee een vermogensdelict kan worden voorbereid, dan omschrijft artikel 234 Sr dus een feit waarin voorbereiding van voorbereiding van een vermogensdelict wordt strafbaar gesteld.

Eerder in deze bijdrage merkte ik op dat de Europese Commissie het kaderbesluit wil vervangen door een richtlijn. Het concept daarvan behelst onder meer een uitbreiding van het begrip betaalmiddelen, zodat daaronder ook vallen 'digitale betaalmiddelen' en 'virtuele valuta' (art. 2, onder e). Tevens wordt voorgesteld strafbaarstelling van het frauduleus gebruik maken van gestolen of anderszins wederrechtelijk toegeëigende betaalinstrumenten of het frauduleus gebruikmaken van een nagemaakt of vervalst betaalinstrument. Ook bevat het concept een voorstel tot strafbaarstelling van het zich wederrechtelijk toe-eigenen van een betaalinstrument, het namaken of vervalsen ervan en het beschikbaar maken met het oogmerk het frauduleus te gebruiken (art. 3 en 4). Een betaalinstrument omvat ook een 'beveiligde registratie, […], waarmee de houder of gebruiker, al dan niet met behulp van een procedure of geheel van procedures, geld of geldelijke waarde kan overmaken of een betaalopdracht kan initië-

52 HR 17 december 2013, *NJ* 2014/75, m.nt. M.J. Borgers.

53 *Kamerstukken II* 2015/16, 34294, 3, p. 1.

54 Koops & De Roos 2007, p. 48-50; Franken e.a. 1987, p. 68-69. De valsheidsdelicten staan in Titel X en XI.

55 De strafbaarstelling kan worden gebruikt in de strijd tegen het zogenoemde skimmen (het wederrechtelijk verkrijgen en kopiëren van betaalgegevens). Zie Rb. Haarlem 3 november 2010, ECLI:NL:RBHAA:2010:BO2789.

56 Zie over wat in de rechtspraak onder betaalpassen wordt verstaan o.a. Koops & De Roos 2007, p. 51.

57 Kaderbesluit 2001/413/JBZ van de Raad van 28 mei 2001 betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, *PbEG* L 149.

58 *Kamerstukken II* 2002/03, 29025, 3, p. 4.

ren, met inbegrip van digitale betaalmiddelen' (art. 2, onder a). Met deze omschrijving moet ook fraude met contactloos pinnen strafbaar worden gesteld. In het geval de richtlijn wordt aangenomen, zal de Nederlandse wetgever een aantal strafbaarstellingen moeten aanpassen, waaronder artikel 226, onderdeel 5° Sr.

3.5 Heling en verduistering van gegevens

Anders dan afpersing, afdreiging en oplichting werden de strafbaarstelling van verduistering (art. 321 Sr) en heling (art. 416 e.v. Sr) in de Wet computercriminaliteit met rust gelaten. Wel zijn met die wet bijzondere helingsbepalingen ingevoerd, namelijk heling van staatsgeheimen (art. 98 e.v. Sr) en van bedrijfsgegevens (art. 273 lid 1, onder 2° Sr). Deze strafbepalingen zijn geen vermogensdelicten.

Heling van gegevens

Een met betrekking tot heling van gegevens relevante bepaling is artikel 139e Sr. Daarin is onder meer strafbaar gesteld het aan een ander bekendmaken van gegevens die hij door wederrechtelijk aftappen heeft verkregen. Deze bepaling is niet bruikbaar in het geval gegevens worden bekendgemaakt door een persoon die deze gegevens niet zelf heeft afgetapt. Artikel 139e Sr stelt ook strafbaar het aan een ander ter beschikking stellen van een voorwerp waarop gegevens zijn vastgelegd die door wederrechtelijk aftappen zijn verkregen. Artikel 139e Sr maakt deel uit van Titel V van het Tweede Boek en is een misdrijf tegen de openbare orde. Het belang dat door deze bepaling wordt beschermd is het privéleven tegen bedreigingen in verband met moderne afluister- en opnameapparatuur.[59] Hoewel deze bepaling oorspronkelijk is bedoeld om het voorhanden hebben of gebruiken van afgeluisterde gesprekken tegen te gaan, is het bereik ruimer, omdat het ook gaat om ander gegevensverkeer. De bepaling is dan ook bruikbaar om het voorhanden hebben of ter beschikking stellen van bij een andere persoon afgetapte gegevens met betrekking tot betalingsverkeer te sanctioneren. Zij is dus relevant in verband met de bestrijding van digitale vermogenscriminaliteit.[60]

In het wetsvoorstel computercriminaliteit III wordt gesignaleerd dat de bestaande wettelijke regeling met betrekking tot heling van gegevens lacunes vertoont. Zo wordt opgemerkt dat heling van gegevens niet strafbaar is 'in situaties waarin niet aangetoond kan worden dat de persoon die deze gegevens bekendmaakt degene is die deze gegevens zelf heeft overgenomen'.[61] Dat is vooral problematisch wanneer het niet-openbare gegevens betreft, bijvoorbeeld naaktfoto's[62] of betaalgegevens. Er is overwogen om het wederrechtelijk overnemen van niet-openbare gegevens en het voorhanden hebben of bekendmaken van door misdrijf verkregen gegevens strafbaar te stellen als diefstal (art. 310 Sr), verduistering (art. 321 Sr) of (schuld)heling (art. 416 e.v. Sr). Daartoe is niet besloten, omdat dat zou neerkomen op het gelijkstellen van gegevens met goederen. Dat zou leiden tot een doorbreking van de systematiek die sedert de Wet computercriminaliteit bestaat (goederen zijn geen gegevens) hetgeen onwenselijk wordt geacht. Het strafbaar stellen van diefstal of verduistering van gegevens is 'een minder geschikte oplossing als de gegevens zijn gekopieerd en de rechthebbende de beschikkingsmacht dus niet heeft verloren'.[63] Wat de samensteller van de Memorie van Toelichting hier naar ik aanneem bedoelt te zeggen is dat het opnemen van gegevens als bestanddeel in artikel 310 en 321 Sr minder gelukkig is. We zullen zodadelijk zien dat in het wetsvoorstel computercriminaliteit III wordt voorzien in strafbaarstelling van verduistering van gegevens.

In het wetsvoorstel computercriminaliteit III wordt gesignaleerd dat de bestaande wettelijke regeling met betrekking tot heling van gegevens lacunes vertoont

Ook de huidige strafbaarstelling van heling van gegevens is minder ruim geformuleerd dan de strafbaarstelling van heling van een goed. Vereist is ofwel het aan een ander bekendmaken van zelf afgetapte gegevens, of het aan een ander ter beschikking stellen van een voorwerp waarop gegevens zijn vastgelegd. Het ter beschikking stellen of voorhanden hebben van gegevens die niet door eigen misdrijf zijn verkregen is strafbaar op grond van artikel 139e Sr, noch op grond van artikel 416 e.v. Sr.[64] De wetgever is hier niet gelukkig mee en introduceert daarom een nieuwe strafbepaling (art. 139g Sr) waarin strafbaar wordt gesteld het verwerven of voorhanden hebben van gegevens, 'terwijl hij ten tijde van de verwerving of het voorhanden krijgen van deze gegevens wist of redelijkerwijs had moeten vermoeden dat deze door misdrijf zijn verkregen' alsmede het ter beschikking van een ander stellen, aan een ander bekendmaken of uit winstbejag voorhanden hebben

59 J.M. ten Voorde, in: *T&C Sr*, aant. 5 bij art. 139e.
60 Zie Rb. Rotterdam 14 april 2010, ECLI:NL:RBROT:2010:BM1172.
61 *Kamerstukken II* 2015/16, 34372, 3, p. 61-62.
62 Zie J.J. Oerlemans, 'De Wet computercriminaliteit III: meer handhaving op internet', *Strafblad* 2017, p. 351.
63 *Kamerstukken II* 2015/16, 34372, 3, p. 65.
64 Zie voor dat laatste HR 10 oktober 2017, *NJ* 2018/19, m.nt. N. Rozemond. Deze zaak betrof de verspreiding via sociale media van gefotografeerde eindexamens die waren gestolen bij de middelbare school Ibn Ghaldoun.

of gebruiken van gegevens, 'terwijl hij weet of redelijkerwijs moet vermoeden dat het door misdrijf verkregen gegevens betreft'. Deze strafbepaling wordt als misdrijf tegen de openbare orde in het wetboek opgenomen. Deze strafbepaling beschermt meerdere belangen: de openbare orde, de privacy en het vermogen van personen.[65]

Verduistering van gegevens

Hiervoor gaf ik aan dat niet zonder meer duidelijk is of verduistering van gegevens strafbaar is gesteld. De hiervoor besproken conceptrichtlijn betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten eist ook strafbaarstelling van het zich wederrechtelijk toe-eigenen van een betaalinstrument. Gelet op de ruime omschrijving van betaalinstrument zou dat ook kunnen neerkomen op het moeten strafbaar stellen van verduistering van gegevens. In het wetsvoorstel computercriminaliteit III wordt in strafbaarstelling van verduistering van gegevens voorzien. In het nieuwe artikel 138c Sr wordt strafbaar gesteld het opzettelijk en wederrechtelijk voor zichzelf of een ander overnemen van niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk.[66] De delictsomschrijving is tamelijk ruim; zo wordt bijvoorbeeld geen opzet op de wederrechtelijkheid geëist. Ook de strafmaxima lopen uiteen: drie jaar gevangenisstraf voor verduistering, één jaar voor overtreding van artikel 138c Sr.[67] Dat roept vragen op bij grensgevallen, dat wil zeggen situaties waarin zowel sprake kan zijn van goed als gegevens. Dat brengt me terug bij het RuneScape-arrest.

3.6 Op en over de grens van goed en gegevens

In paragraaf 2.2 besprak ik het RuneScape-arrest niet volledig. Een belangrijke rechtsoverweging liet ik achterwege. Deze overweging (3.6.2) gaat over grensgevallen tussen goed en gegevens en luidt als volgt:

'de enkele omstandigheid dat een object ook de eigenschappen heeft van gegevens in de zin van art. 80quinquies Sr brengt niet mee dat dit object reeds daarom niet meer als goed in de zin van art. 310 Sr kan worden aangemerkt. Opmerking verdient daarbij dat zich gemakkelijk grensgevallen kunnen voordoen, waarbij de desbetreffende niet-stoffelijke zaken zowel kenmerken van een goed als van gegevens vertonen. In een dergelijk geval is de kwalificatie sterk afhankelijk van de omstandigheden van het geval en de waardering daarvan door de rechter.'[68]

De overweging is bijzonder. De wetgever maakt immers weluitdrukkelijk onderscheid tussen goed en gegevens. Volgens Koops heeft dat tot een wetssystematiek geleid waarbij een handeling ten aanzien van hetzelfde object bijvoorbeeld 'niet tegelijkertijd zaaksbeschadiging en gegevensbeschadiging' kan zijn. En zelfs al vormt de grens tussen goed en gegevens een grijs gebied, aangenomen moet worden dat gegevens zich niet helemaal hetzelfde 'gedragen' als goederen. Het wegnemen van gegevens bestaat uit het kopiëren en vervolgens vernietigen van de oorspronkelijke bron. Dat is niet hetzelfde als het wegnemen van een goed, aldus nog steeds Koops.[69]

De vermenging tussen goed en gegevens in het geval van artikel 310 Sr kan vanuit rechtstheoretisch perspectief worden gebillijkt, omdat er geen verandering optreedt in de bescherming van de door artikel 310 Sr beschermde belangen

Koops' kanttekeningen zijn tamelijk algemeen geformuleerd, terwijl de Hoge Raad expliciet naar artikel 310 Sr verwijst. Dat laatste ligt gelet op het cassatieberoep voor de hand, tegelijkertijd is het door die expliciete verwijzing naar artikel 310 Sr niet zonder meer evident dat de Hoge Raad deze overweging ook voor andere strafbepalingen toepasselijk acht. De achtergrond van de overweging is volgens mij dat de Hoge Raad wil voorkomen dat een grijs gebied ontstaat tussen goed en gegevens waarop geen enkele strafbepaling van toepassing is. Dat is vooral relevant voor strafbepalingen waar goed en gegevens allebei deel uitmaken van de delictsomschrijving (zoals art. 317 Sr), maar ook wanneer een zusterbepaling naast het oorspronkelijke (vermogens)delict bestaat, zoals artikel 350a na artikel 350 Sr. Het argument gaat niet op bij artikel 310 Sr. Niet alleen ontbreekt het bestanddeel 'gegevens' in artikel 310 Sr, ook kan geen overduidelijke zusterbepaling worden aangegeven (het dichtst in de buurt komt wellicht artikel 139c Sr dat het aftappen van gegevens strafbaar stelt). Komt de overweging van de Hoge Raad dan neer op een verruiming van de reikwijdte van artikel 310 Sr, die de wetgever niet voor ogen had en, zoals we in de vorige subparagraaf zagen, nog steeds niet wenselijk acht? Ik meen van niet; we hebben hier namelijk te maken met gegevens met de bijzondere eigenschap dat zij ook als goed kunnen worden beschouwd. Dat betekent geen volledige vermenging van

65 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 81.
66 Zie *Kamerstukken II* 2015/16, 34372, 3, p. 64.
67 Overigens zien we dat ook bij heling van goederen en van gegevens: vier jaar gevangenisstraf bij opzetheling (art. 416 Sr) of één jaar bij schuldheling (art. 417bis Sr), respectievelijk één jaar bij heling van gegevens (art. 139g Sr). Het strafmaximum in art. 139g Sr laat zich goed verklaren (zie de strafmaxima in art. 138ab tot en met art. 139f Sr), maar het verschil ten opzichte van de 'gewone' vermogensdelicten is niettemin opvallend.
68 HR 31 januari 2012, *NJ* 2012/536, m.nt. N. Keijzer.
69 Koops 2013, par. 5.

goed en gegevens, omdat er ook gegevens zijn die niet kunnen worden beschouwd als een goed.[70]

De vermenging tussen goed en gegevens in het geval van artikel 310 Sr kan ook worden gebillijkt, omdat er geen verandering optreedt in de bescherming van de door artikel 310 Sr beschermde belangen. Artikel 310 Sr beschermt, gelet op de door de Hoge Raad geformuleerde argumenten, ook na het RuneScape-arrest het vermogen (ook al is dat virtueel) van een ander.

Bij andere vermogensdelicten, zoals artikel 317 en 326 en artikel 350a e.v. Sr, is de overweging van de Hoge Raad weliswaar verklaarbaar, maar minder vanzelfsprekend. Dat goed en gegevens in één delictsomschrijving staan, heeft bij de genoemde vermogensdelicten ertoe geleid dat de door die delicten beschermde belangen diffuus zijn geworden. Nog wat scherper gesteld staat bescherming van het vermogen bij het ter beschikking stellen of beschadigen van gegevens niet voorop. Strafbaarstellingen van aanvallen op gegevens strekken tot bescherming van de privacy, de openbare orde of de integriteit van informatiesystemen. De bescherming van het vermogen komt op de tweede plaats en moet met die andere belangen concurreren, ook indien de delicten gelet op hun plaats in het Wetboek van Strafrecht tot de vermogensdelicten worden gerekend. Heeft deze concurrentie gevolgen voor de interpretatie van een delict? Moet afpersing van gegevens anders worden uitgelegd dan afpersing van een goed, omdat met afpersing van gegevens ook andere belangen zijn gemoeid? Kan dat eigenlijk wel in dezelfde strafbaarstelling? En hoever mag die afwijking dan gaan? Zou het voor de interpretatie van de nieuwe strafbaarstelling heling van gegevens (art. 139g Sr) uitmaken wanneer het vermogen is aangetast? Zowel een positief als een negatief antwoord op deze vraag roept nieuwe vragen op, bijvoorbeeld naar de relatie tussen de door de vermogensdelicten beschermde belangen en de openbare orde of integriteit van informatiesystemen. Wanneer de rechtsbelangen die door de vermogensdelicten worden beschermd irrelevant zijn voor de uitleg van een strafbaarstelling als heling van gegevens, wordt de houdbaarheid van strafbaarstellingen waaraan de bescherming van meerdere belangen ten grondslag liggen een punt van zorg en aandacht. Deze vragen zijn ook voor de rechtspraktijk relevant. 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? Met een vervaagde grens tussen goed en gegevens lijkt mij dat moeilijk uit te leggen. Het RuneScape-arrest lijkt al met al implicaties te hebben voor de plaats en betekenis van digitale vermogensdelicten in het Wetboek van Strafrecht.

Het RuneScape-arrest lijkt implicaties te hebben voor de plaats en betekenis van digitale vermogensdelicten in het Wetboek van Strafrecht

4 Conclusie

Aan het begin van deze bijdrage stelde ik de vraag met behulp van welke strafbaarstellingen in het Wetboek van Strafrecht digitale vermogenscriminaliteit kan worden bestraft en welke belangen daarmee worden beschermd. Tot de vermogensdelicten reken ik de strafbepalingen in Titel XXI tot en met XVII en XXX en XXXA. De belangen die met deze titels worden beschermd houden verband met het vermogen. We zagen dat er niet één belang is, maar een pluriformiteit van belangen die zich laten onderscheiden tussen individuele en collectieve belangen. Vanouds beschermen de vermogensdelicten eigendom of bezit van een persoon. Daar zijn naar verloop van tijd andere belangen bij gekomen, waaronder een open economie die draait op eerlijke concurrentie, alsmede het belang dat ongerechtvaardigde verrijking moet worden bestreden. Deze belangen hebben tot nieuwe vermogensdelicten geleid. Tevens is de reikwijdte van bestaande vermogensdelicten veranderd, mede doordat het individuele rechtsbelang een ruimere betekenis heeft gekregen.

De komst van computercriminaliteit heeft tot nieuwe vermogenscriminaliteit geleid, namelijk die betrekking heeft op gegevens. Gegevens worden van goederen onderscheiden; zij zijn – net als goederen – van groot belang voor (rechts)personen en voor de samenleving en economie als geheel. Het maken van inbreuk op gegevens rechtvaardigt strafbaarstelling. De wetgever heeft ervoor gekozen strafbaarstelling deels te incorporeren in bestaande strafbaarstellingen, deels werden nieuwe strafbaarstellingen ingevoerd.

70 HR 3 december 1996, *NJ* 1997/574, m.nt. A.C. 't Hart. Vgl. N. Keijzer onder HR 31 januari 2012, *NJ* 2012/536.

Het incorporeren van gegevens in bestaande strafbaarstellingen heeft tot differentiatie van het door de strafbaarstelling beschermde rechtsbelang geleid. Ik observeerde dit ten aanzien van oplichting en afpersing en afdreiging. Ook bij witwassen van gegevens die volgens rechtspraak ook voorwerpen zijn (cryptogeld zoals bitcoins) is de vraag of daarmee hetzelfde rechtsbelang wordt beschermd als bij witwassen van andere voorwerpen.

Het incorporeren van gegevens in bestaande strafbaarstellingen heeft tot differentiatie van het door de strafbaarstelling beschermde rechtsbelang geleid

Nieuwe strafbaarstellingen die werden ingevoerd in een titel die vanouds tot de vermogensdelicten wordt gerekend (Titel XXVII), lijken de door de vermogensdelicten te beschermen rechtsbelangen niet op de voorgrond te stellen. Artikel 350a tot en met 350d Sr beogen andere belangen te beschermen die dicht tegen de door Titel VII van het Tweede Boek beschermde rechtsbelangen aan liggen. Strafbaarstellingen die ook belangen beogen te beschermen die de vermogensdelicten beschermen vinden we verspreid over het wetboek. Ik besprak op enkele valsheidsdelicten en misdrijven tegen de openbare orde. Het voorstel om heling en verduistering van gegevens als misdrijf tegen de openbare orde in het wetboek op te nemen lijkt door het gebruik van termen als heling en verduistering vreemd (horen dergelijke delicten niet thuis in respectievelijk Titel XXX en Titel XXIV?), maar dat heeft eerder te maken met de gebruikte termen (heling en verduistering) dan met de delicten zelf. Deze delicten beogen *ook* belangen te beschermen die door de vermogensdelicten worden beschermd; zij beogen primair de privacy (en daarmee de openbare orde) te beschermen.

Dat deze delicten meerdere, om het zo te noemen, 'heren dienen' roept de vraag op of zij dat op adequate wijze kunnen, zonder dat binnen een delict te veel (of niet genoeg) verschillen in interpretatie ontstaan. Een andere, daarmee samenhangende vraag is of het beschermen van meerdere rechtsbelangen ten goede komt aan de duidelijkheid van strafbaarstellingen, ook bezien in onderlinge samenhang met andere strafbaarstellingen. Waarom is afpersing van goed en gegevens wel in één delict opgenomen (en worden zij met hetzelfde strafmaximum bedreigd) en moeten we voor verduistering van gegevens naar een andere strafbaarstelling in een andere titel en is het strafmaximum lager dan in artikel 321 Sr? Deze verschillen kunnen natuurlijk van een verklaring worden voorzien. Of daarmee de aanpak van digitale vermogenscriminaliteit is geholpen kan worden betwijfeld. Of deze methodiek de houdbaarheid van het Wetboek van Strafrecht verlengt, valt te bezien.