Hack van de Dam?

Bijlagen

Een onderzoek naar aandachtspunten die in een toekomstig verweer met betrekking tot de nieuwe strafbaarstelling van online handelsfraude en/of de nieuwe opsporingsbevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk kunnen worden toegepast

Student:	Angela van der Linden
Studentnummer:	2063642
Opleiding:	Juridisch Hogeschool Avans-Fontys te ’s-Hertogenbosch
Eerste afstudeerdocent:	dhr. mr. B. Kratsborn
Tweede afstudeerdocent:	mw. mr. S. Adjiembaks
Opdrachtgever:	Aarts & Nijenhuis Advocaten te Nijmegen
Afstudeermentor:	mw. mr. M. Lamers
Afstudeerperiode:	februari 2017 – mei 2017
Plaats en datum:	Nijmegen, 29 mei 2017

Bijlagen

Student:	Angela van der Linden
Studentnummer:	2063642
Opleiding:	Juridisch Hogeschool Avans-Fontys te ’s-Hertogenbosch
Eerste afstudeerdocent:	dhr. mr. B. Kratsborn
Tweede afstudeerdocent:	mw. mr. S. Adjiembaks
Opdrachtgever:	Aarts & Nijenhuis Advocaten te Nijmegen
Afstudeermentor:	mw. mr. M. Lamers
Afstudeerperiode:	februari 2017 – mei 2017
Plaats en datum:	Nijmegen, 29 mei 2017

INHOUDSOPGAVE

BIJLAGE 1 VERANTWOORDING

In deze bijlage is een uitgebreide verantwoording opgenomen, zodat de gebruikte bronnen en methoden zo goed mogelijk verantwoord worden. Om te beginnen wordt de algemene verantwoording per hoofdstuk gegeven. Daarna komt de manier waarop de jurisprudentie is geraadpleegd, aan bod. Tot slot worden enkele keuzes die zijn gemaakt, toegelicht.

Algemene verantwoording

Voor de beantwoording van de centrale vraag zijn meerdere bronnen geraadpleegd. Voor hoofdstuk 2 is informatie geraadpleegd uit literaire boeken, tijdschriftartikelen, de MvT en aanverwante kamerstukken betreffende het wetsvoorstel Computercriminaliteit III. De boeken zijn geschreven door professoren en experts op het gebied van computercriminaliteit. Dit geldt ook voor de artikelen. Deze gerenommeerde handboeken worden beschouwd als gezaghebbende bronnen waarvan het gezag algemeen gedeeld wordt.[1] De informatie uit hoofdstuk 3 is vooral afkomstig uit jurisprudentie, de MvT, de wet, Tekst & Commentaar en afgenomen interviews. Voor dit hoofdstuk zijn meer dan honderd uitspraken en arresten van rechtbanken, gerechtshoven en de Hoge Raad geanalyseerd. Het gebruik van jurisprudentie is vanzelfsprekend verantwoord. De interviews zijn afgenomen bij een parketsecretaris en een raadsheer van het gerechtshof. Zij zijn beide experts op het gebied van computercriminaliteit en hebben een wezenlijke bijdrage kunnen leveren aan dit onderzoek. Tot slot zijn de wet en de MvT aan te merken als bronnen waarvan het gezag algemeen gedeeld wordt.[2] Voor hoofdstuk 4 zijn de MvT, de wet, Tekst & Commentaar, tijdschriftartikelen en interviews geraadpleegd. Deze interviews zijn zelf afgenomen. Dit zijn dezelfde interviews die ook in hoofdstuk 3 genoemd worden. De interviews zijn als bijlagen toegevoegd. In de bijlagen zijn de interviews zo letterlijk mogelijk uitgewerkt. Deze uitwerking is tot stand gekomen door de interviews op te nemen en daarna zo letterlijk mogelijk uit te werken. In sommige gevallen is de zinsopbouw veranderd, zodat de interviews prettiger te lezen zijn. Er is gekozen voor deze letterlijke weergave, omdat op die manier de validiteit het beste bewaard blijft. Niet alle informatie die verteld is, wordt namelijk opgenomen in dit onderzoeksrapport. Aan de hand van de bijlagen kan de lezer precies nalezen wat tijdens het interview besproken is. De tijdschriftartikelen zijn geschreven door experts op het gebied van computercriminaliteit. Daarom is het gebruik van deze artikelen verantwoord. Tekst & Commentaar is geschreven door experts en professoren. Daarnaast zijn in het gehele onderzoek enkele websites geraadpleegd. De informatie op deze websites worden door professionals gegeven. Daarom kunnen deze sites als betrouwbaar worden aangemerkt. Concluderend kan gesteld worden dat alle geraadpleegde bronnen valide, betrouwbaar en verantwoord zijn.

Interviews

In de meeste scripties worden de interviews over het gehele onderzoeksrapport in de hoofdtekst verwerkt. In dit onderzoeksrapport is in hoofdstuk 3 en hoofdstuk 4 een aparte paragraaf besteed aan de interviews. Hier is voor gekozen, omdat uit de interviews informatie naar voren kwam die niet in de rest van het onderzoeksrapport behandeld is. Omdat deze informatie te belangrijk is om weg te laten, is daarom bewust gekozen de interviews in een aparte paragraaf uit te werken. Op die manier kan alle relevante informatie behandeld worden. De volledig uitgewerkte interviews zijn in bijlage 6 en bijlage 7 opgenomen. Deze interviews zijn een exacte weergave van het gesprek. Daarom is de formulering van sommige zinnen niet perfect. Daarnaast worden in sommige zinnen spreektaal of spreekwoorden gebruikt.

[1] Van Schaaijk 2011, p. 36.
[2] Van Schaaijk 2011, p. 36.

Verantwoording jurisprudentie-analyses

Internetoplichting

Op www.rechtspraak.nl is gezocht naar jurisprudentie met betrekking tot online handelsfraude. In eerste instantie is gezocht naar de term ‘internetoplichting’. Hieruit kwamen 46 bruikbare resultaten naar voren. Daarna is op de term ‘internetfraude’ gezocht. Van deze resultaten zijn zes zaken geanalyseerd. De zaken die resulteerde uit bovengenoemde twee zoektermen zijn uitgebreider geanalyseerd. Om een zo compleet mogelijk beeld te krijgen van het aantal vrijspraken, bewezenverklaringen en aantal slachtoffers is tevens gezocht op de term ‘Marktplaats + oplichting’.

Op deze manier is geprobeerd alle zaken betreffende online handelsfraude te analyseren. Het gaat natuurlijk alleen om zaken die gepubliceerd zijn op www.rechtspraak.nl. Niet alle zaken die door de rechtbank of het gerechtshof worden behandeld met betrekking tot online handelsfraude zijn op de website geplaatst.

Flessentrekkerij

In eerste instantie is alleen op de zoekterm ‘flessentrekkerij’ gezocht. Hieruit kwamen 249 resultaten. Om het aantal resultaten te verkleinen, zijn de uitspraken en arresten in de periode van 2013 tot en met 2017 geraadpleegd. Alleen de uitspraken en arresten waarin informatie met betrekking tot ‘een gewoonte of beroep maken’ naar voren kwam, zijn gebruikt voor de analyse. In bijlage 4 staan deze uitspraken en arresten in de tweede en derde tabel.

Daarna is gezocht op de zoekterm ‘flessentrekkerij + vrijspraak’. Hier kwamen 123 resultaten uit. In eerste instantie zijn alleen de uitspraken en arresten geraadpleegd waaruit een vrijspraak volgde. Naderhand zijn ook nog zaken geraadpleegd waarin een verweer van de verdachte is opgenomen. Deze resultaten zijn te vinden in de eerste tabel van bijlage 4.

Bijlage 4

In bijlage 4 zijn drie tabellen te vinden. In de eerste tabel zijn uitspraken en arresten opgenomen van de rechtbank en het gerechtshof. Deze uitspraken en arresten zijn naar voren gekomen uit de zoekopdracht ‘flessentrekkerij + vrijspraak’. In deze tabel staat de betreffende uitspraak of het betreffende arrest genoemd, de inhoud van het verweer van de verdediging en of een vrijspraak of bewezenverklaring is gevolgd. In de tweede tabel staan alleen uitspraken van de rechtbank vermeld. Ook hier is weer aangegeven van welke uitspraak sprake is. Daarnaast is aangegeven of de rechtbank ‘een beroep of gewoonte maken’ heeft aangenomen. Tot slot is aangegeven hoeveel slachtoffers met betrekking tot flessentrekkerij zijn gemaakt in die zaak. De derde tabel geeft alleen arresten van het gerechtshof weer. In deze tabel is dezelfde weergave gegeven als in de tweede tabel. Sommige uitspraken en arresten zijn opgenomen in meerdere tabellen. Een uitspraak van de rechtbank kan dus zijn opgenomen in de eerste tabel en de tweede tabel. Een arrest van het gerechtshof kan in de eerste en in de derde tabel zijn opgenomen.

BIJLAGE 2 TABEL UITGEBREIDE ANALYSE INTERNETOPLICHTING

Rechtbank

Uitspraak	Oplichting	Bewezenverklaard	Straf	Slachtoffers	Marktplaatsoplichting
AV2491	Ja	Medeplegen van oplichting + in bezit hebben van kinderpornografie	Gevangenisstraf 24 maanden, 8 maanden voorwaardelijk, 2 jaar proeftijd	tientallen	Nee (webwinkel opgericht)
BA1487	Ja	Oplichting (internetoplichting + klassieke oplichting)	Gevangenisstraf 7 maanden	24	Nee (bemiddeling bij vinden van een baan)
BE9908	Ja	Oplichting	Gevangenisstraf 22 maanden	6	Ja
BI2037	Ja	Oplichting + valsheid in geschrifte	Gevangenisstraf 21 maanden	86	Ja
BK4742	Nee	X	X	X	X
BK6187	Ja	Oplichting + poging tot oplichting + valsheid in geschrifte	Gevangenisstraf 24 maanden	6	Ja
BL8051	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 24 maanden, 14 maanden voorwaardelijk, proeftijd 3 jaar	11	Nee (bestellen eten + vakantie + vervalsing loonstrook)
BM6703	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 24 maanden, 12 maanden voorwaardelijk, proeftijd 2 jaar	34	Ja
BO0111	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 18 maanden, 6 maanden voorwaardelijk	50	Ja
BP9283	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 3 maanden	18	Ja
BQ4797	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 10 maanden, 4 maanden voorwaardelijk, proeftijd 2 jaar	37	Ja
BR4481	Ja	Oplichting, meermalen gepleegd + wederrechtelijk binnendringen + vernieling + wederspannigheid	Gevangenisstraf 12 maanden, 6 maanden voorwaardelijk, proeftijd 2 jaar	23	Ja
BL0027	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 4 maanden voorwaardelijk + 120 uur taakstraf	22	Ja

BU5753	Ja	Oplichting, meermalen gepleegd (internetoplichting + klassieke oplichting)	Gevangenisstraf 6 maanden, 5 maanden voorwaardelijk, proeftijd 2 jaar + 180 uur taakstraf	10	Ja
BV1594	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 3 maanden voorwaardelijk + 240 uur taakstraf	26	Ja
BV1498	Ja	Oplichting, meermalen gepleegd	Taakstraf 100 uur	6	Ja
BV1510	Ja	Oplichting, meermalen gepleegd	Taakstraf 60 uur	2	Ja
BV9321	Nee	X	X	X	X
BZ1862	Ja	Oplichting, meermalen gepleegd + zware mishandeling + bedreiging met zware mishandeling + flessentrekkerij + verduistering + het in strijd handelen met de Wet wapens en munitie	Gevangenisstraf 2 jaar en 301 dagen, 2 jaar voorwaardelijk, proeftijd 3 jaar	4	Ja
2415	Ja	Oplichting, meermalen gepleegd + vernieling	Gevangenisstraf 9 maanden, 6 maanden voorwaardelijk	9	Ja
CA1872	Ja	Oplichting, meermalen gepleegd + witwassen	Gevangenisstraf 3 maanden voorwaardelijk	16	Ja
CA1885	Ja	Oplichting, meermalen gepleegd + witwassen	Gevangenisstraf 3 maanden voorwaardelijk + 180 uur taakstraf	16	Ja
BZ9266	Nee	x	x	x	x
7777	Ja	Oplichting, meermalen gepleegd + valsheid in geschrifte	Gevangenisstraf 12 maanden, 3 maanden voorwaardelijk, proeftijd 2 jaar	49	Ja
7979	Nee	X	X	X	X
7103	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 36 maanden, 12 maanden voorwaardelijk	206	Ja
845	Ja	Oplichting, meermalen gepleegd + diefstal	Gevangenisstraf 15 maanden, 3 maanden voorwaardelijk, proeftijd 2 jaar	16	Ja
2180	Ja	Medeplegen van oplichting	Taakstraf 100 uur	9	Ja
3710	Ja	Oplichting, meermalen gepleegd + poging tot oplichting + verduistering	Gevangenisstraf 24 maanden, 8 maanden voorwaardelijk, proeftijd 3 jaar	46	Nee (plaatsen van advertenties voor casting en fotoshoot)

3966	Ja	Medeplegen van oplichting, meermalen gepleegd	Gevangenisstraf 4 maanden + 180 uur taakstraf	63	Ja
3967	Ja	Medeplegen van oplichting, meermalen gepleegd	Gevangenisstraf 12 maanden, 6 maanden voorwaardelijk	63	Ja
4656	Ja	Oplichting meermalen gepleegd	Gevangenisstraf 3 maanden voorwaardelijk + 200 uur taakstraf	21	Ja
6400	Ja	Medeplegen van oplichting, meermalen gepleegd	Taakstraf 140 uur	8	Ja
6401	Ja	Medeplegen van oplichting, meermalen gepleegd	Taakstraf 140 uur	8	Ja
15159	Ja	Medeplichtigheid oplichting, meermalen gepleegd + poging zware mishandeling	Jeugddetentie 76 dagen, 60 dagen voorwaardelijk	4	Ja
1388	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 70 dagen	10	Ja
825	Ja	Oplichting, meermalen gepleegd + poging tot oplichting	Jeugddetentie 171 dagen, 90 dagen voorwaardelijk, proeftijd 2 jaar	19	Nee (aanbieden marketingdiensten)
2104	Ja	Medeplegen van oplichting, meermalen gepleegd + voorhanden hebben van een wapen + voorhanden hebben van XTC + belediging van politieambtenaren + openlijke geweldpleging + deelnemen aan een criminele organisatie + witwassen	Gevangenisstraf 660 dagen, 297 dagen voorwaardelijk	18	Ja
4946	Ja	Medeplegen van oplichting, meermalen gepleegd + witwassen	Gevangenisstraf 2 jaar	+- 500	Nee (oprichten webwinkel)
904	Ja	Oplichting, meermalen gepleegd + identiteitsfraude	Gevangenisstraf 18 maanden, 6 maanden voorwaardelijk + 240 uur werkstraf	17	Ja
909	Ja	Medeplegen van oplichting, meermalen gepleegd + oplichting	Gevangenisstraf 10 maanden	35	Ja
917	Ja	Medeplegen van oplichting, meermalen gepleegd + witwassen	Gevangenisstraf 6 maanden	7	Ja

Gerechtshof

BA2770	**Nee**	**Beklag procedure (artikel 12)**			
BT1911	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 3 maanden voorwaardelijk + 120 uur taakstraf	15	Ja
BW5086	Nee	X	X	X	X
BX4194	Ja	Oplichting, meermalen gepleegd + diefstal	X	16	Ja
4093	Ja	Oplichting, meermalen gepleegd + bedreiging met enig misdrijf tegen het leven gericht	Gevangenisstraf 4 maanden voorwaardelijk + 240 uur taakstraf	20	Ja
4498	Ja	Medeplegen van oplichting, meermalen gepleegd	Gevangenisstraf 4 maanden	3	
3013	Ja	Oplichting, meermalen gepleegd + diefstal met bedreiging en geweld	Gevangenisstraf 3 jaar en 6 maanden	6	Ja
121	Ja	Oplichting, meermalen gepleegd	Gevangenisstraf 7 maanden, 4 maanden voorwaardelijk, proeftijd 2 jaar	37	Ja
1214	Nee	X	X	X	X
4390	Ja	Oplichting, meermalen gepleegd	Nvt	Tientallen	Nee (tickets verkoop)

BIJLAGE 3 TABEL ANALYSE INTERNETOPLICHTING

Uitspraak	Vrijspraak/veroordeeld	Aantal slachtoffers
ECLI:NL:GHLEE:2009:BJ6902 03-09-2009	Veroordeeld	3 slachtoffers
ECLI:NL:RBSGR:2009:BI7328 08-06-2009	Veroordeeld	18 slachtoffers
ECLI:NL:RBSGR:2006:AY9483 04-10-2006	Veroordeeld	Meer dan 80 slachtoffers
ECLI:NL:GHLEE:2011:BP6255 01-03-2011	Veroordeeld	3 slachtoffers
ECLI:NL:GHDHA:2015:1440 04-02-2015	Vrijspraak	Juiste contactgegevens
ECLI:NL:RBASS:2010:BM2269 23-04-2010 ECLI:NL:GHLEE:BO2524	Vrijspraak Vrijspraak	Wist niet dat bankrekening voor oplichting werd verwerkt
ECLI:NL:GHLEE:2011:BR0614 05-07-2011	Veroordeeld	2 slachtoffers
ECLI:NL:RBZUT:2009:BJ1414 03-07-2009	Veroordeeld	5 slachtoffers
ECLI:NL:RBARN:2010:BL5523 25-02-2010	Veroordeeld	5 slachtoffers
ECLI:NL:RBGEL:2013:BZ9709 28-05-2013	Veroordeeld	1 slachtoffer
ECLI:NL:GHDHA:2014:1647 16-04-2014	Veroordeeld	19 slachtoffers
ECLI:NL:RBALM:2009:BJ6223 18-08-2009	Veroordeeld	8 slachtoffers
ECLI:NL:RBHAA:2010:BO8294 29-10-2010	Veroordeeld	11 slachtoffers
ECLI:NL:RBMAA:2009:BI4842 06-04-2009	Veroordeeld	6 slachtoffers
ECLI:NL:RBHAA:2009:BL7294 15-09-2009	Veroordeeld	14 slachtoffers
ECLI:NL:RBZUT:2009:BJ0009 26-06-2009	Veroordeeld	16 slachtoffers
ECLI:NL:RBZUT:2011:BT8503 18-10-2011	Veroordeeld	6 slachtoffers
ECLI:NL:GHDHA:2014:1640 16-04-2014	Veroordeeld	4 slachtoffers
ECLI:NL:RBMAA:2006:AY8467 16-08-2006	Veroordeeld	19 slachtoffers
ECLI:NL:GHDHA:2015:3256 17-11-2015	Veroordeeld	20 slachtoffers
ECLI:NL:RBDHA:2013:19224 20-12-2013	Veroordeeld	82 slachtoffers
ECLI:NL:RBDHA:2013:8128 03-07-2013	Vrijspraak	Geen sprake van een oorzakelijk verband tussen het aanwenden van het bedrieglijk middel (de valse

		naam) en het afgeven van geld
ECLI:NL:GHLEE:2011:BR5593 12-08-2011	Vrijspraak	Onvoldoende bewijs
ECLI:NL:RBMAA:2009:BK1160 02-02-2009	Veroordeeld	17 slachtoffers
ECLI:NL:RBBRE:2008:BC8213 ECLI:NL:RBBRE:2008:BC8241 01-04-2008	Veroordeeld	13 slachtoffers
ECLI:NL:RBZLY:2011:BR1736 14-04-2011	Veroordeeld	5 slachtoffers
ECLI:NL:RBOBR:2016:1811 19-04-2016	Veroordeeld	24 slachtoffers
ECLI:NL:RBLIM:2015:3669 29-04-2015	Veroordeeld	16 slachtoffers
ECLI:NL:RBGRO:2008:BG3284 03-11-2008	Veroordeeld	7 slachtoffers
ECLI:NL:RBDOR:2007:AZ9390 07-02-2007	Veroordeeld	7 slachtoffers
ECLI:NL:RBNHO:2013:11557 02-12-2013	Veroordeeld	33 slachtoffers
ECLI:NL:GHAMS:2013:BZ5771 27-03-2013	Veroordeeld	2 slachtoffers
ECLI:NL:RBZLY:2011:BR1716 14-04-2011	Vrijspraak	Geen motivering
ECLI:NL:RBZUT:2010:BM8948 ECLI:NL:RBZUT:2010:BM8951 23-06-2010	Veroordeeld	16 slachtoffers
ECLI:NL:RBSGR:2010:BL1143 29-01-2010	Veroordeeld	1 slachtoffer
ECLI:NL:GHARL:2016:1647 04-03-2016	Veroordeeld	143 slachtoffers
ECLI:NL:RBDOR:2009:BJ8215 17-09-2009	Veroordeeld	8 slachtoffers
ECLI:NL:RBALM:2008:BG8562 30-12-2008	Veroordeeld	77 slachtoffers
ECLI:NL:RBMID:2008:BD0409 23-04-2008	Veroordeeld	20 slachtoffers
ECLI:NL:RBALK:2006:AZ1790 07-11-2006	Veroordeeld	15 slachtoffers
ECLI:NL:RBMNE:2016:5781 01-11-2016	Veroordeeld	20 slachtoffers
ECLI:NL:GHAMS:2006:AY0307 28-06-2006	Veroordeeld	34 slachtoffers
ECLI:NL:RBGEL:2016:6275 18-11-2016	Veroordeeld	29 slachtoffers
ECLI:NL:RBMNE:2015:3908 01-05-2015	Veroordeeld	4 slachtoffers

BIJLAGE 4 TABELLEN ANALYSE FLESSENTREKKERIJ

Uitspraak	Verweer	Vrijspraak
ECLI:NL:RBSGR:2005:AS8906 4 maart 2005	Ontbreken oogmerk bij verdachte	Nee
ECLI:NL:RBDOR:2006:AV1905 16 februari 2006	Onbetrouwbaar bewijs	Nee
ECLI:NL:RBSGR:2006:AV9196 7 april 2006	Rechtbank: overnachting in een hotel is niet aan te merken als het kopen van een goed	Ja
ECLI:NL:RBSHE:2009:BI1886 23 april 2009	Overweging rechtbank: Geen oogmerk geweest op de beschikking krijgen over de gekochte auto's	Ja
ECLI:NL:RBZUT:2009:BK4976 1 december 2009	Ontbreken oogmerk	Nee
ECLI:NL:RBARN:2010:BM3281 4 mei 2010	Ontbreken oogmerk Sprake van betalingsonmacht door faillissement. Rechtbank: dit neemt de omstandigheid dat de goederen niet betaald zijn niet weg.	Nee
ECLI:NL:RBLEE:2010:BN2401 23 juli 2010	Ontbreken oogmerk Verdachte wilde nog betalen	Nee
ECLI:NL:RBASS:2011:BQ4020 19 april 2011	Ontbreken oogmerk Verdachte heeft achteraf betaald. Rechtbank: ontbreken oogmerk kan niet weerlegd worden door betaling achteraf	Nee
ECLI:NL:GHLEE:2011:BT6410 30 september 2011	Gerechtshof: in de tenlastelegging is de plaats waar het delict heeft plaatsgevonden verkeerd ten laste gelegd. Verdachte wordt derhalve vrijgesproken.	Ja
ECLI:NL:RBBRE:2012:BV7195 29 februari 2012	Ontbreken oogmerk	Nee
ECLI:NL:RBGEL:2012:BX3786 7 augustus 2012	Ontbreken oogmerk	Nee
ECLI:NL:GHSHE:2013BZ2702 7 februari 2013	Ontbreken oogmerk Verdachte zou de intentie nog hebben gehad om te betalen	Nee
ECLI:NL:GHSHE:2013:BZ2652 18 februari 2013	1. Ontbreken oogmerk 2. Geen sprake van 'gewoonte of beroep maken'	Nee
ECLI:NL:RBOVE:2013:BZ6029 2 april 2013	Ontbreken oogmerk	Nee
ECLI:NL:RBOVE:2013:CA3835 17 juni 2013	Bewijs voor betrokkenheid bij het delict ontbreekt	Nee
ECLI:NL:RBZWB:2013:8025 8 november 2013	Geen sprake van 'gewoonte of beroep maken' Verdediging: te lange periode tussen de feiten Rechtbank: wel vrijspraak voor overnachting in hotel, dit is namelijk niet aan te merken als een goed	Nee
ECLI:NL:RBGEL:2013:6182	Ontbreken oogmerk	Nee

24 december 2013		
ECLI:NL:GHSHE:2014:1007 2 april 2014	1. Nuttigen van ontbijt kan niet aangemerkt worden als het kopen van goederen 2. Ontbreken oogmerk	Nee
ECLI:NL:RBGEL:2014:2641 22 april 2014	Een andere persoon heeft zich uitgegeven als verdachte. Verdachte heeft de feiten zelf niet gepleegd	Nee
ECLI:NL:RBOVE:2014:2378 2 mei 2014	In dit geval is sprake van civielrechtelijke wanprestatie in plaats van flessentrekkerij Rechtbank: het delict is fout ten laste gelegd, daarom volgt een vrijspraak	Ja
ECLI:NL:RBAMS:2014:5735 1 september 2014	1. Gebrek aan wettig en overtuigend bewijs 2. Geen sprake van 'gewoonte of beroep maken' 3. Geen sprake van medeplegen Rechtbank: geen sprake van 'gewoonte of beroep maken' nu dit feit ziet op een kort tijdsbestek	Ja
ECLI:NL:RBNNE:2015:3023 26 februari 2015	Geen sprake van 'gewoonte of beroep maken'	Nee
ECLI:NL:RBOVE:2015:2677 3 juni 2015	Gerefereerd aan oordeel rechtbank	Nee
ECLI:NL:RBLIM:2015:6360 27 juli 2015	Ontbreken oogmerk	Nee
ECLI:NL:RBMNE:2015:5831 4 augustus 2015	Geen verweer opgenomen in uitspraak Rechtbank: geen aanknopingspunten dat verdachte bij zaken betrokken is geweest	Ja
ECLI:NL:RBDHA:2015:13065 16 november 2015	Ontbreken oogmerk	Nee
ECLI:NL:RBOVE:2016:213 26 januari 2016	Geen sprake van medeplichtigheid Rechtbank: niet voldaan aan de voor medeplichtigheid vereiste dubbele opzet	Ja
ECLI:NL:RBGEL:2016:4531 1 augustus 2016	Ontbreken oogmerk Rechtbank: verdachte wordt veroordeeld voor oplichting in plaats van flessentrekkerij	X
ECLI:NL:RBOBR:2016:6767 7 december 2016	Onbetrouwbare getuige	Nee
ECLI:NL:RBNNE:2017:565 16 februari 2017	Ontbreken oogmerk Rechtbank: verdachte heeft het oogmerk niet gehad om de beschikking over goederen te verkrijgen zonder te betalen	Ja

<u>Rechtbank</u>

Uitspraak	**Beroep of gewoonte aangenomen**	**Slachtoffers gemaakt**
ECLI:NL:RBNNE:2015:3023 26-02-2015 (ook oplichting)	Ja, de vijf tenlastegelegde feiten zijn begaan in een periode van circa negen maanden.	2 bedrijven is flessentrekkerij toegepast

		2 bedrijven hebben ze gekozen voor oplichting ipv flessentrekkerij
ECLI:NL:RBGEL:2013:6182 24-12-2013	Ja, er is sprake van herhaaldelijk welbewust kopen zonder betaling in een korte periode van enkele weken	7 auto's gekocht zonder te betalen
ECLI:NL:RBDHA:2015:13050 16-11-2015	Op rekening goederen gekocht en daarvoor niet betaald. Nu verdachte blijkens de tenlastelegging verweten wordt dat zij één bestelling bij slachtoffer 12 heeft gedaan die zij niet heeft betaald, kan niet worden gesteld dat daarmee sprake is van een gewoonte.	8 (periode van vier maanden)
ECLI:NL:RBDHA:2015:13065 16-11-2015	-	12
ECLI:NL:RBLIM:2015:6353 07-07-2015	Voor een bewezenverklaring van het bestanddeel een beroep of een gewoonte maakt is volgens de Hoge Raad een meervoud van handelingen vereist waartussen verband bestaat. Verschillende slachtoffers kan als verband worden aangemerkt indien op dezelfde manier te werk werd gegaan.	2 (meerdere goederen per slachtoffer afgenomen)
ECLI:NL:RBLIM:2015:6360 27-07-2015	Geen relevante motivering	9 (verblijf in hotels met ontbijt)
ECLI:NL:RBZWB:2013:8025 08-11-2013	Geen relevante motivering	4
ECLI:NL:RBDHA:2014:11793 26-09-2014	Verdediging: oogmerk ontbrak op het middels onvolledige betaling verkrijgen van auto's. Altijd de intentie gehad om de koopsom te voldoen als ze over voldoende middelen beschikte. (omstandigheden noemen waaruit de intentie volgt) Rechtbank: in 8 maanden 35 auto's gekocht, verdachte reeds bij verkoop op de hoogte van slechte financiële situatie	35
ECLI:NL:RBNNE:2015:897 03-03-2015	Niet duidelijk waarom de rechtbank 2 gevallen van flessentrekkerij als een gewoonte of beroep ziet.	2 bouwbedrijven
ECLI:NL:RBOVE:2013:CA3835 17-06-2013	Geen motivering mbt flessentrekkerij	4
ECLI:NL:RBGEL:2014:2641 22-04-2014	Verdediging: getuige zou zich voor hebben gedaan als verdachte. Niet vastgesteld kan worden dat	14

	verdachte het ten laste gelegde heeft begaan. Rechtbank: uit bewijsmiddelen volgt dat verdachte het tenlastegelegde heeft gedaan.	
ECLI:NL:RBOVE:2016:3429 13-09-2016	Sprake van een gewoonte maken nu verdachte blijkens de aangiftes veelal hanteerde volgens eenzelfde aanpak.	24
ECLI:NL:RBOVE:2015:2677 03-06-2015	Geen motivering	15

Gerechtshof

Arrest	**Beroep of gewoonte aangenomen**	**Slachtoffers gemaakt**
ECLI:NL:GHSHE:2014:1007 02-04-2014 (ook oplichting)	Verdachte wist dat zij geen geld had om goederen te betalen, maar door desondanks deze goederen af te nemen en gebruik te maken van deze diensten is naar het oordeel van het hof aan het vereiste oogmerk voldaan. De duur van de periode doet niet af aan het feit dat verdachte meerdere keren heeft getankt zonder te betalen.	7
ECLI:NL:GHARL:2014:7098 09-09-2014 Hoger beroep op ECLI:NL:RBGEL:2013:6182	Uit feiten en omstandigheden wordt afgeleid dat verdachte het oogmerk heeft gehad om niet te betalen (gebruik valse naam, rekening met onvoldoende saldo, gebruik gemaakt van naam bedrijf dat niet meer ingeschreven was in het handelsregister)	6 (een minder dan de rechtbank bewezen heeft verklaard)
ECLI:NL:GHDHA:2016:1102 21-04-2016 Hoger beroep op ECLI:NL:RBDHA:2015:13050	Vonnis wordt bevestigd	
ECLI:NL:GHSHE:2013:BZ2702 07-02-2013	Naar het oordeel van het hof moet de verdachte ten tijde van de aankopen op zijn minst hebben geweten dat hij deze niet (volledig) zou gaan betalen. Zie verdediging en verdere motivering hieronder	3 bedrijven (meerdere goederen)

ECLI:NL:GHSHE:2013:BZ2652 18-02-2013	Raadsvrouw voert aan dat geen sprake is van een gewoonte maken van omdat tweemaal goederen kopen zonder te betalen onvoldoende is. Het hof is van mening dat sprake is van een gewoonte maken nu verdachte herhaaldelijk soortgelijke goederen heeft gekocht en mede gelet op zijn Justitiële Documentatie. Het hof vat dit op als een door de pluraliteit van handelingen gevormde en voortgezette gewoonte.	2x gegeten en gedronken zonder betaling
ECLI:NL:GHARL:2016:7861 03-10-2016	Geen relevantie motivering/verdediging	11 hotels

BIJLAGE 5 TABEL RICHTLIJNEN STRAFVORDERING INTERNETOPLICHTING

Aantal slachtoffers	First offender		1x recidive	Meermalen recidive
1	TS 50 uur	5 jaar 2 jaar	TS 70 uur Idem of GS 5 weken	TS 100 uur of GS 7 weken ov
2-4	TS 80 uur	5 jaar 2 jaar	TS 120 uur Idem of GS 2 maanden	TS 160 uur of GS 11 weken ov
Reeks	GS 2 weken per feit		GS 5 weken per feit	GS 2 maanden ov per feit

Bijzonderheden
Uitgangspunt is tevens dat de (totale) schade is/wordt vergoed.
Strafverzwarend onder andere:

- Medeplegen
- Mate van professionaliteit

Let op eventueel taakstrafverbod (artikel 22b Sr) en of sprake is van een (zeer actieve) veelpleger of stelstelmatige dader.[3]

Afkortingen
GB = Geldboete
TS = Taakstraf
GS = gevangenisstraf
Ov = onvoorwaardelijk
5j = recidive binnen 5 jaar
2j = recidive binnen 2 jaar

[3] Deze tabel is een exacte weergave van de tabel op de website www.om.nl. Voor de duidelijkheid en het gemak is besloten deze tabel in de bijlagen op te nemen.

BIJLAGE 6 INTERVIEW DE HEER HERSMUS

Interview met de heer mr. Hersmus
Plaatsgevonden: woensdag 29 maart 2017 te 's-Hertogenbosch
De heer Hersmus is als parketsecretaris werkzaam bij het OM. De heer Hersmus heeft onder andere de portefeuille cybercrime onder zich.

Er is een Landelijk Meldpunt Internetoplichting heet dat. Dat wordt gerund door een OvJ en de parketsecretaris van het parket Noord-Holland samen met de politie. Mensen kunnen sinds een bepaalde tijd online bij de politie aangifte doen van Marktplaatsoplichting. Dit landelijk meldpunt verzamelen alle aangiftes die binnen zijn gekomen in het hele land via de politie en die gaan dan kijken kunnen wij die aangiftes met elkaar vergelijken en kunnen wij zien dat daar dezelfde dader acht zit. Dat kan bijvoorbeeld zijn, omdat in meerdere aangiftes van mensen hetzelfde rekeningnummer wordt gebruikt waar mensen geld op overmaken of een e-mailadres dat steeds terugkomt of een bepaalde specifieke advertentie op Marktplaats. Voorheen was de situatie er was niks anders, jij wil iets hier bestellen, iemand in Utrecht wil iets bestellen iemand in Groningen wil iets bestellen en iedereen ging naar het lokale politiebureau. De politie had onvoldoende zicht dat er allemaal dezelfde dader achter zit. Toen is het landelijk meldpunt opgericht. Wat zij doen is die aangiftes verzamelen en bundelen waarvan zij zien dat ze bij elkaar horen. Zij kunnen ook bepaalde bevoegdheden uitoefenen. Bijvoorbeeld bij Marktplaats gegevens opvragen of bij de bank opvragen wie is nou de rekeninghouder van een bepaald bankrekeningnummer. Als daar nou een specifieke dader uitkomt, dan gaan ze kijken waar woont die verdachte. Stel voor dat hij hier in Den Bosch woont, dan draagt het LMIO de hele zaak met alle aangiftes die ze dan hebben over aan de lokale politie hier in Den Bosch zodat die aan de slag kunnen met verder onderzoek naar deze verdachte. Dat zijn per definitie die OvJ en parketsecretaris die heel veel van Marktplaatsoplichting weten, omdat zij dat landelijk coördineren en zo uitzetten naar allerlei parketten in de regio.

Ik: want zij bereiden dan die zaak eigenlijk helemaal voor?

Ja, zij doen dus een stukje projectvoorbereiding. Zij analyseren dus die aangiftes die binnenkomen. Zij kijken ook is er voldoende verdenking. Daarnaast kunnen zij bepaalde bevoegdheden toepassen. Wat ze heel vaak doen is informatie bij Marktplaats of banken opvragen en daar komt dan vaak een bepaalde verdachte of dadergroepering uit en zij zetten dat dan weer weg bij de politie meestal in het gebied waar die verdachte woont. Dit is wel goed om te weten dat er een onderdeel van het OM is die deze politiezaken in samenwerkingsverband coördineren. Dat moet ook wel, bij computercriminaliteit dat is grenzeloos. Dat is niet aan een bepaald gebied gebonden en het is maar net de vraag waar een slachtoffer van Marktplaatsoplichting achter zijn computer zit en die goederen besteld. Dat is dus hun taak en dat zijn mensen die er dus heel veel vanaf weten.

Deze bevoegdheid raakt heel de opsporing. Zelfs, dat zat ik nog te denken, hoewel het dan heet de wijziging van het WvSr en het WvSv in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit, denk ik als ik deze bevoegdheid zie, dat deze ook ingezet kunnen worden voor andere delicten. Bijvoorbeeld de lokpuber. Lokpuber is ook een zedendelict wat je via computers pleegt, maar ik sluit niet uit dat deze bevoegdheid in heel veel andere juist in veel andere misdrijven zal worden toegepast dan alleen maar computercriminaliteit, omdat het gewoon een gat in de opsporing dicht moet maken. Maar ik zou zeggen we beginnen gewoon aan jouw vragen.

Ik: eerste vraag is eigenlijk met welke werkzaamheden houdt u zich vooral bezig als parketsecretaris? Want dat is mij niet helemaal duidelijk.

Ik werk hier op het parket, we hebben hier een aantal officieren die zich bezig houden met de vervolging van strafbare feiten en die optreden in de zittingszaal. En parketsecretarissen zijn eigenlijk juridisch ondersteuners, zoals advocatenkantoren ook wel juridisch medewerkers in dienst hebben, zijn parketsecretarissen dat bij het OM. Wat wij met name doen is de OvJ ondersteunen in het hele proces in aanloop naar de behandeling op zitting. Dan moet je denken aan dat wij voorbewerking maken. De politie levert een dossier aan van een bepaald delict en wij maken daar een samenvatting van op juridische punten voor de OvJ, wij maken de tenlastelegging, het hangt er een beetje vanaf op welke afdelingen je bij ons zit. Ik zit op een soort van onderzoeksafdeling. Daar draaien we de wat grotere zaken. Dan ben je ook best nauw betrokken als sparringpartner voor de OvJ om samen met de politie te kijken hoe gaan we dit strafbare feit onderzoeken, welke dwangmiddelen gaan we inzetten, welke tactiek gaan we toepassen. Nou dus een hele leuke baan.

Maar de parketsecretarissen zijn eigenlijk de juridische ondersteuning van de OvJ en hebben dan in bepaalde mate bevoegdheden om ook beslissingen namens de OvJ te mogen nemen. Dat kan dan in bepaalde eenvoudige zaken. Zij kunnen zaken afdoen, transactiegesprekken met verdachte voeren, tot op zekere hoogte beslissingen nemen over in beslag genomen goederen, dat soort dingen. Dus eigenlijk alles buiten de zittingszaal om.

Ik: wat voor zaken behandelt u hier vooral?

Ja, wat ik nou zei ik zit op een onderzoeksafdeling. Uhm, ik heb twee specifieke portefeuilles. Eentje is cybercrime en eentje is zedenzaken. Cybercrimezaken die dan bij mij terecht komen zijn, ja hoe kan je dit uitleggen. Er is een onderscheid in cybercrime zaken in enge zin en wat tegenwoordig heet gedigitaliseerde criminaliteit. En gedigitaliseerde criminaliteit zijn eigenlijk klassieke delicten die worden gepleegd met de computer omdat dat gewoon eigenlijk makkelijker is. Marktplaatsoplichting is er eigenlijk al een voorbeeld van. Je kunt ook klassiek iemand oplichting door met een smoes bij iemand aan de deur te gaan ofzo en een mooi product aan te prijzen, een zak met bakstenen te verkopen, maar dat gebeurt dan via een computer. Een ander voorbeeld is belediging op social media zeg maar. Je kunt ook een advertentie in de krant zetten ofzo dat je iemand een vreselijk persoon vindt om het maar netjes uit te drukken. Maar dat gebeurt dan via een computer. En computercriminaliteit in enge zin, dat is meer waar ik me echt specifiek mee bezig hou, zijn die zaken waarbij een computer/geautomatiseerd werk echt het doel van de aanvaller is zeg maar of het onderwerp van het strafbare feit. Dan moet je dus echt denken aan computervredebreuk, dus mensen die inbreken in andermans computers en moet je denken aan DDoS-aanvallen dus het platleggen van computernetwerken van mensen, je kunt denken aan vernieling van computergegevens dat soort dingen. Dus met die delicten houd ik me bezig. Die komen niet heel veel binnen bij ons, omdat er wat mij betreft nog te weinig capaciteit van de politie is op het gebied van cybercrime. Daar worden nu wel stappen ingezet. Ik houd me bezig met zedenmisdrijven en ik zit in een team onderzoeken waarbij ik me bezighoud met allerlei onderzoeken die projectmatig worden opgepakt. Laten we het er maar op houden dat ik me ook bezighoud met allerlei zwaardere delicten en dat varieert van overvallen, ernstige vermogensdelicten, drugscriminaliteit en er zijn ook zaken waarin bij wijze van spreken de politie wordt gebeld er is hier een dood iemand aangetroffen en die is vermoord of er is iets mee gebeurd dan wordt er meteen een heel groot politieteam mee opgezet en dan wordt ook meteen een OvJ en parketsecretaris aangekoppeld die dat hele onderzoek gaan doen. Gaat meestal om de zwaarste categorie delicten. Dus het is eigenlijk een mengelmoes van alles en wij hebben twee afdelingen bij ons. Een afdeling onderzoek die zich met dit soort zwaardere delicten bezighouden en we hebben een afdeling dat heet interventies en daar zitten ook veel mensen die bijvoorbeeld continu op het politiebureau zitten. Ik weet niet of je ook ooit van z.s.m. hebt gehoord. Z.s.m. wil eigenlijk zeggen dat er gestreefd wordt om daar direct op het politiebureau

ofwel tot een afdoening te komen of mensen meteen een boete te geven/transactie te bieden ofwel een dagvaarding te geven. En dat gebeurt meestal met de lichtere misdrijven en overtredingen. Dus ik zit in de onderzoeksomgeving.

Ik: dan bent u denk ik ook wel meer bekend met hoe zo'n onderzoek te werk gaat? En dan vraag ik me vooral af op welke manier op dit moment computercriminaliteit opgespoord wordt? Dus als er een delict plaatsvindt, hoe gaan jullie dan te werk?

Dat ligt er heel erg aan wat voor type delict het is en hoe het gepleegd is. Dus dat is heel casuïstisch. Meestal komt het erop neer, of ja laat ik beginnen met de meeste zaken die voorkomen of een variant die heel veer voorkomt is: twee mensen hebben een relatie, die relatie gaat uit en de ene partner heeft nog gegevens van het Facebookaccount of social media van de andere partner en die partner gaat dan inloggen in het Facebookaccount van de ex en gaat daar vervelende berichten op zetten. Dat soort zaken wordt dan aangifte van gedaan, dan heb je vaak al direct, vaak heeft de ex al meteen de indruk hier zou mijn partner wel eens in kunnen zitten. Wat je dan kunt doen is een vordering indienen bij bijvoorbeeld Facebook in Amerika om bijvoorbeeld te vragen van goh kunt u aangeven van dit bericht wat op dat moment is geplaatst vanaf welk IP-adres is dat geplaats en als je dan IP-adres weet, dan kun je soms afhankelijk van hoe iemand zich verborgen houdt, kun je soms aan de internetprovider vragen van kunt u mij vertellen wie de abonnee is aan wie op dat moment het IP-adres is toegewezen. Daar komt dan een naam uit rollen. Dat is een manier van opsporen.

Ik: kost dat niet heel veel tijd als je elke keer die gegevens moet opvragen?

Ja, soms dat kost dat heel veel tijd. Gelukkig zijn er wel afspraken gemaakt, ook met grote aanbieders en met grote buitenlandse aanbieders. De regelgeving is eigenlijk zo dat als je, veel bedrijven zitten eigenlijk in Amerika. De Amerikaanse wetgeving die is zo dat als je inhoudelijke gegevens wil hebben van die provider, dus stel je voor dat je van Facebook wil weten van allerlei (privé)berichten die zijn geplaats en die hebben ze vaak nog wel opgeslagen ofzo, maar als jij die wil hebben, dan moet je dat doen via een rechtshulpverzoek. Dus dat betekent dat de Nederlandse staat aan de Amerikaanse staat moet vragen: wij willen graag van u hebben die gegevens en dan moet de Amerikaanse rechter dat goedvinden. Die geeft dan vaak een bevel aan Facebook. Dat gaat dan vaak via de FBI. Facebook moet dat dan weer leveren aan de FBI en dan wordt dat zo weer aan Nederland overgedragen. Daar gaat dan vaak veel tijd overheen. Maar er zijn afspraken met grote aanbieders als Facebook, Instagram, dat is een partij, Google, Apple dat zij alle gegevens op basis van een vordering van een Nederlandse OvJ vrijwillig al leveren. Dat gaat dan niet om inhoudelijke gegevens, dan gaat het bijvoorbeeld om wie is de gebruiker van het account huppelupup, of vanaf welk IP-adres is op datum x ingelogd op dit account. Dat gaat dan om zogenaamde verkeersgegevens of identificerende gegevens, dus niet om inhoud van communicatie en daar zijn afspraken mee dat als wij die vorderen bij dat soort bedrijven, dat zij die over het algemeen vrijwillig leveren op moment dat de Nederlandse OvJ daar een vordering voor indient. Voor de Amerikaanse wetgeving is het niet vereist dat voor dat soort informatie nog via een rechtshulpverzoek bekrachtigd wordt. Maar dat is een middel dat heel veel ingezet wordt. Wat ook gebeurt, is dat inbeslagneming vaak heel belangrijk is. Zeker bij de wat grotere cybercriminelen, dan komt het ook voor dat er internettaps worden gezet, IP-taps zeg maar. Dan komen we daar dalijk denk ik wel op met die bevoegdheid. Wat je dan doet dan plaats je een tap eigenlijk bij de internetprovider en alle eentjes en nulletjes die over de internetverbinding van de verdachte worden verzonden, die krijgt de politie ook van de internetprovider en de politie heeft dan bepaalde software om dan te kunnen zien van wat is iemand op dat moment aan het doen. Dus zit hij op een webbrowser iets in te typen of is hij met andere dingen bezig. Alleen een van de problemen daarvan is dat heel veel van die communicatie tegenwoordig ook versleuteld is zeg maar. En vroeger had je alleen je internetbrowser en misschien af en toe een mailprogramma. Tegenwoordig hebben mensen een firewall een virusscanner een Cloudomgeving, ze skypen, ze spelen online spellen en dat

is zoveel verkeer over die lijn zeg maar dat het heel moeilijk is om die informatie uit te pluizen wat hoort nou bij welk programma en ook nog is heel veel van die informatie versleuteld zoals ook in dat wetvoorstel staat. Skype is een heel bekend voorbeeld. Je kunt internetbellen eigenlijk via dat programma maar dan wel versleuteld. Dus ook al tap je dan af zeg maar, dan nog heb je daar niks aan, want dat kun je niet zien, omdat wat tussen jou en Skype gebeurt, is eigenlijk versleuteld en dat pakken wij van de provider en dat krijg je dus gewoon niet mee. Uhm dat zijn de belangrijkste klassieke middelen voor de opsporing van computercriminaliteit.

Ik: en zou de nieuw voorgestelde opsporingsbevoegdheid dat probleem kunnen oplossen?

Ja, dat kan. Wat je dan doet zeg maar, is, stel je voor dat je weet dat een bepaalde verdachte altijd via Skype communiceert met een medeverdachte. Laten we uitgaan van iemand die regelmatig op dievenpad gaat met een kompaan of inbreken gaat plegen, ik noem maar iets. En je weet dat die twee over die delicten communiceren via Skype. Als wij nu een tap zetten, dan geeft die provider al die eentjes en nulletjes, maar omdat die Skype- gesprekken versleuteld zijn kan de politie niet zien, ook al krijgen ze alle gegevens van de providers van wat er dan precies gezegd wordt. Als jij weet in te breken op de computer van de verdachte zeg maar en je schrijft een programma die zegt van alles wat op die computer gebeurd m.b.t. het programma Skype, die gegevens daar rechtstreeks die moet je ook sturen naar mijn IP-adres van de politie, ik noem maar wat, dan omzeil je die versleuteling zeg maar, omdat je dan op het gebied van het programma gaat onderscheppen. En dan kun je dus horen waar ze het over hebben.

Ik: dus dat zou wel echt een oplossing zijn ja.

Ja, en dat geldt heel breed. Het probleem van versleuteling is best groot, omdat er heel veel aanbieders zijn en bedrijven die hun communicatie gaan versleutelen en mensen ook steeds meer gebruik ervan gaan maken. Skype zit het standaard ingebouwd, je kunt ook vrij eenvoudig programmatjes downloaden of add-ons op je e-mail te zetten zodat ook je e-mailverkeer versleuteld wordt. Pretty Good Privacy is daar een goed voorbeeld van. Dus wat we voorheen nog konden opvangen met de klassieke inzet van bevoegdheden, is nu gewoon niet meer toereikend.

Ik: dus dat is ook het grootste knelpunt? Dat de opsporingsbevoegdheden nu niet meer toereikend zijn?

Nee. Eigenlijk is het zo dat de technische mogelijkheden van opsporing groter zijn dan dat daar juridisch in is voorzien door de wetgever. Dus de politie zou dingen kunnen, alleen ja die kunnen niet of die mogen niet omdat daar niet in wetgeving in is voorzien. De is wetgeving teveel verouderd of de wetgeving is niet geschreven. Toen ooit de telefoontap in het wetboek is gekomen, had iedereen een huistelefoon van KPN en was het heel makkelijk. Je stak daar een stekker in en je kon gewoon meeluisteren. En tegenwoordig heeft iedereen een smartphone waarmee je niet alleen gewoon mee kan bellen, maar ook via internet kan bellen en Skype- en WhatsApp-gesprekken kan voeren. Dus de technologie gaat eigenlijk soms harder dan de wetgeving bij kan houden. Dus dit is een middel om bij te komen zal ik maar zeggen. Volgens mij is versleuteling een van de dingen. Clouddiensten is ook zoiets. Wat voor de opsporing soms heel lastig is, dat mensen vaak ook gegevens in een Cloud hebben staan. Het moeilijke aan een Cloud is van waar is die informatie nou precies. Het kan zijn dat het op een server op een computer in Nederland staat. Het kan ook zijn dat het een server in Ierland of de VS is. Het kan ook zijn dat het op meerdere computers tegelijk staat.
Het kan ook dat het in land A op een computer staat die weer door een bedrijf van land B gehuurd wordt enzo. En dat maakt het territoriaal soms heel lastig. Want wil je dan bij die gegevens, dan zal je over het algemeen een rechtshulpverzoek sturen naar het land wat gaat over die gegevens. Ja welk land is dat dan al, want de Cloud is heel onbestendig.

Ik: en met het heimelijk binnendringen kun je dat eigenlijk omzeilen?

Ja. Stel je voor dat een verdachte die heeft een smartphone zeg maar en die bekijkt gegevens op zijn smartphone die ofwel door hemzelf ofwel door een medeverdachte ergens in een Cloudomgeving zijn opgeslagen. Wat heel lastig is dat, stel je voor dat die Cloud van Google of Microsoft is en die gegevens staan ergens in Amerika voor zover je dat al weet. Nou dan zou je dus een rechtshulpverzoek moeten doen aan Amerika van wij willen graag gegevens die bij jullie op een computer staan van het Cloudabonnement van pietje pluk. Voordat zo'n rechtshulpverzoek in behandeling is genomen, dan ben je al maanden verder. Dat is allemaal vanaf de gedachte die gegevens staan feitelijk in Amerika dus wij moeten daar zijn. Nederland is daar altijd heel braaf in als het op soevereiniteit zeg maar aankomt. Dus die gegevens staan in Amerika dus dan moeten we de gegevens aan de Amerikanen vragen om die gegevens te krijgen, want wij willen niet zomaar in een Cloud gaan zoeken die in een ander land staat. Want dan ben je eigenlijk als Nederlandse opsporingsambtenaar onderzoek aan het verrichtten in ieder geval juridisch op het grondgebied van de VS, en dat is een beetje ja dat willen we niet, want wij willen ook niet dat anderen buitenlandse opsporingsdiensten in computers in Nederland gaan rondneuzen. Met dit wetsvoorstel zou je dus in dit voorbeeld kunnen inbreken in de telefoon van die verdachte en daar een programma op zetten en op het moment dat hij dan een document bekijkt en uit de Cloud haalt en op zijn gsm bekijkt zeg maar, dan is hij er hier gewoon in Nederland mee bezig en dan kun je zeggen van dan stuur mij die informatie toe die hij op dat moment bekijkt en dan heb je de informatie die hij op dat moment aan het bekijken is terwijl hij gewoon in Nederland is. Je kunt veel gerichter zoeken. Op een Cloud kunnen heel veel gegevens staan. Op een apparaat kunnen heel veel gegevens staan, gigabytes en gigabytes aan data, maar als je gaat kijken in de computer, de laptop of de gsm van verdachte en je wil gewoon kijken waar is hij nu mee bezig, wat voor document is hij nu aan het bekijken, dan heb je meteen die informatie als je op dat apparaat zit, omdat je weet hij is nu dit document aan het bekijken. In tegenstelling tot dat je bijvoorbeeld die gegevens ergens moet vorderen en je krijgt de hele inhoud van de Cloud en iemand moet dus ook gaan analyseren van die gigabytes aan data wat is hier nou relevant of wat heeft hij hiervan bekeken.

Ik: en wat denkt u dat de grootste gevaren zijn als deze bevoegdheid wordt ingezet? Want het is natuurlijk best wel een grote inbreuk op het privéleven van een persoon.

Ja, dat is zo, maar daarvoor zijn denk ik de waarborgen in het leven geroepen en er zijn verschillende waarborgen. Een van de waarborgen is dat om deze bevoegdheid toe te passen een machtiging van de rechter-commissaris nodig is. Dus dat betekent dat per definitie dat als je deze bevoegdheid wil inzetten, dat je aan de rechter hebt moeten vragen: dit zijn wij van plan, dit is de bedoeling, dat moet ook in de vordering omschreven worden, op deze manier willen wij de bevoegdheid in gaan zetten en daar zit dus een rechterlijke toets aan waarbij de rechter-commissaris bepaalt of die vindt dat die bevoegdheid rechtmatig mag worden ingezet. En dat vind ik wel een belangrijke waarborg, omdat er zijn ook bevoegdheden die de OvJ kan inzetten zonder dat daar een rechter aan te pas komt. Bijvoorbeeld stelselmatige observatie. De OvJ kan een bevel geven om iemand stelselmatig te observeren. Daar komt geen rechter aan te pas zeg maar. Die observatie kan ook plaatsvinden op internet, social media bijvoorbeeld. De OvJ kan toestemming geven om zeg maar een soort patroon in iemands leven vast te leggen door een opsporingsdienst. Hetzelfde geldt voor een bevel stelselmatige informatie-inwinning. Die kan de OvJ ook geven zonder dat daarvoor een machtiging nodig is. Dus dat zijn al best vergaande bevoegdheden. Wat het hier natuurlijk gevoelig maakt, is dat je echt inbreekt op een telefoon, laptop of computer. Dit wordt toch gezien door iemand als een heel persoonlijk iets, wat je echt gebruikt voor persoonlijke communicatie. Want jouw gsm is jouw smartphone en die zal je niet snel aan iemand anders uitlenen zeg maar en dat is per definitie wel een apparaat dat erg privacygevoelig is. Dus ik vind het goed dat die rechtelijke toetsing erop zit en dan is het afhankelijk van waarvoor je die bevoegdheid wil inzetten, wat er

nog meer aan extra waarborgen nodig is. Want je kunt hem inzetten, ten behoeve van een stelselmatige observatie of het aftappen van gegevens, maar dan heb je zoals ik het begrijp ook naast die bevoegdheid nog steeds een aparte machtiging van de rechter-commissaris nodig om dan te mogen tappen of vertrouwelijke communicatie op te nemen. Dus ik denk ook dat het in een groot aantal gevallen meer gaat om een praktische manier die het juridisch mogelijk maakt om bevoegdheden toe te passen die eigenlijk al bestaan. Alleen nu gaat het veel meer naar het apparaat zelf toe. Een mooi voorbeeld is opnemen van vertrouwelijke communicatie zeg maar. Dat is dus al mogelijk. Stel je voor jij bent hier vandaag met je auto gekomen en jij bent verdachte en wij willen jou afluisteren, dan kan de politie met de machtiging van de rechter-commissaris afluisterapparatuur in jouw auto stiekem inbouwen, waardoor alles wat jij in die auto zegt wordt afgeluisterd. Stel je voor dat jij een vrij moderne auto hebt en daar zit een heel nieuwe navigatiesysteem in, waarmee jij ook kunt bellen, die ook verbinding heeft met het internet en file informatie kan ophalen, dan zou je deze bevoegdheid in kunnen zetten voor zover dat dan technisch mogelijk is dat de politie i.p.v. stiekem in jouw auto gaan inbreken op het moment dat jij daar niet bij bent en een microfoontje gaan inbouwen, zouden ze met deze bevoegdheid op afstand met de computer verbinding kunnen maken met jouw auto met de navigatie en daar software op kunnen zetten en met dat microfoontje wat daar toch al in zit mee dingen kunnen afluisteren. Ik denk dat er goed over is nagedacht en dat er genoeg waarborgen zijn. En ik denk ook zeker nu dit is allemaal relatief nieuw is, dat het in het begin sowieso ingezet gaat worden op de zwaarste zaken. De politie zal hier ook software voor moeten ontwikkelen en manieren bedenken. Wat daarbij een rol speelt, is dat je als politie niet direct te koop wil lopen op welke manieren en welke tactieken je gaat gebruiken om die bevoegdheden toe te passen. Het zal in eerste instantie vooral in grotere zaken ingezet worden. Ik verwacht ook veel meer in zaken van doorgewinterde beroepscriminelen en niet degene die een keer in de fout gaat. Ik denk dat de doelgroep aanvankelijk echt beroepscriminelen zijn die zelf bewust gebruik maken van allerlei manier om buiten het zicht van de politie te blijven door bewust gebruik te maken van encryptie en jammers in hun auto's.

Ik: verwacht u ook dat als er dan een rechtszaak komt en die bevoegdheid is gebruikt, dat er in het begin veel verweren gevoerd worden op de inbreuk van die grondrechten? En denkt u dat de rechter daarin mee zal gaan of niet?

Het is nu aan de wetgever om die bevoegdheid te creëren. Volgens mij is de stand van zaken dat het nu door de Tweede Kamer is goedgekeurd en dat het door de Eerste Kamer nog behandeld moet worden. Er is nog geen uitsluitsel over. Dus ja je kunt wel verweer voeren dat met de inzet van deze bevoegdheid de grondrechten van de cliënt worden geschonden, maar dan is de vraag hoort die discussie in de zittingszaal thuis of is dit gewoon een bevoegdheid die de wetgever bewust heeft willen creëren. Kijk het kan natuurlijk interessant worden, want dit is nu wetgeving, maar er gaan altijd casussen komen van in hoeverre is wat de politie nu gedaan heeft en verzonnen heeft, is dat wat beoogd is met deze bevoegdheid. Want het is best wel ruim he. Er wordt gezegd er mag feitelijk worden ingebroken op een geautomatiseerd werk. Er zullen altijd casussen zijn die niet in het wetsvoorstel voorzien zijn en dat zal zeker jurisprudentie gaan opleveren. Ik denk niet dat dat echt de principiële discussie van deze bevoegdheid is. Ik denk niet dat je daar heel erg ver mee zal komen in de zittingszaal, omdat de wetgever ervoor gekozen heeft om deze bevoegdheid in het leven te roepen en als die wordt toegepast moet er al een vordering en machtiging van de rechter-commissaris liggen en die kan natuurlijk altijd getoetst worden bij de inhoudelijke behandeling van een strafzaak. Maar ik denk dat het argument van dit vind ik een te grote inbreuk op de grondrechten, dat dat al te laat is omdat dat iets is dat bij de wetgever ligt en niet bij de rechter.

Ik: maar u denkt dan wel dat vooral opgelet moet worden dat het niet gebruik gaat worden voor kleine zaken?

Nou ja kleine zaken. Er is al een wettelijk kader waarin die bevoegdheid gebruikt kan worden. Het gaat om zaken waarvan sprake moet zijn van een verdenking van een delict waarop een

voorlopige hechtenis is toegelaten. Het moet gaan om zaken die een ernstige inbreuk op de rechtsorde opleveren gelet op de aard van het feit of de samenhang met andere misdrijven van de verdachte en het onderzoek moet het dringend vorderen. Dus dat zijn al drie criteria waaraan voldaan moet worden bij toepassing van de bevoegdheid. Dat zijn eigenlijk dezelfde criteria die ook worden gebruikt bij de bevoegdheid van gegevens aftappen (artikel 126m en 126l Sv). Dat zijn eigenlijk de zwaardere privacyinbreukmakende bobmiddelen. Daar lijkt aansluiting bij te worden gezocht. Tot slot moet het onderzoek het dringend vorderen. Dus dat wil zeggen van je moet dit ook wel echt moeten doen en er moet niet een andere minder inbreuk makende mogelijkheid zijn om op dezelfde manier aan die gegevens te komen. En dat zal de rechter-commissaris moeten toetsen op het moment dat de OvJ dat wil aanvragen. In eerste instantie moet de OvJ zelf toetsen of aan de criteria is voldaan voordat besloten wordt tot inzet van dit middel of in ieder geval een aanvraag tot een machtiging. En dan controleert de rechter-commissaris dat. Dit geeft ook al aan dat deze bevoegdheid niet zomaar voor elke winkeldiefstal zal kunnen worden ingezet. Bij eenvoudige winkeldiefstallen gaan wij ook geen verdachte aftappen. Dan zit je automatisch al in een wat zwaarder segment van zaken. Ik denk dat zeker in het begin heel nauwkeuring bij politie en justitie gekeken zal worden in wat voor zaken zullen wij dit nou inzetten en dat dit automatisch echt in eerste instantie in de zwaarste categorie zaken zal gebeuren.

Ik: wat maakt het moeilijk om internetoplichting te bewijzen aan de hand van het artikel oplichting? dus waarom wordt een nieuwe strafbaarstelling ingevoerd?

Ja, dat is voor dit onderwerp denk ik de belangrijkste vraag van het interview. Laten we vooropstellen dat oplichting ooit in het WvSr is terechtgekomen en op dat moment heeft de wetgever nog helemaal niet de situatie voorzien van internetoplichting. Er bestonden nog geen computers. Laat staan dat mensen op afstand zo handig met elkaar handel kunnen drijven. Dus dat betekent dat oplichting nooit specifiek voor Marktplaatsoplichting is geschreven. Een ander probleem is dat we volgens mij niet moeten willen dat elke civielrechtelijke wanprestatie in het strafrecht getrokken wordt. Maar wat we wel moeten willen, is dat mensen die bewust continu goederen aanbieden op Marktplaats en van allemaal mensen geld krijgen voor die goederen en nooit de bedoeling hebben om die producten te leveren en op die manier geld afhandig willen maken van die mensen, dat die mensen wel bestraft worden en onder het strafrecht vallen. Maar je moet op de een of andere manier een grens trekken tussen niet alle civielrechtelijke wanprestatie, want stel je voor wij hebben overeenkomst gesloten en ik kom die niet na, nou daar is het civiele recht voor. Dan stuur je mij een ingebrekestelling, etc. en dan kun je mij daar civielrechtelijk op aanspreken. Je moet daar het strafrecht ook niet mee willen belasten. Bij oplichting en met name Marktplaatsoplichting is vooral het probleem voor de mensen die daar slachtoffer van worden dat die vaak niet de mogelijkheid hebben om civielrechtelijk de tegenpartij aan te spreken, omdat je niet weet wie dat is. Je hebt er geen gegevens van of de gegevens de je hebt zijn telefoonnummers en e-mailadressen waar je geen reactie op krijgt. Dus daar zit al een discrepantie. Wat ook opmerkelijk is, is dat het wel strafbaar is om een beroep of gewoonte te maken van het kopen van producten en die niet te betalen. Dus dat je bij een bedrijf goederen besteld en die worden keurig geleverd, maar je betaalt die niet. Dat is strafbaar gesteld als flessentrekkerij. Maar andersom is de situatie niet strafbaar. En dat is nou precies wat Marktplaatsoplichting is. Dat is namelijk het aanbieden van goederen of diensten om daar geld voor te krijgen, maar vervolgens die goederen of diensten niet te leveren. Volgens mij wat hier strafbaar is gesteld, is het omgekeerde van wat flessentrekkerij nu al is in de wet. Dat dicht een gat zeg maar voor de situatie dat het bewijstechnisch lastig is mensen voor oplichting te vervolgen. Wat maakt het nou lastig om in bepaalde situaties mensen voor oplichting te vervolgen. Stel je nou voor: ik plaats een Marktplaatsadvertentie, ik heb een gsm, ik maak daar een mooie foto van en ik plaats er een advertentie van en dan ga ik kijken wie er mij allemaal gaat betalen. Maar ik ga het goed niet leveren maar gewoon met het geld ervandoor. Stel je voor dat ik die advertentie gewoon zet onder mijn eigen naam en met mijn eigen e-mailadres en ik maak er een foto van en jij ziet die advertentie oh dat is een mooie telefoon die wil ik hebben ik bied daar geld voor en ik ga

akkoord met dat bod, maak maar over op mijn rekeningnummer en dan stuur ik jou die telefoon op. En niet alleen jij, maar nog 20 anderen reageren op die advertentie. Dan is het heel moeilijk om mijn situatie op grond van oplichting te vervolgen. Je hebt voor oplichting een van vier oplichtingsmiddelen nodig. Wat heb ik feitelijk in deze situatie gedaan? Ik bied jou iets te koop aan onder mijn eigen naam, ik heb al de intentie om dat helemaal nooit te leveren, maar ja wat doe ik om jou te bewegen tot de afgifte? Dat is juridisch een heel interessante vraag. Dan kun je zeggen ik doe me voor als bonafide verkoper. Daar is in de jurisprudentie al van uitgemaakt dat het enkele voordoen als bonafide verkoper zonder dat daar iets anders bijkomt, dat dat niet automatisch oplevert dat ik daarmee een valse hoedanigheid heb aangenomen waardoor jij wordt gedwongen tot afgifte van een goed. Dus in die situatie zou die oplichting heel moeilijk bewezen kunnen worden terwijl ik heel bewust die telefoon en advertentie plaats om zo het geld van mensen te incasseren. Dus eigenlijk gewoon de tegenhanger van flessentrekkerij. En dat zou bij het nieuwe artikel wel strafbaar zijn. Dan moet je nog wel kunnen bewijzen dat het een beroep op gewoonte is. Maar dat is makkelijker dan al die listige kunstgrepen omdat het vaak zo is dat jij dan niet het enige slachtoffer bent van mij, maar vaak zijn er ook veel andere mensen die betaald hebben. Vaak zijn er meerdere advertenties voor meerdere producten die worden aangeboden voor een langere periode.

Ik: wat mij opviel in de jurisprudentie is dat het laatste jaar oplichting wel vaak aangenomen wordt. Is een nieuwe strafbaarstelling wel noodzakelijk?

Je moet er dus ook wel een hoop onderzoek naar doen. Je moet al nagaan wat hield de communicatie tussen al die slachtoffers in, wat voor e-mailadressen zijn er allemaal gebruikt, eventueel ook de inhoud nog opvragen, wat voor een bankrekening en op wiens naam allemaal. Dus daar komt ook een behoorlijke investering bij kijken en die investering is nog groter omdat bij de gemiddelde oplichtingszaak van het LMIO meestal tientallen aangevers zitten. Je moet daar ook onderzoek naar doen. Je moet bij banken gegevens opvragen, je moet gaan kijken op welke manieren is er allemaal gecommuniceerd, met welke e-mailadressen, soms is er ook een samenwerkingsverband tussen verdachten, wie heeft wat gedaan. Dat maakt het ook weer ingewikkelder.

Ik: zou de nieuwe strafbaarstelling/het nieuwe wetsvoorstel die problemen dan wegnemen? Of zou dit dan nog steeds hetzelfde zijn?

Nou ja, als jij dan kan bewijzen dat Piet 10 advertenties op Marktplaats heeft geplaats en van die 10 advertenties dat meerdere mensen geld hebben aangeboden en hij heeft dat aangenomen en meerdere mensen hebben geld overgemaakt naar Piet, dan ben je al een heel eind voor het bewijzen van de nieuwe strafbaarstelling. Omdat hij de advertenties plaatst en het feit dat je op een advertentie al meerdere biedingen van meerdere mensen accepteert, maakt al dat jij nooit dat ene product aan al die mensen kan leveren. Dus dan wordt het bewijstechnisch alweer makkelijker. Dus dan krijg je niet al die problemen met het bewijzen van een van de vier oplichtingsmiddelen. Dit voorkomt ook zeg maar dat je het juridische begrip van oplichting, namelijk de valse hoedanigheid, verder en verder moet oprekken om Marktplaatsoplichters op basis van die strafbepaling te kunnen aanspreken.
Het enkele voordoen als bonafide verkoper, levert die valse hoedanigheid nog niet op maar als er iets bijkomt van een valse naam of een vals e-mailadres kan dit wel oplichting opleveren. Wat je tegenwoordig ook hebt, zijn mensen die een valse webwinkel maken. Die bouwen een site waar je bepaalde producten kunt kopen. Jij zoekt een bepaald product op google en komt op die site. Je gaat dat product bestellen en morgen of overmorgen is heel die site weg. Het geld wat jij betaald hebt is ook verdwenen. Per definitie mensen die er een beroep of gewoonte van maken om geld te incasseren en dat ze niet van plan zijn te gaan leveren. Dit is iets wat direct onder het artikel zou kunnen vallen zonder dat je daarmee dat juridische delict van oplichting zou hoeven op te rekken.

BIJLAGE 7 INTERVIEW DE HEER KUIJPER

Interview met de heer mr. Kuijper
Afgenomen op: dinsdag 4 april 2017 te 's-Gravenhage
De heer Kuijper is raadsheer bij het gerechtshof 's-Gravenhage. Tevens is de heer Kuijer lid van het Kenniscentrum Cybercriminaliteit van het gerechtshof 's-Gravenhage.

Ik: Wat voor zaken heeft u behandeld betreffende internetoplichting? Welke ontwikkelingen zijn waar te nemen in de jurisprudentie met betrekking tot internetoplichting?

Laat ik het zo zeggen: ik werk nu een jaartje of zestien in de strafrechtspraak. Marktplaatsfraude is echt iets van de laatste vijf jaar. Daarvoor kwam het eigenlijk niet voor. Het kwam wel voor, maar er werd geen werk van gemaakt. Politie is dit voorzichtig aan het oppakken, met het landelijk meldpunt computercriminaliteit. Marktplaatsfraude zag zijn model onder druk komen. Dus die is eigenlijk wat meer gaan bewegen. In de jurisprudentie zag je eigenlijk twee scholen heel lang. De ene school is eigenlijk heel formalistisch. Die zei van ja oplichting is er als je bewogen wordt door oplichtingsmiddelen tot iets anders te doen dan je anders had gedaan. En alleen op een knop drukken omdat iemand iets te koop aanbiedt, dan ben je nog niet bewogen. Dan moet je gewoon maar beter opletten. En de andere school, daar hoor ik vanaf het begin bij, die ziet de hele internetontwikkeling als ook wel een zelfstandig iets. Je moet ook even kijken welke plaats Marktplaatsplatforms in het handelsverkeer innemen. Wat eigen is aan die vorm, dat je niet meer op de markt face to face handelt, maar dat je op afstand op basis van vertrouwen en in producten met vaak niet extreem hoge waarde handelt. Dan kan je wel iets ruimer zijn. Wat is er nou gebeurd? Wat heeft zich voorgedaan op internet. Is gebruik gemaakt van technieken om zich vertrouwenwekkender voor te doen. Die jurisprudentie heb je waarschijnlijk wel gezien. Daar is die lijn uitgekomen. Den Bosch is daar leidend in geweest en wij zitten daar ook bij. We kijken veel meer naar het totale plaatje en is dat dan bewegen dat tegen die drempel wat lager. Valse hoedanigheid, als je valse btw-nummers vermeldt, als je je voordoet als een heel bonafide bedrijf met valse keurmerken, dan verdient dat ook gewoon oplichtingsmiddelen, dan ga je bij mij gewoon voor een bewezenverklaring.
Dat zijn eigenlijk de twee scholen. En wat ik waarneem de laatste twee/tweeëneenhalf jaar, is dat de laatste school aan de winnende hand is. Dat je ziet dat we het iets minder formalistisch gaan bekijken en iets meer kijkt van ja wat is gebruikelijk op platforms en wat is de voorzorg die je kan nemen. Het enige is als er staat nieuwe iPad 6 voor honderd euro en je drukt dan op de knop, ja dan ben je wel een beetje de Sjaak. Al het andere is toch wel snel een vorm van Marktplaatsfraude. En dat is ook een lijn waar ik wel mee kan leven. De wetgever is wat dat betreft eigenlijk wel een beetje mosterd na de maaltijd. Die nu eigenlijk gewoon generiek strafbaar stelt, zonder dat je ingewikkelde discussies krijgt over welke oplichtingsmiddelen zijn gebruikt en waaruit blijkt dat iemand heeft bewogen tot, die specifieke oplichtingsmiddelen. De nieuwe wet zal het voor een deel makkelijker maken.

Ik: maar naar uw mening had dat niet per se gehoeven de nieuwe strafbaarstelling?

Nou, dat kon de wetgever natuurlijk ook niet weten toen ze daar mee begon. Dit soort trajecten loopt natuurlijk heel langzaam en ja ik denk dat het wel goed is. Voor hetzelfde geld zegt ineens een Hoge Raad combinatie die het toch weer anders ziet en ze moeten gewoon beter opletten, toedeledokie en we draaien de boel terug. Dat is niet wat ik ervaren heb of de mensen ook ervaren hebben. Dat zie je ook in aangiftes terug, die zeggen gewoon ik ben gewoon opgelicht. Dat is het rechtsgevoel. Wat daar gebeurt, je ziet het dus de laatste jaren professioneler en doortrapter geworden, dat past daar ook wel bij. Ik vind het niet zo gek dat de wetgever dan

zijn verantwoordelijkheid neemt en zegt van we vullen het zelf in. Ik ben er wel blij mee, het maakt de zaken wel wat makkelijker. Ook om andere redenen. Dat je niet meer om getuigenverzoeken heen kan om al die aangevers te horen. De processen-verbaal zijn nog steeds matig van kwaliteit. Dus daar kom je als rechter bijna niet onderuit en dat maakt de doorlooptijd van die zaken, dat gaat waarschijnlijk buiten bereik van je scriptie, wel heel erg lang. Het zijn ook hele bewerkelijke zaken daardoor voor rechters en de rechtspraak. Als het gaat om normhandhaving, natuurlijk niet zo'n gelukkige kwestie. De jongens kunnen best heel lang doorgaan en dat rechtssysteem neemt wel erg de tijd. En ja je ziet ook nog steeds een juridisch probleem met benadeelde partijen enzo. Het is in aard een delict dat veel slachtoffers kan maken.

Ik: maar wat ik heb gelezen in de MvT is dat er een bewijstechnisch probleem zou zijn waardoor ze die nieuwe strafbaarstelling invoeren. Maar ziet u dat probleem dan in de huidige rechtspraak van de laatste tijd minder terug? Ook met het bewijzen van de valse hoedanigheid?

Zowel de oplichtingsmiddelen als het bewegen tot, die twee begrippen worden ruimer uitgelegd dan vijf jaar geleden zeg maar gebruikelijk was. En daarop wordt het wat betreft de bewezenverklaring minder prangend. Het probleem van hoe rechters ermee om moeten gaan, dat blijft echter nog wel steeds problematisch. We hadden laatst een zaak daarin waren 90 slachtoffers. Alleen al in het dossier dat wij hadden. Waarschijnlijk waren er nog oneindig veel meer. Maar als je dan ziet, dat levert een arrest op van 40 kantjes. Iedereen die schade heeft geleden en zich wil stellen, die moet ook in zo'n dagvaarding terechtkomen, want anders kan je dat niet als slachtoffer aanmerken. Dus dat betekent dat dat soort delicten, en dat is typisch natuurlijk aan computerdelicten, wat snel veel slachtoffers kan maken, dat dat eigenlijk niet zo goed meer in ons systeem past. Het moet op de dagvaarding, anders kun je iemands schadevergoeding niet vergoeden, maar als het op de dagvaarding komt dan krijg je dus in feite 80 tot 100 zaken. Allemaal met mogelijk ook getuigen horen en onderzoek en een dossier en ja dit betekent dat er weer specifiek extra tijd voor moet worden ingeruimd om dat in het systeem te krijgen. Die tijd is maar beperkt beschikbaar. De handhaving komt daarmee in het gedrang. Dat miste ik wel nog een beetje in de hele wetsgeschiedenis van dit onderdeel van WCC III. Namelijk hoe gaan we nou met dit soort zaken, van wat ik dan noem massacriminaliteit, dan eigenlijk om. Dat zal voor toekomst steeds meer een probleem worden. Ook met phishing enzo. Dat soort delicten gaat heel snel veel slachtoffers brengen, daar zijn we eigenlijk niet op gebouwd. We zijn gebouwd op de manier met de marktkraam die iemand oplicht. Maar we zijn niet gemaakt op de digitale marktkraam, die in een keer duizend mensen aanschrijft of honderdduizenden.

Ik: maar dat lost in principe het nieuwe wetsvoorstel ook nog niet op? Of wel?

Nee, maar ze hadden wel zoiets van ja we moeten gewoon iets gaan bedenken misschien maar ook. Dit maakt het misschien ietsje makkelijker, als de Hoge Raad ook eens ietsje soepeler wordt. Je kan nu ook anders ten laste leggen. In feite ging het erover of iemand was bewogen en nu gaat het erom of de verdachte heel vaak iets aangeboden heeft en niet heeft geleverd. Dat is een ander perspectief op de zaak. Dus dat is een wat andere eis aan de bewijsvoering. Dus dat maakt het in geschil wat makkelijker. Dat de zaken misschien wat sneller door het systeem kunnen gaan.

Ik: maar ziet u ook knelpunten in de nieuwe strafbaarstelling? Daar kan in principe ook tegenaan gelopen worden, waar bij de huidige strafbaarstelling geen sprake van was.

Het probleem dat we nu hebben, even los van de technische juridische bewijsvoering, is natuurlijk de feitelijke bewijsvoering. Dat zijn de oorzaken geplaatst vaak op digitale platforms of de koopplatforms. Vaak is het niet zo heel erg moeilijk om die gegevens terug te geleiden tot een plek, of een IP, of een server, maar in het strafrecht gaat het niet over apparaten, gaat

het niet over gegevens. Dat gaat over personen. Het aanplakken van wie heeft nou de boel geüpload. Vaak zijn het wel andere mensen die de cash out doen. Dus die eigenlijk de boel witwassen en doen verdwijnen. Dat is niet altijd dezelfde persoon als de mensen die de advertenties hebben geplaatst. Vaak zijn dat losse samenwerkingsverbanden. Dat probleem, dat blijft. Dat wordt eigenlijk steeds lastiger. Die jongens worden steeds knapper om hun identiteit te verbergen. Dat gaat het dus niet oplossen. Ik verwacht dat we een systeem hebben, Marktplaats is natuurlijk ook wel echt bezig de laatste tijd zoals ik al zei: als het vertrouwen in hun platform afneemt omdat mensen denken dat er alleen maar oplichters rondlopen, dan verdienen ze ook niks meer. Ze worden makkelijker met het verstrekken van gegevens, dus je komt nu wel veel makkelijker bij IP's enzo uit waar een meneer of mevrouw aan geplakt kan worden. Wie was dat nou? Je kan niet automatisch zeggen: degene die het geld uit de automaat heeft getrokken, zal ook wel degene zijn geweest die die oplichtingshandeling heeft gepleegd. Alleen het geld ophalen is natuurlijk nog geen oplichting plegen. Waarschijnlijk wel witwassen of misschien zelfs medeplichtigheid van oplichting, maar het is niet helemaal hetzelfde. Dus dat probleem blijven we wel houden. Dat lost de nieuwe strafbaarstelling niet op.

Ik: Dus als ik het goed begrijp dan ligt het probleem meer bij de persoon die het heeft gedaan, dan dat bewezen kan worden of sprake is van oplichting?

De laatste tweeëneenhalf jaar, bij de overgrote meerderheid van de uitspraken zie je nu een ruimere lijn. Daar hoort nog alles bij van dit voorgedaan, valse naam, valse locaties, valse bedrijfsnaam, btw, valse waarmerken, je hebt gecorrespondeerd en hij heeft ook nog eens voorgedaan van het is al weg. Het hele plaatje bij elkaar wordt dan een beetje een soort van samenweefsel van verdichtsels of listige kunstgrepen, de andere twee oplichtingsmiddelen. Maar dat lukt wel, maar de bewijsvoering wordt lastiger op het vlak van hoe krijg ik deze meneer, het zijn meestal meneren, hoe krijg ik die bij deze handelingen. Dat zijn vaak een heleboel omstandigheden die ze verdacht maken, maar het harde bewijs is nog niet altijd zo makkelijk te leveren. Een goed crimineel tegenwoordig, die zorgt dat hij z'n spullen heel snel weggooit. Je hebt natuurlijk ook tegenwoordig goedkope gsm's en weg bewijs. Dat wordt wel een ding. Dat lossen we denk ik niet zo heel erg makkelijk op. Dus daar ligt denk ik ook nog steeds een taak voor de platforms zelf. Dit zijn zaken die kan je niet alleen maar met repressief strafrechtelijk toezicht aanpakken. Ook aan de provinciekant moet echt hard gewerkt worden. Persoonlijk vind ik dat Marktplaats dat veel te veel heeft laten liggen met hun Albert Heijn verhaal.

Ik: Wat vindt u dan dat zij voor verantwoordelijkheid moeten nemen daarin?

Er zijn technieken, algoritmes om gossomode een beetje te screenen van wie biedt wat aan, zijn we de persoon al vaker tegengekomen, zijn we het IP-adres al vaker tegengekomen of device nummers vaker tegengekomen. Zij kunnen daar algoritmes op loslaten en Marktplaats heeft natuurlijk hele geavanceerde algoritmes, daar kan je wel wat informatie uit halen. Ik denk dat ze ook hier en daar wel eens wat guller mogen zijn met er zelf achteraan gaan en verstrekken van data van mensen die geplaatst hebben. Persoonlijk vind ik dat als je dit soort platforms aanbiedt, dat je ook een verantwoordelijkheid hebt dat het een beetje netjes loopt. Je hebt enige verantwoordelijkheid. Naarmate je ook meer middelen hebt en mensen minder andere middelen, wordt je verantwoordelijkheid ook wat groter. Maar de markt heeft ze nu ook een beetje gedwongen, hopelijk helpt dat wat. Maar ja, mensen zullen op een gegeven moment ook iets beter moeten opletten. Dat gebeurt ook wel. Maar dat kan ook makkelijker gemaakt worden met nog meer banners van deze meneer is al gemeld als verdachte. Ik denk dat je jongens dan makkelijker uit de markt drukt. Ze zijn ook slim he. Ze uploaden vaak op vrijdagmiddag en dan de maandagochtend zijn ze weg. Dat zijn inderdaad technieken. Maar daar zou je voor een groot deel ook techniek tegenover moeten stellen en we moeten inderdaad de mensen ook een beetje opvoeden. Als het te mooi is om waar te zijn, dan is het te mooi om waar te zijn. Dus dan moet je ook een klein beetje opletten, maar soms zijn ze

super doortrapt. Nepsites die lijken op echte sites. Dat is net even anders dan de echte Marktplaatsfraude. Dat mensen daarin trappen, dat is volstrekt begrijpelijk.

Ik: komt u dat meer tegen dan Marktplaatsoplichting?

Marktplaatsfraude zien we vaker, omdat de drempel voor aangifte natuurlijk ook vrij laag is. Die websites zien we ook wel. Sites waarop elektronica 20% goedkoper wordt aangeboden. Binq volgens mij, die site was één op één aangebouwd. Die jongens hadden hun beveiliging niet op orde, dus die merkte het zelf pas na het weekend. Die zien we ook. Wel minder moet ik zeggen. Maar mijn zorg en van een aantal van mijn collega's is dat dat meer is dan wat de politie eigenlijk ziet, dan dat het niet gebeurt. Marktplaatsfraude, een niet al te domme rechercheur, die een beetje wordt aangestuurd vanuit het meldpunt, die kan daar nog wel wat mee. Maar als het wat ingewikkelder wordt, wordt het lastig. Het is natuurlijk geen enkel probleem om te achterhalen waar die website vandaan komt, maar plak er maar weer een mannetje aan. Er worden vaak ook jongens vanuit Rusland erop gezet, daar zitten de techneuten, die krijgen de instructies vanuit Nederland hoe het er uit moet zien. Die krijgen aangeleverd van zo ziet het er uit, maak maar één op één na. En die russen maken de website na. Van de russen medewerking, no way. Dat hoef je niet eens op papier te zetten zo'n rechtshulpverzoek. Dat is zonde van je tijd.

Ik: zou het onderzoek in een geautomatiseerd werk, de nieuwe opsporingsbevoegdheid, dat probleem kunnen oplossen?

Ik denk dat je wel verder komt in de lijn. Dat je verder kan komen dan nu. Omdat je ook streaming data een tijdje kan opvangen. En dat zegt vaak wel iets over identiteit. Het verleden kunnen ze afschermen, kunnen ze zelfs deleten, maar zegt niet altijd wat. Maar stromende data opvangen, mensen laten daar vaak toch wel wat zien van geografische locaties, soms ook mailachtige berichten waar je toch identiteiten aan kan koppelen of in ieder geval identiteiten van degene aan wie het geadresseerd is. En daar kan je vaak toch dan net vernauwen en dan uiteindelijk bij een persoon terechtkomen. Dus ik denk dat de bevoegdheid wel gaat helpen. Daarnaast zal die bevoegdheid ongetwijfeld ook wel gebruikt gaan worden om sites te blokkeren.

Ik: Wat is uw eigen mening over die bevoegdheid?

Dat is altijd moeilijk te vragen aan rechters die die zaken zelf gaan beoordelen.

Ik: misschien dat het te ver gaat, maar meer van dat er natuurlijk de discussie is geweest dat de bevoegdheid een inbreuk op grondrechten maakt. Maar denkt u dat het opsporingsbelang prevaleert boven het belang van de grondrechten op dit gebied. Of dat het zo beveiligd is omdat er eerst een machtiging van de rechter-commissaris nodig is?

Laat ik het zo zeggen. De oude systematiek van een rechtshulpverzoekje, dat is totaal onwerkzaam gebleken. Dat is volstrekt hopeloos. Tegen de tijd, na zes maanden, dat je zo'n papiertje had, was de verdachte allang weg, verdwenen en veranderd. Dus ik denk inderdaad, wil je enigszins kunnen optreden tegen een brede waaier aan vormen van cybercriminaliteit, dat zo'n bevoegdheid op zich onmisbaar is. De vraag is alleen een beetje van waar leg je de drempel voor de inzet en hoe controleer je de uitvoering. Nou die drempel voor inzet is redelijk hoog gelegd uiteindelijk. Wat ook wel meevalt als je goed naar het wetboek kijkt hoeveel er wel onder valt, maar goed het is niet helemaal voor de kleinste winkeldiefstallen. Daar is in ieder geval in zekere mate nog wel over nagedacht. Daar is in de rechtspraak ook al wel wat over gezegd. Het tweede is de controle. Dat blijft een heel zwak punt. Een rechter-commissaris aan het begin van het onderzoek, weet gewoon vaak weinig, de politie weet ook nog maar weinig. Er is wat gebeurd en we willen wel weten wat, maar heel veel meer weet je vaak ook niet. Je kan eigenlijk nog niet zo heel veel beoordelen. Dus de neiging om te zeggen van nou

ja, zeker als het wat zwaardere delicten zijn, van ga je gang maar is natuurlijk best wel groot. Dat hebben we bij de telefoontap ook gezien. Dat zou nog niet zo erg zijn als vervolgens de controle achteraf heel sterk zou zijn. Als er een ding opvallend is voor het zwaardere segment van cybercrime is: wel strafbare feiten, maar heel weinig verdachten en nog veel minder strafzaken. Zonder zo'n verdachte kan dus die controle achteraf op de zitting eigenlijk van wat is er gebeurd niet plaatsvinden. Dus je creëert eigenlijk een heel veld van inzet van bevoegdheden die eigenlijk achteraf nooit meer worden gecontroleerd of dat eigenlijk wel klopt wat gedaan is, of dat wel goed is uitgevoerd, of dat wel binnen de kaders is gebleven. Als rechter-commissaris machtig je feitelijk eenmalig vooraf. Je ziet het dan daarna ook eigenlijk niet meer. Daar hebben we het met elkaar wel over gehad of we daar nog iets in konden voorzien, maar dat is toch wel heel lastig. Misschien moet je dan zo'n soort commissie maken als voor de AIVD geldt. Die gewoon steekproefsgewijs dingen kunnen bekijken en onderzoeken hoe dat gegaan is. Want het is mijn ervaring: alle bevoegdheden die kunnen worden ingezet zonder afdoende controle worden uiteindelijk misbruikt, of ja krijgen een breder gebruik en inzet dan bedoeld. De verdachten gaan meestal ook niet klagen, want ja dan maakt hij zich bekend. Dus de neiging om breed in te zetten, de tap eraf te gooien, noem het maar op, zal heel groot zijn. Er zal niet veel over geklaagd worden door de verdachten en de zittingsrechter ziet die zaken nooit, want ja het probleem is opgelost, de verdachte die gaan we toch niet vinden, dus laat maar zitten. De controle op de inzet dat blijft ook in deze context een heel zwak punt. Ik verwacht zelf dat het over vijf tot tien jaar uit de klauwen gelopen is. Dat is gewoon de aard van het beestje. Ik heb ook tussen die techneuten gezeten in Delft en ik weet hoe dat werkt. Je wil het gewoon oplossen. Net als bij bijvoorbeeld Volkswagen, hebben de opdracht gekregen zorg dat die Volkswagentjes een beetje leuk door de uitlaatgassen test komen en dat hebben ze perfect gedaan. De technische opdracht hebben ze perfect uitgevoerd. Dan zie je ook, zit de jongens dwars en wees daar slim in. Dat doen ze dus. Maar of dat eigenlijk dan nog binnen het bredere rechtmatigheidskaders valt, ja daar is vanuit die organisatie zelf en de manier van denken niet heel veel aandacht voor. Ik heb groot respect voor veel jongens bij KLPD die digitaal onderzoek doen op zeer hoog niveau. Maar het juridisch bewustzijn is heel gering. Het zijn techneuten die achter de boeven aangaan. Het is fantastisch wat ze daar bedacht hebben, maar of dat nou eigenlijk wel mag, dat kan ze niet boeien. Dat zit er niet in. Dat is de aard van het technische beestje is mijn ervaring wel. Of het allemaal in rechterlijk plaatje past, dat zoeken anderen wel uit. Dat zit niet in het systeem zelf, dus dat moet je extern aanbrengen.
De controle vooraf voor dit type dingen, daar zie ik een lacune, daar zie ik echt een gat. En de toetsing van de inzet achteraf is eigenlijk nog inconsistenter, zal blijken in heel veel zaken.

Ik: maar dat zijn dan die zaken waarbij geen verdachte is? Maar die komen dan niet allemaal bij de rechter terecht?

Ja inderdaad en dat zijn er heel veel. Nee juist niet.

Ik: nee oke, dan heb ik het goed begrepen. En stel dat er een zaak wel bij een rechter terechtkomt, is het dan al mogelijk om goed te controleren of dat die opsporingsbevoegdheid juist is ingezet?

Jawel, wij mogen alles vragen. Het hangt ook een beetje af van het verweer dat wordt gevoerd. Nou is de advocatuur ook niet over de hele breedte even goed ingevoerd in dit soort onderwerpen, maar er zitten echt wel een paar slimmerds tussen en die beginnen daar dan over. Welke middelen ze hebben ingezet, was dat wel, staat dat technisch hulpmiddel wel op lijst X, was dat wel gekeurd. Nou ja je moet erover beginnen. Als zij dat opwerpen, ja je moet natuurlijk eerst de feiten wel even vaststellen. Je wil weten wat is er precies gebeurd. Maak maar een verbaal op, laat maar zien, zijn er nog loggegevens. Nou ja daar is juridisch natuurlijk ook wel weer iets over te zeggen. Is er gelogd en waar staat dat. En dan hopen dat ze het niet allemaal kwijt zijn. De politie heeft op dat vlak niet een hele goede reputatie. Maar ja je probeert eerst vast te stellen wat is er precies gebeurd. Ja, dan zeg je gewoon ben je binnen de kaders

gebleven en dat zou ook in extreme gevallen kunnen leiden tot een beslissing over de ontvankelijkheid, over toelaatbaarheid van bewijs, strafvermindering, de bekende vormfouten discussies en de gevolgen. Dus dat kan wel, maar op zitting. En ja het is eigen aan veel van dit soort zaken dat ze niet op zitting komen. En dat is iets wat ook in de wetsgeschiedenis onvoldoende onderkend is. We hebben daar wel iets over gezegd in een van onze commentaren aan de minister. Dat het onze zorg is dat normhandhaving bij de inzet niet voldoende afgedicht is. Maar dat is dus wat ontbreekt. Maar nogmaals, ik vind het drempelniveau niet zo slecht. De machtiging vooraf door de rechter-commissaris dat werpt ook wel een hobbeltje op tegen al te lichtvaardige inzet, maar je moet je van de materiële toetsing door de rechter-commissaris niet al te veel voorstellen. En toetsing achteraf is toch wel het zwakke punt in de regeling.

Ik: met het wetgevingsadvies van de raad voor de rechtspraak (mede opgesteld door u) is niet veel mee gedaan?

Nee, maar dat is, dan heb je weer een commissie weet je wel kost dat allemaal geld en vertrouwen de politie niet. Dijkhof is natuurlijk ook een slimme staatsecretaris. In de kamer kreeg hij weinig tegengas. Hij heeft het er vrij soepeltjes doorheen geloosd. Dus we moeten even kijken. We beginnen eigenlijk aan iets nieuws. Ik denk dat Kamerleden ook moeite hadden zich voor te stellen wat gaan we hier nou eigenlijk doen. Dat ze dan ook nog niet helemaal zien van waar het ook hier natuurlijk mis kan gaan. Ik hoop alleen dat het niet al te veel schandalen gaat geven. Dat het hele computers van alle zalen leeg trekt ofzo. Dat is denk ik het zwakke punt van de regeling. Ik denk zelf dat het met de inzet van de bevoegdheid deels nog wel gaat meevallen, ze hebben gewoon de capaciteit niet. Je moet mensen hebben die weten wat ze doen, die de datastroom kunnen verwerken. Als je ziet hoe weinig echte digitale recherche van dat niveau er in de uitvoerende dienst is. Ze zijn al ongeveer een derde of zelfs meer van hun tijd kwijt aan het uitvoeren van buitenlandse rechtshulpverzoeken over gegevens die op Nederlandse servers staan. Ik denk dat het wel voor een aantal grote spraakmakende zaken zal worden ingezet. Maar dat het niet een hele brede toepassing zal gaan krijgen. En als dat het wel is, dat het dan heel lang duurt voordat we daar iets van gaan horen. Omdat er gewoon geen belanghebbenden zijn die erover gaan klagen.

Ik: deze bevoegdheid zou eigenlijk goed gebruikt kunnen worden voor het opsporen van bijvoorbeeld internetoplichting?

Zou ook kunnen. Ja, je kan eigenlijk makkelijker bij alle computers die mensen hebben gebruikt om cyberdelicten te plegen. Niet alleen Marktplaatsfraude, maar eigenlijk alles, ook die phishing. Je kan dieper in de systemen, je kan volgen wat het systeem doet. Daardoor kom je veel dichter bij de mensen. En het gaat vooral om de identificeerbaarheid van mensen. Want men weet vaak wel van welke computer of wat voor IP-adres het afkomt, maar verder kom je dan niet. Want daar gaat het in de opsporing om, tenminste, daar ging het in de strafrechtelijke opsporing altijd om. Er zijn geluiden, en niet van de minste, uit het opsporingsland die zeggen we moeten ophouden met opsporen klassieke manier. We moeten van vervolgen naar verstoren. We moeten gewoon blokkeren, we moeten onklaar maken, zodat iets niet meer functioneert en laat die vervolging maar zitten. Daar is dit middel op zich ook wel geschikt voor. Maar het is de vraag of we dat moeten willen.

Ik: u geeft aan dat u zelf ook zaken met betrekking tot Marktplaatsoplichting hebt behandeld. Wat ziet u het meeste terugkomen of naar voren komen in die zaken?

Nou, wat me eigenlijk het meeste opvalt, is de verschuiving in de verdachtesfeer. In het begin waren het redelijk handige jongetjes die vrij handig waren met computers en nu zijn het echt gewoon straatbendes die in het internetcafé in het weekend hun slagje slaan. Dus de drempel om dit delict te plegen die lijkt lager te liggen. De hele pientere nerds die je eerst had, die zien

we niet meer. We zien nu gewoon straatschoffies. Het is makkelijker voor ze geworden. Dat valt nog het meeste op.

Ik: Als ik het goed begrijp, jullie zijn de experts op dit gebied en jullie proberen te zorgen voor meer eenheid in de rechtspraak op dit gebied?
Nou, die formele functie hebben we niet. Want nogmaals elke rechter beslist uiteindelijk in zijn eigen zaak. Wat wij wel doen is jurisprudentie verzamelen, de gedachte verzamelen hoe ze in de wetsgeschiedenis duiden over dit soort dingen. Kijken of je vergelijkingsmateriaal uit andere oplichtingsvelden erbij kan pakken. Met mensen erover praten, want sommige collega's voelde ook wel ja dit valt gewoon heel slecht bij de burger. Die gozer belazert bewust de boel en hij loopt lachend weer naar buiten en mensen zijn hun geld kwijt. Dan wordt er gezegd, moet je maar niet zo dom zijn, maar je kan ze wel een ander perspectief voorhouden. Een andere redenering voorhouden. Kijk wat ze dan kiezen is nogmaals aan hen. We kunnen niks voorschrijven. Je kan wel zeggen van ja dit is er ook over te zeggen. Met enige kracht van overtuiging, dan neemt die overtuiging vaak ook toe. Zo werkt het meer. Het is meer een vorm van onderop dan van bovenaf. Het is heel casuïstisch wat de Hoge Raad allemaal doet. Die beoordeelt alleen maar of het begrijpelijk is wat een hof heeft gedaan en of het in strijd is met het recht. Maar er zullen nog wel grensgevallen komen. De Hoge Raad zal het dan waarschijnlijk wel wat lastiger gaan vinden. Als jij onder je echte naam een iPhone aanbiedt voor €300,00 en jij levert hem niet, dan is dat natuurlijk niet per definitie oplichting.

Ik: maar dat zou in principe die nieuwe strafbaarstelling dan wel kunnen oplossen?

Ja, als dat een aantal malen achter elkaar gebeurt, en je hebt ook de bedoeling gehad om te leveren. Wat heb je ingekocht, daar is natuurlijk onderzoek naar te doen. Het begint al met dat heel veel mensen aangifte doen: ik heb iets gekocht en dat is niet geleverd. Dus je hebt het bewijsvermoeden al tegen. En als je dan niks uitlegt, dan mag de rechter daaruit de conclusie trekken dat dit opzettelijk voortdurend is gedaan. Maar je kunt ook zeggen: ja ik wilde wel leveren, maar de leverancier bleef in gebreke, daarom kon hij ook niet leveren. Dan heb je de vraag van had iemand opzet op die gedraging, want feitelijk heeft hij stelselmatig niet geleverd, maar had hij ook de opzet daarop? Dat hangt er vanaf hoeveel hij hard kan maken over die bestellingen. Als die er nooit zijn geweest, ja hallo. Dus zo kan dat schuiven al naar gelang de positie die die procespartijen innemen. Maar het blijft lastig. Ik denk dat het meest rendeert aan inzet aan de provincie kant. Slimme algoritmes inzetten om de foute jongens eruit te halen. Ook bij Marktplaats in het weekend mensen op de veiligheidsafdeling. Daar moeten ze echt nog van leren bij Marktplaats. Het gaat beter, maar ze kunnen nog wel stapjes maken. Dat zal voor meer platforms gaan gelden. Mensen moeten ook opgevoed worden. Niet gaan kopen bij sites die niet aan eisen voldoen. Maar er is wel meer aan te doen. Aan de opsporingskant, ze pakken er een paar, maar het zijn moeilijk bewijsbare zaken. Plak er maar achter, degene die zijn advertentie plaatst die heeft het geld niet gehaald. Als iemand anders dan dat geld haalt, die oplichting waarbij geld is afgegeven, heeft die dan medegepleegd, was hij medeplichtig omdat hij een middel ter beschikking heeft gesteld. Begreep hij helemaal niet dat het oplichting was en heeft hij alleen maar een advertentie gezet en dacht hij dat de ander gewoon ging leveren? Dat is allemaal nog niet zo heel erg makkelijk. Wat is nou ieder zijn rol. Daarop merken we wel dat het recht op dit moment erg achter de veranderende samenleving aanhobbelt. Onze samenleving is steeds meer horizontaal en daar kunnen we met de verticale juridische begrippen als medeplegen, daar heb je alles gedaan, en als medeplichtige heb je een stukje gedaan, daar kunnen we eigenlijk niet zo veel mee. Dat zijn allemaal wel onmisbare onderdelen van een bepaalde keten, maar je kunt niet zeggen dat degene aan het einde van de keten ook volledig verantwoordelijk is voor wat in het begin gebeurde. Vaak worden andere mensen, bijvoorbeeld russen, betaald om een productje te maken die niet in verhouding staan tot de opbrengsten.

De mensen bij het LMIO doen echt ongelofelijk hard werk, met hele knappe analyses vaak ook, maar vervolgens moet een regionale eenheid het oppakken en die moet er mee aan de

slag. Die moet mensen gaan aanhouden en verhoren. Dat krijgt prioriteit 0. Geen bloed, alleen maar geld. Het komt onderop de lijst. En ook het computersysteem is zeek sterk verouderd. Dus daar loop je ook tegen heel veel beperkingen aan. Wij hebben geklaagd op een gegeven moment over de processen-verbaal. Dat voor het bewijs van bewegen tot en de oplichtingsmiddelen vaak onvoldoende feitelijke informatie aanwezig was. Toen zijn wij daar geweest. Waarom vraag je niet aan de mensen een vraag. Waarom heeft u bij deze website besteld. Dan kunnen ze precies vertellen waarom ze dachten dat hij eerlijk was en dat is precies wat ik wil weten. Toen kregen we het gortdroge antwoord dat wat we nu in het systeem hebben is alles wat er in kan. We hebben gewoon geen enkele capaciteit meer om zo'n vraag ook te stellen. De politie is weinig gelukkig met zijn investeringen in de ICT. Verkeerde prioriteiten, verkeerde spullen en verkeerde mensen.
Ik denk dat het van de provincie voor het grootste gedeelte moet komen. Elk jaar pakken we een paar van die jongens waar wel een zaak tegen kan worden opgebouwd, maar dat zal steeds moeilijker worden omdat die jongens steeds beter hun identiteit gaan afschermen. We komen er gewoon niet meer bij. Dan komt het dus neer op toch een beetje die bedrijven opvoeden en de burgers een beetje opvoeden. Daar zullen mensen aan moeten wennen.

Ik: dus u bent eigenlijk van mening dat het probleem alleen maar groter wordt en niet dat het opgelost wordt?

Naarmate steeds meer transacties digitaal zullen gaan, ook aankopen digitaal zullen gaan, zal misdaad het geld volgen. Als het geld digitaal gaat, gaat de misdaad digitaal. Dat is onontkoombaar. Dat is de aard van het beestje.
De echte Marktplaatsfraude is in de termen van fraude toch een beetje kruimelwerk. Deze vorm van criminaliteit kan niet anders dan toenemen. Daar kan strafrecht maar heel beperkt tegengas tegen bieden. Daar moet de provincie in het beeld komen. Tenminste dat is mijn persoonlijke overtuiging.

Ik: Hoe bedoelt u dat, dat het uit de provincie moet komen? Wat moeten zij dan doen?

Nou ja, een betere bewaking op je systeem. Sneller eventuele aanwijzingen van misbruik en oneigenlijke gebruik bij fraude doorzetten naar die website, die mensen eraf flikkeren, waarschuwingen bij producten zetten, dat soort dingen. Het mensen makkelijker maken ook. Dus als zo'n persoon weer op popt met een nieuwe advertentie dat hij een banner erbij krijgt: pas op er zijn al klachten over deze man. Dan doe je wat. Misschien moet Marktplaats ook maar eens wat meer gaan nadenken over psychologie. Met extra knoppen waarop staat wilt u de verkoper nog een keer controleren. Er is weinig affiniteit met dit onderwerp onder rechters.