Aruba: one hacking island?
Bijzondere opsporingsbevoegdheden in een digitale omgeving

Erik Witjens

1. Inleiding

Als men vijfentwintig jaar geleden als bezoeker de binnentuin van de Universiteit van Aruba was binnengewandeld, dan was men waarschijnlijk – en niet anders dan nu – aangenaam verrast geweest door de sfeervolle omgeving die de tuin biedt aan de studenten en medewerkers van de universiteit. Wat echter toen niet, maar nu wel tot de mogelijkheden behoort, is om via het Wi-Fi netwerk een draadloze verbinding tot stand te brengen met het internet. De technologische vooruitgang heeft, met andere woorden, ook het historische De La Salle-gebouw niet overgeslagen.

Tot voor kort vond die technologische vooruitgang niet veel weerslag in de strafwetgeving van Aruba. Daar is echter recent verandering in gekomen, aangezien het vernieuwde Wetboek van Strafrecht begin 2014 in werking is getreden[1] en enige tijd daarvoor een concept van het herzien Arubaans Wetboek van Strafvordering (verder: concept-ASv) aan de Minister van Justitie is aangeboden.[2] In dit laatstgenoemde concept-wetboek heeft een opvallende bevoegdheid een plaats gekregen: de bevoegdheid voor opsporingsambtenaren om op afstand binnen te dringen in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager en daarin onderzoek te doen (art. 168a concept-ASv).[3]

De Memorie van Toelichting van het Nederlandse wetsvoorstel waaruit deze bevoegdheid overgenomen is (waarover later meer), neemt tot uitgangspunt dat het niet noodzakelijk is om de verhouding tussen de bevoegdheden rond de doorzoeking ter vastlegging van gegevens en de bijzondere bevoegdheden tot

---

1 Het nieuwe Wetboek van Strafrecht is op 15 februari 2014 van kracht geworden, zie het Landsbesluit van 14 februari 2014 no. 1, houdende inwerkingtreding van het Wetboek van Strafrecht van Aruba, *AB* 2014, no. 12.

2 Het concept Wetboek van Strafvordering zoals dat is aangeboden aan de Minister is gepubliceerd: H. de Doelder e.a. (red.), *Caribisch Wetboek van Strafvordering. Concept*, Oisterwijk: Wolf Legal Publishers 2013 (verder: Concept Wetboek 2013). De auteur maakt deel uit van de gezamenlijke Commissie voor herziening van het Wetboek van Strafvordering voor Aruba, Curaçao en Sint Maarten, waarin het in deze bijdrage te bespreken wetsvoorstel is doorgevoerd.

3 De bevoegdheid is gelet op het gezamenlijke wetgevingstraject dus ook voor Curaçao en Sint Maarten voorgesteld. Hetgeen in deze bijdrage wordt opgemerkt, zal ook voor die landen relevant kunnen zijn.

opsporing te herzien, maar te volstaan met een aanvulling van de bestaande bevoegdheden.[4] De bedoeling van dit artikel is om een inschatting mogelijk te maken of de voorgestelde bevoegdheid, ook wel kortweg aangeduid als de 'hackbevoegdheid' voor de politie, een meerwaarde zal kunnen vormen voor het Arubaanse (en Nederlandse) wetboek. Met het oog daarop schets ik allereerst de redenen die aangedragen worden om de bevoegdheid in te voeren. In paragraaf 3 ga ik vervolgens in op de kern van de voorgestelde bevoegdheid, waarna in paragraaf 4 de verhouding met de bestaande bijzondere opsporingsbevoegdheden aan bod komt. De vijfde paragraaf besteedt aandacht aan de verhouding van strafvorderlijke opsporingsbevoegdheden tot de digitale omgeving van computernetwerken, hetgeen leidt tot kanttekeningen bij de wijze van codificatie van de voorgestelde bevoegdheid. Een aantal opmerkingen dat specifiek de kleinschalige rechtsorde van Aruba (en Curaçao en Sint Maarten, gelet op het gezamenlijke wetgevingstraject van het wetboek) betreft, heeft een plek gevonden in paragraaf 6 en het artikel wordt afgesloten met een korte slotbeschouwing.

2. Redenen voor invoering van de 'hackbevoegdheid'

Het binnendringen in een geautomatiseerd werk[5] is opgenomen in het Arubaanse concept-ASv naar aanleiding van het Nederlandse concept-wetsvoorstel Computercriminaliteit III, dat de bevoegdheid in art. 125ja NSv voorstelt. Dat (overigens ruimere)[6] concept-wetsvoorstel was dusdanig spraakmakend, dat het zelfs buiten het Koninkrijk door de media werd gemeld.[7] Ten tijde van het schrijven van deze bijdrage is het Nederlandse voorstel net naar de Raad van State gezonden voor advies.[8] In het onderstaande zal ik uitgaan van de Arubaanse regeling, die voor wat betreft de hackbevoegdheid grotendeels gelijk is aan het in Nederland voorgestelde art. 125ja NSv. Ik zal daarbij echter gebruikma-

---

4 MvT bij het Nederlandse concept-wetsvoorstel Computercriminaliteit III (verder: MvT), p. 14. Te vinden op: http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/02/memorie-van-toelichting-wetsvoorstel-versterking-aanpak-computercriminaliteit.html.

5 Ik zal zowel 'bevoegdheid tot binnendringen in een geautomatiseerd werk' als 'hackbevoegdheid' gebruiken en doel daarmee steeds op de bevoegdheid van art. 168a concept-ASv.

6 Het Nederlandse voorstel behelst ook aanpassingen in het Wetboek van Strafrecht en een zogeheten decryptiebevel, dat onder omstandigheden zelfs aan de verdachte gegeven kan worden. Deze onderdelen zijn echter niet overgenomen in het Arubaanse concept-ASv, c.q. ASr.

7 BBC News 'Dutch police may get right to hack in cyber crime fight', http://www.bbc.co.uk/news/world-europe-22384145 (laatst bezocht op 20 februari 2014).

8 Persbericht Ministerie Veiligheid & Justitie, 25 februari 2014, http://www.rijksoverheid.nl/ministeries/venj/nieuws/2014/02/25/opstelten-investeert-in-bestrijding-computercriminaliteit.html (laatst bezocht op 3 maart 2014).

ken van de Memorie van Toelichting bij het *Nederlandse* concept-wetsvoorstel (verder: MvT), aangezien deze veel completer is dan de Arubaanse toelichting.[9] Waar in deze bijdrage gesproken wordt van 'MvT' gaat het derhalve om de *Nederlandse* MvT, behalve waar uitdrukkelijk vermeld wordt dat het de Arubaanse Memorie van Toelichting betreft.

De Arubaanse toelichting gaat overigens niet in op de vraag, waarom er voor gekozen is deze bevoegdheid uit een Nederlands *concept*-wetsvoorstel over te nemen. Dat verbaast, omdat het kennelijk om een ingrijpende bevoegdheid gaat waarvan het nog te bezien valt of de Nederlandse tegenhanger inderdaad in deze vorm gehandhaafd zal blijven.[10] Dat gezegd hebbende, is het interessant om te kijken welke redenen de Nederlandse Memorie van Toelichting noemt ter adstructie van de noodzaak tot invoering van een hackbevoegdheid.

Volgens de Memorie van Toelichting voorziet het concept-wetsvoorstel in een leemte in de bestaande wettelijke bevoegdheden en sluit het aan bij de snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit.[11] De Memorie van Toelichting bespreekt een aantal ontwikkelingen die deze stellingen moeten staven.

Als eerste wordt de versleuteling van communicatie genoemd. Omdat, aldus de Memorie van Toelichting, steeds meer communicatie versleuteld is, is in steeds minder gevallen de met een internettap (art. 126m NSv) afgetapte communicatie leesbaar voor de opsporingsautoriteiten. Daarom heeft de opsporing dringend behoefte aan de mogelijkheid om communicatie te onderscheppen 'voordat deze wordt versleuteld of nadat deze is ontsleuteld'.[12] De Memorie van Toelichting schetst hier met wat grove streken het probleem, hetgeen spijtig is omdat de werkelijke situatie genuanceerder ligt.[13] Hieronder zal ik dieper ingaan

---

9 De gepubliceerde Memorie van Toelichting bij het Arubaanse art. 168a concept-ASv is een sterk ingekorte versie van de MvT van het Nederlandse concept-wetsvoorstel, zie Concept Wetboek 2013, p. 395-401. Omdat de Arubaanse bevoegdheid rechtstreeks is overgenomen uit het Nederlandse concept-wetsvoorstel is er, mede gelet op wat er wél bij het Arubaanse artikel 168a concept-ASV is opgemerkt, geen reden om aan te nemen dat men heeft willen afwijken van de uitgangspunten van het Nederlandse concept-wetsvoorstel. Onduidelijkheid bestaat wel ten opzichte van enige waarborgen die de Nederlandse MvT bespreekt, maar in de Arubaanse MvT ontbreken. Zie daarover paragraaf 6.

10 Het concept-wetsvoorstel was in Nederland ten tijde van het aanbieden van het Arubaanse concept-wetboek van Strafvordering op 31 oktober 2013 nog niet eens aan de Raad van State voor advies toegezonden. Dat is echter inmiddels wel gebeurd, zie noot 8.

11 MvT, p. 4, 6.

12 MvT, p. 6.

13 Wellicht is hier debet aan dat de Memorie van Toelichting zich lijkt te verlaten op een enkele publicatie van het WODC: Justitiële Verkenningen 3/12 (WODC), themanummer Tappen en infiltreren (verder: Justitiële Verkenningen).

op deze problematiek, waarbij ik me omwille van de ruimte zal beperken tot versleuteling bij e-mails.[14]

Er is een onderscheid tussen de beveiliging van het communicatieproces door versleuteling en het versleutelen door encryptie van de informatie *zelf*, bijvoorbeeld door de inhoud van e-mails van encryptie te voorzien. In het laatstgenoemde geval hoeft goed beschouwd geen gebruikgemaakt te worden van beveiliging van het communicatieproces zelf, omdat ook als de informatie onderschept wordt, deze onleesbaar is.

De versleuteling van het communicatieproces wordt vrijwel standaard gedaan door gebruik te maken van het *Hypertext Transfer Protocol Secure* (verder: https),[15] dat bijvoorbeeld gebruikt wordt voor internetbankieren. De bedoeling van https is om een beveiligde verbinding te creëren tussen twee computers, waardoor de gegevens in versleutelde vorm uitgewisseld kunnen worden. Deze beveiliging is niet volmaakt. Ten tijde van het schrijven van deze bijdrage is bijvoorbeeld de zogeheten '*heartbleed*' *bug* uitgebreid in het nieuws geweest.[16] Het veel gebruikte Open SSL-protocol, dat de daadwerkelijke encryptie van het in het kader van https kan verzorgen, bevatte gedurende enkele jaren een programmeerfout waardoor versleutelde informatie (waaronder wachtwoorden en creditcardnummers) door kwaadwillenden was te achterhalen.[17] De voorgestelde hackbevoegdheid zou het mogelijk maken om een dergelijke zwakheid in de beveiliging van het internet te exploiteren.

De Memorie van Toelichting stelt: 'Diensten als Gmail en Twitter zijn standaard van versleuteling voorzien en andere populaire diensten zoals Facebook en Hotmail bieden versleuteling als optie aan'.[18] Om misverstanden te voorkomen: het gaat hier om de beveiligde verbinding tussen de gebruiker en de dienst

---

[14] De MvT merkt bijvoorbeeld op dat communicatie die via Skype en WhatsApp verloopt, versleuteld is. Van belang is dat versleuteling, op zichzelf, niet betekent dat de communicatie volledig veilig is, en zeker niet dat de communicatie voor de betreffende bedrijven niet in te zien zou zijn. Zie over de beveiliging van WhatsApp bijvoorbeeld http://fileperms.org/whatsapp-is-broken-really-broken/ (laatst bezocht op 8 maart 2014). Voor Skype: http://www.slate.com/blogs/future_tense/2012/07/20/skype_won_t_comment_on_whether_it_can_now_eavesdrop_on_conversations_.html (laatst bezocht op 8 maart 2014).

[15] Herkenbaar aan het voorafgaan van een webadres door 'https://'. Er is echter een veiliger alternatief, dat nog weinig gebruikt wordt: HSTS. Zie daarover https://www.eff.org/deeplinks/2014/02/websites-hsts (laatst bezocht op 26 april 2014).

[16] Zie o.a. BBC News: Heartbleed bug: What you need to know, http://www.bbc.com/news/technology-26969629 (laatst bezocht op 18 april 2014); New York Times: Experts find a door ajar in an Internet security method thought safe, http://nyti.ms/1qgWWf2 (laatst bezocht op 18 april 2014).

[17] Zie voor een toegankelijke uitleg bijvoorbeeld: http://gizmodo.com/how-heartbleed-works-the-code-behind-the-internets-se-1561341209 (laatst bezocht op 18 april 2014).

[18] MvT, p. 6. De MvT lijkt hier bijna woordelijk J.J. Oerlemans, 'Mogelijkheden en beperkingen van de internettap', *Justitiële Verkenningen* 2012, p. 29 (verder: Oerlemans 2012) te citeren.

als men de betreffende berichten leest op (bijvoorbeeld) www.gmail.com. Dit staat er echter niet aan in de weg dat de informatie zelf na verzending weer in leesbare vorm beschikbaar is. Evenmin doet het er aan af, dat het daadwerkelijk verzenden van de e-mail, van Gmail naar de geadresseerde buiten Gmail, onversleuteld plaatsvindt.[19] Voor het versleutelen van de *inhoud* van e-mails zelf kan men bijvoorbeeld gebruikmaken van programma's als PGP, maar dit is geen standaard bij Gmail, noch de andere aanbieders.

Versleuteling wordt ook steeds vaker toegepast bij gegevensdragers, bijvoorbeeld het opslagmedium van computers (zoals de harde schijf). Dit betekent dat zonder het juiste wachtwoord de gegevens op de gegevensdrager onleesbaar zijn, omdat een dergelijke versleuteling bijna niet te kraken is. Dat heeft gevolgen voor de bruikbaarheid van een inbeslaggenomen harde schijf. Het in beslag nemen heeft in de bedoelde gevallen weinig nut, omdat onderzoek naar de opgeslagen gegevens onmogelijk is. Het onderzoeken van het geautomatiseerde werk zal dan alleen plaats kunnen hebben indien het wachtwoord door de gebruiker is ingevoerd, en de data leesbaar zijn.[20]

Een tweede punt dat de Memorie van Toelichting aanvoert, betreft het gebruik van draadloze netwerken.[21] Als gebruik wordt gemaakt van meerdere netwerken, is de communicatie niet goed aftapbaar, omdat gebruik wordt gemaakt van meerdere aanbieders en de internettap bij een bepaalde aanbieder wordt gezet. Het aftappen van alle aanbieders waarvan de verdachte mogelijkerwijs gebruik zou kunnen maken, is niet goed werkbaar. Dit is een probleem dat ook speelt bij het aftappen van telecommunicatie – niet zelden hebben criminelen een groot aantal telefoons, om het aftappen van hun communicatie te frustreren.[22] Een verschil met het gebruik van telecommunicatie is echter dat op het internet veelal gebruik zal worden gemaakt van communicatiediensten die gebruikmaken van het internet. Denkbaar zou zijn, dat deze diensten (waaronder Whatsapp en Skype) als aangrijpingspunt zouden worden gezien voor het zetten van een tap. Ik kom daar later in deze paragraaf op terug.

Daarnaast wordt in dit kader het probleem aangestipt dat indien achter een internetverbinding een ander netwerk van gebruikers schuilt, niet nagegaan kan worden welke informatie bij welke gebruiker behoort. Dit kan ertoe leiden dat een tap ruimer is dan gewenst; een wegens de proportionaliteit minder gewenste

---

19 Daar wordt namelijk geen https voor gebruikt, maar SMTP. Zie over SMTP bijv. http://www.experts-exchange.com/Networking/Protocols/Email/A_1807-A-CrashCourse-in-Email-SMTP.html (laatst bezocht op 21 april 2014).

20 Met het oog daarop voorziet het Nederlandse concept-wetsvoorstel in een wijziging van art. 125k lid 3 NSv, waarin de mogelijkheid wordt geschapen een decryptiebevel aan de verdachte te geven. In het Arubaanse concept-ASv is dit niet overgenomen.

21 MvT, p. 8.

22 G. Odinot en D. de Jong, 'Wie belt er nou nog? De veranderende opbrengst van de telefoontap', *Justitiële Verkenningen* 2012, p. 9 (verder: Odinot en De Jong 2012).

situatie.[23] Dat argument is naar mijn mening niet zo sterk, nu ook veel tablets en computers door meerdere mensen worden gedeeld. Ook in dergelijke gevallen zal een internettap bijvangst kennen; dat is nu eenmaal moeilijk te voorkomen. Om dat vervolgens aan te voeren als reden voor een nog indringender bevoegdheid, lijkt het paard achter de wagen spannen.

Als laatste reden wordt de opmars van *cloud computing* aangevoerd.[24] Grof gezegd gaat het bij het verschijnsel '*cloud computing*' om de situatie, dat gebruikers via een netwerk op externe computersystemen bijvoorbeeld bestanden opslaan (bijvoorbeeld Apple iCloud) of programma's kunnen gebruiken (zoals Google Apps). Een verschil met de traditionele wijze van computergebruik is dat programma's en bestanden niet meer op de computer van de gebruiker staan.

De premisse achter de redenering van de minister is dat de bevoegdheid tot doorzoeking ter vastlegging van gegevens (eventueel met aanvullende toepassing van een netwerkzoeking (art. 168 concept-ASv / art. 125j lid 1 NSv)) niet meer afdoende is in de huidige situatie, waarin gegevens tevens op smartphones, laptops en, in toenemende mate, in de '*cloud*' staan. Volgens de Memorie van Toelichting kan niet volstaan worden met bevoegdheden die de *doorzoeking* van een bepaalde plek mogelijk maken, omdat steeds vaker zal blijken dat de gegevens waarnaar gezocht wordt, niet op een specifieke plek te vinden zijn, maar '*in the cloud*', op externe systemen.

Terugvallen op een internettap is volgens de Memorie van Toelichting in die gevallen niet mogelijk, omdat aanbieders van *cloud computing* diensten niet noodzakelijkerwijs als aanbieder van een communicatiedienst in de zin van de Telecommunicatiewet kunnen worden aangemerkt.[25] In Nederland is het van deze kwalificatie afhankelijk of (onder andere) een internettap tot de mogelijkheden behoort. Voor Aruba geldt dat op basis van art. 1 (concept-)ASv onder 'aanbieder van een communicatiedienst' wordt verstaan: 'de natuurlijke persoon of rechtspersoon die in de uitoefening van een beroep of bedrijf aan de gebruikers van zijn dienst de mogelijkheid biedt te communiceren met behulp van een geautomatiseerd werk, of gegevens verwerkt of opslaat ten behoeve van een zodanige dienst of de gebruikers van die dienst.' Deze definitie laat meer ruimte dan de Nederlandse – het is verdedigbaar dat Skype, Whatsapp en wellicht zelfs Google Drive hier wel degelijk onder vallen.

---

23 MvT, p. 8-9.

24 MvT, o.a. p. 9-10, 75.

25 MvT, p. 10. Communicatie kan worden afgetapt en opgenomen, al dan niet met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst (art. 126m, 126t en 126zg NSv). Ook kan van een aanbieder worden gevorderd gegevens te verstrekken (art. 126n, 126na, 126u, 126ua, 126zh en 126zi NSv). Het al dan niet gekwalificeerd kunnen worden als aanbieder van telecommunicatiediensten is derhalve een belangrijk onderscheid.

De mogelijkheden die door de bevoegdheden van internettap, doorzoeking en netwerkzoeking worden geboden, zijn, met inachtneming van de bovenstaande kanttekening, volgens de Memorie van Toelichting kennelijk onvoldoende. Echter, bij het beweerdelijk tekortschieten van de bestaande bevoegdheden komt een aspect om de hoek kijken dat het wetsvoorstel wat dat betreft enigszins in een ander daglicht stelt. Met betrekking tot de inzet van bevoegdheden die fysieke toegang tot plekken verschaffen concludeert de Memorie van Toelichting namelijk: 'Belangrijk bezwaar van deze bevoegdheden is voorts dat de verdachte doorgaans op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Dat kan strijdig zijn met het belang van het onderzoek'.[26] En ten aanzien van de bevoegdheden het aftappen en opnemen van communicatie betreffende, concludeert de Memorie van Toelichting: 'De opsporing heeft behoefte aan de mogelijkheid om heimelijk toegang te kunnen verkrijgen tot gegevens die in de Cloud zijn opgeslagen, zonder dat de verdachte of de aanbieder daarbij is betrokken'.[27]

De indruk ontstaat aldus dat het tekortschieten van de bestaande bevoegdheden niet zozeer zit in het onuitvoerbaar worden van de opsporing wegens het tekortschieten van bestaande bevoegdheden (zij het door de opkomst van versleuteling of anderszins), maar dat de voorgestelde bevoegdheid de opsporing gemakkelijker zou kunnen maken. Alvorens terug te keren naar die kwestie, zal ik in de onderstaande paragraaf eerst ingaan op de hackbevoegdheid zoals de wetgever die voorstelt naar aanleiding van de hierboven geschetste punten.

3. Onderzoek in een geautomatiseerd werk

De hackbevoegdheid is gecodificeerd in art. 168a concept-ASv / art. 125ja NSv. In het eerste lid wordt bepaald dat de officier van justitie onder voorwaarden kan bevelen dat een opsporingsambtenaar binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en met een technisch hulpmiddel onderzoek doet.[28]

---

[26] MvT, p. 10.

[27] MvT, p. 10. Ook hier lijkt de MvT zich op Justitiële Verkenningen te hebben gebaseerd, vergelijk de vrijwel gelijkluidende conclusie in Odinot en De Jong 2012, p**.** 17. Het is echter onduidelijk op basis van welke gegevens die conclusie wordt getrokken.

[28] Het volledige art. 168a lid 1 concept-ASv luidt: 'In geval van verdenking van een misdrijf als omschreven in artikel 100, eerste lid [de gevallen van voorlopige hechtenis – EMW], dat gezien zijn aard of de samenhang met andere vermoedelijk door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie indien het onderzoek dit dringend vordert, na door de rechter-commissaris verleende machtiging, bevelen dat een opsporingsambtenaar binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en met een technisch hulpmiddel onderzoek doet met het oog op:

Het begrip 'geautomatiseerd werk' wordt gedefinieerd in art. 1:197 ASr / art. 80sexies NSr: 'Onder geautomatiseerd werk wordt verstaan een inrichting die bestemd is om langs elektronische weg gegevens op te slaan, te verwerken en over te dragen.' Vanzelfsprekend kan het dan gaan om een computer, van server tot laptop, maar ook een smartphone en (zelfs) het computersysteem van (moderne) auto's is hieronder te brengen.

Het eerste lid noemt, limitatief, vijf doeleinden met het oog waarop de bevoegdheid kan worden ingezet:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;
b. het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag brengen;
c. de ontoegankelijkmaking van gegevens;
d. een bevel tot het opnemen van vertrouwelijke communicatie (art. 177q ASv) en 'telefoontap' (art. 177r ASv);
e. een bevel tot planmatige observatie (art. 177l ASv)

Het moge duidelijk zijn, dat van deze limitatieve opsomming geen enorme beperking uitgaat.[29] Immers, vrijwel alle mogelijke doelen die men in de opsporingspraktijk zou kunnen nastreven, worden gedekt: van zeer algemeen (de waarheid aan de dag brengen) tot zeer specifiek (planmatige observatie). Opvallend is dat onder 'd' en 'e' doelen zijn opgenomen die niet voortvloeien uit de redenen die hierboven zijn beschreven. Deze twee doelen lijken meer te maken te hebben met het aspect dat in de vorige paragraaf als laatste gesignaleerd werd: het vergemakkelijken van de opsporing.

---

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;
b. het overnemen van gegevens die in het geautomatiseerde werk of een daarmee in verbinding staande gegevensdrager zijn verwerkt, of die eerst na het tijdstip van afgifte van het bevel worden verwerkt, voor zover redelijkerwijs nodig om de waarheid aan de dag brengen;
c. de ontoegankelijkmaking van gegevens;
d. een bevel als bedoeld in de artikelen 177q en 177r;
e. een bevel als bedoeld in artikel 177l.

In het belang van het onderzoek kunnen gegevens worden vastgelegd.'

[29] De MvT, p. 39 stelt daarentegen: '(…) de inzet van de bevoegdheid [is] beperkt tot de in het voorgestelde artikel 125ja, eerste lid, Sv omschreven doelen. Deze doelen zijn limitatief omschreven. (…) De limitatieve opsomming van de doelen vereenvoudigt een zorgvuldige afweging door de officier van justitie inzake de noodzaak van de inzet van de afzonderlijke bevoegdheden in een concreet geval.' Zoals in de tekst opgemerkt, zijn deze doelen zo divers, dat daar nauwelijks beperkende werking van uitgaat.

Het 'binnendringen' waarover de bevoegdheid spreekt betreft het daadwerkelijke '*hacken*' van het geautomatiseerde werk, een (technische) exercitie met als doel het veiligstellen van toegang tot het geautomatiseerde werk in kwestie. Ik zal dat onderwerp, gelet op de technische aard ervan, hier laten rusten.[30] De kwestie die ik hieronder wil aansnijden, is wat de bevoegdheid inhoudt wanneer men eenmaal het geautomatiseerde werk is binnengedrongen.

De codificatie van de hackbevoegdheid betreft niet een enkele opsporingsmethode.[31] De voorgestelde bevoegdheid is namelijk op zeer verschillende wijzen toe te passen. Ik zal om te illustreren wat ik bedoel eerst een voorbeeld uit de fysieke wereld geven. Bij een bevoegdheid tot binnentreden (bijvoorbeeld art. 121 ASv / art. 96 NSv: binnentreden ter inbeslagneming) heeft de Hoge Raad zoals bekend uitgemaakt dat er 'zoekend rondgekeken' mag worden, terwijl de bevoegdheid van doorzoeking (bijvoorbeeld art. 137 ASv / art. 110 NSv) gebruikt moet worden als ingrijpender onderzoek noodzakelijk is.[32]

Een dergelijk onderscheid kan bij toepassing van art. 168a concept-ASv niet gemaakt worden. In de Memorie van Toelichting wordt weliswaar in het kader van de proportionaliteit opgemerkt '(…) dat deze [bevoegdheid] wordt toegepast in een zo beperkt mogelijk deel van een geautomatiseerd werk', maar daarbij lijkt uitsluitend gedacht te worden aan het zoeken naar gegevens.[33] Inderdaad kan men zich voorstellen dat in een bevel wordt aangegeven dat bijvoorbeeld wél in de bestandsmappen wordt gekeken waarin bijvoorbeeld spreadsheetbestanden staan met de vermoedelijke schaduwboekhouding, maar (in ieder geval in eerste instantie) niet in de bestandsmap die 'vakantie Bonaire 2013' heet.

Stel echter dat het doel is om de locatie te bepalen van een geautomatiseerd werk. Het is in een dergelijk geval weinig zinnig om te spreken over het in een 'zo beperkt mogelijk deel' van het automatische werk toepassen van de bevoegdheid. De ingrijpendheid van die toepassing is namelijk geen afgeleide van de hoeveelheid van gegevens die wordt onderzocht of waar die gegevens wor-

---

30 In de MvT, p. 13 wordt opgemerkt dat is aangesloten bij de regeling van de computervredebreuk in het Nederlandse Wetboek van Strafrecht (art. 138ab, eerste lid, Sr). Op grond van deze regeling is van binnendringen in ieder geval sprake indien de toegang tot het geautomatiseerde werk wordt verworven door het doorbreken van een beveiliging, door een technische ingreep, met behulp van valse signalen of een valse sleutel, of door het aannemen van een valse hoedanigheid.

31 In vergelijkbare zin (onder verwijzing naar Buermeyer) J.J. Oerlemans, 'Hacken als opsporingsbevoegdheid', *DD* 2011/62, par. 3 (verder: Oerlemans 2011).

32 Zie bijv. HR 18 november 2003, *NJ* 2007, 8 m.nt. Mevis.

33 MvT, p. 40. Op diezelfde pagina: 'Deze beperking (…) waarborgt dat de overheid geen onbegrensde toegang heeft tot gegevens die zijn opgeslagen in een geautomatiseerd werk. Wanneer tijdens de toepassing van de bevoegdheid blijkt dat de bevoegdheid in een ander deel van het geautomatiseerde werk moet worden toegepast, dan is daarvoor een aangepast bevel en uitdrukkelijke toestemming van de rechter-commissaris nodig.'

den gevonden, maar van de aard van de gegevens, de vertrouwelijkheid van de informatie die onderzoek van het geautomatiseerde werk oplevert.[34]

De inbreuk op de persoonlijke levenssfeer kan dus, zo blijkt uit het voorgaande, aanzienlijk variëren. Desondanks verschaft de Memorie van Toelichting weinig duidelijkheid over hoe de bevoegdheid moet worden toegepast als het binnen te dringen werk, bijvoorbeeld een laptop, meerdere mogelijkheden biedt om het doel, bijvoorbeeld het identificeren van de verdachte, te bereiken. Dat doel is te bereiken door identificerende gegevens op te zoeken in bijvoorbeeld mailprogramma's, in (onder andere) Word-bestanden, of zelfs door de ingebouwde camera aan te zetten om te zien of het gezicht dat verschijnt een bekende van politie is. Hoe definieert men dan 'een beperkt deel' waar de Memorie van Toelichting over rept? En hoe bepaalt men welke methode het minst ingrijpend zal zijn?[35]

4. Verhouding met de bestaande bevoegdheden

'De bevoegdheid tot onderzoek in een geautomatiseerd werk of de daarmee in verbinding staande gegevensdrager kan slechts worden toegepast als uit het opsporingsonderzoek blijkt dat met de bestaande wettelijke bevoegdheden niet hetzelfde doel kan worden bereikt', aldus de Memorie van Toelichting.[36] Hoewel de bevoegdheid van art. 168a concept-ASv / art. 125ja NSv kennelijk subsidiair aan de al bestaande bevoegdheden moet worden ingezet, zou de bevoegdheid uiteraard niet worden voorgesteld als de wetgever niet van mening was dát

---

[34] Vgl. C. Conings & J.J. Oerlemans, 'Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?', *Computerrecht* 2013/5, par. 3, die constateren dat er een discrepantie bestaat tussen waarborgen die gepast zijn bij een zoeking in een computersysteem en de (verschillende) garanties die vereist zijn in het kader van de verschillende bestaande doorzoekingsmogelijkheden. Volgens deze benadering is het niet op voorhand logisch dat een laptop die aangetroffen wordt in een auto aan een ander regime onderworpen is dan een laptop die in een woning wordt aangetroffen.

[35] Overigens is het naar mijn mening de vraag, of een bevoegdheid die zo ruim is gecodificeerd, maar tevens zo weinig duidelijkheid verschaft over de wijze van toepassing, voldoet aan de eisen die het EHRM pleegt te stellen. Met name is kwestieus, of de voorgestelde bevoegdheid voldoende 'voorzienbaar' is, dat wil zeggen dat voldoende kenbaar is wat de reikwijdte en de wijze van uitoefening van de inbreuk is, nu in het kader van deze bevoegdheid zeer verschillende inbreuken mogelijk zijn. Vgl. EHRM 24 april 1990, *NJ* 1991, 523 (Kruslin & Huvig v Frankrijk); EHRM 26 april 1979, *NJ* 1980 m.nt. EAA (Sunday Times v Verenigd Koninkrijk). Zie hierover uitgebreider Oerlemans 2011, par. 6.1; J.L.M. Boek, 'Hacken als opsporingsmethode onder de Wet BOB', *NJB* 2000, p. 591 (verder: Boek 2000).

[36] MvT, p. 39.

de huidige bevoegdheden tekortschieten.[37] In het voorgaande is dit aan bod gekomen ten opzichte van onder meer de netwerkzoeking en de internettap.

De duidelijkheid van de Memorie van Toelichting laat echter te wensen over als het aankomt op de vraag *hoe* invulling moet worden gegeven aan het uitgangspunt dat de hackbevoegdheid een aanvulling vormt op de bestaande wettelijke bevoegdheden. Er laten zich diverse scenario's denken.

Indien een bepaald doel niet kan worden bereikt met een bepaalde bevoegdheid, moet dan eerst naar mogelijke inzet van de andere bestaande bevoegdheden worden gekeken, voordat art. 168a concept-ASv / art. 125ja NSv voor dat doel mag worden ingezet? Of verplicht het aanvullende karakter van de hackbevoegdheid daar niet toe? De Memorie van Toelichting lijkt van het tweede uit te gaan, aangezien gesteld wordt: 'Niet uitgesloten is dat een geautomatiseerd [werk - EMW] zodanig is beveiligd dat het niet lukt om binnen te dringen. Dan resteert de toepassing van andere opsporingsbevoegdheden dan wel de beëindiging of onderbreking van het opsporingsonderzoek'.[38] Kennelijk kan de inzet van art. 168a concept-ASv / art. 125ja NSv reeds overwogen worden als met een specifieke bestaande bevoegdheid een bepaald doel niet (maar kennelijk met andere bestaande bevoegdheden wel) bereikt kan worden, anders resteerden er immers geen andere opsporingsbevoegdheden meer. Deze passage lijkt immers niet uit te gaan van een volgorde waarin hacken als laatste komt, maar van een keuzeproces waarin verschillende mogelijkheden openstaan.

In het verlengde hiervan ligt de vraag, of de nieuwe bevoegdheid ook mag worden ingezet als met de bestaande bevoegdheden het doel *wel* kan worden bereikt, maar daarvoor meer risico genomen moet worden. In dit kader wordt betreffende het opnemen van vertrouwelijke informatie (art. 177q ASv / art. 126l NSv), opgemerkt dat het fysiek plaatsen van een technisch hulpmiddel 'een grote belemmering' kan zijn in gevallen waarin óf de locatie van het geautomatiseerde werk niet bekend is, óf de locatie wél bekend is, 'maar de kans bestaat op ontdekking of op onvoorziene omstandigheden ter plaatse'.[39] Ik kan me echter voorstellen dat de afweging daaromtrent anders uitvalt in (bijvoorbeeld) de situatie waarin het huisadres van de verdachte niet bekend is,[40] dan wanneer het

---

37 In het huidige Arubaanse Wetboek van Strafvordering zijn overigens (in tegenstelling tot in Nederland) de doorzoeking ter vastlegging van gegevens en de netwerkzoeking nog niet gecodificeerd.

38 MvT, p. 26.

39 MvT, p. 11. Zie ook p. 19: 'Het is dan niet nodig een besloten plaats of een woning binnen te dringen, met alle risico's van dien.'

40 Overigens zal in een deel van de gevallen een International Mobile Subscriber Identity- of IMSI-catcher gebruikt kunnen worden om de verblijfplaats te achterhalen, een andersoortige technische methode, die overigens evenmin expliciet gecodificeerd is. Zie R. Chavannes en N. van der Laan, 'Kroniek Technologie en recht', *NJB* 2012, 2524 (verder: Chavannes en Van der Laan 2012).

argument (slechts?) is dat een grotere kans op ontdekking bestaat bij het installeren van een fysieke *bug* in de woning van een verdachte.

Als laatste laat zich de vraag stellen op welke wijze de hackbevoegdheid moet worden ingezet indien de bestaande bevoegdheden tekortschieten, bijvoorbeeld in het aangehaalde geval dat geen locatie bekend is. Mag de hackbevoegdheid in een dergelijk geval alleen worden ingezet om de locatie vast te stellen, waarna verder (weer) gebruik moet worden gemaakt van de reguliere opname vertrouwelijke communicatie (verder: OVC)? Of mag de hackbevoegdheid dan (ook) gebruikt worden om (bijvoorbeeld) de computer van de verdachte in te schakelen voor de OVC?

Het antwoord op deze vragen, die de nadere invulling van de subsidiariteitsgedachte betreffen, zal samenhangen met het oordeel over hoe ingrijpend men de voorgestelde bevoegdheid acht, afgezet tegen de reeds bestaande bevoegdheden.

De Memorie van Toelichting merkt ter zake op: 'Het op afstand heimelijk binnendringen in een geautomatiseerd werk door de politie vormt een ernstige aantasting van het privéleven van de burger, doordat de overheid inzage krijgt in gegevens die in het geautomatiseerde werk worden verwerkt of opgeslagen. Dit betreft een vergaande bevoegdheid'.[41] Maar dat moet men blijkbaar niet begrijpen in die zin, dat de hackbevoegdheid per definitie ingrijpender zou zijn dan de bestaande bevoegdheden. Want direct daarna wordt gesteld: '(…) ook thans, bij het gebruik van bestaande opsporingsbevoegdheden, [kan] inzage (…) worden verkregen in de gegevens die door burgers worden verwerkt met behulp van een geautomatiseerd werk'.[42]

Op de pagina's waar ingegaan wordt op de verhouding met specifieke bevoegdheden, wordt veelal het standpunt ingenomen dat de voorgestelde bevoegdheid te prefereren is boven een bestaande bevoegdheid die hetzelfde resultaat kan opleveren. Naast de hierboven al aangehaalde praktische argumenten van (onder andere) het verminderen van de kans op ontdekking, wordt meermalen aangevoerd dat de inbreuk die gemaakt wordt minder groot is. Bijvoorbeeld in de situatie dat de hackbevoegdheid zou worden ingezet voor OVC in een woning, wordt tevens als voordeel van de hackbevoegdheid aangemerkt het niet hoeven betreden van de woning voor het plaatsen van een *bug*, waardoor '(…) geen inbreuk behoeft te worden gemaakt op het grondwettelijke beschermde recht van onschendbaarheid van de woning (artikel 12 GW)'.[43] Eenzelfde rede-

41 MvT, p. 37.

42 MvT, p. 37. Zie ook p. 38-39: 'De inbreuk van het onderzoek in een geautomatiseerd werk is vergelijkbaar met de toepassing van andere bevoegdheden *waarbij een computer wordt doorzocht* [mijn cursivering – EMW], zoals bij de doorzoeking ter vastlegging van gegevens, de netwerkzoeking en bij het direct afluisteren en het aftappen van communicatie.'

43 MvT, p. 11.

nering wordt gebruikt voor inbeslagneming: 'Het kennisnemen van een grote hoeveelheid persoonsgegevens met het oog op het selecteren van voor de opsporing relevante gegevens zal veelal als disproportioneel moeten worden aangemerkt in de gevallen waarin een voorwerp in beslag wordt genomen uitsluitend om bepaalde gegevens vast te leggen'.[44]

De gevolgtrekking dat de inbreuk 'minder groot' is, is echter betwistbaar. De Memorie van Toelichting miskent naar mijn mening dat de voorgestelde bevoegdheid op een andere wijze functioneert dan de bevoegdheden die voor de fysieke omgeving zijn ontwikkeld. Dit heeft tot gevolg, dat de bestaande manier om de ingrijpendheid van een bevoegdheid te beoordelen, niet zonder meer kan worden toegepast op de voorgestelde bevoegdheid.

5. De aard van de hackbevoegdheid

In art. 168a concept-ASv / art. 125ja NSv is gekozen voor term 'onderzoek in een geautomatiseerd werk' om het verschil aan te duiden met het doorzoeken, dat altijd in een fysieke plaats geschiedt. Door te spreken van 'onderzoek in een geautomatiseerd werk' is, aldus de Memorie van Toelichting, voorzien in een 'duidelijk onderscheid' van de eerstgenoemde opsporingsmethode die in een digitale omgeving wordt ingezet, ten opzichte van opsporingsbevoegdheden die in de fysieke wereld worden toegepast.[45] Dat onderscheid is naar mijn mening echter minder duidelijk dan de toelichting het doet voorkomen.

Om dat op waarde te kunnen schatten, is het dienstig om eerst een voorbeeld van de 'klassieke' situatie te bespreken, zoals een onderzoek aan de kleding (art. 78 ASv / art. 56 NSv). Een fouillering kan verschillende dingen opleveren, zij het drugs, een wapen of een identificatiebewijs. De inbreuk die door opsporingsambtenaren gemaakt wordt, is echter steeds hetzelfde: de verdachte wordt aan zijn kleding onderzocht, waarbij niet al te grote voorwerpen kunnen worden gevonden.

Onderzoek in een geautomatiseerd werk door middel van een technisch hulpmiddel omvat echter een groter aantal methoden. Ter illustratie: een zogenaamde slimme thermostaat is een thermostaat die via internet benaderbaar is, om bijvoorbeeld programma's in te programmeren of om juist de verwarming aan of uit te zetten omdat de bewoner van het pand op een ander tijdstip thuiskomt dan gebruikelijk. Deze data geven – tot op zekere hoogte – inzicht in de levenspatronen van de bewoner(s) van een huis. Door de internetconnectiviteit zal het in beginsel voor de opsporingsautoriteiten mogelijk zijn om deze gegevens in te zien, om zo bijvoorbeeld de tijden waarop een observatieteam in positie moet zijn af te stemmen, of het moment van een doorzoeking te plannen.

---

[44] MvT, p. 11.
[45] MvT, p. 76.

De hackbevoegdheid kan echter ook op een veel ingrijpender wijze ingezet worden. De Memorie van Toelichting geeft aan dat de bevoegdheid zelfs op tot nu toe ondenkbare wijze zou kunnen worden toegepast: op basis van jurisprudentie van de Rechtbank 's-Hertogenbosch wordt verdedigd dat een smartphone geen heimelijk op het lichaam geplaatst hulpmiddel is in de zin van de wet in het kader van planmatige[46] observatie (art. 177l lid 3 ASv / art. 126g lid 3 NSv).[47] Hoewel de wet bepaalt dat een technisch hulpmiddel niet op een persoon wordt bevestigd (tenzij met diens toestemming), zou dat bij toepassing van de hackbevoegdheid op de smartphone van de verdachte niet opgaan omdat gebruik wordt gemaakt van een voorwerp dat de verdachte reeds voor een ander doel bij zich draagt.

De houdbaarheid van deze uitspraak van de Rechtbank te 's-Hertogenbosch daargelaten; van het inzicht geven in rudimentaire levenspatronen van de verdachte enerzijds, kan de bevoegdheid aan de andere kant van het spectrum kennelijk naar het oordeel van de wetgever ingezet worden om gedurende enige tijd een smartphone als persoonlijk peilbaken en afluisterapparaat te gebruiken. Deze plooibaarheid onderscheidt de hackbevoegdheid mijns inziens van de onderzoeksbevoegdheden die in de fysieke wereld worden ingezet. Bij de bestaande bevoegdheden is de diversiteit van de toegepaste methode(n) bij de inbreuk veelal minder groot; vergelijk het eerder aangehaalde voorbeeld van onderzoek aan kleding.

De benadering die uit de Memorie van Toelichting spreekt, houdt weinig rekening met het feit dat de methoden bij de voorgestelde bevoegdheid zo uiteenlopend kunnen zijn en de inbreuk dus eveneens kan variëren. Dat leidt tot problemen aangezien de maatstaven die worden aangelegd om de zwaarte van de inbreuk te kwalificeren, deze veelal benaderen vanuit een perspectief dat is toegesneden op de fysieke wereld.[48] Aan het eind van de vorige paragraaf kwam dit al kort in een tweetal voorbeelden aan bod. Eén daarvan betrof de stelling dat door toepassing van de voorgestelde bevoegdheid het huisrecht niet hoeft te worden geschonden om een *bug* te plaatsen. Naar de letter genomen zal die toepassing inderdaad waarschijnlijk niet het huisrecht van art. 12 GW schenden omdat geen van de opsporingsambtenaren de woning hoeft te betreden om een softwarematige *bug* te plaatsen. Maar is deze inbreuk op de privésfeer van de verdachte

[46] De bevoegdheid 'planmatige observatie' is de Arubaanse pendant van het Nederlandse 'stelselmatige observatie'. Zie over het verschil: E.M. Witjens, 'De Wet BOB tegen het (zon)licht gehouden. De Wet Bijzondere Opsporingsbevoegdheden in Aruba', *Caribisch Juristenblad* 2013, p. 18-19.

[47] De MvT p. 21 haalt Rechtbank 's-Hertogenbosch 14 juni 2012, *LJN* BW8619 en BW8633 aan ter ondersteuning van deze opvatting.

[48] In een andere context signaleren Chavannes en Van der Laan 2012, p. 2523, ditzelfde probleem bij de omgang met technologie bij de opsporing in het algemeen.

daadwerkelijk minder ingrijpend, gelet op het feit dat het netto eindresultaat is dat de overheid heimelijk *alle* gesprekken in een woning kan afluisteren?[49]

Deze kwestie speelt overigens in meer gevallen dan alleen bij de voorgestelde bevoegdheid: het doorzoeken van een woning wordt gezien als een grotere inbreuk op de privésfeer dan het doorzoeken van een auto, hetgeen geldt ongeacht de gevoeligheid van de informatie die wordt gezocht.[50] Een dergelijke benadering, die aangrijpt bij de plek van de doorzoeking, past niet bij een digitale omgeving waarbij de *fysieke* inbreuk op de privésfeer per definitie geringer is. Dat betekent echter niet dat de inbreuk op de privésfeer (daardoor) ook geringer is. Gezien het feit dat de rol van technologie steeds belangrijker wordt in de samenleving, en de invloed die dat heeft en nog gaat hebben op de opsporingspraktijk, is de vraag of de klassieke benadering nog voldoet.

Hoewel de toenmalige gedachtegang van de wetgever logisch was, is het een graadmeter die steeds minder houdbaar blijkt. Maakt het werkelijk verschil of gegevens door het binnendringen op afstand worden overgenomen, door een internettap worden onderschept of zelfs door een opsporingsambtenaar die naast een verdachte is gezeten in een openbare ruimte is afgekeken van het scherm van de laptop van de verdachte? Waar de Memorie van Toelichting opmerkt dat art. 12 Gw niet wordt geschonden door de voorgestelde bevoegdheid, blijkt daaruit misschien vooral dat de huidige grondwettelijke waarborgen hun relevantie aan het verliezen zijn in een veranderende samenleving, waarin gegevens in een digitale omgeving steeds belangrijker worden.[51] Ik zal hier in de conclusie op terug komen.

6. Kanttekeningen voor Aruba

Voordat we bij de conclusie aankomen, wil ik enkele punten bespreken die specifiek voor Aruba (en de andere kleinschalige rechtsordes in het Koninkrijk) van belang zijn.

Eén van de waarborgen die in het Nederlandse wetsvoorstel wordt voorzien, is dat de uitvoering van de bevoegdheid in de handen ligt van gespecialiseerde opsporingsambtenaren, die niet betrokken zijn bij het onderzoek. In de Arubaanse Memorie van Toelichting wordt niet nader ingegaan op de vraag welke func-

---

[49] Ook het andere voorbeeld overtuigt niet: weliswaar is er door gebruik van de nieuwe bevoegdheid geen noodzaak meer om de gegevens door inbeslagname (tijdelijk) aan de beschikkingsmacht van de verdachte te onttrekken, maar de kern van de inbreuk is hier naar mijn mening gelegen in het kennisnemen van persoonlijke bestanden of gegevens, niet zozeer in het in beslag nemen van de gegevensdrager waarop die gegevens staan.

[50] Vgl. het opgemerkte *supra* noot 34.

[51] Vgl. de bevindingen van de Commissie Grondrechten in het digitale tijdperk, met name p. 205 e.v.; http://www.ivir.nl/dossier/grondrechten/bronnen/rapport_gdt_5-00.pdf (laatst bezocht op 26 april 2014).

tionarissen de bevoegdheid kunnen uitoefenen. Dat is vreemd, omdat het onopgemerkt binnendringen in (veelal beveiligde) geautomatiseerde systemen, tenzij men de beveiliging kan omzeilen door bijvoorbeeld een wachtwoord te ontfutselen, niet goed denkbaar is indien men geen deskundigheid ter zake heeft.[52] Er komt bepaaldelijk meer bij kijken dan (bijvoorbeeld) het simpelweg binnentreden in een te doorzoeken plaats. Het is onwaarschijnlijk dat reguliere opsporingsambtenaren, in plaats van daarvoor opgeleide specialisten, deze bevoegdheid effectief zouden kunnen toepassen.[53] Het is niet duidelijk hoe de Arubaanse wetgever tegen deze problematiek aankijkt.

Tevens schrijft de Nederlandse Memorie van Toelichting voor dat de opsporingsambtenaren die zijn belast met het plaatsen van het technische hulpmiddel, niet behoren tot het opsporingsteam dat het tactische onderzoek verricht. 'Deze functiescheiding, die ook bij de plaatsing van een telefoon-, of internettap gebruikelijk is, vermindert het risico op tunnelzicht. De opsporingsambtenaren die zijn belast met de plaatsing van het technisch hulpmiddel zijn niet betrokken bij het operationele onderzoek en kunnen daardoor niet worden beïnvloed bij het maken van afwegingen ter zake van de haalbaarheid en de wijze [van] uitvoering van het onderzoek in een geautomatiseerd werk', aldus de Nederlandse Memorie van Toelichting.[54] De Arubaanse Memorie van Toelichting zwijgt echter in alle talen over deze waarborg. Wederom is de vraag welke conclusies daaraan verbonden moeten worden.

Een tweede punt betreft de eisen waaraan het technisch hulpmiddel, veelal een softwareapplicatie, moet voldoen. Om de integriteit van de opsporingsmethode te waarborgen, moet deze volgens de Nederlandse Memorie van Toelichting voldoen aan de regels die opgenomen zullen worden in het Besluit Technische Hulpmiddelen Strafvordering.[55] 'Met deze voorwaarden wordt voorzien in adequate en effectieve waarborgen tegen willekeurige inmenging en misbruik alsmede voor het verzekeren van de authenticiteit en integriteit van door middel van het technische hulpmiddel vastgelegde gegevens', aldus de Memorie van Toelichting.[56]

---

52 Odinot en De Jong 2012, p. 14.

53 Vgl. MvT, p. 22: 'Te allen tijde staat voorop dat de uitvoeringshandelingen op professionele wijze worden uitgevoerd, door daarvoor opgeleide specialisten.' Zie ook p. 74: 'Het is gewenst dat een ingrijpende en risicovolle bevoegdheid als deze alleen kan worden opgedragen aan een beperkte categorie opsporingsambtenaren die over specialistische kennis beschikken.'

54 MvT, p. 23.

55 Vgl. de Nederlandse MvT, p. 27: 'Het technische hulpmiddel moet zijn goedgekeurd en moet voldoen aan de normen [van] het Besluit technische hulpmiddelen strafvordering, dat in verband met de voorgestelde bevoegdheid wordt aangepast. (…) Ook (…) moeten de authenticiteit en integriteit van de gegevens die door middel van het technische hulpmiddel worden vergaard, zijn gewaarborgd.' Zie ook p. 23, 29, 79.

56 MvT, p. 41.

Het wekt dan ook verbazing dat in de toelichting bij het Arubaanse art. 168a lid 7 concept-ASv wordt gesteld: 'Omdat het onderzoek doorgaans via het internet wordt verricht, bestaat het technische hulpmiddel uit een softwareapplicatie door middel waarvan het onderzoek wordt verricht. Het is van groot belang dat de software voldoet aan eisen op het gebied van controleerbaarheid en integriteit, zodat de uitvoering van het onderzoek in een geautomatiseerd werk en de vastlegging van gegevens te allen tijde kan worden getoetst. Vandaar dat wordt opgenomen dat bij Landsbesluit, houdende algemene maatregelen, regels *kunnen* [mijn cursivering – EMW] worden gesteld'.[57] Dat lijkt op zijn zachtst gezegd innerlijk tegenstrijdig: het is van groot belang dat de software aan eisen voldoet, maar regels ter zake zijn optioneel.

De waarborgen die het technisch hulpmiddel betreffen zijn zo belangrijk, omdat data in de digitale omgeving gemakkelijk te manipuleren zijn. Het is op dit moment onduidelijk hoe de integriteit gewaarborgd kan worden bij bevoegdheden die ingrijpen in de digitale omgeving.[58] Als gevolg daarvan zal het voor rechters zeer moeilijk zijn het bewijs dat door deze bevoegdheid wordt gegenereerd op waarde te schatten. Dat het gebruikte technisch hulpmiddel aan de toepasselijke vereisten voldoet, lijkt me in ieder geval een ondergrens.

Beide bovenstaande punten betreffen uiteindelijk (ook) de vraag, of het Korps Politie Aruba (KPA) voldoende budget krijgt om de bevoegdheid toe te kunnen passen. Enerzijds gaat het dan om personeelskosten, maar anderzijds ook om de kosten voor de ontwikkeling en het onderhoud van de vereiste technische hulpmiddelen. Indien de gedachte is, dat Aruba de bevoegdheid niet zelfstandig zal inzetten, maar men eigenlijk wil 'meeliften' op de bevoegdheid in Nederland door verzoeken tot steun te doen, zou het me niet onverstandig lijken om eerst af te wachten of, en zo ja in welke vorm, Nederland deze bevoegdheid zal codificeren.

7. Conclusie

Naar aanleiding van het voorgaande betwijfel ik of de Arubaanse wetgever (en de Nederlandse evenzeer) er goed aan zou doen om de bevoegdheid in de huidige vorm kracht van wet te geven.

Het eerste argument tegen de nieuwe bevoegdheid is dat simpelweg niet erg overtuigend wordt dat er echt een leemte in de opsporingsbevoegdheden bestaat. Er laten zich wellicht situaties denken waarin de bestaande bevoegdheden tekort

---

[57] Concept Wetboek 2013, p. 400.

[58] Oerlemans 2011, par. 7; Vgl. B. Jacobs, 'Policeware', *NJB* 2012, p. 2762 die een actieve inbreng van de politie bij dergelijke bevoegdheden verwerpt, juist omdat het naar zijn inschatting 'volstrekt onduidelijk' is hoe de waarborgen (zoals '*secure logging*') gerealiseerd kunnen worden.

schieten – denk aan iemand die een zeer goed beveiligde laptop gebruikt waarop informatie versleuteld is opgeslagen terwijl de communicatie op willekeurige plekken geschiedt waar een publieke wifi-verbinding beschikbaar is, terwijl ook de data versleuteld wordt verzonden. Maar zal in een dergelijk geval de voorgestelde bevoegdheid het verschil gaan maken? In de Memorie van Toelichting wordt toegegeven dat indien de beveiliging sterk genoeg is, (ook) de hackbevoegdheid niet toegepast zal kunnen worden.[59]

In paragraaf 2 werd opgemerkt dat de indruk wordt gewekt dat de bevoegdheid vooral voorgesteld wordt voor toepassing in de gevallen waarin de bestaande bevoegdheden ook zouden kunnen worden toegepast, maar 'slechts' een groter afbreukrisico kennen. Alternatieven voor de voorgestelde bevoegdheid, bijvoorbeeld het aanpassen van de definitie van communicatiedienst in de zin van de Telecommunicatiewet, worden nergens in de Memorie van Toelichting besproken.[60] Een dergelijke aanpassing zou de inzet van de bestaande tapbevoegdheden en het vorderen van verkeersgegevens mogelijk maken bij (bijvoorbeeld) Skype, aangezien die bevoegdheden (in Nederland) aangrijpen bij die kwalificatie.[61] Tevens wordt wel heel gemakkelijk aangenomen dat het aftappen van (onder andere) Skype door versleuteling onmogelijk is, terwijl dat geen uitgemaakte zaak is.[62] Er lijkt dus meer ruimte te zijn voor toepassing van de bestaande bevoegdheden dan de Memorie van Toelichting wil erkennen.

Het tweede punt dat tegen de hackbevoegdheid in de huidige vorm pleit, is dat onvoldoende rekenschap is gegeven van de afwijkende aard van de voorgestelde bevoegdheid. De Memorie van Toelichting geeft een voorstelling van zaken die gebaseerd is op maatstaven die bedoeld zijn voor het vaststellen van (de ernst van) inbreuken in de fysieke werkelijkheid. Begrippen als planmatigheid / stelselmatigheid, of duur van de inbreuk hebben echter een andere doorwerking bij de hackbevoegdheid. Indien in luttele seconden het volledige archief aan camerabeelden uit een beveiligingsinstallatie van een huis kan worden overgenomen, een archief dat een halfjaar aan beeld bevat van camera's in het merendeel van de vertrekken, maakt het dan echt uit dat de inbreuk kort was? Gaat het er niet eerder om wat de inbreuk *oplevert*? De hackbevoegdheid functioneert in een digitale omgeving waarbij de fysieke inbreuk op de privésfeer wellicht geringer is vergeleken met de toepassing van de bestaande bevoegdheden in de fysieke werkelijkheid, maar de uitkomst geenszins minder ingrijpend hoeft te zijn.

---

59 Zie MvT, p. 26.

60 Vgl. een Belgisch perspectief: P.J.A. De Hert & G. Boulet, 'De Yahoo-saga: de keuze tussen nationale opsporingsmethoden en internationale rechtshulpinstrumenten', *Computerrecht* 2012/152, m.n. paragraaf 9.

61 In dezelfde zin: Oerlemans 2012, p. 35. De MvT stelt slechts vast dat Skype niet onder de definitie van de Telecommunicatiewet valt.

62 Zie de bronnen *supra* noot 14.

Terughoudendheid is temeer geboden, omdat de bevoegdheid een gigantische reikwijdte heeft. Door deze bevoegdheid kan iedere smartphone en iedere laptop als peilbaken worden ingezet, als richtmicrofoon worden gebruikt of als verdekt opgestelde camera worden aangewend. Zonder dat enige inspanning van de opsporingsautoriteiten noodzakelijk is, is bijna iedere burger voorzien van alle technologische snufjes die voor het toepassen van (bijvoorbeeld) OVC benodigd zijn. Met de opmars van techniek in alle hoeken van de samenleving, zal de bevoegdheid steeds ruimer worden – niet te overzien is wat er in de (nabije) toekomst allemaal onder de definitie 'geautomatiseerd werk' zal gaan vallen. Ter illustratie: ook auto's zullen steeds vaker als zodanig zijn aan te merken, waardoor bijvoorbeeld met de reeds aanwezige microfoons de gesprekken van de inzittenden kunnen worden afgeluisterd.[63] Nu kan men tegenwerpen, dat in het huidige voorstel de bevoegdheid alleen in de ernstigste gevallen kan worden ingezet, maar als de ervaring iets leert, dan is het dat een dergelijke drempel meestal na enige tijd verdwijnt als er een incident is geweest dat daadkrachtig optreden van een politicus vergt.

Op basis van het voorgaande is mijn conclusie dat onvoldoende reden bestaat om de voorgestelde bevoegdheid kracht van wet te geven. Dat is overigens geen principiële stellingname tegen bevoegdheden die het binnendringen in een geautomatiseerd werk zouden kunnen behelzen. Echter, een bevoegdheid met de reikwijdte zoals die is voorgesteld, lijkt mij niet te rechtvaardigen. Een dergelijk middel vergt een veel preciezere codificatie, in het kader waarvan de verhouding tussen de bevoegdheden rond de doorzoeking ter vastlegging van gegevens en de bijzondere bevoegdheden tot opsporing zal moeten worden herzien.[64]

In paragraaf 5 is behandeld dat zeer verschillende situaties onder art. 168a concept-ASv / art. 125ja NSv kunnen vallen. Ik ben van mening dat daarom een '*one size fits all*' bevoegdheid als de voorgestelde niet geschikt is om de juiste balans te vinden tussen de reikwijdte in een specifiek geval, de ingrijpendheid daarvan en de waarborgen die daar bij moeten horen. Zoals hierboven uitgebreid is behandeld, heeft het de nodige haken en ogen om alleen al tot een beeld te komen van hoe de 'aanvullende' aard van deze bevoegdheid er in de praktijk uit zou zien. Een meer gedifferentieerde benadering verdient daarom de voorkeur, omdat die de praktijk meer houvast zou bieden, terwijl dat tevens zou kunnen leiden tot een duidelijker reikwijdte van bevoegdheden die in de digitale omgeving kunnen worden ingezet. Deze gedifferentieerde benadering zou bijvoorbeeld specifieker kunnen voorschrijven wanneer de bevoegdheid kan worden

[63] Dit is ook de auto-industrie niet ontgaan, zie http://www.manager-magazin.de/unternehmen/autoindustrie/vw-chef-winterkorn-fordert-allianz-der-autobauer-fuer-mehr-datenschutz-a-957772.html (laatst bezocht op 10 maart 2014).

[64] Dit in tegenstelling tot de opvatting die in de MvT wordt aangehangen, *supra* noot 4.

ingezet, hetgeen ook de toezichthoudende taak van de rechter-commissaris beter uitvoerbaar zou maken.[65]

Het gaat het bestek van dit artikel te buiten om precies uit te werken hoe het dan wél zou moeten. Op dit moment is er in de literatuur volop debat of bepaalde (reeds bestaande) bevoegdheden de ruimte bieden om daar ook een hackbevoegdheid onder te verstaan, denk bijvoorbeeld aan het binnendringen van een computer om deze te gebruiken bij OVC.[66] Bij beantwoording van de vraag hoe het wel moet, is het echter van belang om rekening te houden met hetgeen hierboven betoogd is over de andere aard van een hackbevoegdheid.[67]

Dat dit nog geen standpunt is dat breed gedeeld wordt, moge dit voorbeeld, waarmee ik zal afsluiten, duidelijk maken. Kooijmans en Mevis schrijven: 'The question rises whether surveillance of 1) open sources on the internet and 2) sources on the internet that require registration can be qualified as systematic observation. In other words, does such an observation create (only) a light interference with a person's privacy, or rather a grave interference?'[68] Bijvoorbeeld Koops acht voor het antwoord op die vraag onder meer relevant of 'eenmalig' wordt gekeken op bepaalde pagina's.[69] Het moge op dit punt in deze bijdrage duidelijk zijn, dat ik die mening niet deel. Een eenmalig bezoek aan een website kan – afhankelijk van wat daar te vinden is – een enorme hoeveelheid informatie opleveren. Een enkel bezoek aan Facebook kan bijvoorbeeld een schat aan informatie opleveren over wie de verdachte kent, waar hij de afgelopen jaren is geweest, met fotografisch bewijs als bonus.[70] Of dat in het kader van een

---

65 Dit te meer omdat hoewel in het Nederlandse wetsvoorstel de Centrale Toetsingscommissie van het OM deel uitmaakt van de toetsingsprocedure, er in het Arubaanse concept voor gekozen is om deze rol in handen te leggen van de P-G, bij gebreke aan een Toetsingscommissie. Het is zeer de vraag, of die toetsing op deze wijze voldoende inhoud zal krijgen.

66 In de literatuur is bijvoorbeeld betoogd dat de Wet BOB geen aanpassing behoeft, nu deze bevoegdheden en geen methoden codificeert. Zie Boek 2000, p. 592-593. Oerlemans 2011, par. 6.1.1 is daarentegen van mening dat de huidige bevoegdheden deze mogelijkheid niet bieden.

67 Zie ook Odinot en De Jong 2012, p. 17, waar zij stellen: '(…) een maatschappelijke discussie over de zwaarte en de waarde van verschillende bijzondere opsporingsmiddelen is zinvol om de opsporingspraktijk in Nederland verder te kunnen ontwikkelen'

68 T. Kooijmans & P. Mevis, 'ICT in the context of criminal procedure: the Netherlands', TLS/EUR/AIDP, p. 28 e.v., via https://pure.uvt.nl/portal/files/1532791/Report_the_Netherlands_19092013.PDF (laatst bezocht op 13 mei 2014), p. 9.

69 B.J. Koops, 'Politieonderzoek in open bronnen op internet. Strafvorderlijke aspecten.', *Tijdschrift voor Veiligheid* 2012 (11), p. 41.

70 Zie Junichi P. Semitsu, 'From Facebook to mug shot: how the dearth of social networking privacy rights revolutionized online government surveillance', 31 *Pace L. Rev*. 291 2011.

planmatige/*stelselmatige* observatie is vergaard, is in de digitale omgeving niet meer zo relevant. Een benadering die aan deze werkelijkheid geen recht doet, heeft naar mijn mening geen toekomst in deze samenleving.[71]

[71] Dit in tegenstelling tot de Faculteit der Rechtsgeleerdheid, die zeer zeker wel recht doet aan deze samenleving en dus naar ik hoop nog een lange toekomst tegemoet kan zien!