Wet computercriminaliteit III

mr. B.W. Newitt[1]

Op 1 maart 2019 treedt de Wet Computercriminaliteit III in werking.[2] De wet begon in 2011 als het conceptwetsvoorstel Versterking Bestrijding Computercriminaliteit,[3] en werd in 2013 het wetsvoorstel Wet Computercriminaliteit III.[4] Deze is na enige zowel geruststellende als zorgwekkende wijzigingen[5] in 2016 naar de Eerste Kamer gestuurd.[6] De nieuwe wet kan, zoals de naam ook al zegt, worden gezien als een aanvulling op de Wet Computercriminaliteit uit 1993 en de Wet Computercriminaliteit II uit 2006.

In die eerdere wetten werd een aantal specifieke cybercrime-feiten strafbaar gesteld, zoals computervredebreuk, het verspreiden van malware en het doen van DDoS aanvallen. Ook werden verschillende digitale opsporingsbevoegdheden ingevoerd die nu haast niet meer uit de opsporingspraktijk weg te denken zijn, zoals de doorzoeking ter onderzoek in geautomatiseerde werken en het opnemen en aftappen van computergegevens.

De nieuwe wet vult door de opsporing gepercipieerde leemten op in de opsporingsbevoegdheden en stelt nieuwe handelingen strafbaar. Als meest ingrijpende wijziging voert de nieuwe wet de hackbevoegdheid voor de opsporingsdiensten in. Ik zal eerst ingaan op de belangrijkste wijzigingen in de materiële wet en zal daarna aandacht besteden aan de nieuwe hackbevoegdheid.

1. Strafbaarstelling heling en verduistering van 'niet-openbare' gegevens (art. 139g en 138c Sr)

In de nieuwe wet wordt de heling en verduistering van 'niet-openbare' gegevens strafbaar gesteld. De *Manon Thomas*-zaak[7] is een katalysator geweest voor de strafbaarstelling van het helen van gegevens. In deze zaak waren enkele privéopnamen, waarop de presentatrice naakt te zien was, van haar computer ontvreemd. Via YouTube en MSN Messenger werd het beeldmateriaal verder verspreid. Door het Hof Leeuwarden werd een hoofdverspreider veroordeeld voor schending van het auteursrecht en portretrecht van de presentatrice, maar de dader kon niet strafrechtelijk worden veroordeeld voor een cybercrimedelict. Dit omdat niet bewezen kon worden dat de verdachte (zelf) computervredebreuk had gepleegd. Het verder verspreiden van door anderen ontvreemde gegevens kon bovendien niet onder de helingsbepalingen worden vervolgd, omdat gegevens binnen het strafrecht in principe niet als 'goed' zijn aan te merken.[8]

Naar aanleiding van deze zaak zijn Kamervragen gesteld,[9] en heeft de wetgever besloten dat het wenselijk zou zijn om het wederrechtelijk overnemen van gegevens uit een niet-openbaar werk, strafbaar te stellen. Dat voornemen heeft uiteindelijk geleid tot art. 138c Sr, de verduistering van gegevens. Het verwerven, voorhanden hebben of beschikbaar stellen van uit misdrijf afkomstige gegevens, wordt in de nieuwe wet in art. 139g Sr strafbaar gesteld als 'heling van gegevens'.

Deze nieuwe strafbaarstelling van heling en verduistering van gegevens kan ook in bredere zin als nuttig worden ervaren, omdat de Hoge Raad gegevens in het algemeen niet als een goed aanmerkt,[10] nu gegevens vallen onder een eigen juridisch begrip zoals beschreven in art. 80quinqies Sr.

Er zijn uiteraard wel enige uitzonderingen gecreeerd in de jurisprudentie waarbinnen de Hoge Raad aanvaardt dat niet-stoffelijke gegevens een goed kunnen opleveren, zoals in de *Runescape*-zaak.[11] De Hoge Raad stelt daarbij in het algemeen wel de voorwaarde dat degene die de feitelijke macht over de gegevens heeft, deze verliest als de ander die verkrijgt. Aan die criteria voldoen veel gegevens binnen cybercriminaliteit echter niet. Als gegevens door hacken worden verkregen worden ze vaak eenvoudigweg gekopieerd, zonder dat de oorspronkelijke bezitter de toegang tot de gegevens verliest. Ook via de Runescape-jurisprudentie zouden computergegevens aldus niet eenvoudig als een te helen of te verduisteren goed kunnen worden gekwalificeerd. In dat licht kunnen deze nieuwe strafbepalingen als een nuttige toevoeging worden aangemerkt.

Er is binnen de strafbaarstelling van heling van gegevens uiteraard wel een uitzondering gemaakt voor journalisten en klokkenluiders, alsmede voor

1. Brendan Newitt is werkzaam als advocaat bij de Roos & Pen
2. *Stb.* 2019, 67
3. https://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit/detail.s
4. *Kamerstukken II* 2015/16, 34372, 2.
5. Als zorgwekkende wijziging valt aan te merken de inzet van de virtuele lokpuber, een geruststellende is bijvoorbeeld het verwijderen van het decryptiebevel aan de verdachte.
6. *Kamerstukken I*, 2016/17, 34372, A.
7. Gerechtshof Den Haag 4 mei 2010, *NJFS* 2010/239, ECLI:NL:GHLEE:2010:BM3169.
8. Zie voor de omschrijving van het begrip gegevens art. 80quinquies Sv.
9. *Aanhangsel Handelingen II* 2007/08, 888.
10. Hoge Raad 3 december 1996, *NJ* 1997, 574.
11. HR 31 januari 2012, *NJ* 2012/536, ECLI:NL:HR:2012:BQ9251.

anderen, voor zover die te goeder trouw gegevens helen in het algemeen belang.[12] Zonder deze uitzondering had deze strafbepaling een onwenselijke inbreuk gemaakt op de persvrijheid. De WikiLeaks kwestie, de Snowden-onthullingen, alsook de Panama Papers zouden dan in beginsel onder de Nederlandse verbodsbepaling vallen.
Hoewel slechts een maximum gevangenisstraf van 1 jaar wordt verbonden aan de heling van gegevens, wordt het toch een feit waarvoor voorlopige hechtenis is toegestaan. Het artikel wordt ingevoegd onder 67 lid 1 sub b Sv. Deze toevoeging zal vermoedelijk bedoeld zijn om bepaalde bijzondere digitale opsporingsmiddelen in te kunnen zetten die vereisen dat sprake is van een feit als bedoeld in art. 67 lid 1 Sv. Art. 138c Sr, de verduistering van gegevens, waarop ook een maximum gevangenisstraf van 1 jaar staat, wordt daarentegen niet opgenomen onder art. 67 lid 1 Sv. Waarop dat onderscheid precies gebaseerd is, wordt niet nader verduidelijkt in de wetsgeschiedenis.

2. Bevel art. 125p Sv

Op grond van art. 54a Sr wordt een dienstverlener op het internet gevrijwaard voor strafrechtelijke vervolging voor de door hem opgeslagen of doorgegeven gegevens, indien hij met de inhoud van die gegevens geen bemoeienis heeft gehad en de strafbare gegevens na bevel van de officier van justitie verwijdert. De officier heeft volgens art. 54a Sr een machtiging van de rechter-commissaris nodig om een bevel om gegevens te verwijderen uit te vaardigen, hetgeen als een belangrijke waarborg voor de uitingsvrijheid en tegen zelfcensuur kan worden gezien.
Art. 54a Sr is een implementatie van de EU Richtlijn inzake de elektronische handel (2000/31/EG) en is de digitale evenknie van art. 53 en 54 Sr. Die laatste artikelen vrijwaren de drukker en de uitgever voor strafrechtelijke vervolging; dit in verband met de vrijheid van drukpers uit art. 7 Grondwet.
Deze vervolgingsuitsluitingsgrond krijgt een tegenhanger in een nieuwe bevelsbevoegdheid. Onder de oude wet volgde de bevoegdheid van de officier tot het geven van een bevel tot verwijderen van gegevens impliciet uit art. 54a Sr, maar de wet Computercriminaliteit III heeft nu de bevelsbevoegdheid uitdrukkelijk gemaakt door deze in een nieuw art. 125p Sv te plaatsen. Dit komt de duidelijkheid van de regeling ten goede. Tegenover een dergelijke vervolgingsuitsluitingsgrond hoort uit oogpunt van de uitingsvrijheid immers een nauwkeurig omschreven bevelsbevoegdheid te staan.
In het oorspronkelijke conceptwetsvoorstel Versterking Bestrijding Computercriminaliteit is door de regering gepoogd om het vereiste van een machtiging van de rechter-commissaris te schrappen. De officier van justitie zou aldus zelfstandig het bevel hebben kunnen geven om bepaalde uitingen te verwijderen. Dat zou ernstig hebben afgedaan aan de rechtswaarborgen rondom de uitingsvrijheid op het internet. Het voorstel van een zelfstandige bevelsbevoegdheid van de officier van justitie is in de Tweede Kamer echter op veel tegenstand gestuit en in de uiteindelijke wet is de voorwaarde van de machtiging van de rechter-commissaris behouden. Qua verandering van regelgeving is tevens van belang dat in art. 552a Sv middels de nieuwe wet ook expliciet de mogelijkheid tot klagen over een bevel ex art. 125p Sv wordt opgenomen. Onder de oude wet werd dat door de Hoge Raad niet mogelijk geacht.[13]

3. Inzet lokpuber bij grooming en verleiding tot ontucht

Art. 248a en 248e Sr worden aangevuld met de zinssnede *'[Hij die zich] […] al dan niet met een technisch hulpmiddel, waaronder een virtuele creatie van een persoon die de leeftijd van zestien jaren nog niet heeft bereikt, voordoet als een persoon die de leeftijd van [zestien/achttien]14 jaren nog niet heeft bereikt […]'*
Aanleiding hiervoor was een uitspraak van het Hof Den Haag dat in 2013 de inzet van de lokpuber (een opsporingsambtenaar die zich voordoet als minderjarige) had afgewezen als voor een veroordeling toereikend opsporingsmiddel.[15] Uit de wetsgeschiedenis volgde naar het oordeel van het Hof dat voor strafbaar handelen noodzakelijk was dat het beoogde slachtoffer daadwerkelijk minderjarig was. Uit de Memorie van Toelichting van de oude wet bleek namelijk dat art. 248e Sr uitvoering gaf aan art. 23 Verdrag van Lanzarote,[16] en strekte tot bescherming van *daadwerkelijke* minderjarigen.[17] De Minister van Justitie heeft tijdens de toenmalige parlementaire behandeling van het wetsvoorstel in dat licht ook uitdrukkelijk gesteld dat als het slachtoffer meerderjarig was, maar de verdachte meende dat het om een minderjarige ging, dat niet strafbaar was.[18] Het arrest en de daarin aangehaalde wetsgeschiedenis maakte het toevoegen van een aanvullende zinssnede in de strafbepaling noodzakelijk om tot een veroordeling te komen bij verleiding of grooming van een lokpuber.
De inzet van de *virtuele* lokpuber speelde bij het originele wetsvoorstel geen rol, en is pas later toegevoegd. In 2016 introduceerde Terre des Hommes, na hun eerste Sweetie-project, Sweetie 2.0 als nieuw wapen in de strijd tegen kindermisbruik.

12. Art. 139g lid 3 Sr.

13. Hoge Raad 15 april 2014, *NJ* 2014, 327.
14. In art. 248a Sr is de leeftijdsgrens gesteld op 18, en in art. 248e Sr is de leeftijdsgrens gesteld op 16.
15. Gerechtshof Den Haag 25 juni 2013, *NJ* 2014, 123, ECLI:NL:GHDHA:2013:2302.
16. Verdrag van de Raad van Europa inzake de bescherming van kinderen tegen seksuele uitbuiting en seksueel misbruik, *Trb.* 2008, 58.
17. *Kamerstukken II* 2008/09, 31808, 6, p. 12.
18. Ibid.

Sweetie 2.0 is een volledig autonome kunstmatige intelligentie die in staat is om zonder menselijke tussenkomst in meerdere chatrooms tegelijkertijd tientallen volwaardige gesprekken te voeren in de vorm van een minderjarig Aziatisch meisje.[19] Terre des Hommes heeft met Sweetie 2.0 gelobbyd om de Nederlandse politiek ervan te overtuigen de virtuele lokpuber in te zetten als opsporingsinstrument bij kindermisbruik en grooming.[20]

Hoewel de regering aldus bij aanvang van de nieuwe wet niet de intentie had om virtuele lokpubers als lokmiddel in de wet op te nemen, stelden Tweede Kamerleden Tellegen en Van Toorenburg op 13 december 2016 bij amendement voor om de inzet van virtuele creaties als Sweetie bij de Nederlandse opsporing van groomers mogelijk te maken.[21] Dit amendement werd door de kamer zonder noemenswaardige discussie aangenomen.

Het verbod op uitlokking en het Tallon-criterium[22] blijven uiteraard ook onder de nieuwe regeling van kracht. De verdachte mag niet gebracht zijn tot een andere handeling dan waarop zijn opzet reeds van tevoren was gericht.

De inzet van de (virtuele) lokpuber kent zoals ook onderkend in de wetsgeschiedenis bepaaldelijk risico's op uitlokking. Zo is het bij de inzet van een (virtuele) lokpuber goed denkbaar dat een sociaal beperkte meerderjarige internetgebruiker niet op zoek is naar romantische contacten met een minderjarige, maar dat hij door bepaalde uitingen van de lokpuber of de chatbot over zijn reguliere grenzen heen stapt. Het is tevens denkbaar dat een eenzaam persoon door de enkele aandacht die zo een zedenrechercheur of chatbot aan hem zou geven, gevoelens zou kunnen ontwikkelen, welke uiteindelijk zouden kunnen leiden tot zedendelinquentie. Het verdient in dat licht vermelding dat na het eerste Sweetie project het OM een tiental van die zaken in onderzoek nam. In geen van die zaken is vervolging ingesteld ter zake van grooming, omdat volgens het OM telkens sprake was van ongeoorloofde uitlokking.[23] De staatssecretaris sprak op 20 juni 2017 zelfs enige tijd na het aannemen van het amendement Tellegen en Van Toorenburg in de Eerste Kamer nog de volgende ongelukkige zin uit: *'Het openbaar ministerie maakt tot nu toe geen gebruik van virtuele kindcreaties bij de opsporing van online zedendelicten, omdat uit praktijkervaringen is gebleken dat uitlokking hierbij onvermijdelijk is.'*[24]

Tot slot speelt bij de lokpuber de problematiek dat met deze wetswijziging *de facto* een nieuw bijzonder opsporingsmiddel wordt gecreëerd, maar dat deze enkel terug te vinden is in het materiële strafrecht.[25] Zo een bevoegdheid zou in beginsel een expliciete tegenhanger moeten krijgen in het formele strafrecht. In de formele wet kunnen aan een bijzondere opsporingsbevoegdheid eisen en waarborgen worden verbonden die nu ten node gemist worden. In ieder geval de virtuele lokpuber verdient een streng kader van waarborgen om erop toe te zien dat het risico op uitlokking geminimaliseerd wordt en geen ontoelaatbare inbreuken worden gemaakt op de persoonlijke levenssfeer.

4. Strafbaarstelling online handelsfraude (art. 326d Sr)

De nieuwe verbodsbepaling van online handelsfraude ziet op het maken van een beroep of gewoonte van het middels het internet aanbieden van goederen of diensten, met het oogmerk die niet te leveren, maar wel de betaling te ontvangen. Er wordt een strafbedreiging aan gekoppeld van 4 jaar, waarmee het een feit als bedoeld in art. 67 lid Sv wordt en het merendeel van de digitale opsporingsbevoegdheden bij een verdenking ingezet kunnen worden.

De aanleiding voor de aanvullende strafbaarstelling kan gevonden worden in de toch wat casuïstische rechtspraak op dit vlak. Voor een veroordeling onder de reguliere verbodsbepaling van oplichting ex art. 326 Sr werd veelal geëist dat er in samenspel met het zich voordoen als een bonafide verkoper, voldoende andere omstandigheden aanwezig waren om van oplichting te spreken. Dit werkt casuistiek in de hand.

Deze strafbaarstelling lijkt daarom ook een aanvaardbare toevoeging aan de Nederlandse wet. Betoogd kan worden dat een groeiende behoefte bestond aan duidelijke regelgeving op dit gebied, nu steeds meer mensen goederen op internet kopen en diensten middels het internet afnemen waarbij het gebrek aan een fysieke winkel of bedrijfsruimte de mogelijkheden tot verhaal bij het uitblijven van de levering van die goederen en diensten beperkt. Hoe het *oogmerk* om niet te leveren maar wel betaling te ontvangen in de praktijk vastgesteld gaat worden, lijkt niet voor eenduidige uitleg vatbaar. Dit kan mogelijk toch weer tot casuïstische rechtspraak leiden.

5. Hacken als opsporingsbevoegdheid: (art. 126nba, uba en zba Sv)

De nieuwe hackbevoegdheid van art. 126nba Sv (alsmede art. 126uba, en 126zba Sv)[26] vormt – samen

19. Anne de Hingh, 'Grooming in het wetsvoorstel Computercriminaliteit III', *Computerrecht* 2018/162.
20. Ibid.
21. *Kamerstukken II* 2016/17, 34372, 15.
22. Zie HR 4 december 1979, *NJ* 1980, 356.
23. *Aanhangsel Handelingen* 2016/17, nr. 948.
24. *Kamerstukken I* 2016/17, 34372, p. 28.
25. Zie voor een uitgebreider bespreking van deze problematiek C. Grijsen, B.J. Polman & A. De Lange, 'De uitbreiding van de strafbaarstelling van grooming met de inzet van de lokpuber tot doel', *Strafblad* 2017, p. 382 -389.
26. Deze verschillende bijzondere opsporingsbevoegdheden zijn opgenomen in de titels IVa, V en Va en zijn buiten de gebruikelijke verschillen in het toepasselijke verdenkingscriterium gelijk. Ik zal hieronder voor

met het gedurende de wetsaanloop verwijderde ontsleutelingsbevel aan de verdachte – het meest controversiële onderdeel van de Wet Computercriminaliteit III. Er speelt door het grensoverschrijdende karakter van de hackbevoegdheid daarbij ook enige complexe rechtsmachtsproblematiek, waaraan ik later in dit artikel nog aandacht aan besteed.

5.1. Mogelijke toepassingen

De mogelijke toepassingen van het voorgestelde art. 126nba Sv worden in de wet zeer breed omschreven. Het hacken door de overheid wordt mogelijk met het oog op:

- Het verrichten van onderzoekshandelingen. Daarbij kan bijvoorbeeld gedacht worden aan het vaststellen van de aanwezigheid van gegevens, het bepalen van de identiteit of de locatie van de gebruiker en het overnemen en tappen van gegevens.
- Het ontoegankelijk maken van gegevens ter beëindiging van strafbare feiten of ter voorkoming van nieuwe strafbare feiten. Daarbij kan gedacht worden aan het stoppen van verder verspreiden van illegaal materiaal zoals kinderpornografie, bedrijfsgeheimen of creditcardgegevens, maar ook aan het verstoren van botnets of DDoS-aanvallen.
- Het mogelijk maken van andere bijzondere opsporingsbevoegdheden. Dit wordt ook wel het hacken als steunbevoegdheid genoemd en houdt in dat gehackt mag worden ter ondersteuning van het aftappen van gesprekken, maar ook voor het OVC-en zonder dat het nodig is fysiek een gebouw of woning binnen te dringen. Hiermee wordt het bijvoorbeeld mogelijk om de microfoon en de camera van een computer of smartphone zonder weten van de gebruiker aan te zetten en de gebruiker middels diens GPS en camera stelselmatig te observeren.

Het hacken wordt toegestaan in een *geautomatiseerd werk* dat bij de verdachte *in gebruik* is. Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken.[27] Naast de computer of smartphone zelf, mag dus gehackt worden in bijvoorbeeld een usbstick die in het apparaat zit of een harde schijf die met het apparaat verbonden is, maar ook aan andere netwerken die met die computer of smartphone verbonden zijn. De voortschrijdende ontwikkeling van '*the internet of things*' brengt mee dat bijvoorbeeld ook navigatiesystemen, slimme koelkasten en slimme thermostaten onder art. 126nba Sv gehackt mogen worden. Het is niet onwaarschijnlijk dat binnen een aantal jaren haast alle apparatuur aanwezig in een woning, kantoor en auto als geautomatiseerd werk is aan te merken. De wetsgeschiedenis stelt daarbij uitdrukkelijk dat het niet de bedoeling is om bij voorbaat enig apparaat uit te sluiten van de hackbevoegheid. Alleen over de pacemaker en het interne gehoorapparaat is door de Minister na veel vijven en zessen toegezegd dat de nieuwe bevoegdheid niet bedoeld was om deze apparaten te hacken.[28]

Onder een geautomatiseerd werk *bij verdachte in gebruik* wordt daarbij niet enkel verstaan een geautomatiseerd werk dat het bezit is van de verdachte. Als men reden heeft om te veronderstellen de verdachte de computer van een derde gebruikt, mag ook die gehackt worden. Het is in dat licht niet onredelijk te verwachten dat ook de computers van ouders, partners of vrienden van een verdachte binnen het bereik van de hackbevoegdheid zullen vallen.

Het is op basis van het bovenstaande niet onredelijk om te betogen dat de hackbevoegdheid de meest potentieel ingrijpende opsporingsbevoegdheid is die de Nederlandse opsporingsdiensten ooit in handen hebben gehad. Daarbij speelt ook dat, anders dan bij andere zeer ingrijpende opsporingsbevoegdheden zoals het opnemen van vertrouwelijke communicatie (OVC) of een infiltratie, de kosten vermoedelijk steeds lager zullen worden en schaarste van tijd en middelen, in ieder geval op termijn minder een rol zal spelen bij het overwegen van een inzet. Technologische ontwikkelingen in de digitale wereld plegen immers, naast exponentieel toenemende rekenkracht, tot steeds lagere kosten te leiden.[29]

5.2. Voorwaarden voor de inzet

De in de wet opgenomen voorwaarden voor het hacken door de opsporingsdiensten luiden als volgt:

- er moet sprake zijn van een dringend onderzoeksbelang en een ernstige inbreuk op de rechtsorde;[30]
- er moet sprake zijn van een voorlopige hechtenisfeit respectievelijk een feit waarop een gevangenisstraf van 8 jaar of meer staat of bij AMvB aangewezen is, afhankelijk van met welk doel de bevoegdheid wordt ingezet;
- de inzet van de bevoegdheid behoeft een bevel van het OM, waarin het doel waarvoor deze bevoegdheid wordt ingezet nauwkeurig wordt omschreven;

het leesgemak enkel art. 126nba Sv aanhalen.

27. Art. 80sexies Sr.

28. *Handelingen I* 2017/18 , 34372, 34, p. 23.
29. Zie voor een toelichting op deze ontwikkeling die als Moore's Law bekend staat: https://en.wikipedia.org/wiki/Moore%27s_law en voor het oorspronkelijke artikel van Moore waaruit de wet voortvloeide: http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf .
30. De Minister was in de wetsgeschiedenis erg stellig dat deze begrippen zeer consistent door de Nederlandse rechter worden uitgelegd (*Handelingen I 2017/18*, 34372, 34, p. 17.) Dat is niet zondermeer de ervaring van de auteur, waarmee een risico van *forum-shoppen* niet ondenkbaar is.

– het bevel dient voorzien te zijn van een machtiging van de rechter-commissaris.

Niet alle mogelijke toepassingen van de hackbevoegdheid mogen bij elk feit worden ingezet. Een voorlopige hechtenisfeit is voorgeschreven bij het hacken met het oog op:
– de vaststelling van identiteit of de gebruiker van het geautomatiseerde werk;
– tappen of OVC-en ; en
– het stelselmatig observeren van een persoon.

Een feit waarop een gevangenisstraf van 8 jaar of meer staat of een bij AMvB aangewezen feit is voorgeschreven bij hacken met het oog op:
– het doorzoeken en kopiëren van op de computer opgeslagen gegevens; en
– het ontoegankelijk maken van gegevens, waaronder bijvoorbeeld het verstoren van een botnet of DDoS aanval.

Het bevel kan worden gegeven voor een periode van maximaal 4 weken. Echter, het bevel kan, als de omstandigheden daartoe aanleiding geven, worden gewijzigd, aangevuld of verlengd.

5.3. Bij AMvB aangewezen feiten

In het *Besluit onderzoek in een geautomatiseerd werk*[31] worden in art. 2 de misdrijven aangewezen die voor de toepassing van de hackbevoegdheid gelijk worden gesteld met feiten waarop een maximum gevangenisstraf van minimaal 8 jaar staat. Het betreffen ten eerste een aantal cyberdelicten, die in het Wetboek vaak met relatief milde straffen worden bedreigd zoals spammen, DDoSen, malware, computervredebreuk, en het beschadigen van gegevens. Het mogelijk maken van het toepassen van de verstoringsbevoegdheid van art. 126nba Sv is begrijpelijk te achten bij deze verder licht bestrafbare computerfeiten. Indien de opsporingsdiensten een grote DDoS-aanval of malware-operatie op het spoor is, is het redelijkerwijs wenselijk hen ook de wettelijke bevoegdheden te bieden om die handelingen nader op te sporen en te verstoren.
De lijst van aangewezen feiten is, zoals ook door leden van de Staten-Generaal opgemerkt, niet kort te noemen.[32] Van de commune delicten worden (onder meer) aangewezen corruptie, spionage, mensensmokkel en rekrutering voor terrorisme, maar ook zedenmisdrijven tegen minderjarigen en kinderporno, en bijvoorbeeld stalking. Ook hier is het niet moeilijk begrip op te brengen voor het feit dat de opsporing het zware middel van hacken inzet ter voorkoming of verstoring van, in ieder geval voor de slachtoffers, toch ernstige strafbare feiten.
De feiten welke helaas ook zijn aangewezen bij de AMvB zijn de *prosecutor's darling's* valsheid in geschrifte en witwassen.[33] Bij zo een beetje iedere denkbare fraude, hoe klein ook, speelt tevens enige vorm van valsheid in geschrifte, en met haast ieder vermogensdelict kan door het OM tevens een daarmee verbonden witwassen worden betoogd. Hiermee kan de ingrijpender variant van de hackbevoegdheid dus plots weer erg breed ingezet worden. De mogelijkheid van een dergelijke brede inzet van de hackbevoegdheid baart zorgen. Omdat de aanwijzing van de aanvullende feiten bij AMvB verder plaats kan vinden bestaat tevens het risico dat de reikwijdte van de inzet van dit zeer ingrijpende opsporingsmiddel zonder parlementaire betrokkenheid in de toekomst verder wordt uitgebreid.[34]

5.4. Nadere waarborgen inzet hackbevoegdheid

Niet in de wet maar bij gedelegeerde regelgeving zijn een aantal van de belangrijkste waarborgen ingebouwd voor de inzet van de hackbevoegdheid. Bij zulke ingrijpende regelgeving als de hackbevoegdheid is dit niet zondermeer wenselijk te achten en zou vanuit het oogpunt van kenbaarheid en rechtszekerheid te verkiezen zijn dat de Staten-Generaal betrokken worden bij het mogelijk later afbouwen van de nu aanwezige waarborgen.
Het eerder genoemde Besluit onderzoek in een geautomatiseerd werk verplicht tot het opmaken van een proces-verbaal indien bij het onderzoek onregelmatigheden hebben plaatsgevonden en regelt de beperking van de functionaliteiten van de software.[35] Van groot belang is tevens dat het Besluit voorschrijft dat bij het hacken een soort van 'zwarte doos' meeloopt die alle handelingen van de opsporingsdiensten vastlegt. Hiermee kan het handelen van de opsporingsdiensten achteraf gecontroleerd worden.
Het Besluit alsmede de wet kent het systeemtoezicht op de hackbevoegdheid toe aan Inspectie Justitie en Veiligheid. Systeemtoezicht is in het kader van de hackbevoegdheid erg belangrijk, want een groot deel van de inzetten van de hackbevoegdheid zal niet tot een zaak leiden die voor de rechter komt. Veel deskundigen en parlementsleden hadden daarom graag een meer gespecialiseerd systeemtoezicht gezien.
In de Aanwijzing opsporingsbevoegdheden wordt geregeld dat de inzet van de hackbevoegdheid voorafwordt getoetst door de Centrale Toetsingscommissie (CTC[36]) van het OM en onderworpen is aan

31. *Stb.* 2018, 340.
32. *Kamerstukken I* 2018/19, 34372, L, p. 2.
33. Het betreft overigens enkel de opzetvariant van art. 240b Sr.
34. Niet onwaarschijnlijk is te achten dat onder druk van de Verenigde Staten in de voorzienbare toekomst bijvoorbeeld auteursrechtelijke inbreuken mogelijk worden toegevoegd aan de lijst.
35. Dat laatste wil zeggen dat niet meer dingen gedaan kunnen worden dan waarvoor een machtiging is gegeven, zoals bijvoorbeeld het op afstand aanzetten van de camera als dat niet geaccordeerd is door de RC.
36. De CTC, samengesteld uit leden van het openbaar ministerie en politie, is een intern adviesorgaan van het openbaar ministerie, dat het College adviseert omtrent de voorgenomen inzet van bepaalde bijzondere

toestemming van het College van Procureurs-Generaal. De cijfers lijken uit te wijzen dat deze voorwaarde normaal gepaard gaat met een minder veelvoudige inzet van een opsporingsmiddel.
In het regeerakkoord is verder afgesproken dat software enkel per operatie wordt aangeschaft en dat de opsporingsdiensten niet over een eigen hacksoftware-omgeving zullen beschikken.[37] Hoewel deze waarborg als een zeer belangrijke kan worden aangemerkt (wat men niet heeft kan men immers niet misbruiken), is een regeerakkoord mijns inziens geen passende plaats om een dergelijke waarborg in op te nemen. Een regeerakkoord heeft immers een zeer beperkte levensduur en de kans dat deze waarborg door een volgende coalitie in verband met bijvoorbeeld de kosten zal worden gewijzigd is allerminst denkbeeldig te achten.

5.5. Rechtsmacht problematiek art. 126nba-hacken

Het is niet eenvoudig om, indien men in een geautomatiseerd werk hackt, en vooral als men verder doorhackt in daaraan verbonden netwerken of gegevensdragers, ervoor te zorgen dat men dat telkens doet op Nederlands grondgebied. Overtredingen van het volkenrecht lijken daarmee allerminst uit te kunnen worden gesloten. Zoals ook werd opgemerkt in de redenen die de wetgever aanvoerde als noodzaak voor de hackbevoegdheid, brengen technologische ontwikkelingen mee dat data overal ter wereld wordt opgeslagen en niet altijd valt te lokaliseren.[38] Het is om diezelfde reden ook goed denkbaar dat (enig onderdeel van) het geautomatiseerde werk dat men hackt, zich in een andere staat bevindt. In dat geval wordt er extraterritoriaal opgespoord, hetgeen volgens het internationaal recht in beginsel niet toegestaan is.
Art. 539a Sv voorziet wel in een wettelijke basis voor extraterritoriale opsporing, maar deze wordt beperkt door het volkenrecht. De bevoegdheid tot inzet van (digitale) opsporingsbevoegdheden is volgens het volkenrecht als uiting van de handhavende rechtsmacht in beginsel beperkt tot het eigen grondgebied.[39] Daarbuiten is een verdragsbasis nodig, dan wel (ad hoc) instemming van de Staat op wiens grondgebied wordt opgespoord.
Het enige concrete verdragsartikel dat zelfstandige extraterritoriale digitale opsporing regelt is art. 32 *Cybercrimeverdrag*.[40] Een verdragsstaat mag op grond van art. 32:

1. zich toegang verschaffen tot openbare data onafhankelijk van waar deze is opgeslagen;
2. toegang verkrijgen tot data opgeslagen in een andere verdragsstaat:
   – met wettige en vrijwillige toestemming van een persoon;
   – die bevoegd is die data te verstrekken; en
   – in de opsporende staat aanwezig is.

Het zelfstandig digitaal opsporen op grondgebied van andere landen is volgens het Cybercrimeverdrag aldus in beginsel beperkt tot zoeken naar openbare informatie op het net of, met toestemming van een gerechtigde in Nederland, gegevens inzien die in het buitenland zijn opgeslagen.[41] Wanneer de bevoegdheid van art. 126nba Sv zodanig wordt ingezet dat opsporingsambtenaren zich daarmee toegang verschaffen tot gegevens die zich in een andere staat bevinden, zonder dat die staat daarmee instemt, maakt de bevoegdheid inbreuk op het volkenrecht en de soevereiniteit van de staat waar de gegevens zijn opgeslagen of worden verwerkt.
Het is overigens wel de bedoeling dat indien Nederlandse opsporingsdiensten erachter komen dat het geautomatiseerde werk of de gegevensdrager die gehackt wordt in het buitenland staat, alsnog een rechtshulpverzoek wordt gedaan.[42] Of deze bedoeling in de praktijk ook werkelijk zal uitwerken tot het staken van kennelijk dringend geachte opsporingshandelingen totdat een rechtshulpverzoek is verzonden en ingewilligd valt helaas te betwijfelen.

5.6. Hoge Raad sanctioneert (enkelvoudige) inbreuken niet binnen art. 359a Sv

Hoewel het grensoverschrijdend toepassen van de hackbevoegdheid zoals gezegd in beginsel niet is toegestaan (maar haast onvermijdbaar lijkt), is op strafrechtelijke normering van grensoverschrijdend hacken het toch wat krappe kader van art. 359a Sv van toepassing. Volgens een toonzettend arrest van de Hoge Raad uit 2010 is binnen dat kader de vraag of door de Nederlandse opsporingsambtenaren het volkenrecht is nageleefd, in het kader van de strafzaak tegen een verdachte in beginsel niet relevant. Dit omdat de belangen die het volkenrecht beoogt te beschermen, volgens de Hoge Raad geen belangen zijn van de verdachte, maar van de staat op wiens grondgebied onrechtmatig is opgespoord.[43] Ondanks dit arrest is echter goed betoogbaar dat wel ruimte bestaat om verweer te voeren op digitale inbreuken op de soevereiniteit

opsporingsbevoegdheden en methodieken.
37. *Vertrouwen in de toekomst* Regeerakkoord 2017 – 21 van VVD, CDA, D66 en ChristenUnie, p. 3.
38. Zie bijvoorbeeld *Kamerstukken II* 2016/17, 34372, 6, p. 3.
39. Vgl. *Frankrijk t. Turkije* (*SS Lotus*-zaak) Permanent Court of International Justice, P.C.I.J. (ser. A) No 10 (1927).
40. Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Cybercrime Verdrag) (*Trb.* 2002, 18 en *Trb.* 2004, 290).
41. Betoogbaar is overigens dat deze twee handelingen volkenrechtelijk ook zouden zijn toegestaan zelfs zonder verdragsbasis.
42. *Kamerstukken II* 2016/17, 34372, 6, p. 94.
43. HR 5 oktober 2010, *NJ* 2011/169.

van andere landen in het kader van stelselmatige vormverzuimen.[44,45]

5.7. Argumenten wetgever

Er zijn verschillende redenen door de wetgever aangevoerd om te rechtvaardigen dat een opsporingsmiddel in het leven is geroepen dat naar alle waarschijnlijkheid zal leiden tot herhaalde inbreuken op het volkenrecht en de soevereiniteit van andere landen, zonder dat in de Nederlandse regelgeving afdoende waarborgen zijn ingebouwd om die inbreuken te voorkomen.
De wetgever beroept zich ten eerste op het slechts zeer beperkt overtuigende argument dat andere landen ook doende zijn gelijksoortige regelgeving in het leven te roepen. Van een dergelijk argument kan niet gezegd worden dat zij vanuit een staats- en volkenrechtelijk legitimiteitsperspectief veel gezag toekomt.
De wetgever beroept zich daarnaast op het feit dat binnen de digitale wereld het territorialiteitsbeginsel onder druk staat. Hoewel voor dit argument veel valt te zeggen, kan een dergelijke vaststelling niet zondermeer leiden tot de conclusie dat gewichtige regels van het volkenrecht eenzijdig door Nederland terzijde mogen worden geschoven. De Staat heeft in dat kader een uitgebreid onderzoek laten doen door Koops en Goodwin[46] omtrent de rechtmatigheid van grensoverschrijdende digitale opsprong, maar ook daarin werd bevestigd dat de rechtsmachtsuitleg van art. 32 Cybercrimeverdrag als volkenrechtelijk grensbepalend moest worden gezien. Wel gaven Koops en Goodwin een voorzet om in afwachting van een verdragskader binnen een legitiem kader voorop te lopen met een transparante en met waarborgen omklede minder strikte interpretatie van volkenrecht in cyberspace, welke door de wetgever gretig werd omarmd.
Ten derde stelt de wetgever dat haast bij cyberdelicten vaak geboden is, wat het afwachten van rechtshulp niet altijd mogelijk maakt. Ook ten gunste van dit argument valt veel te zeggen. Het is in ieder geval betoogbaar dat soms niet zonder grote schade gewacht kan worden op een uitvoering van een rechtshulpverzoek. Als een dienst van een vitale infrastructuur of overheid wordt lamgelegd door een DDOS aanval uit een ander land of als de computers van een ziekenhuis zijn geïnfecteerd door een uit het buitenland aangestuurd botnet, kan het wachten op het inwilligen van een rechtshulpverzoek grote en onomkeerbare schade met zich meebrengen.
Deze steekhoudende argumenten ten spijt kan toch bezwaarlijk gezegd worden dat het door de wetgever omarmde standpunt van in afwachting van een verdragskader met legitiem kader voorop lopen met een transparante en met waarborgen omklede minder strikte interpretatie van internationaal recht in cyberspace, als alternatief voor het volkenrecht voldoende overtuigend is. Zulks temeer nu de inzet van de bevoegdheid van art. 126nba Sv zich niet beperkt tot cyberdelicten waarbij de bijzondere omstandigheden zoals door de wetgever aangevoerd zich voordoen en het optreden in strijd met het volkenrecht vergoelijken.

5.8. Resterende zorgen over art. 126nba-hacken

Zowel binnen als buiten het volkenrechtelijke kader leeft bij velen nog een aantal grote zorgen over de bevoegdheden van art. 126nba Sv. Een aantal daarvan wordt hieronder kort uiteengezet.

5.9. Meest ernstige vorm van inbreuk op privacy

Bij inmiddels de meeste Nederlanders staat op hun computer en telefoon hun hele leven. Qua inbreuk op de persoonlijke levenssfeer zal het doorzoeken van hun computer of smartphone niet zelden als meer ingrijpend dan een huiszoeking of telefoontap worden ervaren. Bij het doorzoeken van een computer of smartphone zullen, door de geautomatiseerde opslagfunctie daarnaast alle berichten en foto's die een onschuldige burger met een verdachte heeft uitgewisseld in het vizier van de opsporingsdiensten komen. De mate van inbreuk op de privacy van de burger kan bij de hackbevoegdheid dan ook niet eenvoudig overschat worden.

5.10. Steeds verdergaande mogelijkheden door nieuwe eigen apparatuur

Door de nieuwe apparaten die in Nederland beschikbaar worden, wordt iedere kamer daarnaast een potentiële verhoorkamer. Daarbij kan niet enkel gedacht worden aan de smartphone of de laptop waarvan de camera op afstand aan kan worden gezet, maar ook aan de XBOX one Kinect of de Amazon Echo, met beiden een zeer goede microfoon die alles in de kamer kan horen en die bovendien altijd aanstaat. De voortschrijdende technologie maakt aldus de mate van potentiële inbreuk op de persoonlijke levenssfeer van de hackbevoegdheid dagelijks groter.

44. Dat wil zeggen de situatie waarin het desbetreffende vormverzuim naar uit objectieve gegevens blijkt zozeer bij herhaling voorkomt dat zijn structureel karakter vaststaat en de verantwoordelijke autoriteiten zich, vanaf het moment waarop dit structurele verzuim hun bekend moet zijn geweest, onvoldoende inspanningen hebben getroost overtredingen van het desbetreffende voorschrift te voorkomen.
45. Daarbij zou enige diplomatieke druk ook een rol kunnen spelen. Indien bemerkt wordt dat Nederland stelselmatig de soevereiniteit van een bepaald land schendt door op diens grondgebied te hacken zou bekendheid daarmee bij de ambassade van dat land mogelijk kunnen lijden tot diplomatieke druk van dat land om die opsporingsresultaten te vernietigen.
46. B.J. Koops & M. Goodwin, *Cyberspace, the cloud, and cross-border criminal investigation The limits and possibilities of international law*, Universiteit van Tilburg - TILT Tilburg Institute for Law, Technology, and Society, WODC 2014.

5.11. Misbruik ligt op de loer

Er bestaat een niet onredelijke vrees dat de hackbevoegdheden relatief eenvoudig misbruikt kunnen worden. Het is erg lastig om functionaliteiten die (al dan niet in opdracht van de rechter-commissaris) uit zijn gezet in bepaalde hacksoftware, ook uit te houden voor de gespecialiseerde gebruikers van die software. In Duitsland is bijvoorbeeld gebleken dat de spyware die bedoeld was om alleen Skype gesprekken af te luisteren, in de praktijk ook ingezet kon worden voor het op afstand aanzetten van de microfoon en de camera van de computer.[47] Zoals eerder opgemerkt zal de inzet van de zeer inbreuk makende hackbevoegdheid door de voortschrijdende techniek vermoedelijk steeds goedkoper en eenvoudiger worden, waardoor de kostenvraag die bij veel van de andere ingrijpende opsporingsmiddelen als rem werken, niet lang meer zal spelen.

5.12. Vertrouwen op niet gangbaar worden

De Minister gaf bij de behandeling van de wet aan dat hij niet verwachtte dat de hackbevoegdheid zou verworden tot een gangbaar opsporingsmiddel, onder meer door de *'strikte wettelijke voorwaarden voor de inzet'*, waaronder een machtiging van de rechter-commissaris.[48] Een dergelijke machtiging van de rechter-commissaris is echter uiteraard ook benodigd voor een telefoontap en niet gebleken is dat de opsporingsdiensten met die bevoegdheid altijd even spaarzaam omspringen. De eis van advisering door de CTC en instemming van het College, vloeit – anders dan de Minister leek te stellen bij de behandeling in de Eerste Kamer – niet voort uit de wet, maar uit de Aanwijzing opsporingsbevoegdheden en kan dus op ieder moment zonder inmenging van de Staten-Generaal worden gewijzigd.

5.13. Inbreuken door andere landen

Indien Nederlandse opsporingsdiensten geautomatiseerde werken in buitenland zullen hacken, biedt dat andere landen een rechtvaardiging om dat ook in Nederland te doen. Andere landen – zoals Rusland of China – zullen dan ook mogelijk sneller mee gaan kijken in geautomatiseerde werken die in Nederland staan. Dit kan in het minst erge geval lopende Nederlandse opsporingsonderzoeken verstoren, maar in het ergste geval kunnen hierdoor ook geautomatiseerde werken van volstrekt onschuldige Nederlanders het slachtoffer worden van meekijken en meeluisteren door buitenlandse overheden.

5.14. Ontoegankelijk maken gegevens in het buitenland

Binnen de hackbevoegdheid van de overheid is daarnaast het verstoren of ontoegankelijk maken van gegevens een mogelijkheid. Hoewel het door de Nederlandse opsporingsdiensten verstoren van bijvoorbeeld een kinderpornowebsite in een ander land door weinig Nederlanders als onwenselijk zal worden ervaren, brengt het risico van reciprociteit gevaren mee voor de uitingsvrijheid. Wat landen als een ernstig misdrijf zien, hangt immers veelal af van de normen en waarden van die landen. Dit roept dan de vraag op of een land als Indonesië of Zuid Korea, waar alle pornografie verboden is, ook Nederlandse pornosites ontoegankelijk zullen willen maken indien die zich (mede) richten op Indonesiërs en Zuid Koreanen. Een toekomstige censuurwedloop tussen landen is daarbij niet denkbeeldig te noemen.

5.15. Staatshacken maakt systemen kwetsbaar

Als de opsporingsdiensten bij computers moet kunnen inbreken, hebben ze er belang bij dat die systemen kwetsbaar blijven. Van die kwetsbaarheid profiteren echter niet alleen de opsporingsdiensten. Ook cybercriminelen en buitenlandse mogendheden zullen makkelijker op systemen kunnen inbreken. Een goed voorbeeld is de kwetsbaarheid *'eternal blue'*, die ooit ontdekt werd door de NSA.[49] Dit betrof een exploit in het Server Message Block van Microsoft. De NSA heeft dit lek niet gemeld bij Microsoft omdat het voor hun onderzoeken goed bruikbaar was en Microsoft bezat daarom dus niet de informatie om dit lek te dichten. Op een later moment is ditzelfde exploit gebruikt door kwaadwillenden voor zowel Wannacry[50] als de NotPetya aanval.[51] Wannacry heeft gezorgd voor een ransomware besmetting van zo een 230.000 computers in 150 landen en NotPetya heeft zelfs een groot deel van de Oekraïne lamgelegd, waaronder vliegvelden, banken en energievoorzieningen. Het is niet eenvoudig om een misdrijf te bedenken waarvan de opsporing zo dringend is dat deze het risico op een nieuwe WannaCry of Notpetya rechtvaardigt. Het nieuwe art. 126ffa Sv geeft in dat kader wel regels voor de opsporing om onbekende kwetsbaarheden te melden, waarbij voor het niet melden in beginsel een machtiging van de rechter-commissaris nodig is. De opsporingsdiensten zullen echter veelal echter hacksoftware gebruiken die door anderen is gemaakt en waarvan zij de broncode niet kennen. Deze verplichting om onbekende kwetsbaarheden te melden zal om die reden in de praktijk weinig gevolgen hebben.

47. https://www.nrc.nl/nieuws/2011/10/19/bespioneren-agenten-hier-ook-burgers-via-de-computer-12040698-a210550.
48. *Kamerstukken I* 2016/17, 34372, D, p.46
49. https://en.wikipedia.org/wiki/EternalBlue.
50. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.
51. https://en.wikipedia.org/wiki/Petya_(malware).

In dat licht is verder vermeldenswaardig dat de Minister gedurende de behandeling van de wet zich op het toch bijzondere standpunt stelde, dat de Nederlandse Staat – ondanks de aanschaf van dergelijke hacksoftware die kwetsbaarheden uitbuit – toch geen markt daarvoor in stand hield. *'De markt voor software ten behoeve van het binnendringen in een geautomatiseerd werk is internationaal van aard en bestaat onafhankelijk van dit wetsvoorstel,* aldus de Minister.[52] Dit argument staat in schril contrast met bijvoorbeeld het standpunt van de Nederlandse Staat omtrent het in stand houden van een markt voor kinderpornografie door verdachten door het bekijken van virtuele kinderpornografie.[53]

5.16. Politieke en diplomatieke problemen

De politieke en diplomatieke problemen die grensoverschrijdend hacken met zich meebrengen moeten niet onderschat worden. Een aanzienlijk deel van de Staten neemt hun soevereiniteit serieus en zal het allerminst op prijs stellen als Nederlandse opsporingsdiensten servers, navigatiesystemen en netwerken op hun grondgebied zullen doorzoeken of zelfs verstoren.

5.17. Waarborgen en kaders in te vullen middels AMvB aanwijzing OM

Tot slot kunnen kanttekeningen worden geplaatst bij de waarborgen en kaders waarmee de overheid schermt, die de zorgvuldigheid, proportionaliteit en subsidiariteit van het hacken dienen te waarborgen, zelfs in zoverre dat zij naar mening van de Nederlandse Staat een voldoende legitiem kader vormen waarbinnen geëxperimenteerd mag worden met extraterritoriale opsporing in strijd met het volkenrecht. Vooral de delegatie van die regelgeving waarin veel van de kaders en waarborgen gevonden moeten worden naar de Kroon dan wel het College van Procureurs-Generaal boezemt weinig vertrouwen in voor de robuustheid, consistentie en democratische legitimatie van die voorwaarden en kaders. Aanwijzingen van het OM en AMvB's bieden niet de juiste democratische en tijdsbestendige kaders om zware privacy-inbreuken met de passende waarborgen te omgeven en soms zelfs het volkenrecht te overtreden.

6. Conclusie

De Wet Computercriminaliteit III brengt grote wijzigingen met zich mee op het steeds relevanter wordende rechtsgebied van computercriminaliteit. Naast een aantal bruikbare en zelfs noodzakelijk te achten wijzigingen ter bescherming van de burger die een steeds groter deel van zijn leven doorbrengt in cyberspace, wordt met de invoering van de hackbevoegdheid een zeer ingrijpende opsporingsbevoegdheid in het leven geroepen, waarvan de inzet zich niet beperkt tot het vlak van computercriminaliteit. Dit opsporingsmiddel bezit de potentie om in de toekomst uit te groeien tot de belangrijkste bijzondere opsporingsbevoegdheid voor de opsporingsdiensten, die vele andere opsporingsbevoegdheden zelfs overbodig zou kunnen maken. Enkel de tijd zal leren of de overheid met dit uiterst ingrijpende en in potentie haast alles omvattende opsporingsmiddel verantwoordelijk zal omgaan.

52. *Kamerstukken I* 2016/17, 34372, D, p. 22.
53. *Kamerstukken I* 2001/02, 299b, p. 8.