Artikel

De bevoegdheid van de politie om computers binnen te treden: tijd voor een grondrecht op de bescherming van informatie-technische systemen?

Dr. B. van der Sloot*

Het wetsvoorstel computercriminaliteit III is bijna aangenomen en kent een aantal nieuwe bevoegdheden aan de politie toe, waaronder de mogelijkheid om computers van burgers binnen te treden. Niet alleen kan de politie zodoende onderzoek doen, ook mag zij gegevens kopiëren en aanpassingen doen aan de computer, bijvoorbeeld om bepaalde malware te verwijderen. Commentatoren hebben erop gewezen dat dit een zware inmenging is in de privésfeer van burgers. Het zou dan ook tijd zijn voor een nieuw grondrecht op de integriteit van digitale gegevensdragers. Dit artikel bespreekt de nieuwe bevoegdheid van de politie en de introductie van een mogelijk nieuw grondrecht.

1. Introductie

De Eerste Kamer moet nog officieel instemmen met het wetsvoorstel computercriminaliteit III,[1] maar op een nacht van de een of andere politicus is nochtans niemand bedacht. Tijd dus om kort stil te staan bij deze wet en met name bij een van de meest controversiële bepalingen, namelijk de mogelijkheid voor opsporingsambtenaren om zich heimelijk toegang te verschaffen tot computers en devices van burgers. De Wet computercriminaliteit III is de opvolger van de Wet computercriminaliteit[2] en de Wet computercriminaliteit II[3] en moet in samenhang worden gezien met onder meer de Wet bevoegdheden vorderen gegevens,[4] de zogenoemde contourennota[5] en de herziening[6] van de Wet op de inlichtingen- en veiligheidsdiensten.[7] Het wetsvoorstel bouwt voort op een aantal rapporten dat over cybercriminaliteit, privacy en infiltratie is verschenen,[8] zoals de justitiële verkenningen over tappen en infiltreren,[9] over vei-

* Dr. B. van der Sloot is senior researcher aan het Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

1. <https://www.eerstekamer.nl/wetsvoorstel/34372_computercriminaliteit_iii>.
2. Wet computercriminaliteit (*Stb.* 1993, 33).
3. Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). E.J. Koops, 'Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', *Computerrecht* 02/2003.
4. Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten in verband met de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens).
5. *Kamerstukken II* 2015/16, 29279, 278. Zie daarover ook: M. Kessler, 'Contourennota modernisering Wetboek van Strafvordering', *Ars Aequi* 65/2016.
6. Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017).
7. Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002).
8. Zie ook: <https://www.wodc.nl/binaries/jv9402-volledige-tekst_tcm28-76385.pdf>.
9. <https://www.wodc.nl/binaries/jv1203-volledige-tekst_tcm28-77167.pdf>.

doi: 10.5553/TBSenH/22956700201700300400 3

ligheid in cyberspace[10] en over privacy en function creep[11] en het WODC-rapport 'Cyberspace, the cloud, and cross-border criminal investigation'.[12]

De meeste aandacht in de discussie over het ontwerpwetsvoorstel computercriminaliteit III is gegaan naar het zogenoemde decryptiebevel, waarin was vervat dat een verdachte kon worden bevolen toegang te verschaffen tot een geautomatiseerd werk (bijvoorbeeld een computer) of delen daarvan, tot een gegevensdrager of tot versleutelde gegevens.[13] Omdat velen meenden dat een dergelijk bevel in strijd moest worden geacht met het nemo-teneturbeginsel (de vrijheid van de verdachte om niet mee te werken aan zijn eigen veroordeling), zoals onder meer volgt uit artikel 6 van het Europees Verdrag van de Rechten van de Mens (EVRM), heeft de regering besloten dit onderdeel van het voorstel te laten vallen. Toch bevat het wetsvoorstel nog de nodige controversiële bepalingen.[14] Een daarvan is de bevoegdheid van opsporingsambtenaren om zich toegang te verschaffen tot de computer of het device van een verdachte om onderzoek te kunnen doen en bewijs te verzamelen.[15] Ook kunnen gegevens worden gekopieerd en aanpassingen aan de computer worden gedaan, bijvoorbeeld door het verwijderen van malware van de computer van een burger.[16]

Deze bepaling is controversieel vanwege de reikwijdte van de bevoegdheid, de onduidelijkheid over de noodzaak en effectiviteit van de inzet van deze bevoegdheid en de evidente gevolgen voor de privacy van burgers.[17] Gegeven deze punten heeft een aantal commentatoren geopperd dat er een nieuw grondrecht zou moeten komen,[18] zoals een digitaal huisrecht of een grondrecht op de integriteit en vertrouwelijkheid van een persoonlijk informatietechnisch systeem. Een recht op de bescherming van een persoonlijk informatietechnisch systeem is reeds aangenomen door het Duitse Bundesverfassungsgericht. Alhoewel een dergelijke oplossing zou kunnen leiden tot een betere bescherming van de digitale privacy van burgers kleeft er ook een aantal onzekerheden aan. Dit artikel bespreekt achtereenvolgens de achtergrond voor de introductie van de nieuwe bevoegdheid van de politie (paragraaf 2), een weergave van het wetsvoorstel zoals dat thans aanhangig is in de Eerste Kamer en het ontwerpbesluit onderzoek in een geautomatiseerd werk (paragraaf 3), de discussies over deze bevoegdheid tijdens de parlementaire behandeling (paragraaf 4), en de vraag of de introductie van een nieuw digitaal grondrecht in dit licht wenselijk zou zijn (paragraaf 5).

2. Achtergrond

In de memorie van toelichting bij de wet spreekt de regering van drie ontwikkelingen die zouden nopen tot de introductie van de bevoegdheid voor de politie om de computer van burgers binnen te treden. Ten eerste wordt communicatie haars inziens in toenemende mate versleuteld, zowel op instigatie van de gebruiker zelf als op initiatief van de aanbieders van providers en applicaties. 'Weliswaar is de aanbieder gehouden mee te werken aan het ongedaan maken van de versleuteling van de communicatie (artikel 126m, zesde lid, en 126nh, eerste lid, Sv), maar de aanbieder is hiertoe soms vaak niet in staat (bijvoorbeeld Skype), valt niet onder definitie van aanbieder (artikel 126la Sv) of is gevestigd in het buitenland. Ook kan er sprake zijn van meerdere lagen beveiliging, waarbij niet de ontsleuteling van iedere laag in handen is van een aanbieder.'[19] Door de invoering van deze bevoegdheid is het mogelijk data te verzamelen voordat ze zijn versleuteld, zo meent de regering. Ten tweede wijst de regering op het gebruik van draadloze netwerken, waarbij een verdachte gebruikmaakt van meerdere hotspots. Zij meent dat het niet efficiënt is om al deze hotspots vervolgens af te tappen en ook wordt dat met het oog op de proportionaliteit onwenselijk geacht. Beter is het dan toegang te hebben tot het apparaat van de verdachte zelf.

Het gebruik van clouddiensten vormt voor de regering een derde reden om deze bevoegdheid te introduceren, min of meer gelijk aan de argumentatie van de tweede voorgenoemde reden. Aangezien de bestanden doorgaans in gedeelten worden opgeslagen, over meerdere servers verspreid, kan dat betekenen dat gegevens van één gebruiker in verschillende landen zijn. 'Als het gaat om communicatie dan kan, op grond van de bestaande wettelijke bevoegdheden, communicatie worden afge-

10. <https://www.wodc.nl/binaries/jv1201-volledige-tekst_tcm28-77157.pdf>.
11. <https://www.wodc.nl/binaries/jv1108-volledige-tekst_tcm28-77152.pdf>.
12. <https://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf>.
13. E.J. Koops, *Het decryptiebevel en het nemo-teneturbeginsel. Nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voor verdachten?*, WODC 2012. Zie voor een kritische bespreking ook D.A.G. van Toor, 'Over het nemo-teneturbeginsel en het decryptiebevel: is een meewerkverplichting bij het ontsleutelen van bestanden gerechtvaardigd?', *Strafblad* 3/2013.
14. Zie over de Notice and Takedown-bepaling o.a. J.J. Oerlemans, 'Conceptwetsvoorstel Computercriminaliteit IIII: Onzorgvuldige Wetgeving?', *Informatiebeveiliging* 4/2011. C. Kus & J.M. Voorde, 'Het bevel Notice and Take Down in het wetsvoorstel Computercriminaliteit III en de vrijheid van meningsuiting op het internet', <https://openaccess.leidenuniv.nl/bitstream/handle/1887/29743/Kus%20en%20Ten%20Voorde%20-%20Strafblad%202014-2.pdf?sequence=1>. A.R. Lodder & M.B. Schuilenburg, 'Politie-webcrawlers en Predictive policing', *Computerrecht* 2016/81.
15. De bevoegdheid die nu reeds in handen ligt van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) wordt zo ook gegeven aan de politie. Artikel 24 WIV 2002.
16. De bepaling bouwt voort op onder meer de mogelijkheid om een computer in beslag te nemen en daarop onderzoek te verrichten, artikel 94 Strafvordering (Sv), en de mogelijkheid tot zogenoemde netwerkdoorzoekingen, zoals geregeld in artikel 125j Sv; een belangrijk verschil is dat deze bevoegdheden doorgaans kenbaar en voor korte tijd worden uitgeoefend, terwijl binnendringen in computers heimelijk en over een bepaalde periode plaatsvindt.
17. Zie ook: B. Jacobs, 'Policeware', *Nederlands Juristenblad* 39/2012.
18. Zie hierover meer de laatste paragraaf van dit artikel.
19. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 9.

doi: 10.5553/TBSenH/229567002017003004003

tapt en opgenomen, al dan niet met medewerking van de aanbieder van het openbare telecommunicatienetwerk of de openbare telecommunicatiedienst (artikelen 126m, 126t en 126zg Sv). Ook kan van een aanbieder worden gevorderd gegevens te verstrekken (artikelen 126n, 126na, 126ng, 126u, 126ua, 126ug, 126zh, 126zi en 126zl Sv). Het gebruik van Cloudcomputing-diensten kan echter tot onduidelijkheid leiden over de vraag wie als aanbieder van een telecommunicatiedienst in de zin van de Telecommunicatiewet kan worden aangemerkt.'[20] Het in beslag nemen van een computer acht de regering een minder wenselijk alternatief omdat de verdachte zich dan bewust zal zijn van het feit dat hij onderwerp is van een onderzoek.

Bij de toepassing van de nieuw te introduceren bevoegdheid onderscheidt de regering drie fasen. Ten eerste de verkennende fase. Hierin wordt bekeken welke bevoegdheid het beste past bij het onderzoek dat wordt verricht, tot wie en welk device het onderzoek op afstand moet zijn gericht en welke reikwijdte het onderzoek dient te hebben. Ten tweede het onderzoek in het geautomatiseerde werk zelf. Het binnendringen van een computer kan op verschillende wijzen geschieden, zoals door social engineering, door het gebruik van kunstmatige intelligentie of door de verdachte te verleiden te reageren op een e-mailbericht of een ander verzoek om contact. Vervolgens kan een bug of een keylogger worden geplaatst om gegevens te verzamelen. Daarbij kunnen kwetsbaarheden in de computer worden gebruikt, zoals gaten in de beveiliging en fouten in software. De derde en laatste fase is de afsluiting van het onderzoek, waarbij onder meer de sporen van het onderzoek zo goed en kwaad als dat gaat worden verwijderd.

De bevoegdheid om binnen te treden binnen een computer is niet alleen van toepassing op verdenkingen voor digitale delicten, maar ook als het gaat om bijvoorbeeld onderzoek naar moord. De regering stelt: '[o]ok bij het voorbereiden en plegen van meer traditionele misdrijven is het gebruik van moderne ICT-voorzieningen een steeds belangrijker component geworden, bijvoorbeeld als het gaat om (versluierde) communicatie tussen criminelen. Het kan gaan om misdrijven als moord, handel in drugs, mensenhandel, omvangrijke milieudelicten, wapenhandel, maar ook ernstige financiële misdrijven, zoals omvangrijke ernstige fraude. De opsporingspraktijk heeft ook in die gevallen de behoefte aan de voorgestelde bevoegdheid, zodat het mogelijk is in voorkomende gevallen een geautomatiseerd werk binnen te dringen en te onderzoeken met het oog op bijvoorbeeld de vastlegging van gegevens.'[21] Het nieuw in het Wetboek van Strafvordering te introduceren artikel kent verschillende bevoegdheden, zoals het binnentreden van een computer, het vastleggen en kopiëren van gegevens en het doen van aanpassingen aan computers.

Dergelijke aanpassingen kunnen bijvoorbeeld inhouden het verwijderen van een botnet of andere malware van de computer van een gebruiker. Naar verluidt heeft de politie reeds eenmaal een dergelijke actie ondernomen toen in 2010 het zogenoemde Bredolab-botnet werd ontmanteld. Het ging dan om 'het waarschuwen van de slachtoffers. Dit gebeurde vlak na de overname via het botnet zelf. Het KLPD zette een *executable file* klaar op de Command & Controlservers, die de geïnfecteerde computers ophaalden en uitvoerden. Dit bestand leidde, zodra de defaultbrowser geopend werd, het slachtoffer naar een waarschuwingspagina. Deze website meldde de virusbesmetting, en gaf een korte uitleg over Bredolab en het publiek-private samenwerkingsverband dat het KLPD voor de ontmanteling had samengesteld.'[22] Door de introductie van het nieuwe artikel zou de politie een formele bevoegdheid krijgen om dergelijke acties uit te voeren.

3. Het wetsvoorstel en het ontwerpbesluit onderzoek in een geautomatiseerd werk

Het wetsvoorstel kent een nogal brede bevoegdheid toe aan opsporingsambtenaren; verschillende pogingen om meer wettelijke waarborgen neer te leggen en de bevoegdheid verder in te kaderen zijn verworpen. Het voorstel dat nu voorligt in de Eerste Kamer en het vermoedelijk gaat halen is hieronder weergegeven.[23] De bevoegdheid ziet blijkens lid 1 van artikel 126nba Sv op vijf specifieke doelen: (1) het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker; (2) het overnemen van gegevens, zoals bij het vastleggen van afbeeldingen van kinderpornografie of van inloggegevens van besloten groepen of wachtwoorden waarmee de versleuteling van gegevens ongedaan kan worden gemaakt; (3) het ontoegankelijk maken van gegevens, waaronder wordt verstaan het treffen van maatregelen om te voorkomen dat de beheerder van een geautomatiseerd werk of derden verder van de gegevens kennisnemen of gebruikmaken en om te voorkomen dat schadelijke gegevens verder worden verspreid; (4) het aftappen en opnemen van communicatie of opnemen van vertrouwelijke communicatie; en (5) stelselmatige observatie. De regering geeft aan dat dit laatste nuttig kan zijn als een verdachte een observatieteam voortdurend weet af te schudden. Hij kan door deze nieuwe bevoegdheid voortdurend worden gevolgd, door de heimelijke toegang tot de smartphone, waarna via de gps-locatie kan worden nagegaan waar de smartphone zich bevindt. Wel merkt de regering op dat het permanent waarnemen in een woning via het op afstand aanzetten van een web-

20. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 11.
21. Concept memorie van toelichting, p. 12. <https://www.internetconsultatie.nl/computercriminaliteit/document/727>.
22. M.E. Koning, 'Van teugelloos "terughacken" naar "digitale toegang op afstand"', *Privacy & Informatie* 2/2012, p. 47.
23. Eerste Kamer, vergaderjaar 2016-2017, 34 372, A.

doi: 10.5553/TBSenH/229567002017003004003

cam van bijvoorbeeld een smartphone of een laptop als even ingrijpend moet worden aangemerkt als het betreden van een woning en het stelselmatig observeren in een woning. Dit is niet toegestaan, aldus de regering, ook niet onder de nieuw te introduceren bevoegdheid.

Daarnaast is er een aantal waarborgen voor de toepassing van deze bevoegdheid. Zo vereist lid 1 dat er sprake is van 'een ernstige inbreuk op de rechtsorde', moet er sprake zijn van een dringend onderzoeksbelang en is de autorisatie van een officier van justitie vereist. Als aan deze voorwaarden is voldaan kan er met behulp van een 'technisch hulpmiddel' onderzoek worden gedaan, waarbij het bevel schriftelijk moet worden gegeven en gezien lid 2 ten minste moet bevatten: het misdrijf en een zo nauwkeurig mogelijke aanduiding van de verdachte, de feiten of omstandigheden waaruit blijkt dat de voorwaarden voor de toepassing van deze bevoegdheid zijn vervuld, een aanduiding van de aard en functionaliteit van het technische hulpmiddel dat wordt gebruikt en het doel met het oog waarop het bevel wordt gegeven. Een bevel mag slechts voor vier weken worden gegeven en moet steeds weer worden verlengd (lid 3) en mag slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris (lid 4).

Ook heeft de regering het ontwerpbesluit onderzoek in een geautomatiseerd werk aangeboden aan het parlement.[24] Dit besluit regelt verder de bevoegdheden in artikelen 126nba, eerste lid, 126uba, eerste lid, en 126zpa, eerste lid van het Wetboek van Strafvordering.[25] De nota van toelichting geeft verdere uitleg bij dit voorgestelde besluit. Artikel 2 geeft verdere duiding over de relevante misdrijven in dit verband. Enerzijds zijn dit computermisdrijven waarbij het misdrijf met een geautomatiseerd werk wordt gepleegd of betrekking heeft op een geautomatiseerd werk, zoals computervredebreuk, waaronder het gebruik van een botnet en van ernstige 'spam' of 'bombing', het onrechtmatig overnemen en helen van gegevens, het aftappen of opnemen van gegevens, de vernieling van geautomatiseerde werken en de beschadiging van computergegevens. Anderzijds gaat het om misdrijven met een grote maatschappelijke impact die in toenemende mate worden gepleegd met behulp van een computer, zoals misdrijven tegen de openbare orde, misdrijven tegen het openbaar gezag, valsheid in geschrifte, rekrutering voor terrorisme, het deelnemen aan een criminele organisatie, mensensmokkel, corruptie, fraude, witwassen, spionagemisdrijven en bepaalde zedenmisdrijven.

Er staat ook een flink aantal regels in om de betrouwbaarheid van de onderzoeksresultaten te garanderen. Zo moeten de verzamelde gegevens worden vastgelegd en mag de inhoud van de vastgelegde gegevens niet worden bewerkt. Opmerkelijk is dat het voorbereidende deel van het onderzoek, het binnendringen in een geautomatiseerd werk, niet hoeft te worden gelogd, omdat de handelingen die in dit deel van het onderzoek plaatsvinden volgens de regering niet van invloed zijn op de betrouwbaarheid en de integriteit van het bewijs. Artikel 10, 11 en 12 van het ontwerpbesluit stellen nadere regels ter garantie van de betrouwbaarheid van de verkregen gegevens en zorgen dat resultaten gelogd worden, zodat naderhand kan worden vastgesteld waar, wanneer en hoe de gegevens zijn verkregen. 'Door middel van de logging van de onderzoekshandelingen en het functioneren van de technische infrastructuur kan controle plaatsvinden op het functioneren van een technisch hulpmiddel. Indien zich gedurende de inzet van een technisch hulpmiddel onregelmatigheden voordoen die van invloed zijn op de kwaliteit van de vastgelegde gegevens kan hierover verantwoording worden afgelegd aan de hand van de logging.'[26]

Tot slot staat er nog een flink aantal bepalingen in het ontwerpbesluit over toezicht op de inzet van deze bevoegdheid en de afronding van het onderzoek. Zo zijn er regels over voorafgaande keuring en herkeuring en over wanneer hier vanwege een dringend onderzoeksbelang uitzondering op kan worden gemaakt, worden er regels gesteld voor een keuringsdienst, een keuringsprotocol, een keuringsrapport en de registratie van keuringsrapporten. Opmerkelijk is nog de clausule rond de wederzijdse erkenning van technische hulpmiddelen, artikel 20. Hieruit volgt dat er ook gebruik kan worden gemaakt van technische hulpmiddelen die rechtmatig zijn vervaardigd of in de handel zijn gebracht in een andere lidstaat van de Europese Unie, in een staat die partij is bij een tot een douane-unie strekkend verdrag of die rechtmatig zijn vervaardigd in een staat die partij is bij een tot een vrijhandelszone strekkend verdrag dat Nederland bindt. Deze bepaling heeft de regering ingevoegd omdat de 'technische eisen die het besluit stelt aan technische hulpmiddelen en de door het besluit voorgeschreven keuring van technische hulpmiddelen kunnen worden opgevat als een inbreuk op het vrije verkeer.'[27]

24. Eerste Kamer, vergaderjaar 2016-2017, 34 372, C.
25. blg-807666 <https://zoek.officielebekendmakingen.nl/blg-807666>.
26. blg-807666, p. 21.
27. blg-807666, p. 24.

doi: 10.5553/TBSenH/229567002017003004003

Tabel 1

Artikel 126nba	Artikel 126uba	Artikel 126zpa
1. In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, kan de officier van justitie, indien het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat bij de verdachte in gebruik is en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:	1. In een geval als bedoeld in artikel 126o, eerste lid, kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat in gebruik is bij een persoon ten aanzien van wie uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat hij betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:	1. In geval van aanwijzingen van een terroristisch misdrijf kan de officier van justitie, indien het belang van het onderzoek dit dringend vordert, bevelen dat een daartoe aangewezen opsporingsambtenaar binnendringt in een geautomatiseerd werk dat in gebruik is bij een persoon en, al dan niet met een technisch hulpmiddel, onderzoek doet met het oog op:
a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;	a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;	a. de vaststelling van bepaalde kenmerken van het geautomatiseerde werk of de gebruiker, zoals de identiteit of locatie, en de vastlegging daarvan;
b. de uitvoering van een bevel als bedoeld in de artikelen 126l of 126m;	b. de uitvoering van een bevel als bedoeld in de artikelen 126s en 126t;	b. een bevel als bedoeld in de artikel 126zg;
c. de uitvoering van een bevel als bedoeld in artikel 126g, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd; en, in geval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;	c. de uitvoering van een bevel als bedoeld in artikel 126o waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd; en, in geval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;	c. een bevel als bedoeld in artikel 126zd, eerste lid, onder a, waarbij de officier van justitie kan bepalen dat ter uitvoering van het bevel een technisch hulpmiddel op een persoon wordt bevestigd; en, in geval van een misdrijf, waarop naar de wettelijke omschrijving een gevangenisstraf van acht jaren of meer is gesteld, dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen;
d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;	d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;	d. de vastlegging van gegevens die in het geautomatiseerde werk zijn opgeslagen, of die eerst na het tijdstip van afgifte van het bevel worden opgeslagen, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.	e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.	e. de ontoegankelijkmaking van gegevens, bedoeld in artikel 126cc, vijfde lid. Artikel 11.7a van de Telecommunicatiewet is niet van toepassing op handelingen ter uitvoering van een bevel als bedoeld in de eerste volzin.
2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:	2. Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt:	2. Het bevel vermeldt, behalve de gegevens, bedoeld in artikel 126za, tevens:

doi: 10.5553/TBSenH/229567002017003004003

Vervolg Tabel 1

Artikel 126nba	Artikel 126uba	Artikel 126zpa
a. het misdrijf en, indien bekend, de naam of anders een zo nauwkeurig mogelijke aanduiding van de verdachte;	a. een omschrijving van het georganiseerd verband en indien bekend de naam of anders een zo nauwkeurig mogelijke aanduiding van de persoon ten aanzien van wie uit feiten en omstandigheden een redelijk vermoeden voortvloeit dat deze betrokken is bij het in georganiseerd verband beramen of plegen van misdrijven;	a. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;
b. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;	b. zo mogelijk een nummer of een andere aanduiding waarmee het geautomatiseerde werk kan worden geïdentificeerd en, indien bekend, dat de gegevens niet in Nederland zijn opgeslagen;	b. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;
c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;	c. de feiten of omstandigheden waaruit blijkt dat de voorwaarden, bedoeld in het eerste lid, zijn vervuld;	c. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;
d. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;	d. een aanduiding van de aard en functionaliteit van het technische hulpmiddel, bedoeld in het eerste lid, dat wordt gebruikt voor de uitvoering van het bevel;	d. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;
e. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;	e. het onderdeel of de onderdelen, genoemd in het eerste lid, met het oog waarop het bevel wordt gegeven en, als dit het onderdeel a, d of e betreft, een duidelijke omschrijving van de te verrichten handelingen;	e. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;
f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;	f. ten aanzien van welk deel van het geautomatiseerde werk en welke categorie van gegevens aan het bevel uitvoering wordt gegeven;	f. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.
g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;	g. het tijdstip waarop, of de periode waarbinnen aan het bevel uitvoering wordt gegeven;	
h. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.	h. in het geval het een bevel, bedoeld in het eerste lid, onderdeel c, betreft, een melding van het voornemen om een technisch hulpmiddel op een persoon te bevestigen.	
3. Het bevel, bedoeld in het eerste lid, wordt gegeven voor een periode van ten hoogste vier weken. Het kan telkens voor een periode van ten hoogste vier weken worden verlengd.	3. Artikel 126nba, derde tot en met negende lid, is van overeenkomstige toepassing.	3. Artikel 126nba, derde tot en met negende lid, is van overeenkomstige toepassing.

doi: 10.5553/TBSenH/229567002017003004003

Vervolg Tabel 1

Artikel 126nba	Artikel 126uba	Artikel 126zpa
4. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. De machtiging vermeldt de onderdelen van het bevel en de periode waarvoor de machtiging van kracht is.		
5. Het bevel, bedoeld in het eerste lid, kan schriftelijk en met redenen omkleed worden gewijzigd, aangevuld, verlengd of beëindigd, met dien verstande dat de officier van justitie voor wijziging, aanvulling of verlenging een machtiging van de rechter-commissaris behoeft. Bij dringende noodzaak kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven. De officier van justitie en de rechter-commissaris stellen deze in dat geval binnen drie dagen op schrift.		
6. Nadat het onderzoek is beëindigd wordt het technische hulpmiddel verwijderd. Indien het technische hulpmiddel niet of niet volledig kan worden verwijderd en dit risico's oplevert voor het functioneren van het geautomatiseerde werk stelt de officier van justitie de beheerder van het geautomatiseerde werk daarvan in kennis en stelt de nodige informatie ter beschikking ten behoeve van de volledige verwijdering. Het bepaalde in artikel 126cc, eerste lid, is van overeenkomstige toepassing.		
7. Het toezicht op de uitvoering van het bevel, bedoeld in het eerste lid, door de ambtenaren, bedoeld in artikel 141, onderdeel d, en de personen, bedoeld in artikel 142, eerste lid, onderdeel b, wordt uitgeoefend door de inspectie, bedoeld in artikel 65 van de Politiewet 2012, overeenkomstig het bepaalde in hoofdstuk 6 van de Politiewet 2012.		
8. Bij of krachtens algemene maatregel van bestuur worden regels gesteld omtrent:		
a. de autorisatie en deskundigheid van de opsporingsambtenaren die kunnen worden belast met het binnendringen en het onderzoek, bedoeld in het eerste lid, en de samenwerking met andere opsporingsambtenaren;		
b. de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.		
9. Bij algemene maatregel van bestuur kunnen regels worden gesteld over de toepassing van de bevoegdheid, bedoeld in het eerste lid, in de gevallen waarin niet bekend is waar de gegevens zijn opgeslagen.		

doi: 10.5553/TBSenH/229567002017003004003

Tabel 2

Artikel 126ffa	Artikel 126ee, aanhef en onderdelen a en b, komt te luiden:	Aan artikel 7 van de Wet op de bijzondere opsporingsdiensten wordt een nieuw lid toegevoegd, luidende:
1. De officier van justitie kan op grond van een zwaarwegend opsporingsbelang bevelen dat het bekend maken aan de producent van een onbekende kwetsbaarheid voor het binnendringen in een geautomatiseerd werk, bedoeld in de artikelen 126nba, 126uba en 126zpa, wordt uitgesteld.	Bij algemene maatregel van bestuur worden regels gesteld omtrent: a. de opslag, verstrekking, plaatsing en verwijdering van de technische hulpmiddelen, bedoeld in de artikelen 126g, derde lid, 126l, eerste lid, 126nba, eerste lid, 126o, derde lid, 126s, eerste lid, 126uba, eerste lid, 126zd, eerste lid, 126zf, eerste lid, en 126zpa, eerste lid, alsmede van de technische hulpmiddelen bedoeld in de artikelen 126m, eerste lid, 126t, eerste lid, en 126zg, eerste lid, voor zover het bevel, bedoeld in artikel 126m, derde of vierde lid, onderscheidenlijk de artikelen 126t, derde of vierde lid en 126zg, derde of vierde lid, ten uitvoer wordt gelegd zonder medewerking van de betrokken aanbieder; b. de technische eisen waaraan de hulpmiddelen voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde waarnemingen of, in geval van toepassing van artikel 126nba, 126uba of 126zpa, de vastgelegde gegevens, en met het oog op het voorkomen van misbruik door derden.	4. Het bepaalde in het eerste lid laat het bepaalde in artikel 126nba, achtste lid, van het Wetboek van Strafvordering onverlet.
2. Een bevel als bedoeld in het eerste lid is schriftelijk en vermeldt: a. de kwetsbaarheid en b. het zwaarwegend opsporingsbelang.		
3. Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris.		
4. Onder onbekende kwetsbaarheid als bedoeld in het eerste lid wordt verstaan een kwetsbaarheid in een geautomatiseerd werk waarvan aannemelijk is dat die niet bekend is of kan worden verondersteld niet bekend te zijn bij de producent van het apparaat of van het programma op basis waarvan automatisch computergegevens worden verwerkt, en die kan worden gebruikt om dat geautomatiseerde werk binnen te dringen.		

4. Parlementaire discussie

Er is de nodige discussie geweest over de nieuw te introduceren bevoegdheid, zowel tijdens de internetconsultatie[28] als tijdens de parlementaire behandeling. Ten eerste is er de kritiek dat de reikwijdte van de bevoegdheid te groot zou zijn. Die splitst zich uit in vijf punten:

1. De bevoegdheid wordt gegeven voor elk 'geautomatiseerd werk', waaronder 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.'[29] Gezien de ontwikkeling op het gebied van het Internet der Dingen is het niet onwaarschijnlijk dat binnen afzienbare tijd hier vrijwel alle apparaten en objecten onder zullen vallen. In het parlement werd een voorstel ingediend om het begrip 'geautomatiseerd werk' nader te definiëren en in te kaderen. Dat amendement werd echter verworpen.[30]
2. Het maakt voor deze bevoegdheid weinig uit of de computer of het device zich in een woning of de privésfeer bevindt of niet, wat kan leiden tot een forse beperking van de privacy van burgers. Tijdens de internetconsultatie wordt daarbij de vraag opgeworpen of de politie bij een botnet dat 100.000 computers heeft geïnfecteerd, al deze computers mag binnentreden.[31] In antwoord daarop stelt de regering dat het 'niet waarschijnlijk is dat een individuele computer die onderdeel vormt van een botnet, wordt binnengedrongen om het botnet onschadelijk te maken. In plaats daarvan ligt het voor de hand om de opsporingshandelingen op de server te richten, door middel waarvan de verschillende computers worden aangestuurd.'[32] Toch sluit het deze mogelijkheid niet uit.
3. Dan wordt er zowel in het parlement als tijdens de internetconsultatie gevraagd om nadere bescherming voor advocaten en journalisten, gegeven hun bijzon-

28. <https://www.internetconsultatie.nl/computercriminaliteit/document/726>.
29. Artikel 80sexies. Eerste Kamer, vergaderjaar 2016-2017, 34 372, A.
30. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 20.
31. 3-blg-651730, p. 15. <https://zoek.officielebekendmakingen.nl/blg-651730>.
32. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 80.

doi: 10.5553/TBSenH/229567002017003004003

dere positie.[33] De regering verwijst echter naar artikel 126aa, tweede lid, Sv. 'Anders dan bij de regeling van artikel 125l Sv bij de doorzoeking ter vastlegging van gegevens, waarbij de verdachte in beginsel op de hoogte is van de uitvoering van die doorzoeking, voorziet de regeling van artikel 126aa, tweede lid, Sv in de verplichting tot vernietiging van de processenverbaal en andere voorwerpen mededelingen behelzen gedaan door of aan een persoon die zich op grond van artikel 218 Sv zou kunnen verschonen indien hem als getuige naar de inhoud van die mededelingen zou worden gevraagd.'[34] Ook wijst ze er op dat indien bij het aftappen en opnemen van telecommunicatie een nummer is betrokken dat door de Orde van Advocaten bij de politie is aangemeld, het opnemen van de communicatie onmiddellijk wordt beëindigd. Voor wat betreft de positie van de journalist verwijst de regering naar het wetsvoorstel bronbescherming in strafzaken.[35] Ook op dit punt worden dus geen aanpassingen gedaan.

4. Er zijn relatief veel misdrijven waarbij de nieuw te introduceren bevoegdheid kan worden ingezet. Verhoeven (D66) stelt voor om in artikelen 126nba, 126uba en 126zpa het eerste lid, in de slotzinsnede na onderdeel c, 'dan wel een misdrijf dat bij algemene maatregel van bestuur is aangewezen' te vervangen door 'dan wel een misdrijf als bedoeld in de artikelen 240b, eerste lid, 248a en 248e van het Wetboek van Strafrecht'.[36] Dit voorstel heeft ten doel om alle misdrijven waarvoor de bevoegdheid tot binnendringen van een geautomatiseerd werk kan worden afgegeven, te regelen in de wet en niet deels bij algemene maatregel van bestuur. Het voorstel wordt niet aangenomen.
5. De regering kent zichzelf ook rechtsmacht toe over computers en devices die zich niet in Nederland bevinden, namelijk als zij betrokken zijn bij delicten in Nederland of die een impact hebben op Nederlandse ingezetenen. 'De botnets vormen een goed voorbeeld van situaties waarin meerdere staten rechtsmacht kunnen hebben en die ook zouden willen uitoefenen, omdat de schadelijke gevolgen van het gebruik van dergelijke botnets zich in een groot aantal staten kunnen manifesteren.'[37] De regering meent dat het verlenen van rechtsbijstand niet altijd soelaas zal bieden en vaak omslachtig is.[38] Het argument dat de rechtsmacht om in andere landen computers te hacken zou kunnen leiden tot een 'wildwestpraktijk',[39] als andere landen gelijksoortige bevoegdheden zouden inzetten ten aanzien van zich in Nederland bevindende computers, wordt niet inhoudelijk behandeld door de regering.

Ten tweede is er de kritiek ten aanzien van de noodzaak van de nieuwe bevoegdheid.[40] De Nederlandse Orde van Advocaten stelt bijvoorbeeld dat 'uit de toelichting bij dit wetsvoorstel niet kan worden afgeleid waar nu precies de noodzaak ligt om deze vergaande maatregelen door te voeren. Er worden immers geen concrete noch cijfermatige voorbeelden gegeven van zaken die door een gebrek aan bevoegdheden zouden zijn "misgegaan". In de concept MvT wordt bij herhaling het voorbeeld van kinderpornografie aangehaald, maar dat is minst genomen misleidend, omdat de voorgestelde bevoegdheid niet beperkt is tot dat type zaken, maar ook toepasbaar is bij zulke buitengemeen ernstige vormen van criminaliteit als herhaalde winkeldiefstal of – onder omstandigheden – het benadelen van de gezondheid of welzijn van een dier.'[41] De regering heeft het zich niet vergund om bij de definitieve memorie van toelichting meer helderheid te scheppen over de noodzaak van deze bevoegdheid, anders dan de opmerking dat er een balans moet zijn tussen veiligheid en privacy, met als bron een masterscriptie uit 2014.[42]

Ten derde is uiteraard de vraag: als er een systeemzwakte is, hoe dan kan worden bewezen dat niet derden eventueel belastend materiaal op de computer van een persoon hebben gezet?[43] 'Het grote nadeel van digitaal bewijs is dat de betrouwbaarheid problematisch is. Als de overheid een systeem kan hacken, kan een derde dit ook en ligt het gevaar op de loer dat het bewijs gemanipuleerd of vervalst kan worden.'[44] Kortom, als de politie dit middel in handen zou hebben, zou het dan inderdaad leiden tot betere opsporing en vergaring van betrouwbaar bewijs? Onder meer om deze problematiek te

33. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/05a358c8-1fa9-47cf-8c75-12eb760dd8b5>. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/253f8f26-c644-48be-981b-4e2396e2f855>.
34. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 17.
35. Tweede Kamer, vergaderjaar 2014-2015, 34 032, nr. 1.
36. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 21.
37. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 44.
38. B.-J. Koops & M. Goodwin, 'Cyberspace, the cloud, and cross-border criminal investigation. The limits and possibilities of international law', <https://www.gccs2015.com/sites/default/files/documents/Bijlage%201%20-%20Cloud%20Onderzoek.pdf>, p. 85 e.v. Zie ook: Cybercrime Verdrag van de Raad van Europa. <https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Dutch.pdf>. Zie ook: E.J. Koops, 'De dynamiek van cybercrimewetgeving in Europa en Nederland', Justitiële verkenningen: Documentatieblad van het Ministerie van Justitie 38(1), 2012. E.J. Koops, 'Het Cyber-crimeverdrag, de Nederlandse strafwetgeving en de (computer)criminalisering van de maatschappij', Computerrecht 02/2003.
39. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/571bc98e-e2fc-4556-8b9b-d3e4666a0286>.
40. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/ddbf9514-0727-4d09-9ca8-f027c4109880>.
41. 3-blg-651732, p. 1. <https://zoek.officielebekendmakingen.nl/blg-651732>.
42. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p. 77.
43. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/246cd483-f724-47b6-b206-7594806b2e95>.
44. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/e8df628b-a70c-44f5-a640-74eb289bc4e8>.

ondervangen hebben Verhoeven, Gesthuizen (SP) en Van Tongeren (Groenlinks) een motie ingediend waarin zij de regering verzoeken 'geen hacksoftware in te kopen waarvan de regering weet dat de software gebruikmaakt van onbekende kwetsbaarheden of waarvan de regering niet zeker weet of de software gebruikmaakt van onbekende kwetsbaarheden; verzoekt de regering voorts, om geen onbekende kwetsbaarheden in te kopen.'[45] Verhoeven stelt een amendement voor van soortgelijke strekking.[46] Beide voorstellen redden het echter niet. Wel is aangenomen[47] een motie van Recourt (PvdA) waarin de regering wordt verzocht 'te bewerkstelligen dat opsporingsinstanties onbekende kwetsbaarheden of software die daarvan gebruikmaakt alleen in het uiterste geval zullen inzetten.'[48] De mogelijkheid voor dergelijke inzet blijft dus wel bestaan.

Ten vierde wordt gewezen op de mogelijke 'perverse prikkel' voor de overheid om veiligheidslekken in systemen niet meer te melden (en mogelijkerwijs juist in stand te laten).[49] De regering stelt dat die vrees ongegrond is. Zij promoot naar eigen zeggen juist de goede bescherming en beveiliging van computers door burgers en zal daar ook in de toekomst mee doorgaan. Ook heeft de politie er doorgaans geen belang bij om zwaktes in het systeem in stand te laten, juist omdat dit de mogelijkheid tot binnendringen in het systeem door derden mogelijk maakt, wat een negatief effect kan hebben op het onderzoek en afbreuk kan doen aan de betrouwbaarheid van het bewijs.[50] Toch stellen de leden Recourt en Tellegen (VVD) voor een nieuw artikel in te voegen.[51] Normaliter moeten de risico's die kwetsbaarheden in een geautomatiseerd werk met zich mee brengen in de regel worden gemeld, om zo de eigenaar van dat werk in staat te stellen die kwetsbaarheid te verhelpen. Dit principe kan in het nieuwe artikel uitzondering lijden als er sprake is van een zwaarwegend opsporingsbelang. Dit amendement wordt aangenomen.[52]

Ten vijfde en tot slot wordt nog gewezen op het gevaar van misbruik, bijvoorbeeld doordat de politie nu de macht heeft om belastende informatie op de computer van een verdachte te plaatsen.[53] De regering wijst dit mogelijke gevaar van de hand. Verhoeven stelt in een amendement voor een nieuw artikel in te voegen waardoor er meer toezicht wordt gehouden op de inzet van deze bevoegdheid. Het voorstel introduceerde een commissie van toezicht op de opsporingsdiensten, die onder meer was belast met het toezicht op de rechtmatigheid van de uitvoering van de bevoegdheden.[54] Ook dit amendement werd in de stemming in de Tweede Kamer echter verworpen.

5. Tijd voor een grondrecht op de bescherming van informatie-technische systemen?

In de Wet computercriminaliteit III staat een nogal brede bevoegdheid voor opsporingsambtenaren om zich toegang te verschaffen tot computers van individuen, daar onderzoek te verrichten en zelfs mogelijke aanpassingen te doen, bijvoorbeeld door malware van de computer te verwijderen. Het ontwerpbesluit onderzoek in een geautomatiseerd werk stelt enige grenzen aan de inzet van deze bevoegdheid, maar staat een brede inzet van deze bevoegdheid toe. Een aantal commentatoren heeft gesteld dat er noodzaak is aan een nieuw grondrecht dat bescherming biedt tegen deze bevoegdheid.[55] In de parlementaire discussie is met name een zaak voor het Bundesverfassungsgericht ter sprake gekomen. In die zaak uit 2008 legde het Hof het op afstand uitlezen van harde schijven door de politie en veiligheidsdiensten aan banden.

Het Hof oordeelde eerst dat de Duitse wet die de bevoegdheid tot onderzoek op afstand neerlegde als zodanig geen inbreuk maakte op bestaande grondrechten zoals het recht op het telecommunicatiegeheim, het huisrecht of het algemene persoonlijkheidsrecht, waaronder het recht op informationele zelfbeschikking. Vervolgens leidt het hof een geheel nieuw grondrecht uit het algemene persoonlijkheidsrecht af, namelijk de bescherming van de vertrouwelijkheid en integriteit van informatie-technische systemen. 'Geschützt vom Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ist zunächst das Interesse des Nutzers, dass die von einem vom Schutzbereich erfassten informationstechnischen System erzeugten, verarbeiteten und gespeicherten Daten vertraulich bleiben. Ein Eingriff in dieses Grundrecht ist zudem dann anzunehmen, wenn die Integrität des geschützten informationstechnischen Systems angetastet wird, indem auf das System so zugegriffen wird, dass dessen Leistungen, Funktionen und Speicherinhalte durch Dritte genutzt werden können; dann ist die entscheidende technische Hürde für eine Ausspähung, Überwachung oder Manipulation des Systems genommen.'[56]

45. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 22.
46. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 13.
47. h-tk-20162017-37-15, Vergaderjaar 2016-2017, Vergaderingnummer 37.
48. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 23.
49. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/6f570666-7670-4576-b796-a3eaacecc657>.
50. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 3, p; 34-35.
51. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 14.
52. h-tk-20162017-37-14, Vergaderjaar 2016-2017, Vergaderingnummer 37.
53. <https://www.internetconsultatie.nl/computercriminaliteit/reactie/a4bc5fac-016e-4158-8dd6-c60db9a7d775>.
54. Tweede Kamer, vergaderjaar 2016-2017, 34 372, nr. 12.
55. Zie breder ook: B. Jacobs, 'Autonomie en Transparantie', <http://www.cs.ru.nl/B.Jacobs/PAPERS/BartJacobs-NISA-2010.pdf>.
56. BVerfG 27 februari 2008, para 204.

doi: 10.5553/TBSenH/229567002017003004003

Niet alleen in het parlement is door enkelen verwezen naar deze uitspraak, met de vraag of ook in Nederland een dergelijk grondrecht zou moeten worden geïntroduceerd.[57] Ook burgerrechten organisaties als Bits of Freedom wijzen in het kader van computercriminaliteit III op de uitspraak van het Bundesverfassungsgericht.[58] Daarnaast stellen commentatoren dat een dergelijke bescherming een aanvulling zou kunnen vormen op het Nederlandse grondrechtensysteem.[59] Zo pleiten Groothuis en De Jong voor de introductie van een dergelijk grondrecht in de Nederlandse context. 'Zwaarwegend voor de besluitvorming over een nieuw grondrecht zou onzes inziens moeten zijn dat het gebruik van informatiesystemen, en in het bijzonder personal computers, voor de persoonlijke ontwikkeling van individuen een grote betekenis heeft gekregen. Het van buitenaf, en zonder medeweten van de betrokken burger, ingrijpen in een ICT-systeem kan voor de persoonlijkheid van de betrokkene ingrijpende gevolgen hebben.'[60]

Anderen wijzen echter ook op de mogelijke vaagheid die de introductie van een dergelijk grondrecht met zich mee kan brengen. Zo stellen De Hert, De Vries en Gutwirth dat ook buiten Duitsland de uitspraak van het Bundesverfassungsgericht als inspiratie kan dienen. Toch menen zij dat 'de formulering van een nieuw grondrecht echter ook veel onduidelijkheid met zich mee [brengt]. De Duitse rechter heeft een moedige aanzet gedaan. Door de lof en kritiek uit de Duitse juridische literatuur is duidelijk geworden waar een toekomstige rechter of wetgever – of het nu binnen of buiten de Duitse context is – mogelijkerwijs nog meer helderheid zal moeten scheppen. Daarbij valt onder andere te denken aan de reikwijdte van wat een "als eigen" gebruikt informatietechnologisch systeem is, een nadere invulling van het begrip "systeem", de verhouding ten opzichte van andere grondrechten, de eventuele horizontale werking van een dergelijk grondrecht, etc.'[61]

Naast de vraag wat onder de definitie van een nieuw te introduceren grondrecht zou vallen is ook de vraag tegen welke inzet van politiebevoegdheden een dergelijk grondrecht bescherming zou kunnen bieden. Het doorzoeken van een computer zou in deze zin gelijk kunnen zijn aan het doorzoeken van een fysieke plaats zoals bijvoorbeeld een woning. In de literatuur en tijdens de parlementaire discussie wordt met name de bevoegdheid om aanpassingen te doen aan de computers van burgers als inbreukmakend gezien. Daarbij moet evenwel worden bedacht dat als deze bevoegdheid door de politie wordt ingezet in de strijd tegen botnets en andere malware, de integriteit van de computer van de burger reeds is gecompromitteerd. In deze zin helpt de politie dus juist de integriteit van de computer te herstellen. Daarbij kan uiteraard wel de vraag worden gesteld of zij dat moet doen buiten het medeweten en zonder de expliciete, voorafgaande toestemming van de burger die het betreft. Toch is het voorstelbaar dat er situaties zijn waarin dergelijke kennisgeving of toestemming niet kan worden afgewacht, met name als de bots worden gebruikt voor het ontplooien van criminele activiteiten die de nationale veiligheid kunnen ondermijnen. Ook is het de vraag of de burger niet is gebaat bij de hulp van de politie om de integriteit van zijn computer te beschermen tegen internetcriminelen, gezien de onbekendheid van velen over het bestaan van botnets en de mogelijke beschermingsmaatregelen die zij daartegen kunnen treffen.

Tot slot komen met rechten ook plichten. Een burger heeft de plicht om er, voor zover redelijk voor te zorgen dat zijn huis niet wordt gebruikt als uitvalsbasis voor criminele activiteiten. Zou een dergelijke plicht ook gelden voor een informatie-technisch systeem, dan zou het kunnen betekenen dat burgers ervoor zorg moeten dragen dat, voor zover dat redelijkerwijs mogelijk is, hun computer niet wordt gebruikt door internetcriminelen voor het uitvoeren van criminele handelingen middels botnets, zoals voor DDOS-aanvallen, clickfraude en zelfs het platleggen van kritische infrastructuur. Kan het de burger worden aangerekend als hij wist of had moeten weten dat zijn informatie-technisch systeem niet goed beveiligd was tegen dit soort misbruik? Kan uit het recht op bescherming van informatie-technische systemen ook een plicht worden afgeleid om deze systemen goed te beveiligen, bijvoorbeeld door een antivirusprogramma te installeren en soortgelijke maatregelen te treffen? En kan een burger zijn eventuele recht op de vertrouwelijkheid en integriteit van informatie-technische systemen verliezen als hij zich niet houdt aan de plichten die uit het hebben van een dergelijk recht volgen?

Artikel 13 van de Nederlandse Grondwet kent thans het briefgeheim. '1 Het briefgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, op last van de rechter. Het telefoon- en telegraafgeheim is onschendbaar, behalve, in de gevallen bij de wet bepaald, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.'[62] Omdat deze bepaling in de jurisprudentie een bredere reikwijdte is gegeven adviseerde de Staatscommissie grondwet in 2010 reeds voor om dit artikel te herformuleren tot een algemeen grondrecht op de vertrouwelijkheid van communicatie: '1. Ieder heeft recht op vertrouwelijke communicatie. 2. Beperking van dit

57. Tweede Kamer, vergaderjaar 2015-2016, 34 372, nr. 5.
58. <https://www.rijksoverheid.nl/documenten/rapporten/2015/12/16/tk-advies-bits-of-freedom-2013-in-verband-met-de-verbetering-en-versterking-van-de-opsporing-en-vervolging-van-computercriminaliteit>.
59. BVerfG 27 februari 2008, Online-Durchsuchung (m.nt. W. Steenbruggen), Mediaforum. Tijdschrift voor Media en Communicatierecht, 20 (5), 2008.
60. M.M. Groothuis & T. de Jong, 'Is een nieuw grondrecht op integriteit en vertrouwelijkheid van ICT-systemen wenselijk?', Privacy & Informatie 6/2010, p. 283.
61. P. De Hert, K. De Vries & S. Gutwirth, 'Duitse rechtspraak over remote searches, datamining en afluisteren op afstand. Het arrest Bundesverfassungsgericht 27 februari 2008 (Online Dursuchung) in breder perspectief', Computerrecht 5/2009 , 200-211.
62. Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815.

doi: 10.5553/TBSenH/229567002017003004003

recht is alleen mogelijk a. in gevallen bij de wet bepaald, met machtiging van de rechter of b. in het belang van de nationale veiligheid door of met machtiging van hen die daartoe bij de wet zijn aangewezen.'[63] Thans ligt er een voorstel om het artikel te wijzingen in: '1. Ieder heeft recht op eerbiediging van zijn brief- en telecommunicatiegeheim. 2. Beperking van dit recht is mogelijk in de gevallen bij de wet bepaald met machtiging van de rechter of, in het belang van de nationale veiligheid, door of met machtiging van hen die daartoe bij de wet zijn aangewezen.'[64]

De introductie van een grondrecht naar Duitse stiel zou betekenen dat niet alleen de communicatie wordt gewaarborgd, maar ook de integriteit van informatiesystemen als zodanig. In deze zin sluit het gedeeltelijk aan bij de bescherming die door de e-Privacy Richtlijn[65] van de Europese Unie wordt geboden tegen het zonder toestemming plaatsen of lezen van gegevens van computers van burgers, bijvoorbeeld door middel van cookies of malware. In het voorstel dat staat in de e-Privacy Regulation, dat op 10 januari 2017 is gepubliceerd door de Europese Commissie en dat op termijn mogelijk deze richtlijn zal vervangen, is deze bescherming als volgt geformuleerd: 'The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds: (a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or (b) the end-user has given his or her consent; or (c) it is necessary for providing an information society service requested by the end-user; or (d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user.'[66]

Alhoewel de introductie van een nieuw grondrecht derhalve een mogelijke bescherming biedt tegen de vergaande bevoegdheid die is neergelegd in de wet Computercriminaliteit III en er ook aanknopingspunten zijn om een dergelijk recht ook binnen de Nederlandse context te ontwikkelen, is er ook nog een aantal vraagstukken dat openligt. Het zou wenselijk zijn als het parlement hier expliciet op in zou gaan om te bezien of er naast extra bevoegdheden voor de politie, ook extra beschermingsrechten voor burgers zouden moeten worden geïntroduceerd en zo ja, welke vorm deze rechten zouden moeten aannemen. Als het dat nalaat, dan is het uiteindelijk aan de Nederlandse rechter om te oordelen of uit EU-recht of de jurisprudentie van het Europees Hof voor de Rechten van de Mens ten aanzien van artikel 8 van het Europees Verdrag voor de Rechten van de Mens[67] een recht op de bescherming van de vertrouwelijkheid en integriteit van informatie-technische systemen kan en moet worden afgeleid.

63. <https://zoek.officielebekendmakingen.nl/blg-86969.pdf>.
64. Eerste Kamer, Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepaling inzake de onschendbaarheid van het brief-, telefoon- en telegraafgeheim, vergaderjaar 2016-2017, 33 989, A.
65. Artikel 5 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie). Richtlijn 2009/136/EG van het Europees Parlement en de Raad van 25 november 2009 tot wijziging van Richtlijn 2002/22/EG inzake de universele dienst en gebruikersrechten met betrekking tot elektronischecommunicatienetwerken en -diensten, Richtlijn 2002/58/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie en Verordening (EG) nr. 2006/2004 betreffende samenwerking tussen de nationale instanties die verantwoordelijk zijn voor handhaving van de wetgeving inzake consumentenbescherming. Zie ook: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).
66. <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241>.
67. Europees Verdrag voor de Rechten van de Mens. <http://www.echr.coe.int/Documents/Convention_NLD.pdf>.

doi: 10.5553/TBSenH/229567002017003004003