Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

B

VOORLOPIG VERSLAG VAN DE VASTE COMMISSIE VOOR VEILIGHEID EN JUSTITIE[1]

Vastgesteld 3 april 2017

Het voorbereidend onderzoek heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de **VVD**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III). Deze leden hebben een aantal opmerkingen en vragen naar aanleiding van dit wetsvoorstel.

De leden van de **CDA**-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. Zij zijn op zichzelf voorstander van het aanpassen van de Wetboeken van Strafrecht en Strafvordering met als doel het opsporen en vervolgen van computercriminaliteit te verbeteren, maar vragen zich af of dit wetsvoorstel daar de beste oplossing voor is. Zij hebben nog een aantal vragen.

De leden van de fractie van **D66** hebben kennisgenomen van het wetsvoorstel Computercriminaliteit III, welke een verregaande uitbreiding behelst van opsporingsbevoegdheden in het kader van strafrechtelijke onderzoeken naar computercriminaliteit door onder meer politie, justitie en bijzondere opsporingsdiensten/ambtenaren. Het wetsvoorstel geeft de politie verregaande bevoegdheden om in te breken op digitale apparaten, waaronder computers, de cloud, camera's en mobiele telefoons. De voornoemde leden hebben zorgen en vragen over de proportionaliteit van

[1] Samenstelling: Kox (SP), Engels (D66), Nagel (50PLUS), Ruers (SP), Van Bijsterveld (CDA), (vice-voorzitter), Duthler (VVD), (voorzitter), Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Backer (D66), Knip (VVD), Barth (PvdA), Beuving (PvdA), Hoekstra (CDA), Schouwenaar (VVD), Schrijver (PvdA), Van Strien (PVV), Kok (PVV), Dercksen (PVV), Bikker (CU), Bredenoord (D66), D.J.H. van Dijk (SGP), Van Rij (CDA), Rombouts (CDA), Wezel (SP) en Van de Ven (VVD).

kst-34372-B
ISSN 0921 - 7371
's-Gravenhage 2017

het wetsvoorstel en de impact op de privacy van burgers. Naar aanleiding daarvan hebben zij een aantal vragen.

De leden van de fractie van de **SP** hebben met interesse kennisgenomen van het wetsvoorstel. Zij erkennen de knelpunten die ontstaan zijn bij de opsporing, door de digitalisering van de wereld. Computercriminaliteit is toegenomen, evenals het gebruik van digitale middelen bij de uitvoering van traditionele criminaliteit. De SP-fractieleden willen graag een aantal vragen stellen aan de regering.

De leden van de **PvdA**-fractie hebben met aandacht kennisgenomen van dit wetsvoorstel en hebben in verband daarmee nog een aantal vragen.

De fractieleden van **GroenLinks** hebben met enige bezorgdheid kennisgenomen van het wetsvoorstel en hebben een aantal fundamentele en praktische bezwaren. Deze willen zij graag aan de regering voorleggen.

De leden van de fractie van de **ChristenUnie** hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij delen de opvatting van de regering dat bij de bestrijding van ernstige misdrijven binnen de grenzen van het grondwettelijk en verdragsrechtelijk beschermde recht op eerbiediging van de persoonlijke levenssfeer, ook van de nieuwe technologische mogelijkheden gebruik moet kunnen worden gemaakt. Zij hebben echter vragen bij de reikwijdte, de materieelrechtelijke effecten en de uitvoerbaarheid van de voorgestelde bevoegdheden.

2. Reikwijdte van het wetsvoorstel

Het wetsvoorstel probeert een oplossing te bieden voor problemen op twee terreinen: de toegenomen computercriminaliteit en het gebruik van digitale middelen bij traditionele criminaliteit. De leden van de fractie van de **SP** willen hun teleurstelling uitspreken over het feit dat de regering deze twee totaal verschillende problemen heeft proberen te vatten in één wetsvoorstel. Dit levert voor hen niet alleen een lastig dilemma op, maar werpt ook de zorgwekkende vraag op waarom dit onderscheid niet is gemaakt. Dat zou kunnen zijn omdat de regering zelf het onderscheid niet heeft kunnen maken, hetgeen een blijk zou kunnen zijn van gebrek aan kennis. Aan de andere kant kan de keuze ook strategisch zijn geweest. Het meenemen van een aantal dringende maatschappelijke problemen op het gebied van computercriminaliteit in een wetsvoorstel dat tevens bevoegdheden in de opsporing regelt, kan er namelijk voor zorgen dat discutabele onderdelen eerder geaccepteerd worden. Kan de regering toelichten waarom zij beide terreinen in één wetsvoorstel heeft willen vatten?
Het meest heikele punt in het wetsvoorstel is de hackbevoegdheid en alle mogelijkheden die deze de politie biedt. De bevoegdheid geeft de politie meer digitale mogelijkheden dan er nu in de offlinewereld mogelijk zijn. De leden van de fractie van de SP maken zich zorgen over deze ontwikkeling. Zij hebben geen kennisgenomen van wetsvoorstellen die het mogelijk maken om camera's te plaatsen in de huizen van verdachte personen. Toch is dit het effect van het voorstel van de regering. De noodzaak van deze drastische uitbreiding van bevoegdheden is voornoemde leden niet helemaal duidelijk. Kan de regering aangeven hoe groot het probleem is dat het wetsvoorstel moet oplossen? Hoeveel zaken kunnen er nu niet opgelost worden, maar zouden met deze wetgeving waarschijnlijk wel worden opgelost?

3. Proportionaliteit en privacy

De leden van de **VVD**-fractie zien ter zake van het wetvoorstel Computercriminaliteit III een samenhang met het wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..[2] (hierna: WIV), dat thans ook in de Eerste Kamer aanhangig is. Deze leden vragen de regering in hoeverre het wetsvoorstel Computercriminaliteit III voldoet aan de vereisten die voortvloeien uit het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM), in het bijzonder ten aanzien van het recht op bescherming van de persoonlijke levenssfeer. Zij verzoeken de regering daarbij de jurisprudentie van het Europees Hof voor Rechten van de Mens (EHRM) te betrekken. In hoeverre spoort het wetsvoorstel Computercriminaliteit III met de uitgangspunten en de vereisten waarin het wetsvoorstel WIV voorziet, en in hoeverre bestaan er verschillen tussen beide wetsvoorstellen op het terrein van de bescherming van de persoonlijke levenssfeer van de burger? Indien er verschillen tussen beide wetsvoorstellen bestaan, verzoeken de voornoemde leden om een overzicht van welke verschillen er zijn. Wil de regering daarbij uitdrukkelijk aangeven waarom die verschillen tussen beide wetsvoorstellen bestaan?

Hoe beoordeelt de regering de kritiek van de Afdeling advisering van de Raad van State op de proportionaliteit van het voorstel[3], zo vragen de leden van de **CDA**-fractie.

De leden van de **D66**-fractie merken op dat het wetsvoorstel de zogenaamde «hackbevoegdheid» introduceert: de bevoegdheid voor de politie om in te kunnen breken in elk digitaal apparaat van willekeurige burgers, inclusief toegang tot alle historische en toekomstige gegevens opgeslagen in randapparatuur en uitgewisseld met alle hiermee verbonden communicatiekanalen. Met de groei van het internet of things zal dit een groeiende lijst (digitale) apparatuur omvatten. Dit zijn niet alleen gegevens die de verdachte betreffen, maar ook gegevens van iedereen die in documenten voorkomt of met wie er digitaal contact is geweest. Daarmee raakt deze bevoegdheid een grote groep onschuldige burgers. Dit is een dusdanig grove en niet verfijnde maatregel dat er zeer goede argumenten tegenover moeten staan om de inbreuk op de privacy van burgers, zoals beschermd door artikel 8 van het EVRM, te rechtvaardigen.
Een beperking van het recht op privacy kan gelegitimeerd zijn indien deze proportioneel en noodzakelijk is. Zowel de Afdeling advisering van de Raad van State[4] als het College Bescherming Persoonsgegevens[5] (thans de Autoriteit Persoonsgegevens) hebben serieuze kritiek geuit ten aanzien van de door de regering gegeven motivatie. Er moet een redelijke verhouding bestaan tussen de inmenging in het recht op de bescherming van de persoonlijke levenssfeer enerzijds en de legitieme doelstelling anderzijds. Kan de regering een nadere toelichting geven op de noodzakelijkheid en proportionaliteit? Kan zij onderbouwen waarom een dusdanige verreikende bevoegdheid daadwerkelijk in lijn is met het recht op privacy, zoals beschermd door artikel 8 van het EVRM?

Het binnendringen van een geautomatiseerd werk heeft altijd tot gevolg dat er veel meer data worden verzameld dan doelmatig gezien nodig is. Ook wordt hierdoor de privacy van onschuldige burgers bedreigd, omdat

---

[2] Kamerstukken 34 588.
[3] Kamerstukken II 2015/16, 34 372, nr. 4, p. 5–6.
[4] Kamerstukken II 2015/16, 34 372, nr. 4, p. 5–6.
[5] Brief van het CBP van 17 februari 2014, p. 8–10; te vinden op https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-hackbevoegdheid-politie-en-opsporingsdiensten.

via het netwerk deze ook in de gaten gehouden kunnen worden. Het College Bescherming Persoonsgegevens (thans: Autoriteit Persoonsgegevens) wees hier ook op. Het geeft tevens aan dat dit in strijd is met artikel 3 van de Wet politiegegevens.[6] Anderen wijzen erop dat dit in strijd is met artikel 8 van het EVRM. De **SP**-fractieleden vragen een reactie van de regering hierop.

De fractieleden van **GroenLinks** begrijpen dat cybercriminaliteit ten gevolge van een gedigitaliseerde wereld om een stevige aanpak vraagt. Tegelijkertijd hechten zij er sterk aan dat een wetsvoorstel voldoende proportionaliteit met zich meedraagt. Meent de regering dat het voorgestelde doel, bestrijding van cybercriminaliteit, de voorgestelde middelen heiligt, namelijk een vergaande inbreuk op individuele grondrechten? Waar zit precies het hiaat in de bestaande wettelijke bevoegdheden op dit terrein? Het antwoord van de regering tijdens eerdere vragenrondes in de Tweede Kamer, is dat de bestaande bevoegdheden tekortschieten, omdat deze ofwel zijn gekoppeld aan een bepaalde fysieke plaats, ofwel niet zijn gericht op de toegang tot elektronische gegevens die zich in een geautomatiseerd werk of op een gegevensdrager elders bevinden.[7] De vraag blijft echter overeind in hoeverre er minder vergaande mogelijkheden beschikbaar zijn, waarbij de privacy beter is gewaarborgd ten aanzien van individuele grondrechten. Welke andere mogelijkheden zijn er exact onderzocht en kan de regering uitleggen waarom deze volgens haar niet voldoen?

De Afdeling advisering van de Raad van State oordeelt onder meer dat de proportionaliteit van de voorgestelde bevoegdheid in het wetsvoorstel, het heimelijk binnendringen in een geautomatiseerd werk, onbewezen is gebleven. Zij benadrukt dat het in strijd is met het erkende recht op eerbiediging van de persoonlijke levenssfeer.[8] Naast de Afdeling advisering van de Raad van State hebben verschillende andere organisaties stevige kritiek geuit op het wetsvoorstel. Het College Bescherming Persoonsgegevens (thans de Autoriteit Persoonsgegevens) heeft zelfs geadviseerd om het wetsvoorstel niet op deze wijze in te dienen, omdat het voorstel een grondwettelijke toetsing niet zou doorstaan vanwege de gebrekkige onderkenning van de eerdergenoemde verstrekkende bevoegdheid.[9] Wat is de verwachting van de regering ten aanzien van een dergelijke grondwettelijke toetsing van het wetsvoorstel, zo vragen de fractieleden van GroenLinks.
Ook de Nederlandse burgerrechtenorganisatie Bits of Freedom vindt het wetsvoorstel te ruim in zijn bevoegdheden.[10] Het inmiddels beruchte voorbeeld is dat de politie je pacemaker zelfs mag hacken bij een klein misdrijf. Waarom is, naast de bestaande mogelijkheden en naast de mogelijkheden in de wetten Computercriminaliteit I en Computercriminaliteit II, nu een extra set vergaande bevoegdheden nodig? En wat is precies de reikwijdte van deze wet? En wordt er in het voorstel voldoende rekening gehouden met eerdere uitspraken van het Hof van Justitie van de Europese Unie, dat de afgelopen jaren meerdere malen kritiek op wetten had die de privacy van burgers te veel schenden? Graag een reactie van de regering.

---

[6] Brief van het CBP van 17 februari 2014, p. 9–10; te vinden op https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-hackbevoegdheid-politie-en-opsporingsdiensten.
[7] Zie bijvoorbeeld Kamerstukken II 2016/17, 34 372, nr. 6, p. 1–2.
[8] Kamerstukken II 2015/16, 34 372, nr. 4, p. 2.
[9] Brief van het CBP van 17 februari 2014, p. 2; te vinden op https://autoriteitpersoonsgegevens.nl/nl/nieuws/cbp-adviseert-over-hackbevoegdheid-politie-en-opsporingsdiensten.
[10] Kamerstukken II 2015/16, 34 372, nr. 3, bijlage Advies Bits of Freedom, p. 3–8.

4. Samenloop bevoegdheden AIVD en MIVD

De leden van de **D66**-fractie merken op dat in het wetsvoorstel staat dat de hackbevoegdheid ook ingezet mag worden tegen terrorismedreiging of een internationale cyberdreiging. Echter, het verzamelen van inlichtingen in de strijd tegen het terrorisme is een taak van de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: MIVD). Zij hebben, zoals in een recente brief van Privacy First wordt benadrukt[11], al de bevoegdheid om een geautomatiseerd werk te hacken. Waarom wil de regering deze bevoegdheid ook uitbreiden naar de politie, als de AIVD en MIVD deze bevoegdheid reeds hebben? Kan zij aangeven of dit de afbakening van taken van deze instanties niet juist versnippert en onduidelijker maakt?

De regering geeft aan dat het wetsvoorstel nodig is om terroristische aanslagen te voorkomen. De leden van de fractie van de **SP** vragen haar of het juist is dat de inlichtingendiensten dit tot taak hebben. Zo ja, waarom wil zij deze bevoegdheid uitbreiden naar de politie?

De leden van de fractie van de **ChristenUnie** merken op dat de bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk op dit moment al kan worden toegepast door de AIVD en MIVD na de toestemming van de Minister van Binnenlandse zaken en Koninkrijksrelaties en/of de Minister van Defensie. Zij vragen naar de noodzaak van de nieuwe voorgestelde bevoegdheid en de ratio achter de geringe clausulering voor het gebruik daarvan door de opsporingsdiensten. Zij lezen dat de nieuwe bevoegdheid met name noodzakelijk is bij de opsporing van (de voorbereiding) van terroristische misdrijven en de bestrijding van kinderpornografie. Deze leden vragen of er andere terreinen zijn waar de opsporingsdiensten onvoldoende resultaat boeken als gevolg van het ontbreken van de voorgestelde hackbevoegdheden. Zij vragen om een nadere cijfermatige onderbouwing van de noodzaak om deze bevoegdheid zo ruim uit te breiden. Tevens krijgen zij graag inzicht in hoe vaak de veiligheidsdiensten op dit moment gebruikmaken van de bevoegdheden tot het heimelijk binnendringen van een geautomatiseerd werk en hoe zich dit verhoudt tot het gebruik van dit instrument in de omliggende landen. Hoe vaak wordt gebruikgemaakt van de bemachtigde gegevens van de veiligheidsdiensten in een strafproces?

5. Kwetsbaarheden

In de Tweede Kamer is uitgebreid debat gevoerd over de in dit wetsvoorstel verleende bevoegdheid aan het Openbaar Ministerie (hierna: OM) om uitstel te verlenen aan het melden van onbekende kwetsbaarheden aan de producent als de opsporing er zwaarwegend belang bij heeft om deze melding nog uit te stellen. In het wetsvoorstel wordt geen termijn aan het – in beginsel ongeoorloofde uitstel tot melding van een kwetsbaarheid gesteld. In het debat wordt gewag gemaakt van een termijn van vier weken, maar die termijn kan door de rechter-commissaris steeds weer (tot in het oneindige) met vier weken worden verlengd.[12] Het lijkt de **CDA**-fractieleden verstandig om de maximale termijn alsnog in de wet te noemen, zodat de onbekende kwetsbaarheid kan worden gerepareerd: het is immers niet alleen de opsporingsambtenaar die van die kwetsbaarheid gebruik kan maken, maar criminelen evenzeer. Kan de regering hier nader op in gaan?

---

[11] Brief van 7 maart 2017, griffienummer: 160847.
[12] Handelingen II 2016/17, 34, item 26, p. 47.

De politie zal gebruikmaken van niet bekende kwetsbaarheden om in te breken in geautomatiseerde apparatuur, en informatie hierover zelfs inkopen bij organisaties die hier geld aan verdienen. Hiermee houdt de politie het bestaan van dergelijke kwetsbaarheden in stand, waarmee het internet en digitale apparaten onveiliger worden in plaats van veiliger. Waarom investeert de regering niet in het veiliger maken van de digitale wereld in plaats van financieren en gebruik van niet bekende kwetsbaarheden, zo vragen de fractieleden van **D66**.

De bevoegdheden die voorliggen worden gegeven aan de politie. De kennis van de politie op het gebied van cybercrime is over het algemeen niet erg groot. De aangiftebereidheid is laag en het justitiële apparaat is niet ingericht op de aanpak van cybercrime. Slachtoffers van *sextortion*, sexting of wraakporno voelen zich vaak niet serieus genomen bij de aangifte. Een wet met deze bevoegdheden heeft niet alleen geen enkele zin wanneer de politie slachtoffers naar huis stuurt met de opmerking dat ze niets voor hen kunnen doen, maar draagt ook grote risico's in zich. De kennis die nodig is om de wet uit te voeren, zal niet intern aanwezig zijn. De **SP**-fractieleden vragen of het klopt het dat de regering hiervoor externe partijen inhuurt. En zo ja, vindt zij dit dan een wenselijke ontwikkeling?
Hetzelfde geldt voor het inkopen van hacksoftware. Deze software zal door externe partijen ontwikkeld worden, maar zonder gedegen kennis weet de politie eigenlijk niet wat zij inkoopt. Hoe voorkomt de regering dat de politie hierbij schadelijke software inkoopt die weliswaar doet wat het zegt, maar tevens informatie over de politie aan derden verschaft? Graag een reactie.

Een grote zorgt leeft bij de SP-fractieleden over het gebruikmaken van de zogenaamde *Zero Day*-zwaktes. De politie krijgt niet de plicht om deze te melden. In de Verenigde Staten heeft dit nu geleid tot het seponeren van een zaak van kindermisbruik.[13] Hoe oordeelt de regering over deze situatie? Is het denkbaar dat de politie een zaak van kindermisbruik (of andere ernstige misdrijven) moet laten varen vanwege het feit dat zij de *Zero Day* niet wil openbaren? Hoe oordeelt de regering over de morele kant van de zaak? De politie is immers op de hoogte van een zwakte waar vele criminelen gebruik van zullen maken. Is het niet de taak van de politie om mensen te beschermen tegen criminaliteit? Is het niet melden van kwetsbaarheden in de beveiliging niet een vorm van medewerken aan de criminaliteit? Graag de mening van de regering.

De **PvdA**-fractieleden vragen de regering of zij het goed hebben begrepen dat de voorgestelde bevoegdheid voor opsporingsinstanties om onder voorwaarden een geautomatiseerd werk dat in gebruik is bij een verdachte, op afstand heimelijk binnen te dringen (ook wel de hackbevoegdheid genoemd) impliceert dat de overheid hackkennis op de markt zal gaan verwerven. Op grond van het voorliggende wetsvoorstel mogen opsporingsinstanties bij het hacken zelfs gebruikmaken van bij producent en gebruikers van software onbekende zwakheden («onbekende kwetsbaarheden») in de software. Die software zal echter niet alleen door verdachten worden gebruikt, maar ook door onschuldige burgers. Loopt de regering zo niet het risico mee te werken aan het in stand houden van de markt van onbekende kwetsbaarheden, waarmee veel geld wordt verdiend ten koste van de digitale veiligheid van de Nederlandse burgers? Weliswaar gaat het wetsvoorstel uit van de regel dat onbekende kwetsbaarheden door de officier van justitie aan de producent moeten worden gemeld, maar de in artikel 126ffa van de voorgestelde regeling maakt het

[13] https://arstechnica.com/tech-policy/2016/04/judge-child-porn-search-warrant-issued-in-va-not-valid-for-pc-in-okla/.

mogelijk dat die melding op grond van een zwaarwegend opsporingsbelang wordt uitgesteld. Bits of Freedom heeft bij brief van 23 februari 2017[14] de volgende kritische kanttekeningen geformuleerd bij dit artikel:

1. De opsporingsinstanties zullen veelal gebruikmaken van softwarepakketten die het hacken sterk vergemakkelijken. Volgens Bits of Freedom zullen opsporingsinstanties vaak niet weten van welke kwetsbaarheden daarbij gebruik wordt gemaakt en of deze gemeld moeten worden: *«Als de Nederlandse opsporingsdiensten niet weten of zij gebruik maken van onbekende kwetsbaarheden, dan hoeven zij deze ook niet te melden. Wat je niet weet kun je immers niet melden. De meldplicht wordt dan omzeild.»*[15]
2. Het is volgens Bits of Freedom zeer aannemelijk dat onbekende kwetsbaarheden gebruikt worden in hacksoftware. Die zullen door het bedrijf dat die software levert, zelf gevonden of ingekocht zijn: *«In ieder geval zal de Nederlandse overheid daarmee wel degelijk een bijdrage leveren aan het vercommercialiseren van onze digitale kwetsbaarheid.»*[16]
3. Als de betreffende opsporingsinstantie al weet welke onbekende kwetsbaarheden worden gebruikt, dan is het nog maar de vraag of zij dat wel zal melden. Op grond van geheimhoudingsverklaringen die de leverancier van de hacksoftware zal bedingen, zal het de opsporingsinstanties verboden zijn om onbekende kwetsbaarheden bekend te maken, aldus Bits of Freedom.[17]
4. Het gebruik van de betreffende hacksoftware is omstreden, omdat deze ook zal worden geleverd aan landen die het niet zo nauw nemen met de grondrechten van hun burgers.[18]
5. Het in artikel 126ffa van het wetsvoorstel voorgestelde meldingsregime werkt in de praktijk niet, omdat het kan betekenen dat het ene opsporingsteam (gezien het zwaarwegende opsporingsbelang) wel machtiging van de rechter-commissaris krijgt voor uitstel van de melding, terwijl een andere opsporingsteam dat gebruikmaakt van dezelfde onbekende kwetsbaarheid, geen toestemming krijgt (vanwege een geringer opsporingsbelang) en dus de betreffende kwetsbaarheid zou moeten melden, waarna het beveiligingsgat gedicht gaat worden. Dat laatste zou echter het werk van het eerstgenoemde opsporingsteam verstoren.[19]

De leden van de PvdA-fractie verzoeken de regering ten gronde te reageren op voornoemde opmerkingen van Bits of Freedom.

De PvdA-fractieleden vragen voorts aandacht voor de aanschaf en veiligheid van de malware die Nederlandse opsporingsinstanties gaan gebruiken. Bits of Freedom wijst in bovengenoemde brief op de *Bundestrojaner*-affaire (waarin de malware die de Duitse politie gebruikte, onveilig was en uitlekte) en op de *Verint*-zaak.[20] De voornoemde leden vragen de regering hoe de opsporingsinstanties aan de benodigde malware komen, of bepaalde voorwaarden voor de aanschaf worden gehanteerd, en of de Nederlandse overheid te allen tijde inzicht in de broncode van de malware eist. Ook vragen zij de regering hoe van derden gekochte malware wordt gecontroleerd op veiligheid, bijvoorbeeld op de aanwezigheid van zogenaamde *backdoors*.

---

[14] Griffienummer: 160847.01.
[15] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2.
[16] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2.
[17] Brief van 23 februari 2017, griffienummer: 160847.01, p. 2–3.
[18] Brief van 23 februari 2017, griffienummer: 160847.01, p. 3.
[19] Brief van 23 februari 2017, griffienummer: 160847.01, p. 3–4.
[20] Brief van 23 februari 2017, griffienummer: 160847.01, p. 6.

Er wordt voorgesteld om gebruik te maken van nog onbekende kwetsbaarheden (onder andere door middel van zogenaamde *Zero Days*) binnen het internet om hacken mogelijk te maken. Wat zijn de gevolgen hiervan voor de veiligheid van het internet en hoe verhoudt dit wetsvoorstel zich daarmee tot het rapport «De publieke kern van het internet» van de Wetenschappelijke Raad voor het Regeringsbeleid[21] (WRR)? De fractieleden van **GroenLinks** vragen de regering om in plaats van te verwijzen naar haar brief van inmiddels een aantal maanden geleden, in haar beantwoording heel precies in te gaan op het gevaar van het laten voortbestaan van een kwetsbaarheid die mogelijk tot meer slachtoffers van criminaliteit leidt. Gaat dit wetsvoorstel juist kwetsbaarheden openhouden in plaats van ze te dichten, om zo van deze gaten gebruik te kunnen maken tijdens het hacken? De voornoemde leden ontvangen graag een toelichting van de regering.

6. Lokpuber en grooming

Klopt het dat poging tot grooming strafbaar blijft in het onderhavige wetsvoorstel? Hoewel daar in de optiek van de fractieleden van het **CDA** inhoudelijk veel voor te zeggen is, is dit volgens de Afdeling advisering van de Raad van State strafbaarstelling van een «poging tot een poging», omdat er volgens staande jurisprudentie nog geen uitvoeringshandeling plaatsvindt[22]. Kan de regering juridisch beargumenteren waarom het advies van de Afdeling niet is gevolgd?

Kan de regering beargumenteren of, en zo ja hoe, het opsporen van pedofielen door middel van een «virtuele lokpuber» door een (meerderjarige) opsporingsambtenaar tot een eventuele strafbaarstelling van de opgespoorde pedofiel kan leiden? De jurisprudentie geeft niet eenduidig aan dat het strafbaar is om in te gaan op de lokroep van een virtuele lokpuber, wanneer daar een meerderjarige ambtenaar achter schuilgaat. Maakt dit wetsvoorstel dat in de ogen van de regering juridisch mogelijk, zo vragen de leden van de CDA-fractie.

De **D66**-fractieleden merken op dat het wetsvoorstel een aantal wijzigingen bevat van de zedendelicten. In een recent artikel in Ars Aequi wijst mr. K. Lindenberg erop dat lokpuberzaken, waarbij een opsporingsambtenaar zich op het internet voordoet als jeugdige en zodoende in staat is «groomers» op heterdaad te betrappen, vooralsnog vaak gedoemd zijn te mislukken, omdat voor de strafbaarheid noodzakelijk is dat de verdachte daadwerkelijk met een minderjarige heeft gecommuniceerd.[23] Het onderhavige wetsvoorstel wil het gebruik van de lokpuber mogelijk maken door aanvullende strafbaarheid te creëren voor het handelen jegens iemand *die zich voordoet als kind*. In hoeverre is de lokpuber in overeenstemming met het instigatieverbod, waarbij opsporingsambtenaren burgers niet mogen brengen tot handelingen waarop hun opzet niet reeds was gericht?

De leden van de fractie van de **ChristenUnie** vragen of het voorgestelde artikel 248a ruimte biedt voor anderen dan opsporingsbeambten om zich voor te doen als een virtuele creatie van iemand die de leeftijd van achttien jaren nog niet heeft bereikt en zo een bijdrage te leveren aan de opsporing. Zij vragen of de regering dergelijke initiatieven wenst of juist

---

[21] Rapport van de Wetenschappelijke Raad voor het Regeringsbeleid, *«De publieke kern van het internet. naar een buitenlands internetbeleid»*, Amsterdam: 2015.

[22] Kamerstukken II 2015/16, 34 372, nr. 4, p. 34–35.

[23] K. Lindenberg, «De lokpuber verstopt zich in het materiële recht. Over het aanpassen van de zedendelicten door Computercriminaliteit III en hoe dit meer is dan het lijkt», Ars Aequi 2016, nr. 12, p. 942–950.

niet, en de opsporing wenst te beperken tot de politie. Zij vragen tevens om een uitleg bij de huidige redactie van het voorgestelde artikel.
De voornoemde leden menen dat er geen advies aan de Nationaal Rapporteur Mensenhandel en Seksueel Geweld tegen Kinderen is gevraagd over de toepassing van het voornoemde artikel. Gelet op het onderwerp zou een advies in de rede liggen en de fractieleden van de ChristenUnie zouden een dergelijk advies dan ook van meerwaarde vinden bij de beoordeling van het wetsvoorstel. Graag een reactie van de regering hierop.

7. Geautomatiseerd werk

De criteria voor de inzet van de hackbevoegdheid zijn dezelfde als voor de inzet van een telefoon- of internettap. Ook geldt de hackbevoegdheid voor «een geautomatiseerd werk», hetgeen vrijwel alle elektronische apparaten omvat (hetgeen de komende jaren met het internet of things alleen maar in omvang zal toenemen). Kan de regering aan de **D66**-fractieleden uitleggen waarom niet gekozen is voor een lijst met een limitatieve opsomming van specifieke misdrijven waarvoor de bevoegdheid beperkt moet worden en specifieke apparaten die gehackt mogen worden?

De hackbevoegdheid is de bevoegdheid binnen te dringen tot geautomatiseerde werken. Het is echter niet duidelijk welke apparaten hier wel en niet onder vallen. Daardoor vallen nagenoeg alle apparaten hieronder. De leden van de fractie van de **SP** zouden graag een lijst zien van de apparaten waarvan de regering van mening is dat deze onder het begrip «geautomatiseerd werk» vallen.

De leden van de fractie van de **ChristenUnie** constateren dat in het voorgestelde artikel 80sexies 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. Zij merken op dat hiermee een zeer brede categorie ontstaat. Naast communicatiemiddelen zullen ook huishoudelijke apparatuur, energiemeters en zelfs apparaten in het menselijk lichaam, zoals de pacemaker, onder deze definitie kunnen vallen. De voornoemde leden vragen of is overwogen een meer limitatieve lijst op te stellen of dat op andere wijze een nadere begrenzing is overwogen. Zij kunnen zich bijvoorbeeld voorstellen dat apparatuur in het menselijk lichaam wordt uitgesloten.

8. Toezicht

Een belangrijk onderdeel van het advies van de Afdeling advisering van de Raad van State betrof het instellen van een orgaan dat dan wel instantie die belast zou worden met het houden van structureel systeemtoezicht op de toepassing van de nieuw voorgestelde bevoegdheden, met name in de gevallen waarin het gebruik van de bevoegdheden ten aanzien van een geautomatiseerde werk niet tot een veroordeling door een (straf)rechter heeft geleid. Zij meende dat in die gevallen een afdoende toetsing achteraf inzake de noodzakelijkheid en proportionaliteit van de inzet van de bevoegdheid ontbreekt.[24] Aan het advies is echter geen gevolg gegeven. Kan de regering aan de fractieleden van **D66** uitleggen waarom er geen structureel toezicht in het leven geroepen wordt? Is er voldoende toezicht en rechtsbescherming voor de verdachte? En is de privacy van onschuldige derden voldoende gewaarborgd?

---

[24] Kamerstukken II 2015/16, 34 372, nr. 4, p. 9–10.

Naast de discutabele voorstellen die voor liggen, ontbreekt er in het wetsvoorstel de zeer nodige vorm van rechtsbescherming. Zo noemt de Afdeling advisering van de Raad van State de noodzaak voor een commissie die bekijkt of inbreken in de digitale omgeving wel terecht was in die gevallen waar de zaak niet voor de rechter is gekomen. Het toezicht hierop zou onafhankelijk geregeld moeten zijn.[25] Waarom heeft de regering niet gekozen om deze wetgeving met goed toezicht te omkleden, zo vragen de fractieleden van de **SP**.
De Afdeling noemt ook het probleem van de internationale omgeving.[26] Wat nu als de indringing heeft plaatsgevonden op het terrein van een ander land, hoe zou de rechter dan moeten oordelen? Daar wordt geen oplossing voor gegeven. Graag hier een reactie op van de regering.

De Afdeling advisering van de Raad van State heeft er in haar advies op gewezen dat het voorliggende wetsvoorstel past in een reeks ontwikkelingen zoals het toenemend gebruik van telefoon- en internettap, de opslag van verkeersgegevens omtrent internet en telefoongebruik, de registratie en opslag van kentekengegevens van burgers, en de toepassing van gezichts- en gedragsherkenningssoftware bij het cameratoezicht. Naar het oordeel van de Afdeling hangt het vertrouwen van de burger in de overheid mede af van het toezicht dat wordt gehouden op de toepassing van deze bevoegdheden. Zij heeft de regering geadviseerd te voorzien in structureel systeemtoezicht op de toepassing van opsporingsbevoegdheden waarbij gebruik wordt gemaakt van de informatie- en communicatietechnologie in zaken die niet aan de strafrechter zijn voorgelegd.[27] De regering heeft aan dat advies geen gevolg gegeven. De leden van de **PvdA**-fractie vragen de regering nog eens ten gronde uiteen te zetten waarom zij meent dat het niet nodig is het advies van de Afdeling en de daarbij gedane concrete suggestie voor de invulling van dat toezicht, op te volgen.

Verzoeken tot hacken mogen niet zomaar gegeven worden. De fractieleden van **GroenLinks** menen dat onafhankelijke controle van fundamenteel belang is voor de Nederlandse rechtsstaat. Kan de regering toezeggingen doen over of, en zo ja hoe, zij het onafhankelijk toezicht op de hackbevoegdheid van de politie wil gaan regelen? In hoeverre is de in het voorstel opgenomen toestemming van de rechter-commissaris en controle door de Centrale Toetsingscommissie hiervoor geschikt? Graag een reactie van de regering.

De leden van de **ChristenUnie**-fractie vragen op welke wijze het gebruik en de effectiviteit van de inzet zal worden gemonitord. Zij vragen waarom niet gekozen is voor een vorm van onafhankelijk toezicht door een orgaan buiten het Ministerie van Veiligheid en Justitie. Tevens vragen zij om een nadere toelichting op welke wijze het structurele toezicht op het gebruik inzichtelijk wordt gemaakt.

9. Begroting

Bij het voorgestelde artikel II, onder EE staat vermeld: «Artikel 592, tweede lid, eerste volzin, komt te luiden: De kosten van het nakomen van een vordering tot het verstrekken van gegevens of tot het medewerking verlenen aan het ontsleutelen van gegevens krachtens de artikelen 125k, 126m, 126n, 126na, 126nc tot en met 126ni, 126t, 126u, 126ua, 126uc tot en met 126ui, 126zg, 126zh, 126zi en 126zja tot en met 126zp kunnen de betrokkene uit 's Rijks kas worden vergoed». Kan de regering aangeven

[25] Kamerstukken II 2015/16, 34 372, nr. 4, p. 9–10.
[26] Kamerstukken II 2015/16, 34 372, nr. 4, p. 13.
[27] Kamerstukken II 2015/16, 34 372, nr. 4, p. 9–10.

wanneer deze kosten wel en wanneer deze kosten niet worden vergoed? Of zouden deze kosten steeds uit 's Rijks kas behoren te worden vergoed, zo vragen de **CDA**-fractieleden.

De leden van de fractie van de **ChristenUnie** krijgen graag meer inzicht in hoe verwacht wordt dat de financiële middelen verschuiven binnen het budget van de nationale politie binnen het totaal beschikbare budget. Zij lezen dat de mate van verschuiving afhankelijk is van de verwachtingen van en ervaring met toepassing van het instrument. Dat zal niet alleen gelden voor de feitelijke ontwikkeling en inzet van onderzoek in een geautomatiseerd werk en het gebruik van technische hulpmiddelen ten behoeve van de uitvoering van die bevoegdheid, maar ook voor de inzet van menskracht. Welke verwachting heeft de regering momenteel, en ten laste van welke andere inzet zal dit wetsvoorstel dan bij de invoering van het wetsvoorstel komen, zo vragen voornoemde leden.
Kan voorzien worden in enkele scenario's en een begroting voor de eerste jaren na inwerkingtreding van het wetsvoorstel? Is voor de inzet van deze bevoegdheden geen extra capaciteit nodig?
Zij krijgen tevens graag inzicht in hoe de extra voorziene structurele last voor de rechtspraak van 500.000 euro wordt gedekt in de begroting van het ministerie. Zij missen duidelijkheid over de gevolgen van dit wetsvoorstel voor de begroting van het OM.

10. Gedelegeerde regelgeving

Toetsingscriteria zullen worden opgesteld en vastgelegd in een AMvB of in een OM-aanwijzing met betrekking tot opsporingshandelingen voor gegevens die niet zijn opgeslagen in Nederland. Zijn deze criteria inmiddels opgesteld, en zo ja, wat zijn deze criteria? Wanneer komt de tekst van de AMvB of OM-aanwijzing naar verwachting beschikbaar, zo vragen de **VVD**-fractieleden.

Het binnendringen op afstand in geautomatiseerde werken mag alleen als er een vermoeden, (verdenking, aanwijzing) bestaat van een misdrijf waarop een gevangenisstraf van vier jaar of meer gesteld is, van ernstige misdrijven dus, maar ook van misdrijven die «bij algemene maatregel van bestuur» worden aangewezen[28]. Dat lijkt de leden van de **CDA**-fractie ongewenst; zonder tussenkomst van de Staten-Generaal kan de regering hierdoor in beginsel ieder misdrijf via een AMvB onder de werking van dit wetsvoorstel brengen. Waarom worden juist deze misdrijven gekozen? Op basis van welke criteria wordt er besloten om eventueel misdrijven toe te voegen? In de optiek van voornoemde leden dient een dergelijke AMvB tenminste worden voorgehangen. Is de regering bereid om een reparatie-wetsvoorstel in te dienen, waarin dit wordt geregeld?
En in vervolg op het bovenstaande: is de regering het met de leden van de CDA-fractie eens dat een eventuele uitbreiding van dit wetsvoorstel met andere misdrijven in het geheel niet bij AMvB geregeld kan worden, maar bij wet moeten worden vastgelegd?

Het wetsvoorstel bevat op verschillende plaatsen delegatiebepalingen. Begrijpen de leden van de **PvdA**-fractie het goed dat het hierbij steeds gaat om het Besluit technische hulpmiddelen strafvordering? Zij wensen van de regering te vernemen op welke termijn de tekst van bedoelde lagere regelgeving (waaronder in ieder geval voornoemd Besluit) beschikbaar zal zijn, of er een voorhangprocedure zal plaatsvinden, en of de betreffende regelgeving ter internetconsultatie zal worden aangeboden.

---

[28] Zie artikel 126nba, eerste lid, van het wetsvoorstel, artikel 126uba, eerste lid, van het wetsvoorstel en artikel 126zpa, eerste lid, van het wetsvoorstel.

11. Internationale aspecten

Tijdens de plenaire behandeling van het wetsvoorstel in de Tweede Kamer op 13 december 2016 heeft de Staatssecretaris van Veiligheid en Justitie aangegeven dat hij streeft naar betere paraplu-afspraken met andere staten in voorkomende gevallen van ernstige strafbare feiten waarbij Nederlandse opsporingsambtenaren onbedoeld toegang krijgen tot geautomatiseerde werken die zich buiten Nederland bevinden. Die afspraken zouden ook voor omgekeerde situaties hebben te gelden wanneer buitenlandse opsporingsambtenaren zich onbedoeld op een Nederlandse server of net bevinden.[29] Wat is het tijdpad dat de regering zich voorstelt voor het maken van deze paraplu-afspraken, zo vragen de leden van de **VVD**-fractie. Kan zij binnen een termijn van één jaar de Kamer informeren over de voortgang wat betreft het maken van deze paraplu-afspraken met andere staten en de inhoud van die afspraken?

Met betrekking tot opsporing van computercriminaliteit die de landsgrenzen overschrijdt, is in internationaal verband kennelijk vastgesteld dat het territorialiteitsbeginsel in «cyberspace» onder druk staat en dat dit beginsel niet kan worden toegepast als de exacte locatie van gegevens onduidelijk is. Kan de regering de leden van de VVD-fractie informeren over de stand van zaken en ontwikkelingen om te komen tot internationale regels met het oog op de bestrijding van internationale computercriminaliteit? Is zij van plan om in dezen initiatieven te ontwikkelen, bijvoorbeeld door het organiseren van een internationale conferentie, mede met het oog op de belangrijke positie die Nederland inneemt op het terrein van de handhaving van de internationale rechtsorde?

De **GroenLinks**-fractieleden hebben enkele vragen over het grensoverschrijdende karakter van cybercriminaliteit in relatie tot dit wetsvoorstel. Hoe verhoudt dit voorstel zich tot de huidige regels op het gebied van internationale samenwerking ten aanzien van cybercriminaliteit? Wanneer kan er precies gebruikgemaakt worden van de voorgestelde grensoverschrijdende bevoegdheid? Volstaat het gebruikelijke rechtshulpverzoek niet voor dit soort gevallen? Hoe verlopen de onderhandelingen in EU-verband en in de Raad van Europa over een helder grensoverschrijdend juridisch kader? De voornoemde leden zijn benieuwd naar de antwoorden van de regering.

12. Overige

Wanneer er bij de provider/aanbieder en de officier van justitie verschil van inzicht bestaat over het ontoegankelijk maken van gegevens in een geautomatiseerd werk, dan wordt er een formele procedure in gang gezet die mogelijk veel tijd in beslag kan nemen, merken de VVD-fractieleden op. Op welke manier wordt gewaarborgd dat deze procedurele route zo spoedig mogelijk verloopt, juist met het oog op de potentiële dreiging die met deze informatie verbonden kan zijn wanneer de informatie voor derden beschikbaar blijft op het net?

De **CDA**-fractieleden merken op dat de bewoordingen van *de aanleiding* tot het mogen binnendringen in een geautomatiseerd werk door de opsporingsambtenaren in de verschillende wetsartikelen verschillend worden omschreven: in artikel 126nba, eerste lid, van het wetsvoorstel staat «In geval van *verdenking* van een misdrijf [...]» en in artikel 126uba, eerste lid, van het wetsvoorstel staat «In een geval als bedoeld in artikel 126o [...]». In artikel 126zpa, eerste lid, van het wetsvoorstel staat: «In geval van *aanwijzingen* van een terroristisch misdrijf [...]». Kan de

[29] Handelingen II 2016/17, 34, item 26, p. 43.

regering de logica van de verschillende formuleringen uitleggen? Mag men in het ene geval eerder binnendringen dan in het andere geval? Zo ja, wat zijn de verschillen en waarom zijn deze gemaakt?

In artikel II, onder X, van het wetsvoorstel is onder punt 9 gesteld: «Acht het gerecht het beklag, bedoeld in het eerste lid, tweede volzin, gegrond, dan kan het het bevel geheel of gedeeltelijk opheffen.» Volgens de leden van de CDA-fractie zou hier geen sprake moeten zijn van «kunnen», maar van «moeten». Dan zou de wettekst moeten luiden: «Acht het gerecht het beklag, bedoeld in het eerste lid, tweede volzin, gegrond, dan wordt het bevel opgeheven.» Aan welke gevallen denkt de regering, waarbij – ondanks de gegrondheid van het beklag – het bevel tóch niet zou moeten of mogen worden opgeheven?

De leden van de fractie van de **SP** hebben vragen over artikel 125p van het wetsvoorstel. Graag willen zij weten wat dit artikel extra beoogt in vergelijking tot artikel 54a van het Wetboek van Strafrecht. Met dit laatste artikel kan een rechter-commissaris bevelen websites met bijvoorbeeld materiaal van seksueel misbruik van kinderen offline te halen. Het voorgestelde artikel 125p lijkt hetzelfde te doen. Kan de regering uitleggen waarom dit artikel nodig is?
De voornoemde leden begrijpen dat content die offline is gehaald, binnen afzienbare tijd weer online kan komen. In artikel 125p, tweede lid, onder b, van het wetsvoorstel staat de zinsnede «[...] of nieuwe strafbare feiten te voorkomen». Suggereert dit dat een internetserviceprovider, nadat deze het materiaal offline heeft gehaald en het materiaal opnieuw op internet verschijnt, aansprakelijk is voor dat materiaal? Graag een toelichting van de regering.

De leden van de fractie van de **ChristenUnie** vragen om een reflectie op het feit dat Nederland bovenmatig vaak gebruikmaakt van telefoon- en gegevenstaps. Is duidelijk te maken of en hoe dit uitwerkt op de veiligheid voor Nederlandse burgers vergeleken met andere EU-burgers? Welke verwachting heeft de regering van het gebruik van de nieuwe voorgestelde bevoegdheid? De voornoemde leden vragen of van de nieuwe bevoegdheid verwacht wordt dat deze zich ontwikkelt tot een ultimum remedium of juist tot een gangbaar gebruikte opsporingsbevoegdheid.

De leden van de fractie van de ChristenUnie vragen voorts hoe de leeftijdsgrenzen in de voorgestelde artikelen 248a en 248e zich verhouden tot de leeftijdsgrens van 21 jaar in het wetsvoorstel Wet regulering prostitutie en bestrijding misstanden seksbranche[30].
Zij vragen tevens met welke reden in het voorgestelde artikel 248a wordt gekozen voor een objectivering van de leeftijdsaanduiding. De voornoemde leden vragen ook of de nieuwe invulling van artikel 248a van het Wetboek van Strafrecht gevolgen heeft voor de interpretatie van de daaropvolgende artikelen en in het bijzonder artikel 248b van het Wetboek van Strafrecht. Zij vragen of «ontucht plegen» in dit artikel door de voorgestelde artikel 248a in het vervolg ook met een webcam of ander technisch hulpmiddel kan plaatsvinden.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Duthler

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren

---

[30] Kamerstukken 32 211.