COLLEGE BESCHERMING PERSOONSGEGEVENS

POSTADRES Postbus 93374, 2509 AJ Den Haag BEZOEKADRES Juliana van Stolberglaan 4-10
TEL 070 - 88 88 500 FAX 070 - 88 88 501 INTERNET www.cbpweb.nl www.mijnprivacy.nl

AAN De Minister van Veiligheid en Justitie

Postbus 20301
2500 EH DEN HAAG

DATUM 17 februari 2014
ONS KENMERK z2013-00349
CONTACTPERSOON

UW BRIEF VAN 2 mei 2013
UW KENMERK

ONDERWERP Consultatie conceptwetsvoorstel Computercriminaliteit III

Geachte ,

Bij brief van 2 mei 2013 heeft u het College bescherming persoonsgegevens (CBP) het concept-wetsvoorstel Computercriminaliteit III toegezonden met het verzoek daarover advies uit te brengen op grond van het bepaalde in artikel 51, tweede lid, Wet bescherming persoonsgegevens. Het CBP heeft u bij brief van 23 mei 2013 bericht zijn advies te zullen uitbrengen wanneer de opmerkingen van de internetconsultatie zijn verwerkt in een aangepaste tekst. Bij e-mail van 23 januari 2014 heeft het CBP van uw ministerie een overzicht van de belangrijkste wijzigingen ontvangen. Het CBP voldoet hiermee aan uw verzoek.

**Inhoud van het voorstel**
Het conceptwetsvoorstel strekt tot 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). Dit wetsvoorstel beoogt het juridische instrumentarium voor de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken. Het wetsvoorstel vormt een uitwerking van eerdere toezeggingen aan de Tweede Kamer alsmede van het in het regeerakkoord van dit kabinet opgenomen voornemen om de toenemende bedreigingen en kwetsbaarheden op het terrein van cybersecurity het hoofd te bieden door het juridisch instrumentarium aan te passen naar aanleiding van de ontwikkelingen op het gebied van de informatie- en communicatietechnologie. Daartoe wordt voorgesteld te komen tot uitbreiding van de strafvorderlijke bevoegdheden en van een aantal strafbepalingen.

**Beoordeling van het voorstel**
Het CBP heeft zijn advies beperkt tot de bespreking van de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk. Zoals hierna in de bijlage bij deze brief is uiteengezet luidt zijn oordeel en vervolgens zijn advies hierover als volgt.

Het CBP onderkent dat het juridisch instrumentarium voor de opsporing en vervolging van computercriminaliteit en strafbare feiten in zijn algemeenheid, zoveel mogelijk gelijke tred dient te houden met de technologische ontwikkelingen.

Het bereik van de thans voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk strekt zich uit tot een zeer grote hoeveelheid gegevens. Het betreft volledige toegang tot alle historische gegevens die op randapparatuur zijn opgeslagen en de gegevens die worden opgeslagen op en uitgewisseld via alle communicatiekanalen waarmee de randapparatuur is verbonden. Bovendien kan deze bevoegdheid ook betrekking hebben op toekomstige gegevens. Daarbij gaat het niet alleen om gegevens die de verdachte zelf betreffen, maar ook om gegevens van alle personen die worden genoemd in documenten of met wie hij/zij digitaal contact heeft gehad. Toepassing van deze bevoegdheid raakt daarmee een grote groep mensen tot wie de verdenking zich niet richt.

Juist om die reden is het van groot belang dat het wetsvoorstel blijk geeft van een zorgvuldige afweging binnen de grondwettelijke kaders van het recht op eerbiediging van de persoonlijke levenssfeer, zoals vastgelegd in artikel 10 Grondwet en artikel 8 Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Op grond van het EVRM en de jurisprudentie van het Europese Hof voor de rechten van de mens (EHRM) zijn inbreuken op fundamentele rechten slechts rechtmatig indien deze voldoen aan strikte voorwaarden, die zien op de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit.

In de toelichting op het thans voorliggende wetsvoorstel zijn overwegingen opgenomen ten aanzien van de noodzaak, proportionaliteit en subsidiariteit. Het CBP is evenwel van oordeel dat het ingrijpende karakter van de voorgestelde bevoegdheid en de uitgebreide kring van personen die de inzet ervan kan betreffen, hierbij onvoldoende zijn onderkend. De overwegingen die ten grondslag liggen aan de voorgestelde bevoegdheid tot onderzoek in een geautomatiseerd werk, worden in belangrijke mate gebaseerd op een aantal concrete situaties dat – wat daar verder overigens van zij – de invoering van de beoogde bevoegdheid op zichzelf onvoldoende kan rechtvaardigen. De dringende noodzaak als bedoeld in artikel 8 EVRM behoeft daarnaast, mede in het licht van de telkens te maken afweging van proportionaliteit en subsidiariteit ook een zelfstandige, boven de casuïstiek verheven beschouwing en onderbouwing.

Gelet hierop adviseert het CBP u om bij de gronden en afwegingen die de noodzaak van aanpassing van de huidige wettelijke bepalingen moeten onderbouwen, nadere aandacht te besteden aan de door artikel 8 EVRM gestelde voorwaarden.

**Advies**

Het CBP adviseert u het voorstel niet aldus in te dienen.

Ik vertrouw erop u hiermee voldoende te hebben geïnformeerd.

Hoogachtend,
Het College bescherming persoonsgegevens,
Voor het College,

Mr. W.B.M. Tomesen
Lid van het College

**Bijlage bij de brief van het College bescherming persoonsgegevens van 17 februari 2014 inzake het conceptwetsvoorstel Computercriminaliteit III**

Opmerkingen vooraf

Het CBP heeft als wettelijke taak om op grond van het bepaalde in artikel 51, tweede lid, Wet bescherming persoonsgegevens te adviseren over voorstellen van wet die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens. Daartoe is het noodzakelijk dat het voorgelegde voorstel een afgeronde versie betreft en dat eventuele wijzigingen naar aanleiding van een internetconsultatie daarin zijn verwerkt. Ten tijde van de ontvangst van uw brief van 2 mei 2013 is de internetconsultatie inzake dit voorstel gestart. Het CBP heeft u bij brief van 23 mei 2013 bericht zijn advies te zullen uitbrengen wanneer de opmerkingen van internetconsultatie zijn verwerkt in een aangepaste tekst. Bij e-mail van 23 januari 2014 heeft het CBP van uw ministerie een overzicht van de belangrijkste wijzigingen ontvangen.

Daarnaast is uit uw brief van 12 december 2013 aan de Tweede Kamer gebleken dat u voornemens bent om een aanvullend voorstel als onderdeel van dit wetsvoorstel in januari 2014 aan de Raad van State voor te leggen[1]. Door uw ministerie werd per e-mail bevestigd dat deze aanvulling en tevens nog enkele andere wijzigingen direct aan de Raad van State zullen worden voorgelegd. Het CBP is (nog) niet in de gelegenheid gesteld om advies uit te brengen omtrent deze onderdelen van het wetsvoorstel.

**Inhoud van het voorstel**

Ten dele heeft het conceptwetsvoorstel, in **Artikel I**, betrekking op wijziging van het Wetboek van Strafrecht (Sr). Het CBP zal dit onderdeel niet bespreken in zijn advies, aangezien het dit vanuit oogpunt van dataprotectie niet aangewezen acht. De onderdelen C, D en F van **Artikel II**, dat betrekking heeft op wijziging van het Wetboek van Strafvordering (Sv) zal het CBP hierna bespreken voor zover dat uit oogpunt van dataprotectie van belang is.

**Onderdeel C – Onderzoek in een geautomatiseerd werk**

Dit onderdeel betreft de invoeging van een nieuw **artikel 125ja** Sv, inhoudende een nieuwe bevoegdheid tot het heimelijk binnendringen in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager die bij de verdachte in gebruik is, en het onderzoek doen met een technisch hulpmiddel.

Op grond van het **eerste lid** van dit ontwerp-artikel kan de officier van justitie in geval van verdenking van een misdrijf waarvoor voorlopige hechtenis is toegelaten en dat gezien zijn aard of de samenhang met andere door de verdachte begane misdrijven een ernstige inbreuk op de rechtsorde oplevert, indien het onderzoek dit dringend vordert, bevelen dat een (volgens het gewijzigde voorstel:) *daartoe aangewezen* opsporingsambtenaar of buitengewoon

[1] Kamerstukken II 2013-2014, 31 015, nr. 95.

opsporingsambtenaar binnendringt in een geautomatiseerd werk of een daarmee in verbinding staande gegevensdrager, bij de verdachte in gebruik, en onderzoek doet met een technisch hulpmiddel met het oog op:

a. het vaststellen van de aanwezigheid van gegevens of het bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker;
b. het overnemen van bestaande of toekomstige gegevens van het geautomatiseerde werk, voor zover redelijkerwijs nodig om de waarheid aan de dag te brengen;
c. de ontoegankelijkmaking van gegevens;
d. een bevel tot het direct afluisteren of opnemen van telecommunicatie, het direct afluisteren of opnemen van telecommunicatie bij verdenking van ernstige criminaliteit in georganiseerd verband en het direct afluisteren of opnemen van telecommunicatie bij aanwijzingen van een terroristisch misdrijf;
e. een bevel tot stelselmatige observatie of stelselmatige observatie bij verdenking van ernstige criminaliteit in georganiseerd verband of bij aanwijzingen van een terroristisch misdrijf.

In het belang van het onderzoek kunnen gegevens worden vastgelegd. Een toegevoegde wijziging op het conceptartikel is de bepaling dat de daartoe aangewezen opsporingsambtenaren dienen te voldoen aan eisen op het gebied van opleiding en expertise, die in het Besluit technische hulpmiddelen strafvordering zullen worden uitgewerkt. Het **tweede lid** omschrijft de inhoudelijke vereisten die aan het bevel worden gesteld. De wijziging van het voorstel houdt de toevoeging in dat indien het bevel de onderdelen a, b of c betreft, in het bevel tevens een duidelijke omschrijving van de handelingen wordt gegeven. Een nieuw onderdeel f. wordt toegevoegd dat de vermelding vereist van het tijdstip waarop, of de periode waarin het bevel ten uitvoer wordt gelegd. Het **derde lid** noemt de maximale periode waarvoor het bevel kan worden gegeven, te weten vier weken met een mogelijke verlenging van telkens vier weken. In het **vierde lid** wordt bepaald dat het bevel slechts kan worden gegeven na schriftelijke machtiging op vordering van de officier van justitie te verlenen door de rechter-commissaris. Bij dringende noodzaak (**vijfde lid**) kunnen de beslissing van de officier van justitie en de machtiging van de rechter-commissaris mondeling worden gegeven, in dat geval binnen drie dagen op schrift te stellen. Het **zesde lid** stelt dat in een algemene maatregel van bestuur (amvb) regels worden gesteld over de opslag, verstrekking en plaatsing van het technische hulpmiddel, de technische eisen waaraan het middel moet voldoen, onder meer met het oog op de onschendbaarheid van de vastgelegde gegevens, de vastlegging van gegevens over de uitvoering van het bevel en de werking van het technische hulpmiddel. De wijziging van het voorstel houdt de toevoeging van een onderdeel c. in dat de mogelijkheid biedt bij amvb nadere regels te stellen omtrent de autorisatie van de opsporingsambtenaren die kunnen worden belast met het verrichten van het onderzoek en de samenwerking met andere opsporingsambtenaren.

**Onderdeel D – Decryptiebevel aan de verdachte**

Dit onderdeel leidt tot wijziging van **artikel 125k** Sv, inhoudende dat het bevel tot ontsleuteling van gegevens onder de daarin gestelde voorwaarden kan worden gericht aan de verdachte. Aangezien dit onderdeel van het voorstel niet in overwegende mate betrekking heeft op de verwerking van persoonsgegevens zal het CBP het voorstel hierna niet verder bespreken.

**Onderdeel F – Ontoegankelijkmaking van gegevens**
Dit onderdeel stelt de invoeging voor van een nieuw **artikel 125p** Sv en betreft een te geven bevel tot ontoegankelijkmaking van gegevens door de officier van justitie aan een aanbieder van een communicatiedienst, na een voorafgaande machtiging daartoe door de rechter-commissaris. Dit onderdeel kan weliswaar betrekking hebben op een verwerking van persoonsgegevens, maar dit leidt niet tot een nieuw soort verwerking van persoonsgegevens. Om die reden acht het CBP de bespreking hiervan binnen de context van dit voorstel uit oogpunt van dataprotectie niet opportuun.

**Beoordeling van het voorstel**

1.1 Toetsingskader
De voorgestelde nieuwe bevoegdheid om heimelijk, op afstand binnen te dringen in een geautomatiseerd werk maakt inbreuk op fundamentele rechten, in het bijzonder op artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikel 10 van de Grondwet, die elk het recht op eerbiediging van de persoonlijke levenssfeer vaststellen. Op grond van het EVRM en de jurisprudentie van het Europese Hof voor de Rechten van de Mens (EHRM) zijn inbreuken op fundamentele rechten slechts rechtmatig indien deze voldoen aan de volgende voorwaarden: de beperking moet zijn "in accordance with the law", "in pursuit of a legitimate aim" en "necessary in a democratic society". Voor de toets van noodzakelijkheid dient op de eerste plaats sprake te zijn van een dringende noodzaak ("pressing social need") die feitelijk moet worden aangetoond, waarbij tevens dient te blijken dat sprake is van maatschappelijke schade die door de voorgestelde maatregel effectief kan worden tegengegaan. Daarnaast moet de beperking evenredig zijn aan het daarmee beoogde doel en mag deze niet verder gaan dan nodig ter vervulling van het legitieme doel (toets van proportionaliteit en subsidiariteit). Hierbij is tevens van belang dat is voorzien in adequate waarborgen ten behoeve van de uitoefening van het fundamentele recht.

1.2 Noodzaak, proportionaliteit en subsidiariteit volgens het voorstel
In de ontwerp-memorie van toelichting worden de achtergrond en redenen voor de voorgestelde wijziging als volgt omschreven. 'Met dit wetsvoorstel wordt aangesloten bij de snelle ontwikkelingen op het terrein van technologie, internet en computercriminaliteit. Deze ontwikkelingen roepen voortdurend de vraag op of de juridische instrumenten voldoende zijn toegesneden op een effectieve bestrijding van computercriminaliteit. Het doel van de bevoegdheid van onderzoek in een geautomatiseerd werk is om toegang te verkrijgen tot de gegevens die in een geautomatiseerd werk zijn of worden verwerkt ten behoeve van de opsporing van ernstige vormen van computercriminaliteit of andere ernstige misdrijven. De voorgestelde bevoegdheid van onderzoek in een geautomatiseerd werk voorziet in een leemte in de bestaande wettelijke bevoegdheden. De bestaande opsporingsbevoegdheden schieten echter in toenemende mate tekort om aan wezenlijke problemen en gebleken knelpunten op het gebied van de bestrijding van computercriminaliteit tegemoet te komen.'[2]

[2] Zie ontwerp-toelichting, p . 4-6.

De toelichting noemt daarvoor de volgende, redengevende ontwikkelingen, die worden toegelicht aan de hand van voorbeelden[3].
- De versleuteling van elektronische gegevens vormt in toenemende mate een probleem voor de opsporing van strafbare feiten.
- Het gebruik van draadloze netwerken, niet alleen in een woning, maar ook op andere plaatsen. Als gebruik wordt gemaakt van verschillende toegangspunten tot het internet, wat in toenemende mate het geval is, is het aftappen van de volledige communicatie van de verdachte vrijwel onmogelijk.
- Het gebruik van Cloudcomputingdiensten. In toenemende mate wordt gebruik gemaakt van zogenaamde "webbased" toepassingen, waarbij gegevens worden opgeslagen in de "Cloud" op servers die zich elders in Nederland of in het buitenland bevinden.
Aan alternatieven om andere (bestaande) opsporingsbevoegdheden in te zetten, worden teveel bezwaren toegedicht[4].

1.3 Algemeen beoordelingskader
De technologische ontwikkelingen in de laatste decennia zijn van grote invloed geweest op ons maatschappelijke leven, in het bijzonder de invloed van elektronische communicatietechnologie. Een steeds groter deel van ons leven speelt zich (louter) digitaal af, zoals onder meer bankieren, winkelen, belasting betalen en onderwijs. De digitaal vastgelegde en uitgewisselde informatie betreft ook in toenemende mate zeer persoonlijke gegevens. Daarbij zijn de technologische mogelijkheden om digitale gegevens toegankelijk te maken en met elkaar te combineren eveneens toegenomen. Het maatschappelijk belang bij adequate bescherming van dit privéleven tegen de toegenomen technologische inbreukmogelijkheden is dan ook groot. Opsporingsbevoegdheden, maar ook privacybescherming moeten gelijke tred houden met de technologische ontwikkelingen. Het EHRM heeft in dat verband onder meer betoogd dat dit een zorgvuldige afweging van belangen vergt en dat een lidstaat die een pioniersrol wenst te vervullen in de ontwikkeling van nieuwe technologieën een bijzondere verantwoordelijkheid draagt dat in dat opzicht de juiste balans wordt gevonden.[5]

Het bereik van de voorgestelde bevoegdheid strekt zich uit tot een zeer grote hoeveelheid gegevens. Het betreft volledige toegang tot alle historische gegevens die op randapparatuur zijn opgeslagen en de gegevens die worden opgeslagen op en uitgewisseld via alle communicatiekanalen waarmee de randapparatuur is verbonden. Het omvat ook observatie van

[3] Zie ontwerp-toelichting p. 6-10
[4] Zie ontwerp-toelichting p. 11-12
[5] EHRM 4 december 2008, nrs. 30562/04 en 30566/04 (S. and Marper/United Kingdom), ro. 112: "*The protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.* (...) any State claiming a pioneer role in the development of new technologies bore special responsibility for striking the right balance in this regard."

historische correspondentie (e-mail en documenten) en zelfs van concepten en gewiste stukken (die veelal nog te achterhalen zijn op harde schijven). Bovendien is de bevoegdheid niet beperkt tot de vastlegging van reeds aanwezige gegevens, maar kan deze ook betrekking hebben op toekomstige gegevens. Bij het binnendringen in een geautomatiseerd werk gaat het niet alleen om gegevens die in de randapparatuur zijn opgeslagen, maar ook om toegang tot gegevens die elders - zoals in de *Cloud* - zijn opgeslagen. Dat kan een medisch dossier zijn, online toegang tot bank- en belastinggegevens, een overzicht van gebruikte zoektermen in een zoekmachine en/of toegang tot iemands profiel en al zijn contacten op een sociale netwerksite. Daarnaast biedt de bevoegdheid de mogelijkheid om ingebouwde camera's en microfoons op afstand aan te zetten. Het gaat daarbij niet alleen om gegevens die de verdachte zelf betreffen, maar ook om gegevens van alle personen die worden genoemd in documenten of met wie hij/zij digitaal contact heeft gehad. De privacyinbreuk treft daarmee in veel gevallen een grote groep burgers tot wie de verdenking zich niet richt. De bevoegdheid ziet bovendien niet alleen op het binnendringen van laptops en computers, maar ook van smartphones, smart tv's en allerlei andere apparatuur die digitaal kan communiceren. De uitbreiding die de voorgestelde nieuwe bevoegdheid biedt is daarmee ongekend omvangrijk.

1.4 Toetsing van noodzaak, proportionaliteit en subsidiariteit

*Noodzaak*
Voor wat betreft de aan te tonen noodzaak voert het voorstel aan de hand van de technologische ontwikkelingen aan dat de bestaande opsporingsbevoegdheden tekort schieten en noodzaken tot verdergaande bevoegdheden. Hoewel wordt gesteld dat de opsporing dringend behoefte heeft aan deze nieuwe bevoegdheid en daarvoor enkele situaties worden aangevoerd waarin de bestaande middelen geen soelaas zouden bieden, is in de toelichting onvoldoende geconcretiseerd noch is aangetoond waaruit de dringende noodzaak voor de samenleving bestaat die tot het invoeren van deze inbreukmakende maatregel noopt. De overwegingen die ten grondslag liggen aan de voorgestelde bevoegdheid worden weliswaar in belangrijke mate gebaseerd op een aantal concrete situaties, doch die kunnen de invoering van de beoogde bevoegdheid op zichzelf onvoldoende rechtvaardigen. De dringende noodzaak als bedoeld in artikel 8 EVRM behoeft daarnaast ook een zelfstandige, boven de casuïstiek verheven beschouwing en onderbouwing. De noodzaak ("pressing social need") voor de invoering van deze nieuwe bevoegdheid dient in objectieve bewoordingen onomstotelijk te worden vastgesteld en is in de toelichting onvoldoende onderbouwd. Het CBP adviseert om de ontbrekende overwegingen alsnog op te nemen.

Bovenstaande laat onverlet dat het CBP ten aanzien van enkele van de genoemde voorbeelden het volgende overweegt.

1. In de toelichting wordt onvoldoende onderscheid gemaakt tussen het versleutelen van bestanden en gegevens door verdachten, het versleutelen van communicatiestromen in transit, en het feit dat mensen gegevens elders opslaan, in de *cloud*. Dit onderscheid is echter wezenlijk om te bepalen in hoeverre toepassing van de bevoegdheid noodzakelijk is, en of er geen andere middelen zijn om dezelfde doelen te bereiken die een geringere inbreuk maken op de persoonlijke

levenssfeer van betrokkenen. In Nederland zijn alle aanbieders van openbare elektronische communicatienetwerken en -diensten verplicht om bij een internettap de communicatie die zij zelf versleutelen, ontsleuteld aan te leveren. Indien voor het opsporingsonderzoek dringend toegang is vereist tot gegevens die in beheer zijn bij de in de toelichting genoemde buitenlandse aanbieders als Google, Skype of Facebook, geldt dat de toelichting niet stelt of onderbouwt dat deze bedrijven niet zouden meewerken aan rechtshulpverzoeken. Het feit dat zij in toenemende mate de communicatie in transit versleutelen, laat onverlet dat zij toegang hebben of kunnen verschaffen tot de onversleutelde inhoud van e-mails en bestanden op hun servers, dan wel gevraagd kunnen worden mee te werken aan een tap op de communicatie van een specifieke verdachte. Indien een verdachte zelf bestanden heeft versleuteld met behulp van de in de toelichting genoemde programma's PGP of TrueCrypt, zou de opsporing gebruik kunnen maken van de eveneens in dit wetsvoorstel voorziene bevoegdheid tot het geven van een decryptiebevel, of van andere bestaande bijzondere opsporingsbevoegdheden. De toelichting onderbouwt niet de noodzaak om de bevoegdheid tot het binnendringen van een geautomatiseerd werk toe te passen, in relatie tot de omvang en ernst van de privacyinbreuk die dit oplevert. Ten aanzien van het gebruik van TOR-netwerken om communicatie in transit te versleutelen, geldt dat de toelichting dient te onderbouwen waarom andere veel gebruikte methoden om ernstige criminaliteit te bestrijden, niet effectief zijn (het vereiste van subsidiariteit).

2. Bij het bestrijden van botnets zijn situaties denkbaar dat specifieke command-and-control-servers zich in het buitenland bevinden of dat de locatie ervan niet kan worden achterhaald. In die gevallen volstaan de bestaande middelen niet en kan het middel van ontoegankelijkmaking door middel van het op afstand binnendringen van een geautomatiseerd werk mogelijk een oplossing bieden. Ook in geval van specifieke situaties waarin bijvoorbeeld een DDoS-aanval gaande is op een bank of andere essentiële voorziening, is denkbaar dat deze combinatie van bevoegdheden doel treft en de aanval op deze wijze kan worden gestopt. Daarnaast lijken in gevallen waarin gebruik wordt gemaakt van de zogenaamde *bulletproof hosting providers* evenmin voldoende effectieve andere middelen voorhanden, zodat in die gevallen de inzet van deze bevoegdheid een optie is. Aan de in de toelichting gevolgde redenering dat effectieve middelen in geval van *bulletproof hosting providers* ontbreken, kan echter niet de conclusie worden verbonden dat de opsporing heimelijk toegang dient te krijgen tot *alle* in de *cloud* opgeslagen gegevens.

*Proportionaliteit*
Voor wat het betreft de proportionaliteit miskent het voorstel de omvang van de inbreuk die het gevolg zal zijn van invoering van deze bevoegdheid. Die inbreuk is gelegen in enerzijds de grote hoeveelheid en het karakter van de betreffende persoonsgegevens en anderzijds de uitgebreide kring van personen wier recht op eerbiediging van de persoonlijke levenssfeer hierdoor wordt aangetast. De vereiste afweging of de ernst van de inbreuk die het middel tot gevolg heeft in verhouding staat tot het daarmee te dienen doel, ontbreekt in de toelichting.

Volgens het voorstel kan de bevoegdheid tot onderzoek in een geautomatiseerd werk slechts worden toegepast met het oog op de hiervoor onder a. tot en met e. geformuleerde doeleinden. Weliswaar wordt het doel onder a. (het vaststellen van de aanwezigheid van gegevens of het

bepalen van de identiteit of locatie van het geautomatiseerde werk of de gebruiker) in de toelichting als niet vergaand gekarakteriseerd, maar wanneer eenmaal de toegang is verkregen door middel van deze bevoegdheid is het resultaat onverminderd vergaand en heeft de opsporing de ongelimiteerde toegang tot *alle* beschikbare digitale gegevens. Dat geldt ook voor de toepassing voor de andere genoemde doeleinden. Na verkregen toegang tot het geautomatiseerde werk door middel van plaatsing van spyware, valt die toegang niet te beperken tot slechts hetgeen werd beoogd met het bevel. Dit is niet alleen disproportioneel te achten, maar leidt ook tot een bovenmatige verwerking van politiegegevens (artikel 3, tweede lid, Wet politiegegevens).

1.5 Waarborgen

Gelet op de reikwijdte van de bevoegdheid en de ernst van de inbreuk op de persoonlijke levenssfeer van de betrokkene dienen tegenover de toepassing van deze bevoegdheid strikte waarborgen te staan. Het voorstel voorziet in een aantal waarborgen, waaronder bepalingen die de toepassing beperken tot verdenking van misdrijven van een bepaalde ernst, de bepaling dat de bevoegdheid slechts met het oog op bepaalde doeleinden mag worden ingezet, het vereiste van de vermelding van de gronden voor het bevel en het vereiste van een voorafgaande machtiging van de officier van justitie door de rechter-commissaris. Naast de in het voorstel genoemde voorwaarden acht het CBP ook de volgende waarborgen wezenlijk.

- *Controlemaatregelen en logging*

Een belangrijke waarborg dient te zijn gelegen in de controleerbaarheid van de toepassing gedurende het gehele proces van de aanvraag tot en met de uitvoering. Artikel 4, derde lid, Wet politiegegevens, dat ziet op de verplichting tot het treffen van passende technische en organisatorische maatregelen, vereist dat een sluitend controlesysteem wordt opgezet bij bevoegdheden als de onderhavige, waarmee door middel van duidelijk controleerbare procedures verantwoording wordt afgelegd over de gehele periode van onderzoek. Tevens is hierbij kennis van en inzicht in de ingezette software noodzakelijk. Kwaliteit en betrouwbaarheid, alsmede eventuele verborgen kwetsbaarheden dienen voorwerp te zijn van voortdurende toetsing.

Naast de "gewone" journaal- en verbaliseerverplichting ten aanzien van de toegepaste middelen, is de logging van belang. Ten aanzien van logging vermeldt de toelichting dat te allen tijde kan worden gecontroleerd welke technische handelingen in dit kader hebben plaatsgevonden door middel van logging, zodat op een later moment geen twijfel kan bestaan over de aard en consequenties van de handelingen die zijn verricht bij de uitvoering van de bevoegdheid.[6] Echter, logging kan vooralsnog niet altijd leiden tot het weergeven van alle relevante handelingen.[7] Daarbij geldt ook hier dat voor zinvolle logging de exacte werking van de gebruikte software bekend moet zijn, waaronder begrepen kennis van de broncode.

[6] Zie ontwerp-toelichting p. 24
[7] Bijvoorbeeld wanneer het binnendringen in het geautomatiseerde werk mislukt en het systeem crasht voordat logging heeft kunnen plaatsvinden.

- *Rechtsbescherming; systematiek strafvordering*

Deze nieuwe bevoegdheid is geplaatst in titel IV inzake enige bijzondere dwangmiddelen. Deze dwangmiddelen worden gekenmerkt door een zekere kenbaarheid van de toepassing voor de betrokkene. De voorgestelde bevoegdheid wordt daarentegen gekenmerkt door de heimelijke toepassing ervan en heeft daarmee onmiskenbaar het karakter van een bijzondere opsporingsbevoegdheid. De bijzondere opsporingsbevoegdheden zijn ondergebracht in afzonderlijke titels in het Wetboek van Strafvordering die voorzien in bijzondere waarborgen bij de toepassing hiervan, sedert de invoering van deze systematiek in 2000 door de Wet bijzondere opsporingsbevoegdheden. Uitgangspunt van deze wet vormde dat opsporingsmethoden die zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing, dan wel die een inbreuk maken op grondrechten van burgers, een voldoende specifieke basis behoeven in het Wetboek van Strafvordering[8]. De in het geding zijnde belangen en fundamentele rechten vereisen dit. De titel van de algemene bepalingen geldend voor alle bijzondere opsporingsbevoegdheden bevat specifieke waarborgen, die – tenminste ten dele – met de voorgestelde plaatsing in de titel van de dwangmiddelen aan de onderhavige bevoegdheid worden onthouden.

- *Kennisgeving aan betrokkene, toezicht en toetsing effectiviteit*

De kennisgeving aan de betrokkene door middel van een notificatie (achteraf) vormt, ook in het licht van de berichten over de gebrekkige mate waarin de notificatieplicht in zijn algemeenheid thans wordt nageleefd, een geringe waarborg voor de af te leggen verantwoording voor de toepassing van het middel. Gelet op de implicaties van de uitoefening van deze bevoegdheid verdient het dan ook aanbeveling dat het voorstel voorziet in een controle-instrument, waarmee direct en effectief toezicht wordt uitgeoefend op de wijze van uitvoering van de bevoegdheid, onder meer door middel van een verplichting regelmatig daarop betrekking hebbende statistieken en overzichten beschikbaar te stellen. Opname van een horizonbepaling is in dit verband eveneens onontbeerlijk te achten.

**Tot slot**

Het CBP wijst u nog op een omissie in het conceptwetsvoorstel ten aanzien van Artikel II onderdeel E, waarin na regel 2 de verdere bewoording van de zin lijkt te zijn weggevallen.

[8] Kamerstukken II 1996-1997, 25 403, nr. 3, p. 3