POLITIE

Onderwerp
Besluit op Wob-verzoek

VERZONDEN 0 5 NOV. 2019

AANTEKENEN
De Volkskrant B.V.
T.a.v. art. 5.1. 2e lid onder e Woo
Postbus 1002
1000 BA AMSTERDAM

Organisatieonderdeel
Korpsleiding
Korpsstaf
Team Juridische Zaken

Behandeld door
art. 5.1. 2e lid onder e Woo

Functie
Juridisch adviseur

Telefoon
088-art. 5.1. 2e lid onder e

E-mail
art. 5.1. 2e lid onder e Woo
art. 5.1. 2e lid @politie.nl

Ons kenmerk
2019-0033028
5992

Uw kenmerk
2018054721

~~**In afschrift aan**~~

Datum
Zie stempel

Bijlage(n)
2

Pagina
1

Geachte art. 5.1. 2e lid onder e Woo

I. Verzoek om informatie

Bij brief van 5 juni 2019 heeft u op grond van de Wet openbaarheid van bestuur (Wob) een verzoek ingediend tot openbaarmaking van:

1. Documenten betreffende het beleid ten aanzien screening van leveranciers van hacksoftware. Dit omvat het beleid waarin staat hoe wordt getoetst of een leverancier levert aan dubieuze regimes en, wanneer een overeenkomst tot stand is gekomen, hoe gecontroleerd wordt of een leverancier aan dubieuze regimes is gaan leveren.
2. Een overzicht van leveranciers van hacksoftware, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop een overeenkomst met het bedrijf is aangegaan, en (eventueel) gevolgd door een datum waarop de overeenkomst is beëindigd. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
3. Een overzicht van leveranciers waarvan expliciet niet hacksoftware afgenomen mag worden, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop de leverancier op de lijst terecht is gekomen, eventueel gevolgd door een datum waarop de leverancier van de lijst is afgehaald. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
4. Documenten en communicatie die betrekking hebben op [redacted], zoals overeenkomsten, nota's en e-mails over de screening van deze leverancier en de afwegingen van het aangaan, het afzien en het verbreken van een overeenkomst met deze leverancier.
5. Een overzicht van de onderzoeken naar leveranciers van hacksoftware. Hier wordt gevraagd om een lijst waarin duidelijk wordt naar wie het onderzoek is ingesteld, wanneer het onderzoek is gestart, wanneer het is afgerond, en wat de conclusie en adviezen voortkomend uit het onderzoek zijn. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan die documenten zelf een overzicht gemaakt kan worden.
6. Documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

II. Overwegingen

Onder inhoudelijke verwijzing naar de bij dit besluit behorende (nadere) overwegingen en motiveringen ben ik van oordeel, dat (a.) openbaarheid van bestuur en de parlementaire inlichtingenplicht een zelfstandige en noodzakelijke voorwaarde vormt voor het functioneren van onze democratie, (b.) er een erkend, maar niet onbegrensd (grond)recht op toegang tot overheidsinformatie bestaat, en (c.) in het onderhavige geval spanning bestaat tussen (1.) het door verzoeker veronderstelde belang van openbaarheid in het belang van een goede en democratische bestuursvoering en (2.) de publieke belangen, zoals het belang /veiligheid van de staat, de opsporing en vervolging van strafbare feiten, de bescherming van de persoonlijke levenssfeer en de bescherming van bedrijfsgeheimen.

A. Informatieverzoek onder punt 1.

Betreffende het informatieverzoek onder punt 1. zijn na onderzoek drie (concept) beleidsnota's en acht e-mails aangetroffen. Na toetsing aan de uitzonderingsgronden en beperkingen omschreven in artikel 10 en 11 van de Wob worden deze documenten deels openbaar gemaakt. De in documenten vervatte informatie waarvan de openbaarmaking geheel dan wel deels is geweigerd, zijn voorzien van een cijfercode[1] die correspondeert met de (algemene) motivering, omschreven in de bij dit besluit behorende bijlage.

B. Informatieverzoek onder punt 2. tot en met punt 6.

Betreffende het informatieverzoek onder punt 2. tot en met punt 6. neem ik het standpunt in om (in het geheel) geen mededeling(en) te doen over: (a.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers van hacksoftware, (b.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers waarvan expliciet geen hacksoftware afgenomen mag worden, (c.) al dan niet bij de politie berustend(e) (communicatie)document(en) van [naam bedrijf] art. 5.1 2e lid onder c. WOO [redacted] (d.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) onderzoek(en) naar een of meer leveranciers van hacksoftware en (e.) (communicatie)documenten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over een of meer de leverancier(s) van hacksoftware.

Voor dit standpunt wordt verwezen naar, c.q. een beroep gedaan op: (1.) de parlementaire geschiedenis van de reikwijdte van het verschoningsgrond bedoeld in artikel 68 Grondwet (Grw) inzake het geven van inlichtingen door de ministers en staatssecretarissen en (2.) de parlementaire geschiedenis van de Wet openbaarheid van bestuur, (mede) gelet op dan wel in samenhang bezien met artikel 10, eerste lid onder b. en/of onder c. van de Wob en/of artikel 11 van de Wob en/of artikel 10, tweede lid onder c. en/of onder d. en/of onder e. en/of onder g. van de Wob en artikel 3 van de Politiewet 2012.

Hieruit vloeit voort, dat in het onderhavige geval de Wob als algemene openbaarmakingsregeling dient te wijken voor de bijzondere openbaarmakingsregeling met een uitputtend karakter, bedoeld in artikel 68 Grw en daarom niet wordt (kan worden) toegekomen aan een beoordeling op grond van de Wob. De motivering is omschreven in de bij dit besluit behorende bijlage.

III. Besluit

I. De documenten onder punt 1. worden deels openbaar gemaakt.
II. Er wordt (worden) geen mededeling(en) gedaan over de (informatie)vraag onder punt 2. tot en met punt 6. of er al dan niet bij de politie in documenten vervatte gegevens berusten, betreffende (a.) de leverancier(s) van hacksoftware, (b.) de leverancier(s) waarvan geen hacksoftware wordt afgenomen, (c.) [naam bedrijf] art. 5.1 2e lid onder c. WOO [redacted] (d.) onderzoek(en) naar de leverancier(s) van hacksoftware en

(e.) communicatie van de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

III. De Wob wijkt als algemene openbaarmakingsregeling voor de bijzondere openbaarmakingsregeling met een uitputtend karakter, bedoeld in artikel 68 Grw.
IV. Gelet op bovenvermelde onder III. verzet artikel 68 Grw zich tegen een inhoudelijke behandeling van het (de) informatieverzoek(en) onder punt 2. tot en met punt 6.
V. Gelet op bovenvermelde onder III. en/of IV. wordt niet (kan niet worden) toegekomen aan een inhoudelijke beoordeling op grond van de Wob met betrekking tot het informatieverzoek onder punt 2. tot en met punt 6.
VI. Gelet op bovenvermelde onder II. tot en met V. wordt het informatieverzoek onder punt 2. tot en met punt 6. niet ingewilligd.

Hoogachtend,
de korpschef van politie,
namens deze,

art. 5.1. 2e lid onder e Woo

Rechtsbescherming

Indien u zich niet kunt verenigen met de inhoud van dit besluit, kunt u in overeenstemming met de Awb binnen een termijn van zes weken na bekendmaking van dit besluit schriftelijk bezwaar maken. Het bezwaarschrift dient te worden gericht aan de korpschef, ter attentie van de Wob-coördinatiedesk, postbus 17107, 2502 CC Den Haag onder vermelding van het kenmerk van de politie zoals deze is vermeld in het colofon van het besluit.

Het bezwaarschrift moet ondertekend zijn en ten minste bevatten: naam en adres, dagtekening, omschrijving van het besluit waartegen het bezwaarschrift is gericht en de gronden van bezwaar. Er dient een volmacht te worden verstrekt, indien het bezwaarschrift niet door de belanghebbende, maar namens deze wordt ingediend.

De elektronische weg voor het indienen van een bezwaarschrift is niet geopend.

[1] De documenten zijn voorzien van een cijfercode. Indien en voor zover van toepassing is de uitzonderingsgronden en beperkingen omschreven in artikel 11 van de Wob voorzien van de cijfercode 1 en de uitzonderingsgronden en beperkingen omschreven artikel 10, tweede lid onder e. en g. van de Wob voorzien van de cijfercode 2 en 3.

Bijlage bij besluit op Wob-verzoek

Kenmerk 2019-0033028 / 5992

Overweging/ motivering

Algemene inleiding

Voorstel voor een Verordening van het Europese Parlement en de Raad tot instelling van een EU- regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik. (2016/0295) COM (2016) 616 final van 28 september 2016.

1. In mei 2009 heeft de Raad van de Europese Unie de Verordening (EG) nr. 428/2009 (hierna Verordening) tot instelling van een communautaire regeling voor controle op de uitvoer, de overbrenging, de tussenhandel en de doorvoer van producten voor tweeërlei gebruik[1] vastgesteld.
2. In april 2014 heeft de Commissie een mededeling[2] aangenomen waarin concrete beleidsopties voor de herziening van de EU-uitvoercontroleregeling en de aanpassing ervan aan de snel veranderende technologische, economische en politieke omstandigheden zijn opgenomen.
3. Aangezien de Verordening herhaaldelijk is gewijzigd en nieuwe wijzigingen nodig zijn, is in het voorstel voor een Verordening van het Europese Parlement en de Raad tot instelling van een EU- regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik[3] (hierna Voorstel) tot herschikking van de Verordening (EG) nr. 428/2009 overgegaan.[4]
4. Ingevolge artikel 2, onder 1. van het Voorstel wordt onder "producten voor tweeërlei gebruik" verstaan:[5] producten, met inbegrip van programmatuur en technologie, die zowel een civiele als een militaire bestemming kunnen hebben, met inbegrip van technologie voor cybertoezicht die kan worden gebruikt bij het zich schuldig maken aan ernstige schendingen van de mensenrechten of het internationaal humanitair recht, of een gevaar kan vormen voor de internationale veiligheid of de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten.[6]
5. Ingevolge artikel 2, onder 21. van het Voorstel wordt verstaan onder "technologie voor cybertoezicht": producten die speciaal zijn ontworpen om het heimelijk binnendringen in informatie- en telecommunicatiesystemen mogelijk te maken met het oog op de monitoring, extractie, verzameling en analyse van gegevens en/of het onklaar maken of beschadigen van het geviseerde systeem.
6. Dit omvat producten die verband houden met de volgende technologieën en uitrusting: a) uitrusting voor het onderscheppen van mobiele telecommunicatie; b) inbraakprogrammatuur; c) monitoringscentra; d) wettelijke interceptiesystemen en systemen voor de bewaring van gegevens; e) digitaal forensisch onderzoek.[7] [8]
7. Ingevolge artikel 3, onder 1. van het Voorstel is voor de uitvoer van de producten voor tweeërlei gebruik die voorkomen op de lijst in bijlage I[9] een vergunning vereist.
8. In de definities van in deze bijlage gebruikte temen wordt onder: "Inbraakprogrammatuur"[10] (intrusion software) (4) verstaan: "programmatuur" die speciaal is ontworpen of aangepast om opsporing door 'bewakingshulpmiddelen'[11] te voorkomen of om 'beschermende tegenmaatregelen'[12] van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: (a.) het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of (b.) het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.[13]

"Informatiebeveiliging"[14] (4 5) verstaan: alle middelen en functies ter verzekering van de toegankelijkheid, geheimhouding of integriteit van gegevens of communicaties, zonder inbegrip van de middelen en functies die zijn bedoeld als beveiliging tegen storingen. Het begrip omvat o.a. "cryptografie", "cryptografische activatie",'cryptanalyse', bescherming tegen confidentiële uitstralingen en computerbeveiliging.
"Programmatuur"[15] (4D001) verstaan: a. "programmatuur", speciaal ontworpen of aangepast voor de "ontwikkeling" of "productie" van apparatuur, materialen of "programmatuur", vermeld in 4A001 tot en met 4A004 of 4D; b. andere dan de onder 4D001.a. genoemde "programmatuur", speciaal ontworpen of aangepast voor de "ontwikkeling" of de "productie" van de onderstaande apparatuur: (1.) "digitale computers" met een aangepast piekvermogen ("APP": Adjusted Peak Performance") van meer dan 1,0 gewogen TeraFLOPS (WT); (2.) "samenstellingen", speciaal ontworpen of aangepast voor verhoging van de prestaties door samenvoeging van processoren zodat de "APP" van de samengevoegde processoren de limiet van 4D001.b.1. overschrijdt. (4D004) "Programmatuur", speciaal ontworpen of aangepast voor het maken, exploiteren of leveren van, of communiceren met, "inbraakprogrammatuur".

Uit het bovenvermelde kan worden afgeleid dat op dit moment de definitie 'intrusion software' ('binnendringsoftware') in het Voorstel voor een Verordening van het Europese Parlement en de Raad tot instelling van een EU- regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik nog niet vast staat.[16]

Wassenaar Arrangement[17] on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public documents, Volume II, List of Dual-Use Goods and Technologies and Munitions List, van december 2018.[18]

9. In the List of Dual-Use Goods and Technologies and Munitions List include the definition:
"Computers" (4.A.5) : Systems, equipment, and components therefor, specially designed or modified for the generation, command and control, or delivery of "intrusion software".
"Software" (4.D.4): specially designed or modified for the generation, command and control, or delivery of "intrusion software". The Note onder 4.D.4 circumscribes that 4.D.4 does not apply to "software" specially designed and limited to provide "software" updates or upgrades meeting all the following: a. The update or upgrade operates only with the authorisation of the owner or administrator of the system receiving it; and b. After the update or upgrade, the "software" updated or upgraded is not any of the following 1. "Software" specified by 4.D.4.; or 2. "Intrusion software". "Technology" (4.E.1) .: a. "Technology" according to the General Technology Note, for the "development", "production" or "use" of equipment or "software" specified by 4.A. or 4.D. b. "Technology" according to the General Technology Note, other than that specified by 4.E.1.a., for the "development" or "production" of equipment as follows: 1. "Digital computers" having an 'Adjusted Peak Performance' ('APP') exceeding 15 Weighted TeraFLOPS (WT);2. "Electronic assemblies" specially designed or modified for enhancing performance by aggregation of processors so that the 'APP' of the aggregation exceeds the limit in 4.E.1.b.1. en c. "Technology" for the "development" of "intrusion software".

Kamervragen over: (1.) het gebruik van (spy)software , (2.) het gebruik van (spionage)software door de Nederlandse overheidsdiensten, (3.) het gebruik van omstreden (spionage)software door de politie en (4.) het gebruik van software van het Hacking Team door de Nationale Politie.

10. In de Kamer zijn vragen gesteld over: (1.) het gebruik van (spy)software[19], (2.) het gebruik van (spionage)software door de Nederlandse overheidsdiensten,[20] (3.) het gebruik van omstreden (spionage)software door de politie[21] en (4.) het gebruik van software van het Hacking Team door de Nationale Politie.[22]
11. De Minister / Staatssecretaris van Veiligheid en Justitie –voor zover hier relevant- als volgt antwoordde op de bovenvermelde Kamervragen:
12. Onder (1.) *(...)Het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken vormt een onaanvaardbaar risico voor de inzetbaarheid van die middelen. Mede om die reden hebben de verwervingstrajecten van deze middelen onder geheimhoudingsverklaring plaatsgevonden. Ik kan hierover dan ook geen mededelingen doen.*
13. Onder (2.) *Voor het antwoord op de vraag 2 verwijs ik hiervoor naar mijn antwoord op de vragen 2, 3 en 4 van de leden Schouw en Berndsen over het gebruik van spysoftware (vraagnummer 2011Z20260. Voor het antwoord op de vraag 3 welke organisaties gebruik kunnen maken van dit middel verwijs ik naar mijn antwoord op de vragen 2, 3 en 4 van de leden Schouw en Berndsen over het gebruik van spysoftware.*
14. Onder (3.) *(...). Het verstrekken van informatie over welke specifieke software de opsporingsdiensten van de politie beschikken, testen en gebruiken brengt grote risico's met zich mee voor de inzetbaarheid van die*

middelen. De verwerving van dergelijke middelen vindt bij de politie onder geheimhouding plaats. Ik kan hier derhalve geen nadere informatie over verstrekken.

15. Onder (4) *Zoals eerder is aangegeven in de beantwoording op de vragen van het lid Oosenbrug (PvdA) over het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten (kenmerk 2015Z09552), brengt het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico's met zich mee voor de inzetbaarheid van die middelen. Dit geldt dus ook voor het verstrekken van informatie omtrent de broncode, de robuustheid en de daarmee samenhangende veiligheidsvraagstukken. Ik kan hier derhalve geen informatie over verstrekken.*

Motivering cijfercode(s) uitzonderingsgronden en beperkingen, omschreven in artikel 10 en 11 Wob

16. Ingevolge vaste rechtspraak moet in beginsel per document of onderdeel daarvan worden gemotiveerd op welke grond openbaarmaking daarvan achterwege wordt gelaten en kan daarvan worden afgezien indien dit leidt tot herhalingen die geen redelijk doel dienen. Gelet op de onderlinge verwevenheid en samenhangend karakter van de in bovenvermelde documenten vervatte gegevens zijn hierop –voor zover van toepassing- één of meerdere uitzonderingsgronden en beperkingen omschreven in artikel 10 en artikel 11 van de Wob van toepassing. Indien –en voor zover de omstandigheid zich voordoet dat- meer dan één weigeringsgrond van toepassing is op een (onderdeel van het) document en uit verschillende (samenhangende) onderdelen bestaat, is uit de verwijzing naar een of meer cijfercode(s) voldoende kenbaar welke uitzonderingsgrond(en) en beperkingen op welk onderdeel ziet.[23] Onder voornoemde omstandigheid kan uit het (de) niet openbaar gemaakte document(en), alinea(s), passage(s), zin(nen) en zinsde(e)l(en), in samenhang bezien met (a.) de aard van de ingeroepen uitzonderingsgrond(en) en beperkingen en (b.) de (algemene) toelichting daarop worden afgeleid welke uitzonderingsgrond(en) en beperkingen op welk(e) onderde(e)l(en) is (zijn) toegepast. Door de(ze) gevolge werkwijze is voldoende inzichtelijk c.q. kenbaar gemaakt welke uitzonderingsgrond(en) en belangenafweging(en) aan de niet openbaarmaking van in het desbetreffende document vervatte informatie ten grondslag is gelegd. In de motivering van de weigeringsgrond(en) is in algemene bewoordingen toegelicht waarom die grond zich in het (de) desbetreffende (onderdeel van het) document(en) voordoet en, voor zover een (samenhangend) beroep is gedaan op een (of meer) uitzonderingsgrond(en), waarom het belang van openbaarmaking daarvan niet opweegt tegen de daar genoemde belangen.

Artikel 11 Wob. (cijfercode 1)

17. Gelet op het interne karakter van de gevraagde informatie en het oogmerk waarmee het (de) bovenvermeld(e) document(en) is (zijn) opgesteld,[24] is hierop –indien en voor zover van toepassing- (me)de weigeringsgrond omschreven in artikel 11 van de Wob van toepassing.[25] De concept beleidsnota(s) betreft een voorstel van een ambtenaar over het (toekomstige) beleid ten aanzien van de screening van leveranciers van hacksoftware beleid. Het betreft interne documenten die persoonlijke beleidsopvattingen bevatten, die in beginsel niet openbaar worden gemaakt teneinde ambtenaren in staat te stellen vrijelijk van gedachten te wisselen over het toekomstige beleid. In de betreffende documenten is sprake van opvattingen, voorstellen, aanbevelingen of conclusies van één of meer personen, die betrekking hebben op het beleid ten aanzien van de screening van leveranciers van hacksoftware en de daartoe door hen aangevoerde argumenten. Openbaarmaking daarvan wordt geweigerd, omdat ambtenaren de vrijheid dienen te hebben ongehinderd hun bijdrage te leveren aan de beleidsvoorbereiding of -uitvoering, en daarover te studeren, te brainstormen, anderszins te overleggen of (concept)nota's te schrijven. Indien en voor zover dit al mogelijk is of zou zijn, biedt het op punten (individueel) weglakken (maskeren) van specifieke (onder)delen en/of passage(s) in het (de) document(en) -gelet op de aard en/of inhoud en/of samenhang en/of verwevenheid van (feitelijke) feiten en/of opvattingen over die feiten- onvoldoende mogelijkheden. Ook dan wordt inzage gegeven in, dan wel kan daaruit een (de) persoonlijke mening(en) c.q. beleidsopvatting(en) in een individueel (individuele) of in een algemeen (algemene) geval(len) worden afgeleid. Het openbaar maken de aanbevelingen, argumenten en/of conclusies van de individueel herleidbare ambtenaren in het (de) documenten doet afbreuk aan bovenvermeld uitgangspunt dat (politie)ambtenaren binnen de (politie)organisatie hun in (elektronische) documenten omschreven gedachten, en/of aanbevelingen en/of argumenten en/of conclusies en/of opvatting(en) vrijelijk (moeten) kunnen wisselen zonder dat de verantwoordelijke bestuurder daarop naderhand kan worden aangesproken. Niet aannemelijk is dat gehele openbaarmaking van de gevraagde informatie uit oogpunt van een goede en democratische bestuursvoering van betekenis is dan wel daarmee is gediend. Daarnaast dient in aanmerking te worden genomen dat –voor zover van toepassing- door openbaarmaking van de gevraagde informatie de relatie(s) tussen het (de) betrokken bestuursorg(a)an(en) en de (politie)ambtenaren onderling onder druk kan zetten, zodat een goede en democratische bestuursvoering niet daarmee is gediend. Gelet op voormelde overwegingen is de openbaarmaking van die onderdelen op grond van artikel 11, eerste lid, van de Wob geweigerd. In het onderhavige geval kan er in redelijkheid vanaf kan worden gezien om gebruik te maken van

de bevoegdheid om op grond van artikel 11, tweede lid, eerste volzin, van de Wob de gevraagde informatie in niet tot personen herleidbare vorm te verstrekken omdat eveneens niet is gebleken dat een goede en democratische bestuursvoering met openbaarmaking is gediend.

Artikel 10, tweede lid onder e. Wob. (cijfercode 2)

18. Gelet op het karakter van de gevraagde gegevens is hierop (me)de weigeringsgrond omschreven in artikel 10, tweede lid, aanhef en onder e van de Wob van toepassing. Bij afweging van het belang van het voorkomen van eerbiediging van de persoonlijke levenssfeer van bij de aangelegenheid betrokken natuurlijke personen, rechtspersonen dan wel derden tegenover het belang van de openbaarmaking, weigert het bestuursorgaan deze in documenten vervatte gegevens openbaar te maken, omdat openbaarmaking van de gevraagde informatie (in)direct leidt tot de identificatie van personen op basis van persoonsgegevens zoals naam (namen), adres(sen), woonplaats(en) en telefoonnummer(s). Het openbaar maken van deze persoonsgegevens -als bedoeld in artikel 4, eerste lid van de Algemene Verordening Gegevensbescherming[26] maakt (kan een) inbreuk (maken) op de persoonlijke levenssfeer van betrokkene(n). Hierbij is van belang dat gelet op de inhoud en/of context en/of samenhang van de onderhavige (persoons)gegevens de eerbiediging van de persoonlijke levenssfeer niet (in) voldoende (mate) beschermd kan worden door anonimisering en/of beperking van openbaarmaking tot (een) bepaalde passage(s) en/of tot een gedeelte van dit (deze) onderde(e)l(en). Op grond hiervan worden in het onderhavige geval eveneens de (in)direct tot de individuele perso(o)n(en) herleidbare gegevens niet openbaar gemaakt.
    Indien in het (de) document(en) de (in)direct tot een (perso(o)n(en) herleidbare gegevens openbaar wordt (worden) gemaakt is de koppeling tussen de identificerende gegevens van de betrokkene(n) en de bestuurlijke aangelegenheid niet onaannemelijk. De eerbiediging van de persoonlijke levenssfeer geldt niet alleen voor (politie)ambtenaren, maar des te meer voor een individuele burger. In aanmerking dient te worden genomen dat de bescherming van de persoonlijke levenssfeer van een burger eveneens door het bestuursorgaan in acht dient te worden genomen indien de (achter)naam van de betrokkene(n) op grond van in de openbaarheid gebrachte informatie op eenvoudige wijze herleidbaar is (zijn). Hierin is geen grond gelegen dat het bestuursorgaan in het onderhavige geval de (achter)naam van de betrokkene(n) ingevolge de Wob voor een ieder openbaar dient te maken. Openbaarmaking van die informatie kan gezien de persoonlijke strekking ervan, eveneens tot persoonlijke schade voor de betrokkene(n) leiden. Omdat het –gelet op bovenvermelde- niet mogelijk is om de in het (de) document(en) vervatte gegevens -niet zijnde politiegegevens- openbaar te maken in een niet tot personen herleidbare vorm, wordt in het onderhavige geval het openbaar maken van deze gegevens achterwege gelaten ter bescherming van de persoonlijke levenssfeer. Ten overvloede wordt opgemerkt dat onder bovenvermelde omstandigheid (gedeeltelijke) openbaarmaking -ook bij anonimisering van de persoonsgegevens- de persoonlijke levenssfeer van de betrokkene(n) raakt omdat een (politie)ambtenaar en/of burger in de (onderlinge) correspondentie er -in beginsel- vanuit mag gaan dat deze informatie niet ingevolge de Wob openbaar wordt gemaakt dan wel in de openbaarheid wordt gebracht. Ten slotte is, zoals in het onderhavige geval, de bekendheid van de identiteit van de persoon of personen op wie de documenten betrekking hebben (mede) aanleiding om de openbaarmaking van de daarin vervatte (politie)gegevens te weigeren, omdat de documenten zien op een dermate eenvoudig identificeerbare persoon of groep personen, dat voor een ieder duidelijk is of kan zijn om wie het gaat. Daarnaast kan openbaarmaking van de (in)direct tot een (perso(o)n(en) herleidbare gegevens, gezien de aard, inhoud en/of persoonlijke strekking daarvan, eveneens tot persoonlijke en/of financiële schade voor de betrokkene(n) leiden. Daarom worden de in documenten vervatte persoonsgegevens op grond van artikel 10, tweede lid, aanhef en onder e. van de Wob niet openbaar gemaakt.

Artikel 10, tweede lid onder g. Wob (cijfercode 3)

19. Indien en voor zover op de gevraagde in documenten vervatte gegevens niet artikel 11 van de Wob en/of artikel 10, tweede lid onder e. van de Wob van toepassing is dan wel zou zijn, is hierop (me)de weigeringsgrond omschreven in artikel 10, tweede lid onder g. van de Wob van toepassing. In het onderhavige geval gaat het (onder meer) om (ambts)handelingen en/of informatie van de betrokkene(n) die -al dan niet in verband met dan wel uit hoofde van diens (hun) beroep die (voorbereidende) informatie hebben vastgelegd en/of verwerkt en/of verstrekt en/of andere (ambts)handelingen hebben uitgevoerd in het kader van de voorliggende bestuurlijke aangelegenheid. Hierop is (me)de uitzonderingsgrond van artikel 10, tweede lid, aanhef en onder g, van de Wob van toepassing. Het is onmiskenbaar van belang dat betrokkene(n) (ook in de toekomst) diens (hun) medewerking slechts wil (blijven) verlenen indien deze gevrijwaard wordt (worden) van het feit dat deze (politie)ambtenaren niet in ernstige mate er rekening mee moeten houden dat de in (beleids)documenten en/of onderlinge interne en/of externe berichtgevingen vervatte (beleids)informatie openbaar wordt gemaakt dan wel in de openbaarheid wordt gebracht. Eveneens dient in aanmerking genomen dat indien (politie)ambtenaren bij

hun interne (ambts)berichtgeving dan wel aan de externe (ambts)berichtgeving onder meer aan het Ministerie van Justitie en Veiligheid er rekening mee moeten houden dat –op verzoek van een ieder- deze informatie achteraf (op grond van de Wob) openbaar wordt gemaakt dan wel (deels) zal (moeten) worden gemaakt. In dat geval bestaat het (meer dan) reële risico dat (politie)ambtenaren zich in hun berichtgeving minder vrij zullen voelen en zich (in de toekomst) terughoudender zullen opstellen en volstaan met een zakelijke weergave (omschrijving) van de hoogst noodzakelijke (beleids- c.q. bestuurlijke) informatie. Tevens wordt in aanmerking genomen dat de betrokkene(n) en/of (politie)ambtenaren er niet op bedacht (be)hoeven te zijn dat (onder meer) hun interne en/of externe overgelegde / verstrekte schriftelijke informatie openbaar gemaakt zou kunnen worden. Daarnaast gaat het hier om het belang van het goed (onderling) functioneren van de betrokken overheidsorganen en hun ambtena(a)r(en). Daarom weegt in dit geval het belang van openbaarmaking van de in de documenten vervatte gegevens niet op tegen dat van het belang van onevenredige benadeling van de betrokkene(n) en/of (politie)ambtenaren en/of overheidsorganen. Daarom worden deze gegevens op grond van artikel 10, tweede lid, aanhef en onder g. van de Wob niet openbaar gemaakt.

Artikel 10 EVRM

20. Indien en voor zover impliciet uit het verzoek kan worden afgeleid, dat openbaarmaking van de gevraagde informatie (mede) berust op artikel 10 van het EVRM, de gevraagde informatie een vraagstuk van publiek belang is en (mede) betrekking heeft op het gebied van een bestuurlijke aangelegenheid, overweegt het bestuursorgaan als volgt. Onder verwijzing naar de uitspraak van het EHRM (GK) 8 november 2016, Magyar Helsinki Bizottságt. Hongarije (nr. 18030/11) kan worden afgeleid dat de onderhavige weigering om de gevraagde in documenten vervatte informatie niet te verstrekken, niet in strijd is met het bepaalde op grond van artikel 10 van het EVRM. Volgens vaste jurisprudentie van de ABRS vereist artikel 10 van het EVRM niet dat alle informatie wordt verstrekt of openbaar gemaakt en biedt dat artikel aan de staten die partij zijn bij het verdrag de mogelijkheid bij wet beperkingen te verbinden aan de verplichting om gegevens en documenten te verstrekken of openbaar te maken. Met de bepalingen omschreven in de bijzondere openbaarmakingsregeling, omschreven in artikel 7 van de Wpg in samenhang bezien met de artikelen 16 tot en met 25 van de Wpg en/of artikel 365 van het WvSv en/of de uitzonderingsgronden en beperkingen omschreven in artikel 10 en artikel 11 van de Wob is de beperking van het in artikel 10, eerste lid, van het EVRM vervatte recht om in documenten vervatte (politie)gegevens te ontvangen bij de wet voorzien.
    De voornoemde bij nationale wet voorziene inbreuk op het recht van artikel 10 EVRM is naar de beoordelingsruimte (margin of appreciation) van de Staat der Nederlanden noodzakelijk in de democratische samenleving, gelet op het beoogde doel, zoals onder meer het belang van bescherming van in de gevraagde documenten omschreven persoonsgegevens van anderen (derden). Door na afweging en toetsing van de betrokken belangen, de gevraagde informatie op grondslag van voornoemd(e) wetsartikel(en) te weigeren, wordt de uitoefening van het recht om informatie te ontvangen en te delen, zoals beschermd door artikel 10 EVRM, niet gehinderd dan wel ingeperkt op een wijze die raakt aan de essentie van rechten die voortvloeien uit dit artikel. In deze context wordt opgemerkt, dat indien en voor zover de (gemachtigde van de) VPRO van oordeel is, dat in zijn concrete situatie aan dit uitgangspunt niet kan worden vastgehouden, ligt het op diens weg om (zeer) bijzondere omstandigheden te stellen en aannemelijk te maken die zouden meebrengen dat de (gemachtigde van de) VPRO, door toepassing van een bijzondere openbaarmakingsregeling dan wel de weigeringsgronden van de Wob, in de uitoefening van het specifieke recht om op grond van artikel 10, eerste lid, van het EVRM inlichtingen te ontvangen, wordt belemmerd zonder dat dit op grond van artikel 10, tweede lid, van het EVRM is gerechtvaardigd. In het informatieverzoek is (zijn) door de (gemachtigde van de) VPRO geen (zeer) bijzondere omstandigheid (omstandigheden) gesteld dan wel aannemelijk gemaakt. Hieruit vloeit voort, dat uitsluitend in het (die) geval(len) waarin dient te worden aangenomen dat dergelijke bijzondere omstandigheden zich voordoen en een weigering om inlichtingen te verstrekken niet op grond van artikel 10, tweede lid, van het EVRM kan worden gerechtvaardigd, de onderhavige weigering in strijd zal zijn met artikel 10 van het EVRM.

Informatieverzoek

21. Uit de aard van het onderhavige informatieverzoek van 5 juni 2019 kan worden afgeleid dat deze is (zijn) gericht op openbaarmaking van de navolgende in documenten vervatte informatie, die volgens verzoeker kennelijk dan wel mogelijkerwijze bij de politie berust(en) en betrekking heeft (hebben) op specifieke soft- en/of hardware en/of een met naam genoemd mondiaal en/of (inter)nationaal bedrijf / onderneming, waarover de politie volgens verzoeker kennelijk de beschikking heeft en die al dan niet onder het begrip technisch hulpmiddel bedoeld in artikel 1, aanhef onder a. van het Besluit technische hulpmiddelen strafvordering valt (vallen):[27]
    1. Documenten die betrekking hebben op het beleid ten aanzien screening van leveranciers van hacksoftware, zoals op welke wijze wordt getoetst of een leverancier levert aan dubieuze regimes en

wanneer een overeenkomst tot stand is gekomen, hoe gecontroleerd wordt of een leverancier aan dubieuze regimes is gaan leveren.

2. Een overzicht van leveranciers van hacksoftware, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop een overeenkomst met het bedrijf is aangegaan, en (eventueel) gevolgd door een datum waarop de overeenkomst is beëindigd. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
3. Een overzicht van leveranciers waarvan expliciet niet hacksoftware afgenomen mag worden, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop de leverancier op de lijst terecht is gekomen, eventueel gevolgd door een datum waarop de leverancier van de lijst is afgehaald. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
4. Documenten en communicatie die betrekking hebben op de [naam bedrijf] art. 5.1 2e lid onder c. WOO [redacted], zoals overeenkomsten, nota's en e-mails over de screening van deze leverancier en de afwegingen van het aangaan, het afzien en het verbreken van een overeenkomst met deze leverancier.
5. Een overzicht van de onderzoeken naar leveranciers van hacksoftware. Hier wordt gevraagd om een lijst waarin duidelijk wordt naar wie het onderzoek is ingesteld, wanneer het onderzoek is gestart, wanneer het is afgerond, en wat de conclusie en adviezen voortkomend uit het onderzoek zijn. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan die documenten zelf een overzicht gemaakt kan worden.
6. Documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

Overwegingen informatieverzoek / informatievraag onder 1.

22. Betreffende de bovenvermelde informatievraag onder 1 neemt de korpschef van politie het standpunt in, dat -na toepassing van de bovenvermelde wettelijke uitzonderingsgronden en beperkingen omschreven in artikel 10 en 11 Wob- de in deze documenten vervatte informatie, zich niet verzetten tegen deels openbaarmaking daarvan.

Overwegingen informatieverzoek / informatievraag onder 2. tot en met 6.

23. Betreffende de bovenvermelde informatievraag onder 2. tot en met 6. neemt de korpschef van politie hierin uitdrukkelijk het standpunt in, om in het openbaar (in het geheel) geen mededelingen te doen dan wel in het openbaar (in het geheel) geen informatie te verstrekken, dan wel (in het geheel) geen informatie openbaar te maken, ook niet ten aanzien van de vraag of dergelijke in documenten vervatte gegevens al dan niet bij de politie berusten.
24. Gelet op de door de regering gegeven antwoorden op de gestelde Kamervragen op het gebied van het gebruik van (spionage)software door de politie verzet het belang / veiligheid van de Staat zich er tegen dat meer en/of andere specifieke informatie openbaar wordt gemaakt dan –indien en voor zover van toepassing- al in openbare bronnen bekend is gemaakt.
25. Voor dit standpunt doet de korpschef van politie een beroep op:
    a. De parlementaire geschiedenis van de reikwijdte van het verschoningsrecht bedoeld in artikel 68 Grondwet inzake het geven van inlichtingen door de ministers en staatssecretarissen,[28]
    b. De parlementaire geschiedenis van de Wet openbaarheid van bestuur,[29] (mede) gelet op artikel 10, eerste lid onder b. en/of onder c. van de Wob en/of artikel 11 van de Wob en/of artikel 10, tweede lid onder c. en/of onder d. en/of onder e. en/of onder g. van de Wob en
    c. Artikel 3 van de Politiewet 2012.
26. Op grond hiervan is de korpschef van politie van oordeel dat het specifieke informatieverzoek (informatievraag): of er al dan niet bij de politie in documenten vervatte gegevens berusten, zoals bovenvermeld onder punt 16, onder 2. tot en met 6. terecht onbeantwoord wordt gelaten omdat -gelet op de inhoud van het informatieverzoek- alleen al door kenbaar te maken of er al dan niet in documenten vervatte gegevens bij het bestuursorgaan berusten, onder meer:
    a. Op grond van het specifieke informatieverzoek, de na(a)m(en) van de rechts- dan wel natuurlijke personen -gelet op de connexiteit met het informatieverzoek- (in)direct herleidbaar dan wel (in)direct identificeerbaar is (zijn),
    b. Voor een ieder openbaar wordt over welke (specifieke) software de politie mogelijkerwijze al dan niet beschikt dan wel mogelijkerwijze al dan niet over kan beschikken,

c. Dat voor een ieder openbaar is gemaakt dat de naam van de leverancier en/of de (handels)naam van (specifieke) hard- en software waarover de opsporingsdiensten van de politie (mogelijkerwijze) al dan niet beschikken en/of (mogelijkerwijze) testen en/of gebruiken niet bekend wordt c.q. hoeft te worden gemaakt.
d. Dit in het onderhavige geval de verschoningsgrond van artikel 68 Grondwet doorkruist en (geheel) illusoir maakt.[30]

27. Ten overvloede wordt opgemerkt dat voor een ieder openbaar is gemaakt:
    a. Dat de politie beschikt over een of meerdere tapkamers,[31]
    b. De inzet van een tap[32] zijnde een technisch hulpmiddel bedoeld in artikel 126m van het Wetboek van Strafvordering beperkt is tot het opnemen van vertrouwelijke communicatie[33] en
    c. De naam van de leverancier van (de hard- en software van een c.q.) het tapsysteem niet bekend wordt gemaakt.[34]
28. Onder verwijzing naar de hierboven en hieronder vermelde overwegingen en motiveringen de korpschef van politie mitsdien het standpunt inneemt dat niet openbaarmaking van de bovenvermelde in documenten vervatte informatie onder punt 2. tot en met punt 6., die al dan niet bij de politie berusten, geboden is om gewichtige redenen.

Artikel 68 Grondwet in samenhang bezien met artikel 3, 10 en 11 van de Wob

29. In de Kamer zijn vragen gesteld over: (1.) het gebruik van (spy)software[35], (2.) het gebruik van (spionage)software door de Nederlandse overheidsdiensten,[36] (3.) het gebruik van omstreden (spionage)software door de politie[37] en (4.) het gebruik van software van het Hacking Team door de Nationale Politie.[38]
30. De Minister / Staatssecretaris van Veiligheid en Justitie –voor zover hier relevant- als volgt antwoordde op de bovenvermelde Kamervragen:
31. Onder (1.) *(...)Het verstrekken van informatie over welke specifieke software opsporingsdiensten beschikken vormt een onaanvaardbaar risico voor de inzetbaarheid van die middelen. Mede om die reden hebben de verwervingstrajecten van deze middelen onder geheimhoudingsverklaring plaatsgevonden. Ik kan hierover dan ook geen mededelingen doen.*
32. Onder (2.) *Voor het antwoord op de vraag 2 verwijs ik hiervoor naar mijn antwoord op de vragen 2, 3 en 4 van de leden Schouw en Berndsen over het gebruik van spysoftware (vraagnummer 2011Z20260. Voor het antwoord op de vraag 3 welke organisaties gebruik kunnen maken van dit middel verwijs ik naar mijn antwoord op de vragen 2, 3 en 4 van de leden Schouw en Berndsen over het gebruik van spysoftware.*
33. Onder (3.) *(...). Het verstrekken van informatie over welke specifieke software de opsporingsdiensten van de politie beschikken, testen en gebruiken brengt grote risico's met zich mee voor de inzetbaarheid van die middelen. De verwerving van dergelijke middelen vindt bij de politie onder geheimhouding plaats. Ik kan hier derhalve geen nadere informatie over verstrekken.*
34. De Staatssecretaris van Veiligheid en Justitie antwoordde –voor zover hier relevant- als volgt op de bovenvermelde Kamervragen:
35. Onder (4) *Herinnert u zich antwoorden op eerdere vragen over vergelijkbare software van 13 oktober 2011 en 7 oktober 2014? Ja. Zoals eerder is aangegeven in de beantwoording op de vragen van het lid Oosenbrug (PvdA) over het gebruik van een softwarefout door de Amerikaanse inlichtingendiensten (kenmerk 2015Z09552), brengt het verstrekken van informatie over welke specifieke software de opsporingsdiensten beschikken, testen en gebruiken grote risico's met zich mee voor de inzetbaarheid van die middelen. Dit geldt dus ook voor het verstrekken van informatie omtrent de broncode, de robuustheid en de daarmee samenhangende veiligheidsvraagstukken. Ik kan hier derhalve geen informatie over verstrekken. (...). De inzet van dit middel beperkt zich, gelet op de bepalingen van het Wetboek van Strafvordering, tot het opnemen van vertrouwelijke communicatie (op basis van artikel 126l van het Wetboek van Strafvordering). (...). De beschikbare technische hulpmiddelen voor het opnemen van vertrouwelijke communicatie worden voorafgaand aan de inzet gekeurd door de onafhankelijke keuringsdienst van de politie. Deze keuring is voornamelijk gericht op de authenticiteit en integriteit van het middel.*
36. Artikel 68 Grw[39] is een politiek instrument[40] op grondslag van een democratisch verankerd inlichtingenstelsel waarin, anders dan het documentenstelsel van de Wob[41] de verstrekte inlichtingen zijn gegeven in het kader van de politieke verantwoordingsplicht en die naar hun aard, niet zijn gericht op rechtsgevolg.[42]
37. Indien een bewindspersoon in eerste instantie een document niet verstrekt, zonder daarbij een uitdrukkelijke weigering uit te spreken, of zich te beroepen op het belang van de staat en de Kamer volhardt in haar verzoek, zal de bewindspersoon het document alsnog moeten verstrekken, of definitief moeten weigeren met een beroep op het belang van de staat.[43]

38. Het inlichtingenrecht van artikel 68 Grw is niet beperkt tot informatie die is vastgelegd in documenten[44] en kan –anders dan de Wob[45] die betrekking heeft op in documenten vervatte informatie- onder meer worden geëffectueerd door:
    a. Mondelinge informatieverstrekking in een besloten vergadering,
    b. Beantwoording van schriftelijke vragen,
    c. Technische briefings door ambtenaren of
    d. Vertrouwelijke inzage van documenten.[46]
39. Het niet gebruikelijk is om de Kamer te informeren door middel van het toezenden van documenten waarin delen onleesbaar zijn gemaakt, tenzij de Kamer om deze documenten verzocht heeft[47] en het aan de Kamer is om af te wegen of zij zich in een concreet geval voldoende geïnformeerd acht.[48]
40. De Wob niet van toepassing is als de Kamer of een Kamerlid een bewindspersoon om informatie vraagt. Indien een bewindspersoon uitlegt waarom hij bepaalde (nadere) mededelingen of informatie niet (in het openbaar) aan de Kamer kan geven, kunnen de belangen die in de Wob genoemd worden en die in de jurisprudentie verder zijn ontwikkeld, wel behulpzaam zijn.[49] De toepassing van artikel 68 Grw en de Wob hebben op grond van reflexwerking mitsdien over en weer invloed op elkaar.
41. Indien de Minister op grond van artikel 68 Grw aan de Kamer in het openbaar informatie verstrekt[50] dat gelet op de betrokken belangen, de bewindspersoon in het openbaar aan de Kamer geen (nadere) mededelingen doet c.q. kan doen c.q. geen informatie verstrekt c.q. kan verstrekken over: (1.) specifiek omschreven (inter)nationale dan wel mondiale onderneming(en) en/of (2.) over welke specifiek omschreven software de opsporingsdiensten van de politie al dan niet beschikken, testen en gebruiken, zou het opmerkelijk zijn dat de korpschef van politie op grond van de Wob, uit oogpunt van een goede democratische bestuursvoering, diezelfde gegevens wél (al dan niet deels) openbaar (moeten) worden gemaakt op grond van het (de) onderhavige specifieke informatieverzoek(en) van 5 juni 2019.
42. In het (de) onderhavige geval(len) kan, gelet op de beantwoording(en) van de Minister van Veiligheid en Justitie, er van worden uitgegaan c.q. uit worden afgeleid, dat de Kamer zich voldoende geïnformeerd acht(te)[51] en het gemotiveerde beroep tot weigering van de gevraagde inlichtingen te verstrekken gelet op de aard van de gegevens, in samenhang bezien met het belang van de Staat, heeft aanvaard.[52]
43. Indien de Kamer in dit (deze) geval(len) zich niet voldoende geïnformeerd acht(te) bestaat voor de bewindspersoon de mogelijkheid om de Kamer vertrouwelijk te informeren door de gegevens te verstrekken in een niet tot specifieke software (technische hulpmiddelen en/of configuraties) en/of tot onderneming(en) te herleiden gegevens. In dat geval komt de vraag of tot het individuele technische hulpmiddel en/of configuratie c.q. tot (een) onderneming(en) herleidbare gegevens wel kunnen worden verstrekt, niet aan de orde.[53]
44. In het onderhavige geval heeft de Minister van Justitie na afweging van de belangen, gelet op de aard van de gegevens en mede gelet op de wettelijke uitzonderingsgronden van de Wet openbaarheid van bestuur, geweigerd mededelingen te doen over dan wel informatie te verstrekken over welke specifieke software de opsporingsdiensten van de politie beschikken, testen en/of gebruiken.
45. Uit de parlementaire geschiedenis van de Wob blijkt, -voor zover hier relevant- dat:
    a. Overwogen is om in de Wob vast te leggen dat informatie die op grond van artikel 68 Grw is geweigerd op grond van strijdigheid met het belang van de Staat, niet (in een procedure) op grond van de Wob[54] kan worden verstrekt,[55]
    b. De Kamer van oordeel is dat het voorgestelde artikel[56] slecht past in de structuur van de wet en het snel verkeerd begrepen zou kunnen worden als een beperkende maatregel,
    c. De Minister de hoop uitspreekt dat dit later niet betreurt moet worden en erop wijst dat de rechter aan de gevallen waarin het parlement in een beleidsmatig-politieke afweging het beroep van de minister juist heeft bevonden, hieraan betekenis zal toekennen,
    d. In het verleden is voorgekomen dat op grond van de Wob, als gevolg van een rechterlijke uitspraak, informatie werd verkregen die aan de Kamer nadrukkelijk, dat wil zeggen terwijl er om was gevraagd, was onthouden,
    e. Dat dit volgens de regering kan voorkomen inherent is aan het gegeven dat over artikel 68 van de Grondwet respectievelijk de Wob uiteindelijk door andere instanties wordt geoordeeld,
    f. Voor dit tamelijk theoretisch probleem geen sluitende oplossing denkbaar is, dat in een beperkt aantal zaken is voorgekomen[57] en (destijds in 1988-1989) volgens de regering beschouwd moet worden als een ongelukkige uitzondering.

46. In bovenvermelde context wordt opgemerkt, dat:
    a. De Wob geen algemeen recht op toegang tot overheidsinformatie kent,[58]
    b. In het advies van de afdeling advisering van de Raad van State naar aanleiding van het voorstel van de Wet open overheid, is vermeld dat:
        - De toegang tot overheidsinformatie niet onbegrensd is,
        - Een spanning kan ontstaan tussen het belang van openbaarheid en andere legitieme belangen zoals bijvoorbeeld de veiligheid van de staat, de opsporing van strafbare feiten, de bescherming van de persoonlijke levenssfeer en de bescherming van bedrijfsgeheimen,
        - Hierbij enerzijds als uitgangspunt hanteert dat de overheid op een ruimhartige wijze uitvoering geeft aan de openbaarheidswetgeving waarbij voldoende oog dient te bestaan voor gerechtvaardigde belangen die aan openbaarheid van bestuur in de weg kunnen staan.[59]
47. De korpschef van politie van oordeel is, dat het opmerkelijk zou zijn, dat indien op grond van het (de) specifieke informatieverzoek(en) van 5 juni 2019 dezelfde gegevens met toepassing van de Wob wél (al dan niet deels) op grond van een rechterlijke uitspraak openbaar gemaakt dienen te worden, die de Minister van Veiligheid en Justitie (mede) gelet op de aard van de gegevens, de belangenafweging aan de van toepassing zijnde uitzonderingsgronden, bedoeld in artikel 10 van de Wob aan de Kamer heeft geweigerd hieromtrent mededelingen te doen dan wel informatie te verstrekken.
48. De korpschef van politie eveneens van oordeel is, dat het niet de bedoeling van de (grond)wetgever kan zijn dat indien de Minister van Justitie na bovenvermelde belangenafweging geweigerd heeft mededelingen te doen over dan wel informatie te verstrekken over welke specifieke software de opsporingsdiensten van de politie al dan niet beschikken, testen en/of gebruiken, deze weigering (alsnog) via een lagere wet kan worden omzeild dan wel kan worden ontkracht.
49. Dat dit in het onderhavige geval tot het ongerijmde resultaat leidt, dan wel zou leiden, dat het informatierecht van de Kamer en de verschoningsgrond van artikel 68 Grw niet zwaarder weegt dan wel zou wegen dan een individueel informatieverzoek op grond van de Wob en mitsdien artikel 68 Grw op onaanvaardbare wijze wordt doorkruist.
50. Dat in bovenvermelde context ten overvloede wordt opgemerkt, dat door de Minister van Binnenlandse Zaken en Koninkrijksrelaties, in het op 20 juli 2018 vastgestelde verslag van een algemene vergadering over de reikwijdte van artikel 68 van de Grondwet stelt, dat de Kamer altijd meer recht op informatie heeft dan iemand die een beroep doet op de Wob.[60]
51. Ingevolge artikel 3, eerste lid, van de Wob kan een ieder een verzoek om informatie neergelegd in documenten over een bestuurlijke aangelegenheid richten tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf.
52. Uit vaste rechtspraak[61] blijkt, dat ingevolge artikel 3, derde lid, van de Wob, de indiener van een Wob-verzoek geen belang bij zijn verzoek hoeft te stellen, onverlet laat dat de bevoegdheid tot het indienen van een informatieverzoek met een bepaald doel is toegekend, namelijk dat in beginsel een ieder kennis kan nemen van overheidsinformatie.
53. Het belang van verzoeker tot indiening van de gevraagde informatie op grondslag van de Wob redelijkerwijs slechts gelegen kan zijn 'in het ten dienste van een goede en democratische bestuursvoering' ter discussie stellen van het beroep door de Minister van Justitie op de verschoningsgrond bedoeld in artikel 68 Grondwet, waarin de Minister van Justitie, gelet op de aard van de gegevens en mede gelet op de belangen bedoeld in artikel 10 van de Wob, aan de Kamer geen mededelingen heeft gedaan dan wel geen informatie verstrekte.
54. De korpschef van politie daartoe overweegt dat het informatieverzoek kennelijk is ingediend met geen ander doel dan met toepassing van een omissie in de wetgeving[62] in samenhang bezien met het gegeven dat over artikel 68 van de Grondwet respectievelijk de Wob door een andere instantie wordt geoordeeld, verzoeker in beginsel oneigenlijk gebruik dan wel misbruik maakt van het (bestuurs)(proces)recht, door na de toetsing van het parlement of de weigering van de Minister om mededelingen te doen dan wel informatie te verstrekken gerechtvaardigd is, een specifiek informatieverzoek in te dienen, en in het bijzonder indien de Wob aan het inlichtingenrecht bedoeld in artikel 68 Grw derogeert.[63]
55. Naar het oordeel van de korpschef van politie het informatieverzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 4. en/of punt 5 en/of punt 6. mitsdien in beginsel niet strekt (strekken) ter bevordering van een goede en democratische bestuursvoering en verzoeker in het onderhavige geval een beroep doet op de toepassing van en toetsing aan de Wob om de korpschef van politie op grond van een besluit informatie te verstrekken / openbaar te maken in een geval waarin het parlement in een beleidsmatig-politieke afweging het beroep van de minister op de verschoningsgrond juist heeft bevonden.
56. Gelet op bovenvermelde heeft verzoeker naar het oordeel van de korpschef van politie in beginsel oneigenlijk gebruik dan wel misbruik gemaakt van de bevoegdheid om het informatieverzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 4. en/of punt 5 en/of punt 6. in te dienen.

57. Bij de beoordeling of (bepaal)de gevraagde informatie al dan niet openbaar moet worden gemaakt dient naast de algemene openbaarmakingsregeling van de Wob tevens beoordeeld te worden of de gevraagde informatie onder een bijzondere openbaarmakingsregeling valt.[64]
58. Zoals eerder vermeld, blijkt uit de parlementaire geschiedenis van de Wob dat overwogen is om in de Wob vast te leggen dat informatie die op grond van artikel 68 Grw is geweigerd op grond van strijdigheid met het belang van de Staat, niet (in een procedure) op grond van de Wob kan worden verstrekt.
59. Het toenmalige oordeel van de Kamer (in 1988-1989) dat het voorgestelde artikel slecht past in de structuur van de wet en begrepen zou kunnen worden als een beperkende maatregel, dat als een theoretisch probleem wordt omschreven waarvoor geen sluitende oplossing denkbaar is en (destijds) beschouwd moet worden als een ongelukkige uitzondering.
60. In het onderhavige geval waarin het parlement in een beleidsmatig-politieke afweging heeft geoordeeld dat aan de inlichtingenplicht is voldaan, hieraan kennelijk de betekenis heeft toegekend, dat de inlichtingenplicht aan de Wob derogeert.
61. Uit de strekking van het in artikel 68 Grw omschreven fundamentele rechtsbeginsel valt af te leiden dat de wetgever met voornoemd artikel heeft beoogd een publieke openbaarmakingsregeling in het leven te roepen die aan de Wob derogeert.
62. Hieruit kan, naar het oordeel van de korpschef van politie, worden afgeleid, dat in het geval waarin het parlement heeft geoordeeld dat de Minister aan de inlichtingenplicht tot niet-openbaarmaking van de gevraagde informatie op het gebied van specifieke (spy)software is voldaan, hieraan eveneens de betekenis kan worden toegekend, dat deze vorm van de inlichtingenplicht aan de Wob derogeert.
63. Indien in het onderhavige geval -waarin het beroep op de verschoningsgrond alle informatie bestrijkt die op grond van het (de) informatieverzoek(en) van 5 juni1 2019 onder punt 2. en/of punt 3. en/of punt 4. en/of punt 5 en/of punt 6. wordt gevraagd- de Wob niet derogeert aan de inlichtingenplicht, is het in de toekomst niet uitgesloten dat op grond van de Wob, als gevolg van een rechterlijke uitspraak, informatie wordt verkregen die aan de Kamer nadrukkelijk, dat wil zeggen terwijl er om was gevraagd, was onthouden en dit fenomeen gelet op de maatschappelijke en digitale ontwikkelingen, de informatiebehoefte en informatievoorziening in de huidige maatschappij niet (langer) meer als een ongelukkige uitzondering kan worden beschouwd.
64. De korpschef van politie neemt mitsdien het standpunt in, dat de Wob als algemene openbaarmakingsregeling wijkt de bijzondere openbaarmakingsregeling met een uitputtend karakter, neergelegd in artikel 68 Grw.
65. Benadrukt wordt, dat in het onderhavige geval de weigering van de Minister van Veiligheid en Justitie tot het doen van (nadere) mededelingen en verstrekking van (nadere) informatie en die (mede) alle in documenten vervatte informatie bestrijkt die op grond van het onderhavige informatieverzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 4. en/of punt 5 en/of punt 6. wordt gevraagd, door het parlement juist is bevonden.
66. De(ze) inlichtingenplicht van de bewindspersoon is, naar het oordeel van korpschef van politie, uitputtend van aard, indien zij zoals in het onderhavige geval, ertoe strekt te voorkomen dat door toepassing van de Wob afbreuk zou worden gedaan aan de goede werking van de inlichtingenplicht.
67. Immers, toepassing van de Wob in het onderhavige geval betekent, dat de informatie en gegevens die ingevolge artikel 68 Grw niet aan het parlement (i.c. de gekozen volksvertegenwoordigers) worden verstrekt (i.c. worden geweigerd) ingevolge de Wob aan een (willekeurige) burger die daaromtrent een informatieverzoek indient, op grond van een rechterlijke uitspraak (deels) openbaar dient te worden gemaakt, terwijl in het geval een Kamerlid eveneens deze weg toepast, deze benadering ingaat tegen de inhoud en strekking van art. 68 Grw, omdat dit niet past in de Nederlandse staatsrechtelijke verhoudingen.[65]
68. Hieruit vloeit voort, dat het beroep van een minister op de verschoningsgrond en de daarop volgende zwaarder wegende toetsing[66] van (door) het parlement in een staatsrechtelijke verhouding, door indiening van een informatieverzoek dat betrekking heeft op dezelfde (soort) informatie, op grond dan wel in het kader van een goede en democratische bestuursvoering, welke het algemene belang verondersteld, (geheel) illusoir wordt.
69. Gelet op bovenvermelde overwegingen is de korpschef van politie van oordeel dat in artikel 68 Grw een algemeen rechts(statelijk)beginsel met grondwettelijke waarde(n) is verankerd, en hierin fundamentele (gedrags)regels zijn opgenomen die wezenlijk zijn voor de inrichting, werking en (democratische) balans tussen het inlichtingrecht, de inlichtingenplicht en de verschoningsgrond.
70. Indien, zoals in het onderhavige geval, bij (kennelijke) strijdigheid van enerzijds het informatierecht in de Wob en anderzijds het (de) in artikel 68 Grw verankerde rechtsbeginsel(en), moet worden nagegaan of de Wob niet kan worden geïnterpreteerd in overeenstemming met de (democratisch gelegitimeerde) weigering van de Minister van Veiligheid en Justitie tot het doen van (nadere) mededelingen en verstrekking van (nadere) informatie en de aanvaarding daarvan door het (democratisch gekozen) parlement.

71. In bovenvermelde context wordt opgemerkt dat de Wob aan een fundamenteel rechtsbeginsel kan worden getoetst, aangezien rechtsbeginselen een leidraad voor de wetgever zijn bij het uitvaardigen van een wet, en in het onderhavige geval, strikte toepassing van de wettelijke bepalingen van de Wob in strijd kan komen met het (de) fundamentele rechtsbeginsel(en) bedoeld in artikel 68 Grw.
72. Uit de geschiedenis van de totstandkoming van artikel 68 Grw blijkt, dat de wetgever de hier bedoelde, specifiek op de toepassing van de Wob betrekking hebbende, problematiek heeft voorzien, maar destijds (1987-1989) niet heeft geeffectueerd.[67] In deze context wordt opgemerkt, dat bij de totstandkoming van de Wob overwogen is om in de wet de mogelijkheid geheel uit te sluiten dat er op basis van de Wob documenten zouden worden verstrekt die eerder aan de Kamer waren geweigerd, maar dit middel als erger dan de kwaal werd beschouwd.[68] Hieruit vloeit voort, dat de wetgever ruimte voor een rechterlijke afweging heeft opengelaten in die gevallen waarin de Kamer zijn mening heeft gegeven over (het niet in de Wob invoegen van), (c.q. het onderhavige beroep op) de verschoningsgrond ex artikel 68 van de Grondwet.[69]
73. Gelet op bovenvermelde overwegingen is de korpschef van politie van oordeel dat:
    a. Openbaarmaking aan een ieder van informatie de meest vergaande vorm van bekendmaking is,
    b. Door de Minister van Veiligheid en Justitie een belangenafweging is gemaakt tussen de hiervoor genoemde belangen die met de geheimhouding van de door het parlement gevraagde informatie zijn gediend en het belang met openbare verstrekking aan het parlement, en
    c. Daarom op grond van het ingediende informatieverzoek niet tot openbaarmaking van de gevraagde informatie onder punt 2. tot en met punt 6. kan worden overgaan.

Eindnoten

[1] PB L 134 van 29.5.2009, blz. 1.
[2] COM(2014) 244 final van 24 april 2014.
[3] COM(2016) 616 final van 28 september 2016
[4] Het voorstel bevat nieuwe bepalingen voor een doeltreffende controle die gericht is op
specifieke en relevante technologieën voor cybertoezicht en dient ter ondersteuning van de algemene beleidsdoelstellingen van de Unie, zoals vastgelegd in artikel 3 van het Verdrag betreffende de Europese Unie, het bijdragen tot vrede en veiligheid, alsmede vrije en eerlijke handel en bescherming van de mensenrechten en ondersteuning van de strategie voor de digitale interne markt omdat de invoering van controles op technologie voor cybertoezicht als doel heeft de risico's in verband met digitale handel aan te pakken.
[5] COM(2016) 616 final, p. 27. De herziene definitie van "producten voor tweeërlei gebruik" wordt samengebracht met de definitie van "technologie voor cybertoezicht" en herziene controlecriteria, waarmee uitdrukkelijk wordt voorzien in controles ter voorkoming van uitvoer wanneer er een duidelijk risico voor schendingen van mensenrechten en terrorisme bestaat.COM(2016) 616 final, p. 11.
[6] Ingevolge Amendement 1 van het Europees Parlement 2014-2019, Zittingsdocument van 19 december 2017, A8-0390/2017, p.75-76 wordt verstaan onder "producten voor tweeërlei gebruik": producten, met inbegrip van programmatuur en technologie, die zowel een civiele als een militaire bestemming kunnen hebben, met inbegrip van producten die kunnen worden gebruikt voor het ontwerp, de ontwikkeling, de productie of het gebruik van nucleaire, chemische en biologische wapens en hun overbrengingsmiddelen, met inbegrip van alle goederen die voor niet-explosieve doeleinden kunnen worden gebruikt en op enige manier bijdragen in de vervaardiging van nucleaire wapens of andere nucleaire explosiemiddelen.
In het Interinstitutional File 2016/0295(COD) van de Council of the European Union from 5 juni 2019 circumscribes for the purposes of this Regulation in Article 2 'dual-use items' means items, including software and technology, which can be used for both civil and military purposes, and shall include [...] items which can be used for the design, development, production or use of nuclear, chemical or biological weapons or their means of delivery, including all items which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices; [...]
[7] Ingevolge Amendement 6 bis van het Europees Parlement aangenomen op 17 januari 2018 op het voorstel voor een verordening van het Europees Parlement en de Raad tot instelling van een EU-regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik (herschikking) (COM(2016)0616 – C8-0393/2016 – 2016/0295(COD) moeten met het oog op de definiëring van technologie voor cybertoezicht de door deze verordening bestreken producten uitrusting voor het onderscheppen van telecommunicatie omvatten, alsmede inbraakprogrammatuur, monitoringscentra, wettelijke interceptiesystemen en aan dergelijke interceptiesystemen gekoppelde systemen voor de bewaring van gegevens, apparatuur voor de ontcijfering van versleuteling, het herstellen van harde schijven, het omzeilen van wachtwoorden en de analyse van biometrische gegevens, alsook surveillancesystemen voor IP-netwerken.
Ingevolge Amendement 1bis van het Europees Parlement 2014-2019, Zittingsdocument van 19 december 2017, A8-0390/2017, p.76-78 4 wordt verstaan onder:
"technologie voor cybertoezicht": producten (hardware, software, technologieën die geen producten voor tweeërlei gebruik zijn) die kunnen worden gebruikt bij het zich schuldig maken aan ernstige schendingen van de mensenrechten of het internationaal humanitair recht, met name het recht op privacy, vrijheid van meningsuiting en vrijheid van bijeenkomst, of die een gevaar kunnen vormen voor de internationale veiligheid of de wezenlijke veiligheidsbelangen van de Unie en haar lidstaten, en die speciaal zijn ontworpen om het heimelijk binnendringen in informatie- en telecommunicatiesystemen mogelijk te maken met het oog op de monitoring, extractie, verzameling en analyse van gegevens en/of het onklaar maken of beschadigen van het geviseerde systeem zonder de specifieke, geïnformeerde en ondubbelzinnige toelating van de eigenaar of de beheerder van de systemen. Dit omvat producten die verband houden met de volgende technologieën en uitrusting:
a) uitrusting voor het onderscheppen van mobiele telecommunicatie;
b) inbraakprogrammatuur;
c) monitoringscentra;
d) wettelijke interceptiesystemen en systemen voor de bewaring van gegevens.

Technologieën voor cybertoezicht omvatten geen producten die specifiek zijn ontworpen voor:
a) facturatie;
b) functies voor gegevensverzameling binnen netwerkelementen (bijv. Exchange of HLR);
c) kwaliteit van dienstverlening van het netwerk (QoS);
d) gebruikerstevredenheid (Quality of Experience – QoE);
e) firewalls voor netwerkbescherming;
f) de bouw, de werking, het onderhoud of de bescherming van: – openbare energie-, gas- of waterinfrastructuur;
– slim beheer van burgervervoer via spoor, weg, lucht en water;
– fabrieksengineering en e-gezondheid;
– industriële productie.

[8] The Interinstitutional File 2016/0295(COD) van de Council of the European Union from 5 juni 2019 circumscribes for the purposes of this Regulation that (21). is deleted ('cyber-surveillance technology')

[9] COM(2016) 616 final ANNEXES 1 to 6.

[10] COM(2016) 616 final ANNEXES 1 to 6, p.17.
"Inbraakprogrammatuur" omvat niet het volgende:
(1.) a. ‹hypervisors›, ‹debuggers› of hulpmiddelen voor de reverse engineering van programmatuur (SRE); b. "programmatuur" voor het beheer van digitale rechten (DRM); of c. "programmatuur" die is ontworpen voor installatie door de fabrikanten, beheerders of gebruikers met het oog op goederenbewaking of -herstel. (2.) Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters. COM(2016) 616 final ANNEXES 1 to 6, p.18.

[11] 'Bewakingshulpmiddelen': "programmatuur" of hardware apparaten die het systeemgedrag of de processen die op een apparaat worden uitgevoerd, bewaken. Dit omvat antivirus (AV) producten, producten voor eindpuntbeveiliging, producten voor persoonlijke veiligheid (PSP: Personal Security Products), inbraakdetectiesystemen (IDS: Intrusion Detection Systems), inbraakpreventiesystemen (IPS: Intrusion Prevention Systems) of firewalls. COM(2016) 616 final ANNEXES 1 to 6, p.18.

[12] 'Beschermende tegenmaatregelen': technieken die zijn ontworpen om te zorgen voor de veilige uitvoering van programmacode, zoals preventie van gegevensuitvoering, (DEP: Data Execution Prevention DEP), willekeurige adresruimte-indeling (ASLR: Address Space Layout Randomisation) of ‹sandboxing›. COM(2016) 616 final ANNEXES 1 to 6, p.18.

[13] Ingevolge Amendement 80 van het Europees Parlement aangenomen op 17 januari 2018 op het voorstel voor een verordening van het Europees Parlement en de Raad tot instelling van een EU-regeling voor controle op de uitvoer, de overbrenging, de tussenhandel, de technische bijstand en de doorvoer van producten voor tweeërlei gebruik (herschikking) (COM(2016)0616 – C8-0393/2016 – 2016/0295(COD) wordt verstaan onder:
"Inbraakprogrammatuur" (intrusion software) (4): "programmatuur" die speciaal is ontworpen of aangepast om opsporing door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: a. het zonder toestemming onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of b. het wijzigen van systeem- of gebruikersgegevens om de toegang tot gegevens die zijn opgeslagen op een computer of apparaat met netwerkcapaciteit mogelijk te maken voor andere partijen dan partijen die hiervoor de toestemming hebben van de eigenaar of beheerder van de computer of het apparaat met netwerkcapaciteit.
"Inbraakprogrammatuur" omvat niet het volgende:
(1.). a. hypervisors, debuggers of hulpmiddelen voor de reverse engineering van programmatuur (SRE); b. "programmatuur" voor het beheer van digitale rechten (DRM); of c. "programmatuur" die is ontworpen voor installatie door beheerders of gebruikers met het oog op goederenbewaking, goederenherstel of het testen van de veiligheid van informatie- en communicatietechnologie (ICT);
c bis. "programmatuur" die wordt verspreid met het uitdrukkelijke doel om toegang door onbevoegden tot computers of apparaten met netwerkcapaciteit te helpen opsporen, ongedaan maken of voorkomen. (2.) Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters.
Onder 'toestemming' wordt verstaan: de geïnformeerde toestemming van de gebruiker (d.w.z. bekrachtiging van het feit dat deze de aard en de gevolgen en toekomstige gevolgen van een actie begrijpt en instemt met de uitvoering van die actie). Onder 'testen van de veiligheid van informatie- en communicatietechnologie (ICT)' wordt verstaan: het opsporen en beoordelen van statische of dynamische risico's en kwetsbaarheid van of fouten en zwakke punten in programmatuur, netwerken, computers, apparaten met netwerkcapaciteit, en onderdelen daarvan of daaraan verbonden apparatuur, met als aantoonbaar doel het wegnemen van factoren die een veilige en zekere werking en inzet en een veilig en zeker gebruik ervan in de weg staan. Zie eveneens Europees Parlement 2014-2019, Zittingsdocument van 19 december 2017, A8-0390/2017, p.49-51.

[14] COM(2016) 616 final ANNEXES 1 to 6, p.17.

[15] COM(2016) 616 final ANNEXES 1 to 6, p.161.

[16] In artikel 1, aanhef en onder f. van het Besluit onderzoek in een geautomatiseerd werk onder technisch hulpmiddel wordt verstaan : softwareapplicatie die gegevens detecteert, registreert en transporteert en waarmee onderzoekshandelingen worden verricht ter uitvoering van een bevel.

[17] The Wassenaar Arrangement (WA) is a global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies, received final approval by 33 co-founding countries.

[18] Zie https://www.wassenaar.org/app/uploads/2018/12/WA-DOC-18-PUB-001-Public-Docs-Vol-II-2018-List-of-DU-Goods-and-Technologies-and-Munitions-List-Dec-18.pdf

[19] Kamerstukken II, 2011-2012, Aanhangsel 1374

[20] Kamerstukken II, 2011-2012, Aanhangsel 1382

[21] Kamerstukken II, 2013-2014 Aanhangsel 2884 / Kamerstukken II, 2014-2015 Aanhangsel 202

[22] Kamerstukken II, 2014-2015 Aanhangsel 3199

[23] De uitzonderingsgronden en beperkingen omschreven in artikel 11 van de Wob is voorzien van de cijfercode 1. De uitzonderingsgronden en beperkingen omschreven in artikel 10, tweede lid onder e. en g. is voorzien van de cijfercode 2 en 3.

[24] In aanmerking dient te worden genomen dat het (de) document(en) is (zijn) opgesteld voor uitsluitend het gebruik binnen de kring van politie en justitie met de bedoeling (het oogmerk) dat deze voor (toekomstige) operationele besluitvormingsproces(sen) en/of interne oordeelsvorming(en) wordt (kan worden) gebezigd.
Het vertrouwelijke karakter van het document wordt bevestigd (benadrukt) door het opschrift van het document en geeft hiermee aan, dat sprake is van een intern document met een aparte status. Uit de (vertrouwelijke)inhoud van (de passages in) het document blijkt dat deze bestemd is voor c.q. betrekking heeft op intern(e) beraad(slaging) en daarin persoonlijke beleidsopvattingen zijn vervat en betrekking heeft op en/of gebezigd wordt (kan worden) voor (toekomstige) gezamenlijke beraadslaging en/of oordeelsvorming over de verantwoordelijkheid en/of ondersteuning en/of input van operationele besluitvormingsprocessen binnen (ten behoeve van) de politie en justitie op het gebied van een (de) betrokken bestuurlijke aangelegenheid.

[25] Uit de wetsgeschiedenis (Kamerstukken II 1986/87, 19 859, nr. 3.) blijkt dat het doel van de in artikel 11, eerste lid, van de Wob neergelegde bescherming van persoonlijke beleidsopvattingen is de bescherming van de vrije meningsvorming, het belang om in vertrouwelijke sfeer te kunnen "brainstormen" zonder vrees voor gezichtsverlies en het kunnen waarborgen dat bij de primaire vormgeving van het beleid de betrokkenen in alle vrijheid hun gedachten en opvattingen kunnen uiten. Onder persoonlijke beleidsopvatting wordt verstaan een opvatting, voorstel, aanbeveling of conclusie van één of meer personen over een bestuurlijke aangelegenheid en de daartoe door hen aangevoerde argumenten. Niet noodzakelijk is dat opvattingen, om te kunnen worden aangemerkt als persoonlijke beleidsopvattingen als bedoeld in artikel 11, eerste lid, van de Wob, herleidbaar zijn tot een individueel persoon. In een document opgenomen opvattingen van personen die bij de opstelling van het document betrokken waren, verliezen, mede in aanmerking genomen de wetsgeschiedenis, hun karakter van persoonlijke beleidsopvattingen niet doordat zij niet herleidbaar zijn tot één bepaalde persoon. De beslissing om over persoonlijke beleidsopvattingen informatie te verstrekken is aan het bestuursorgaan. Indien het op basis van zijn discretionaire bevoegdheid, met het oog op een goede en democratische bestuursvoering, besluit om over persoonlijke beleidsopvattingen informatie te verstrekken, kan het dit slechts in tot personen herleidbare vorm doen indien de betrokkene daarmee heeft ingestemd. Dat neemt echter niet weg dat het bestuursorgaan, dat verantwoordelijk is voor de betrokken bestuursvoering, bevoegd is om, los van de bereidheid van betrokkenen om in te stemmen met openbaarmaking, de informatie niet te verschaffen.

[26] Ingevolge artikel 4, eerste lid van de AVG wordt verstaan onder persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;

[27] Zie bijvoorbeeld uitspraak Gerechtshof Amsterdam van 23 december 2009, (ECLI:NL: GHAMS:2009: BK7941 / ECLI: NL: GHAMS:2009: BK7623), uitspraak Hoge Raad van 12 juli 2011 (ECLI: NL: HR:2011: BP4651)Rechtbank Amsterdam van 16 maart 2017 (ECLI: NL: RBAMS:2017:1627)

[28] Kamerstukken II, 28 362 Reikwijdte van artikel 68 Grondwet, Kamerstukken II, 14225 / 19014 Verklaring dat er grond bestaat een voorstel in overweging te nemen tot verandering in de Grondwet van de bepalingen inzake het geven van inlichtingen door de ministers en staatssecretarissen en het recht van onderzoek

[29] Kamerstukken II 19859 Wet openbaarheid van bestuur. Zie in deze context ook Kamerstukken II 33 328 Voorstel van wet houdende regels over de toegankelijkheid van informatie van publiek belang (Wet open overheid)

[30] Vragen van het lid Gesthuizen (SP) aan de Minister van Veiligheid en Justitie over het gebruik van omstreden spionagesoftware door de politie (ingezonden 11 augustus 2014).Antwoord van Minister Opstelten (Veiligheid en Justitie) (ontvangen 7 oktober 2014) Zie Aanhangsel Handelingen 2013-2014 Aanhangsel 2884 / Aanhangsel Handelingen 2014-2015 Aanhangsel 202.

[31] Kamerstukken II 2013-2014 Aanhangsel 2884 / Kamerstukken II 2014-2015 Aanhangsel 202, Kamerstukken II 2014-2015 Aanhangsel 3199.

[32] In het Besluit technische hulpmiddelen strafvordering wordt in artikel 1 onder a onder technisch hulpmiddel verstaan: een configuratie van componenten die signalen detecteert, deze transporteert, hun registratie activeert en de signalen registreert.

[33] In het Besluit technische hulpmiddelen strafvordering wordt in artikel 1 onder c. opnemen van vertrouwelijke communicatie verstaan: het opnemen van vertrouwelijke communicatie met een technisch hulpmiddel, ter uitvoering van een bevel als bedoeld in artikel 126l, eerste lid, of artikel 126s, eerste lid, van het Wetboek van Strafvordering.

[34] Brief van de Minister van Veiligheid en Justitie aan de Voorzitter van de Tweede Kamer der Staten-Generaal Den Haag, 5 februari 2015, en 12 februari 2016, Evaluatie van hoofdstuk 13 van de Telecommunicatiewet, Kamerstukken II 2014–2015, 30 517, nr. 27 en Kamerstukken II, 2015–2016, 30 517, nr. 29.

[35] Kamerstukken II, 2011-2012, Aanhangsel 1374

[36] Kamerstukken II, 2011-2012, Aanhangsel 1382
[37] Kamerstukken II, 2013-2014 Aanhangsel 2884 / Kamerstukken II, 2014-2015 Aanhangsel 202
[38] Kamerstukken II, 2014-2015 Aanhangsel 3199
[39] Artikel 68 van de Grondwet bepaalt: *'De Ministers en de Staatssecretarissen geven de kamers elk afzonderlijk en in verenigde vergadering mondeling of schriftelijk de door een of meer leden verlangde inlichtingen waarvan het verstrekken niet in strijd is met het belang van de staat.'*
[40] De verschoningsgrond van het 'belang van de staat' is door opeenvolgende kabinetten beperkt uitgelegd en er in de praktijk slechts zelden een beroep op is gedaan, geheel in lijn met wat daarover in de notitie uit 2002 staat. In verband hiermee zijn bewindslieden gehouden om een voornemen tot een beroep op het belang van de staat eerst aan de orde te stellen in de ministerraad. Zie TK 2014-2015 28362, nr. 8, p. 3 en TK 2016-2017 28362, nr. 10, p. 9.
[41] De Wob is een juridisch instrument. Een belangrijk verschil tussen regime van de Grondwet en de Wob is dat de Wob aan rechterlijke controle is onderworpen en artikel 68 Grondwet niet. Zie bijvoorbeeld ABRvS 21 april 2004, ECLI:NL:RVS:2004: AO7921. Daardoor kan het voorkomen dat informatie die aan de Kamer is geweigerd (later) op grond van de Wob bijvoorbeeld als gevolg van een rechterlijke uitspraak, alsnog wordt openbaar gemaakt. De Minister van Binnenlandse Zaken verwijst in deze context naar de notitie van 21 januari 2002 waarin dit ongelukkige uitzonderingen worden genoemd, waarvan er destijds twee bekend waren. De notitie onderscheidt dit soort gevallen van de situatie waarin een bewindspersoon in eerste instantie een document niet verstrekt, zonder daarbij een uitdrukkelijke weigering uit te spreken, of zich te beroepen op het belang van de staat. De Kamer kan in dit niet-verstrekken (eventueel na overleg) berusten. Maar als de Kamer volhardt in haar verzoek, zal de bewindspersoon het document alsnog moeten verstrekken, of definitief moeten weigeren met een beroep op het belang van de staat. Zie Kamerstukken II, 2001-2002 28362, nr. 2, p. 5-6, Kamerstukken II, 2014-2015 28362, nr. 8, p. 3. en Kamerstukken II, 28 362, nr. 9, p. 2–3.
[42] Zie ECLI:NL:RVS:2004:AO7921, r.o. 2.7
[43] Kamerstukken II, 1985-1986, 19014, nr. 5, p. 2, Kamerstukken II, 2001-2002, 28 362, nr. 2, p. 5–6
[44] Kamerstukken II, 2016-2017 28362 nr. 10, p. 20.
[45] De informatieplicht in artikel 68 Grondwet reikt in alle gevallen ten minste even ver en soms verder dan de verplichtingen in het kader van de Wob (zie Handelingen II 50-5012-5013) en is in een aantal opzichten breder dan het recht op openbaarheid onder de Wob. (zie Kamerstukken II, 2015-2016 nr. 8, p. 3.)
[46] De verschillen in de regimes van de Wob en artikel 68 van de Grondwet leiden tot een andere wijze van informatie verstrekking en verschillen in de gedetailleerdheid van de informatie. Daardoor valt niet uit te sluiten dat er in het kader van de Wob documenten openbaar worden gemaakt waarin informatie is opgenomen waarover de Kamer nog niet beschikt. Zie Kamerstukken II, 2014-2015 28362, nr. 8, p. 5.
[47] Kamerstukken II, 2015-2016 28362 nr. 9, p. 4.
[48] Kamerstukken II, 2016-2017 28362 nr. 10, p. 22.
[49] Een weigering om inlichtingen te verstrekken kan uiteindelijk alleen gerechtvaardigd worden met een beroep op het belang van de staat. Deze verschoningsgrond biedt weinig zicht op de materiële redenen. Het begrippenkader van de Wob kan dan gebruikt worden om meer inzicht te geven in de redenen waarom bepaalde informatie niet (openbaar) aan de Kamer verstrekt wordt. Kamerstukken II, 2016-2017 28362 nr. 10, p. 11.
[50] Bij de beslissing of openbare verstrekking mogelijk is, dient een afweging te worden gemaakt tussen het belang dat de controle door de Kamers en het afleggen van verantwoording in het openbaar plaatsvindt en de aspecten die zich in het concrete geval verzetten tegen openbaarmaking. In de notitie van 21 januari 2002 zijn een aantal aspecten beschreven die een rol kunnen spelen bij deze afweging zoals de vertrouwelijkheid van verstrekte bedrijfsinformatie. Indien de beslissing leidt tot niet openbaarmaking van de informatie, heeft de bewindspersoon de plicht om deze beslissing te motiveren en daarover – indien gewenst – in overleg te treden met de Kamer. Kamerstukken II, 2015-2016 28362 nr. 9, p. 10.
[51] Uit de openbare bronnen blijkt (dan wel kan) niet worden afgeleid dat door de Kamer (alsnog) aan de bewindspersoon is gevraagd om bepaalde documenten te verstrekken. In het onderhavige geval zal de bewindspersoon er vanuit (kunnen) gaan dat de Kamer zich voldoende geïnformeerd acht(te) door de verstrekte inlichtingen.
[52] Voor een beroep op het staatsbelang is vereist dat het staatsbelang om de inlichtingen te weigeren zo zwaar weegt dat het eveneens zwaar wegende belang de Staten-Generaal te informeren daarvoor niettemin moet wijken. De regering wordt erdoor genoopt daarop uitdrukkelijk een beroep te doen en voor dat beroep argumenten aan te voeren. In welke gevallen sprake zal zijn van belangen die zo zwaarwegend zijn dat zij als belang van de staat aangemerkt kunnen worden is in abstracto niet aan te geven. Van geval tot geval zal de Regering moeten beoordelen of de argumenten die pleiten tegen het verstrekken van gevraagde inlichtingen zwaarwegend genoeg zijn om een beroep op het belang van de staat te rechtvaardigen. In deze afweging kunnen, afhankelijk van het concrete geval, meerdere elementen een rol spelen. Daarbij kan naast het mogelijk schaden van het belang van de betrokkene(n) die bij de verstrekking in het geding is, gedacht worden aan de relatie van de betrokkene(n) tot de overheid, de aard van de gegevens, de vraag of met verstrekking financiële en economische belangen van de staat in het geding zijn, een wettelijke geheimhoudingsplicht en dergelijke. Een weigering van de Regering om gevraagde inlichtingen te verstrekken omdat dat in strijd zou zijn met het belang van de staat, dient door de Kamer getoetst te worden aan de vraag of naar het oordeel van de Kamer terecht een beroep op deze verschoningsgrond is gedaan. Pas indien de Kamer na deze toetsing van oordeel is dat de Regering terecht een beroep op de verschoningsgrond heeft gedaan, zal het weigeren van de verlangde inlichtingen door de Kamer aanvaard kunnen worden. Hieruit blijkt dat de Regering en Staten-Generaal op dit punt een eigen verantwoordelijkheid hebben. TK 1979-1980, 14225, nr. 3, p. 5, nr. 7, p. 6 en nr. 12, p. 5., TK 1985-1986, 19014, nr.5, p.3-5 en p. 7. In de uitspraak van de Hoge Raad van 28-03-2003 (ECLI:NL:PHR:2003:AE5149) overweegt de Raad in rechtsoverweging 3.6.2 dat geen nauwkeurige afbakening kan worden gegeven van het begrip 'het belang van de staat' in de zin van art. 68 Grw en aan 'het belang van de staat' ontleende uitzondering niet te eng moet worden uitgelegd. Als voorbeeld van gevallen waarin een weigering inlichtingen te verschaffen op het belang van de staat kan worden gebaseerd, wordt –onder verwijzing naar de parlementaire geschiedenis- als gevallen waarin de aard van de gegevens zich tegen (openbare) verstrekking aan het parlement verzet onder meer genoemd: vertrouwelijk verstrekte bedrijfsinformatie, gegevens over lopende of afgesloten strafrechtelijke onderzoeken, gegevens die onder een wettelijke geheimhoudingsplicht en gevallen waarin afspraken omtrent de behandeling van de gegevens zijn gemaakt met degene van wie de gegevens oorspronkelijk afkomstig zijn.
[53] Zie Kamerstukken II, 2001-2002, 28 362, nr. 2, p.7-9.
[54] Zie Handelingen II 50-5035. In de MvA is omschreven dat een dergelijke expliciete bepaling in de Wob zou vastleggen dat op grond van de Wob geen informatie kan worden verstrekt over of uit gegevens die bij een expliciet beroep op de verschoningsgrond ex artikel 68 van de Grondwet niet zijn verleend. De regering meent op dit punt nog geen conclusie te moeten trekken omdat het in deze gaat om een onderwerp dat zozeer de positie van de kamers en hun leden aangaat dat een conclusie in gemeen overleg zou moeten worden getrokken.
De regering vervolgd dat daarbij de vraag onder ogen moeten worden gezien of en in hoeverre de conclusie als materieel recht in de wet moet worden neergelegd en zulks samenhangt met de ruimte die voor rechterlijke afweging zou worden opengelaten in die gevallen waarin de kamer zijn mening heeft gegeven over het naar haar oordeel al of niet terecht invoegen van de verschoningsgrond ex artikel 68 van de Grondwet. Kamerstukken II, 1987-1988, 19859, nr. 6, p. 12.
[55] Zie Kamerstukken II, 2001-2002, 28 362, nr. 2, p.7, noot 5, Handelingen II 1988-1989, p. 5012-5013. Kennelijk wordt met 'verstrekken' van informatie hier bedoeld (deels) openbaarmaking van informatie.
[56] Het artikel zou als volgt luiden: Een verzoek om informatie wordt niet ingewilligd, indien en voor zover het betrekking heeft op informatie vervat in documenten waaruit met een uitdrukkelijk beroep op het belang van de Staat, bedoeld in artikel 68 van de Grondwet, geen inlichtingen zijn verstrekt.
[57] Zie Kamerstukken II, 2001-2002, 28 362, nr. 2, p. 7, noot 4.
[58] Kamerstukken II, 2011-2012, 33328, nr. 3., p.19. Artikel 110 Grondwet bevat geen subjectief recht van de burger op toegang tot overheidsinformatie, maar slechts een plicht voor de overheid om bij de uitvoering van haar taak openbaarheid te betrachten volgens regels bij wet te stellen.
[59] Kamerstukken II, 2013-2014, 33 328, nr. 7, p. 9.
[60] Kamerstukken II, 2017-2018, 28362, nr.12, p. 12. Hierin is verder het navolgende omschreven: Het grote verschil tussen de inlichtingenplicht aan de Kamer en de Wob is dat artikel 68, en ook de actieve informatieplicht, een politiek instrument is. De Wob is een juridisch instrument waar mensen gebruik van mogen en kunnen maken. Datgene wat je op basis van de Wob kunt krijgen, is een soort bodem waar de Kamer in ieder geval over geïnformeerd moet worden. Het geheel niet verstrekken van informatie aan de Kamer is weer iets anders. Dat kan alleen aan de orde zijn als de veiligheid van de Staat in het geding is of als die vertrouwelijkheid via een andere wet wordt geregeld.
[61] Zie onder meer uitspraak van de Afdeling van18 februari 2015, ECLI:NL:RVS:2015:426
[62] Het artikel zou als volgt luiden: Een verzoek om informatie wordt niet ingewilligd, indien en voor zover het betrekking heeft op informatie vervat in documenten waaruit met een uitdrukkelijk beroep op het belang van de Staat, bedoeld in artikel 68 van de Grondwet, geen inlichtingen zijn verstrekt.
[63] Uitspraak ABRvS 4 maart 2015 r.o. 3.1.(ECLI:NL:RVS:2015:641)
[64] In artikel 8.8 van het Voorstel van wet houdende regels over de toegankelijkheid van informatie
van publiek belang (Nieuwe Wet openbaarheid van bestuur) kan van deze wet slechts worden afgeweken, voor zover hierin bij wet is voorzien en die wet is opgenomen in bijlage 2 bij deze wet. Hierin is artikel 3, derde lid, van de Wet politiegegevens als Lex specialis vermeld. Kamerstukken II, 2011-2012, 33328, nr. 2, p. 18.
[65] Kamerstukken II 2001/02, 28362, 4, p. 1, Brief vicepresident Raad van State bij de Notitie inzake de reikwijdte van art. 68 Grondwet) en Kamerbrief over toepassing art. 68 Grondwet van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties van 25 april 2016 kenmerk 20160000241963.
[66] De afweging of in een concreet geval de gevraagde inlichtingen met een beroep op de in artikel 68 Grw opgenomen verschoningsgrond geweigerd dient te worden, is een andere dan de afweging die in het kader van een informatieverzoek op grond van de Wob wordt gemaakt en zal in het algemeen gesproken zal de afweging van artikel 68 Grw een zwaardere moeten zijn. TK 1987-1988, 19859, nr. 6, p. 12.
[67] Zie voetnoot 40
[68] Kamerstukken II, 2015-2016, 28362, nr. 8, p.4 en nr. 2, p. 7, noot 5
[69] Zie uitspraak Afdeling bestuursrechtspraak Raad van State van 4 maart 2015, ECLI:NL:RVS:2015:641, r.o. 3.1

Van: [redacted] - BD/DRC/CV [redacted]@minvenj.nl>
Verzonden: woensdag 13 maart 2019 15:29
Aan: [redacted] - BD/DGPenV/PPBT/PBO; [redacted]
[redacted] BD/DGPenV/PPBT; [redacted]; [redacted]
CC: [redacted]); [redacted] BD/DRC/CV; [redacted] - BD/DRC/CV
Onderwerp: FW: Concept uitwerking dubieuze regimes ihkv CCIII
Bijlagen: Leveranciers binnendringsoftware.docx

Hallo [redacted],

We hebben eerder contact gehad over de uitwerking van het regeerakkoord op de passage dat producenten van binnendringsoftware, in het kader van de aanschaf voor de opsporing (Computercriminaliteit III), niet mogen leveren aan 'dubieuze regimes'.

Aan de hand van de actualisering van de verordening voor dual-use goederen, The Wassenaar Arrangement en de criteria die horen bij het Gemeenschappelijk Standpunt inzake wapenexport is bijgevoegde uitwerking tot stand gekomen.

Ik zou deze graag met jullie willen bespreken, schikt 3 april 10:00-11:00?

Alvast bedankt.

Met vriendelijke groet,

[redacted]
[redacted]

M 06 [redacted]
[redacted]@minvenj.nl

Ministerie van Justitie en Veiligheid

Dep. **VERTROUWELIJK**
Beleidsnota

Versie **13 maart 2019**

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
[redacted] 2

T 070 [redacted]
F 070 [redacted] 2

Datum

Ons kenmerk

nota

Leveranciers binnendringsoftware

Aanleiding

In het regeerakkoord 'Vertrouwen in de Toekomst' van het kabinet Rutte III staat de volgende passage over het wetsvoorstel Computercriminaliteit III:

"Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen." [1]

Deze beleidsnota zet uiteen welk beleid wordt gevoerd binnen de opsporing ten aanzien van aanschaf van binnendringsoftware van particuliere leveranciers.

Beleid

Het regeerakkoord vereist dat leveranciers van binnendringsoftware worden gescreend door de AIVD en dat deze leverancier niet aan dubieuze regimes verkopen. Commerciële binnendringsoftware is prominent onderwerp geweest in het debat over de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Commerciële binnendringsoftware maakt (mogelijk) gebruik van onbekende kwetsbaarheden in software. In plaats dat deze kwetsbaarheid wordt gemeld waardoor de software veiliger wordt, wordt deze kwetsbaarheid commercieel geëxploiteerd. Daarnaast kunnen leveranciers van deze software ook leveren aan regimes die de producten kunnen gebruiken voor het (ernstig) schenden van mensenrechten. Om de markt van binnendringsoftware niet meer dan strikt noodzakelijk te betreden is de aanschaf beperkt tot een specifieke zaak en worden aanvullende eisen gesteld aan leveranciers. Deze eisen betreffen 1) screening door de AIVD, 2) beoordeling of een bedrijf heeft geleverd aan dubieuze regimes.

Wat is binnendringsoftware?
Voor binnendring software wordt de definitie van de concept-verordening 2016/0295, annex I als uitgangspunt gebruikt.

[1] Regeerakkoord 2017-2021 'Vertrouwen in de toekomst'.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

De actualisering van de verordening is nog gaande daarmee staat de definitie nog niet vast.

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht:

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Zie bijlage 1 voor de (technische) noten die horen bij deze definitie.

Binnen de wet Computercriminaliteit III is onderscheid gemaakt tussen het technisch hulpmiddel dat bewijs vergaart en binnendringsoftware die de beveiliging van een geautomatiseerd werk doorbreekt. Het technisch hulpmiddel wordt geïnstalleerd nadat toegang is verkregen tot een geautomatiseerd werk. Binnendringsoftware omzeilt de beschermende tegenmaatregelen van een computer of apparaat met netwerkcapaciteit. Het beleid in deze nota zich op binnendringsoftware.

Screening AIVD

1/3 [redacted]

Levering van binnendringsoftware aan dubieuze regimes
Binnendringsoftware kan een essentieel middel zijn in de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk, maar kan ook worden misbruikt door repressieve regimes. Het is een zogenaamd product voor tweeërlei gebruik[2], oftewel een dual-use goed. In de kamerbrief over kwetsbaarheden in hard- en software van november 2016 staat dat de regering hecht aan beperking van uitvoer van ICT-goederen en –software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] In onderstaand beleid wordt uiteengezet hoe hier in het kader van de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk vorm aan wordt gegeven.

[2] COM(2016), 2016/0295
[3] Kamerstukken TK, 2016/17, 26 643, nr. 428

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

Binnen het recht of beleid bestaat geen eenduidige definitie van een dubieus regime. [redacted]

1/3 [redacted]

1/3 [redacted]

Bij The Wassenaar Arrangement wordt de reikwijdte van de export controle bepaald door de lijsten die zijn opgesteld onder het arrangement, de praktische implementatie varieert van land tot land.[6] Er zijn ook zogenaamde 'best practices' gepubliceerd. De bescherming van mensenrechten speelt in deze best practices een rol bij de uitvoer van conventionele wapens, handvuurwapens en lichte wapens, maar nog niet bij 'intrusion software'. Deze software wordt wel genoemd in de lijst met dual-use items. In de categorie computers (p. 79) wordt *software* die speciaal ontwikkeld of aangepast is voor de ontwikkeling, controle, of aflevering van 'intrusion software' op de dual-use lijst geplaatst, alsook de *technologie* voor de ontwikkeling van 'intrusion software' (p. 80).[7] [Nota bene, het arrangement reguleert niet de binnendringsoftware zelf, maar software of technologie die deze software ontwikkelt, controleert of aflevert.] De definitie van 'intrusion software' komt overeen met die uit de concept-verordening 2016/0295 (p. 221)[8] [9] . [redacted]

1/3 [redacted]

Leveranciers binnen de Europese Unie

In de Europese Unie bestaat sinds 2009 een verordening die een exportcontrole regime vereist op dual-use goederen[10]. Een dergelijk regime stelt voorwaarden aan exporteurs van dual-use goederen om misbruik te voorkomen. [redacted]

1/3 [redacted] De Europese Commissie is bezig deze te actualiseren en heeft in haar ontwerpverordening voorgesteld om

---

[4] [redacted]

3 [redacted]

3 [5] [redacted]

[6] https://www.wassenaar.org/about-us/#faq

[7] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public documents Volume II List of Dual-Use Goods and Technologies And Munitions List (December 2018)

[8] Idem.

[9] Annex I, COM(2016, 2016/0295: p. 2, p.15

[10] VERORDENING (EG) Nr. 428/2009 VAN DE RAAD

[11] [redacted]

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

'technologieën voor cybertoezicht' onder het exportcontrole regime te brengen[12]. "Inbraakprogrammatuur" (intrusion software)is onderdeel van deze technologieën voor cybertoezicht en zoals in tabel 1 aangegeven is binnendringsoftware een onderdeel van deze definitie .[13] Het Europees Parlement heeft op het moment van het schrijven van deze nota reeds haar amendementen aangenomen[14], de Raad poogt om voor de Europese verkiezingen een algemene oriëntatie aan te nemen[15].

Wanneer deze verordening in werking treedt moeten Europese producenten voldoen aan de eisen in de verordering, waaronder de controle op het mogelijke schenden van mensenrechten door de software. Europese leveranciers dienen dan daarmee aan de eisen uit het regeerakkoord 2017-2021 'Vertrouwen in de Toekomst' te voldoen.

1/3

Leveranciers buiten de Europese Unie

1/3

1/3

[16].

1/3

12
13
14
15
16

3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3

1/3

1/3

1/3

17

1/3

17

3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3

1/3

1/3

Bijlage 1 Definitie Inbraakprogrammatuur

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: .

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Noten:

1."Inbraakprogrammatuur" omvat niet het volgende: .
a.‹hypervisors›, ‹debuggers› of hulpmiddelen voor de reverse engineering van programmatuur (SRE); .
b."programmatuur" voor het beheer van digitale rechten (DRM); of .
c."programmatuur" die is ontworpen voor installatie door de fabrikanten, beheerders of gebruikers met het oog op goederenbewaking of -herstel. .
2.Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters.

Technische noten:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1.'Bewakingshulpmiddelen': "programmatuur" of hardwareapparaten die het systeemgedrag of de processen die op een apparaat worden uitgevoerd, bewaken. Dit omvat antivirus (AV)-producten, producten voor eindpuntbeveiliging, producten voor persoonlijke veiligheid (PSP: Personal Security Products), inbraakdetectiesystemen (IDS: Intrusion Detection Systems), inbraakpreventiesystemen (IPS: Intrusion Prevention Systems) of firewalls. .

2.'Beschermende tegenmaatregelen': technieken die zijn ontworpen om te zorgen voor de veilige uitvoering van programmacode, zoals preventie van gegevensuitvoering, (DEP: Data Execution Prevention DEP), willekeurige adresruimte-indeling (ASLR: Address Space Layout Randomisation) of <sandboxing>.

1/3

1/3

1/3

18

3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3

1/3

1/3

1/3

1/3

1/3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

Ministerie van Justitie en Veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
[redacted] 2

T 070[redacted]
F 070[redacted] 2

Datum

Ons kenmerk

Dep. VERTROUWELIJK
Beleidsnota

Versie **13 maart 2019**

nota

Leveranciers binnendringsoftware

Aanleiding

In het regeerakkoord 'Vertrouwen in de Toekomst' van het kabinet Rutte III staat de volgende passage over het wetsvoorstel Computercriminaliteit III:

"Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen." [1]

Deze beleidsnota zet uiteen welk beleid wordt gevoerd binnen de opsporing ten aanzien van aanschaf van binnendringsoftware van particuliere leveranciers.

Beleid

Het regeerakkoord vereist dat leveranciers van binnendringsoftware worden gescreend door de AIVD en dat deze leverancier niet aan dubieuze regimes verkopen. Commerciële binnendringsoftware is prominent onderwerp geweest in het debat over de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Commerciële binnendringsoftware maakt (mogelijk) gebruik van onbekende kwetsbaarheden in software. In plaats dat deze kwetsbaarheid wordt gemeld waardoor de software veiliger wordt, wordt deze kwetsbaarheid commercieel geëxploiteerd. Daarnaast kunnen leveranciers van deze software ook leveren aan regimes die de producten kunnen gebruiken voor het (ernstig) schenden van mensenrechten. Om de markt van binnendringsoftware niet meer dan strikt noodzakelijk te betreden is de aanschaf beperkt tot een specifieke zaak en worden aanvullende eisen gesteld aan leveranciers. Deze eisen betreffen 1) screening door de AIVD, 2) beoordeling of een bedrijf heeft geleverd aan dubieuze regimes.

1/2/3

Met opmerkingen [redacted]

Wat is binnendringsoftware?
Voor binnendring software wordt de definitie van de concept-verordening 2016/0295, annex I als uitgangspunt gebruikt.

[1] Regeerakkoord 2017-2021 'Vertrouwen in de toekomst'.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

De actualisering van de verordening is nog gaande daarmee staat de definitie nog niet vast.

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht:

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Zie bijlage 1 voor de (technische) noten die horen bij deze definitie.

Binnen de wet Computercriminaliteit III is onderscheid gemaakt tussen het technisch hulpmiddel dat bewijs vergaart en binnendringsoftware die de beveiliging van een geautomatiseerd werk doorbreekt. Het technisch hulpmiddel wordt geïnstalleerd nadat toegang is verkregen tot een geautomatiseerd werk. Binnendringsoftware omzeilt de beschermende tegenmaatregelen van een computer of apparaat met netwerkcapaciteit. Het beleid in deze nota zich op binnendringsoftware.

1/2/3

Met opmerkingen [redacted]

Screening AIVD

[redacted]

1/3

Levering van binnendringsoftware aan dubieuze regimes
Binnendringsoftware kan een essentieel middel zijn in de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk, maar kan ook worden misbruikt door repressieve regimes. Het is een zogenaamd product voor tweeërlei gebruik[2], oftewel een dual-use goed. In de kamerbrief over kwetsbaarheden in hard- en software van november 2016 staat dat de regering hecht aan beperking van uitvoer van ICT-goederen en -software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] In onderstaand beleid wordt uiteengezet hoe hier in het kader van de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk vorm aan wordt gegeven.

[2] COM(2016), 2016/0295

[3] Kamerstukken TK, 2016/17, 26 643, nr. 428

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

Binnen het recht of beleid bestaat geen eenduidige definitie van een dubieus regime. [redacted]

1/3 [redacted]

1/3 [redacted]

Bij The Wassenaar Arrangement wordt de reikwijdte van de export controle bepaald door de lijsten die zijn opgesteld onder het arrangement, de praktische implementatie varieert van land tot land.[6] Er zijn ook zogenaamde 'best practices' gepubliceerd. De bescherming van mensenrechten speelt in deze best practices een rol bij de uitvoer van conventionele wapens, handvuurwapens en lichte wapens, maar nog niet bij 'intrusion software'. Deze software wordt wel genoemd in de lijst met dual-use items. In de categorie computers (p. 79) wordt *software* die speciaal ontwikkeld of aangepast is voor de ontwikkeling, controle, of aflevering van 'intrusion software' op de dual-use lijst geplaatst, alsook de *technologie* voor de ontwikkeling van 'intrusion software' (p. 80).[7] [Nota bene, het arrangement reguleert niet de binnendringsoftware zelf, maar software of technologie die deze software ontwikkelt, controleert of aflevert.] De definitie van 'intrusion software' komt overeen met die uit de concept-verordening 2016/0295 (p. 221)[8] [9] . [redacted]

1/3 [redacted]

Leveranciers binnen de Europese Unie

In de Europese Unie bestaat sinds 2009 een verordening die een exportcontrole regime vereist op dual-use goederen[10]. Een dergelijk regime stelt voorwaarden aan exporteurs van dual-use goederen om misbruik te voorkomen. [redacted]

1/3 [redacted] De Europese Commissie is bezig

3 [4] [redacted]

3 [5] [redacted]

[6] https://www.wassenaar.org/about-us/#faq

[7] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public documents Volume II List of Dual-Use Goods and Technologies And Munitions List (December 2018)

[8] Idem.

[9] Annex I, COM(2016, 2016/0295: p. 2, p.15

[10] VERORDENING (EG) Nr. 428/2009 VAN DE RAAD

3 [11] [redacted]

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

deze te actualiseren en heeft in haar ontwerpverordening voorgesteld om 'technologieën voor cybertoezicht' onder het exportcontrole regime te brengen[12]. "Inbraakprogrammatuur" (intrusion software)is onderdeel van deze technologieën voor cybertoezicht en zoals in tabel 1 aangegeven is binnendringsoftware een onderdeel van deze definitie .[13] Het Europees Parlement heeft op het moment van het schrijven van deze nota reeds haar amendementen aangenomen[14], de Raad poogt om voor de Europese verkiezingen een algemene oriëntatie aan te nemen[15].

1/2/3

Met opmerkingen

Wanneer deze verordening in werking treedt moeten Europese producenten voldoen aan de eisen in de verordering, waaronder de controle op het mogelijke schenden van mensenrechten door de software. Europese leveranciers dienen dan daarmee aan de eisen uit het regeerakkoord 2017-2021 'Vertrouwen in de Toekomst' te voldoen.

1/3

Leveranciers buiten de Europese Unie

1/3

1/3

1/2/3

Met opmerkingen

1/3

3

12
13
14
15
16

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3

[redacted]

1/3

[redacted]

1/3

[redacted]

1/2/3

Met opmerkingen

[redacted]

1/3

[redacted]

17

3

[redacted]

f

Directoraat-Generaal
Rechtspleging en
Rechtshandhaving
Directie Rechtshandhaving en
Criminaliteitsbestrijding

Datum

Ons kenmerk 1/2/3

1/3

1/3

1/3

Met opmerkingen

1/2/3

Met opmerkingen

1/2/3

Met opmerkingen

Bijlage 1 Definitie Inbraakprogrammatuur

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: .

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Noten:

1."Inbraakprogrammatuur" omvat niet het volgende: .
a.‹hypervisors›, ‹debuggers› of hulpmiddelen voor de reverse engineering van programmatuur (SRE); .
b."programmatuur" voor het beheer van digitale rechten (DRM); of .
c."programmatuur" die is ontworpen voor installatie door de fabrikanten, beheerders of gebruikers met het oog op goederenbewaking of -herstel. .
2.Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters.

Technische noten:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1.'Bewakingshulpmiddelen': "programmatuur" of hardwareapparaten die het systeemgedrag of de processen die op een apparaat worden uitgevoerd, bewaken. Dit omvat antivirus (AV)-producten, producten voor eindpuntbeveiliging, producten voor persoonlijke veiligheid (PSP: Personal Security Products), inbraakdetectiesystemen (IDS: Intrusion Detection Systems), inbraakpreventiesystemen (IPS: Intrusion Prevention Systems) of firewalls. .

2.'Beschermende tegenmaatregelen': technieken die zijn ontworpen om te zorgen voor de veilige uitvoering van programmacode, zoals preventie van gegevensuitvoering, (DEP: Data Execution Prevention DEP), willekeurige adresruimte-indeling (ASLR: Address Space Layout Randomisation) of ‹sandboxing›.

1/3

1/3

1/3

18

3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3

1/3

1/3

1/3

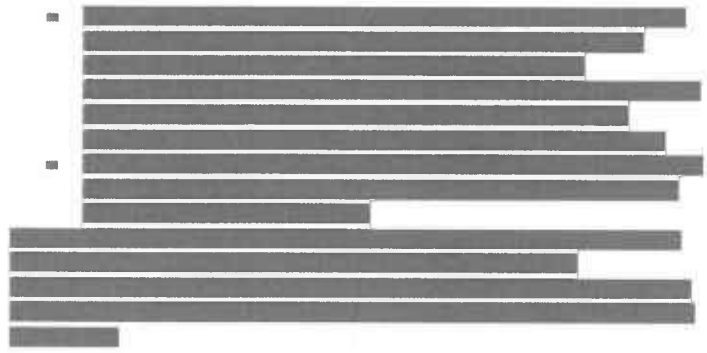
1/3

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1/3



1/3

1/3

1/3

Van: [redacted] - BD/DRC/CV [redacted]@minjenv.nl> 2
Verzonden: vrijdag 12 april 2019 16:02
Aan: [redacted] 2
CC: [redacted] - BD/DRC/CV 2
Onderwerp: Dubieuze regimes

2

Hoi [redacted], dinsdagmiddag hebben we een gesprek met de LA om te kijken of zij een rol in kunnen vervullen bij het invullen van het RA. Vandaag heb ik ook overleg gehad met de interne advocaat van J&V die veel doet met inkoop en aanbesteding. Hem leek het goed als [redacted] 1/3 [redacted] Hij vroeg in dat verband onder welk aanbestedingsregime dit valt. Eerder heb ik begrepen dat [redacted]
Heb jij hier de juiste info over? Dan kunnen we dat dinsdag meenemen in het gesprek met de LA. (Ik heb begrepen dat hierover eerder contact is geweest met [redacted], een aanbestedingsjurist van de politie, misschien heeft hij hier een antwoord op?). 2

Groet,
[redacted] 2

Van: 2 [redacted]
Verzonden: donderdag 14 maart 2019 09:49
Aan: 2 [redacted]
Onderwerp: FW: Concept uitwerking dubieuze regimes ihkv CCIII
Bijlagen: 2 Leveranciers binnendringsoftware_[redacted].docx

2 Hoi [redacted]

Bijgevoegd mijn eerste opmerkingen in het doc. [redacted]
1/3 [redacted]

1/3 [redacted] zou m.i. voldoende moeten zijn.
Lijkt me goed dit [redacted]

Groeten,

2 [redacted]

2 **Van:** [redacted] BD/DRC/CV [mailto:[redacted]@minjenv.nl]
Verzonden: donderdag 18 april 2019 15:50
2 **Aan:** [redacted]@politie.nl>
2 **CC:** [redacted]@minjenv.nl>; [redacted]@minjenv.nl>
Onderwerp: Toets dubieuze regimes
Urgentie: Hoog

2 Hallo [redacted]

We zijn invulling aan het geven aan de voorwaarde uit het regeerakkoord dat leveranciers van binnendringsoftware niet mogen hebben geleverd aan dubieuze regimes.

1/3 [redacted]

1/3 [redacted]

We willen op 24 april in de ochtend samen komen. Deze termijn is vrij strak, maar als we voor de zomer een beslissing willen hebben moeten we nu snel blijven handelen.

Kun je ons verder helpen?

Alvast bedankt.

Met vriendelijke groet,

2 [redacted]

M 06 [redacted]
2 [redacted]@minvenj.nl

Van: 2 [redacted]
Verzonden: donderdag 18 april 2019 16:05
Aan: 2 [redacted]
CC: [redacted]
Onderwerp: 2 FW: Toets dubieuze regimes

Urgentie: Hoog

Beste allemaal,

Zie onderstaand verzoek van het departement. Kan een van jullie hierbij aanschuiven? Ik weet dat het erg kort dag is, maar het zou mooi zijn als we hier een bijdrage aan kunnen leveren.

2 Ik ben zelf op vakantie en kan er dus helaas niet bij zijn. Mochten jullie niet kunnen, is het dan toch mogelijk dat 1 van jullie even contact met [redacted] opneemt? Dan kunnen we op die manier wellicht een bijdrage leveren.

Voor de volledigheid is het goed om op te merken dat [redacted]
1/3 [redacted] Ik begreep gisteren van [redacted] 2

Alvast bedankt voor de hulp!

Mochten er nog vragen zijn, ik ben telefonisch en via de mail te bereiken.
Met vriendelijke groet,
2 [redacted]

2 [redacted]

[redacted]

Postbus 100, 3970 AC Driebergen-Rijsenburg
2 M: +31 (0)6 [redacted]
E: [redacted]@politie.nl
PGP: [redacted]

Van: 2 [redacted]
Verzonden: donderdag 18 april 2019 16:30
Aan: 2 [redacted]
Onderwerp: FW: Toets dubieuze regimes

Urgentie: Hoog

2 [redacted]
1/2/3
Als dit overleg doorgaat lijkt het mij verstandig om ook iemand van ons mee te laten gaan. Zeker als het gaat om [redacted] Dan dank ik al gauw aan [redacted]
Misschien jij? Of [redacted]

Missschien nog even over bellen?
2 Gr [redacted]

Van: [redacted] - BD/DRC/CV [mailto:[redacted]@minjenv.nl]
Verzonden: dinsdag 23 april 2019 19:02
Aan: [redacted] - BD/DII/BJZ <[redacted]@minjenv.nl>; [redacted]
[redacted]l@politie.nl>; [redacted]@politie.nl>; [redacted]
BD/DRC/CV [redacted]@minjenv.nl>; [redacted] - BD/DGPenV/PPBT [redacted]@minjenv.nl>;
[redacted] - BD/DRC/CV [redacted]@minjenv.nl>
Onderwerp: Aanbesteding binnendringsoftware overleg morgen

Hallo allen,

Voor morgen heb ik nog even een aanvullende nota gemaakt zodat jullie iets meer een idee hebben bij het overleg.

Nogmaals dank voor de beschikbaarheid op deze korte termijn.

Tot morgen.

Met vriendelijke groet,

[redacted]
[redacted]

M 06 [redacted]
[redacted]@minvenj.nl

Van: 2 [redacted]
Verzonden: donderdag 25 april 2019 14:20
Aan: 2 [redacted]
Onderwerp: FW: Aanbesteding binnendringsoftware overleg morgen
Bijlagen: Nota voor overleg.docx

2 Ha [redacted],

Zag dat jij deze mail nog niet had ontvangen. Bij deze.....

3 Hierbij nog wat bespreekpunten om mee te nemen [redacted]

1/3
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

2 Kun jij uitkomst ook doormailen aan [redacted]

Fijne vakantie.....nog

2 [redacted]

Aan politie, DIenI, DPOL, DRC

1. Aanleiding

Het regeerakkoord stelt voorwaarden aan de aanschaf van binnendringsoftware bij de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk door de opsporing. Aanschaf gebeurt in een specifieke zaak en leveranciers worden gescreend door de AIVD en leveren niet aan dubieuze regimes. Deze nota ziet op de uitwerking van de toets op dubieuze regimes.

2. Toelichting

1/3

1/3

1/3

1/3

3. Tijdspad; doel voor de zomer beleid omtrent dubieuze regimes

24 april – overleg politie voor het vergroten van het begrip van de markt en toepasbare sancties

27 april – volgende versie van beleid

29 april – 3 mei – beleid afstemmen tot directeur DRC/POL(/ DPOL?)

6 -10 mei – aanpassing/afstemming/voorbereiding overleg minister

13-17 mei – 'bespreking aan de voorkant'? met de minister

24 mei – nota aan minister

31 mei – beslissing minister

4. Bijlages

Passage regeerakkoord

"Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen."

Achtergrond bij de procedure tot aanschaf van binnendringsoftware na het Regeerakkoord

De bevoegdheid tot het heimelijk binnendringen vereist op zich al een dringend opsporingsbelang en een misdrijf dat een ernstige inbreuk op de rechtsorde oplevert. Binnen deze bevoegdheid is het gebruik van commerciële binnendringsoftware beperkt tot het uiterste geval. Deze software kan alleen worden gebruikt wanneer minder ingrijpende middelen zoals het gebruik van inloggegevens, social engineering of bekende kwetsbaarheden niet toereikend zijn om heimelijk toegang te verkrijgen tot een geautomatiseerd werk. [1] Het Regeerakkoord 2017–2021 beperkt bovendien het betreden van de markt voor commerciële binnendringsoftware die mogelijk gebruik maakt van onbekende kwetsbaarheden. In plaats daarvan wil de regering meer inzetten op de eigen ontwikkeling van methoden voor het binnendringen, daartoe zal de ontwikkeling van passende producten binnen de politie worden gestimuleerd. De beperking in het Regeerakkoord van het gebruik van software van derden zal leiden tot een grotere belasting van het technisch team van de Landelijke Eenheid dat met de uitvoering is belast en dat zelf passende methoden moet ontdekken en ontwikkelen, vooral in zaken waarin inzet zonder de aanschaf van software nodig is. Bij de toedeling van de financiële middelen voor de uitvoering van dit wetsvoorstel is hiermee rekening gehouden (politie ontvangt 8 van de 10 miljoen). Niettemin is het gebruik van software die mogelijk gebruik maakt van onbekende kwetsbaarheden soms onvermijdelijk om ernstige criminaliteit te kunnen bestrijden.

Politiek beeld bij de markt

in het debat rond CCIII zijn leveranciers onderwerp geweest van het debat in de Tweede Kamer, "sinistere bedrijven"[2] werden zij genoemd door Verhoeven (D66) en het betreden van de markt werd beschreven als een "ongemakkelijk hoekje"[3] door de toenmalige staatssecretaris van Veiligheid en Justitie of een "graat in de keel"[4] van de PvdA. Het is een 'ongemakkelijk hoekje' omdat een product wordt aangeschaft van een bedrijf "dat op zich legitiem opereert en dat wellicht ook andere klanten kan aanspreken [...] die minder fris zijn" en omdat software wordt ingekocht waarvan we niet zeker weten of daar een onbekende kwetsbaarheid in zit.[5] Daarbij heeft de staatssecretaris wel aangegeven dat de markt bestaat onafhankelijk van de wet en deze wet geen cruciale rol speelt in de markt aangezien de vraag reeds bestaat en het aanbad op de markt is afhankelijk van de beschikbare kwetsbaarheden.[6] De afweging is toen gemaakt dat de wet CCIII het juist beter mogelijk maakt om criminelen die misbruik maken van onbekende kwetsbaarheden beter te bestrijden. [7] In het regeerakkoord is de afweging software aan te schaffen geclausuleerd.

[1] Handelingen TK, 2017-2018, 34 372, G, p. 11
[2] Handelingen TK, p. 5, 21
[3] Handelingen TK, p. 40
[4] Handelingen TK, p. 58
[5] Handelingen TK, p. 41
[6] Handelingen TK, p. 40
[7] Idem.

Onderwerp
1. Intrekking primair besluit van 5 november 2019 onder punt 2. t/m punt 6.
2. Nieuw primair besluit onder punt 2. tot en met punt 6.

AANTEKENEN
De Volkskrant B.V.
T.a.v. art. 5.1. 2e lid onder e Woo
Postbus 1002
1000 BA AMSTERDAM

Organisatieonderdeel
Landelijke Eenheid
Staf
Afdeling Bestuursondersteuning
Juridische Zaken

Behandeld door
art. 5.1. 2e lid onder e Woo

Functie
Bedrijfsvoeringspecialist

Telefoon

E-mail
art. [redacted]@politie.nl

Ons kenmerk
2019-0033028
5992

Uw kenmerk
2018054721

In afschrift aan

Datum
28 maart 2022

Bijlage(n)
-

Pagina
1

Geachte art. 5.1. 2e lid onder e Woo

I. Informatieverzoek / procesverloop

Bij brief van 5 juni 2019 is op grond van de Wet openbaarheid van bestuur (Wob) een verzoek ingediend tot openbaarmaking van:

1. Documenten betreffende het beleid ten aanzien screening van leveranciers van hacksoftware. Dit omvat het beleid waarin staat hoe wordt getoetst of een leverancier levert aan dubieuze regimes en, wanneer een overeenkomst tot stand is gekomen, hoe gecontroleerd wordt of een leverancier aan dubieuze regimes is gaan leveren.
2. Een overzicht van leveranciers van hacksoftware, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop een overeenkomst met het bedrijf is aangegaan, en (eventueel) gevolgd door een datum waarop de overeenkomst is beëindigd. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
3. Een overzicht van leveranciers waarvan expliciet niet hacksoftware afgenomen mag worden, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop de leverancier op de lijst terecht is gekomen, eventueel gevolgd door een datum waarop de leverancier van de lijst is afgehaald. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
4. Documenten en communicatie die betrekking hebben op [redacted] zoals overeenkomsten, nota's en e-mails over de screening van deze leverancier en de afwegingen van het aangaan, het afzien en het verbreken van een overeenkomst met deze leverancier.
5. Een overzicht van de onderzoeken naar leveranciers van hacksoftware. Hier wordt gevraagd om een lijst waarin duidelijk wordt naar wie het onderzoek is ingesteld, wanneer het onderzoek is gestart, wanneer het is afgerond, en wat de conclusie en adviezen voortkomend uit het onderzoek zijn. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan die documenten zelf een overzicht gemaakt kan worden.

Postbus 100
3970 AC Driebergen-Rijsenburg
Hoofdstraat 54
3972 LB Driebergen-Rijsenburg

www.politie.nl

6. Documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

Bij besluit van 5 november 2019 is op het informatieverzoek van 5 juni 2019 als volgt beslist.

A. Betreffende het informatieverzoek onder punt 1 zijn drie (concept) beleidsnota's en acht e-mails deels openbaar gemaakt.

B. Betreffende het informatieverzoek onder punt 2. tot en met punt 6. wordt (worden) (in het geheel) geen mededeling(en) gedaan over: (a.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers van hacksoftware, (b.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers waarvan expliciet geen hacksoftware afgenomen mag worden, (c.) al dan niet bij de politie berustend(e) (communicatie)document(en) van [naam bedrijf] art. 5.1 2e lid onder c. WOO [redacted], (d.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) onderzoek(en) naar een of meer leveranciers van hacksoftware en (e.) (communicatie)documenten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over een of meer de leverancier(s) van hacksoftware.

Bij brief van 12 december 2019 is bezwaar ingediend gericht tegen het besluit van 5 november 2019.

II. Wettelijk kader / overwegingen tot intrekking primair besluit van 5 november 2019 onder B.

Ingevolge artikel 6:19, eerste lid van de Algemene wet bestuursrecht (Awb) heeft het bezwaar of beroep van rechtswege mede betrekking op een besluit tot intrekking, wijziging of vervanging van het bestreden besluit, tenzij partijen daarbij onvoldoende belang hebben. Ingevolge het tweede lid van dit artikel geldt het eerste lid ook indien het bezwaar is gemaakt of het beroep is ingesteld nadat het bestuursorgaan het bestreden besluit heeft ingetrokken, gewijzigd of vervangen.

Hoewel en in beginsel een besluit tot intrekking, wijziging of vervanging van een primair besluit op grondslag van een bezwaar dient te geschieden in een beslissing op bezwaar als bedoeld in art. 7:11, tweede lid van de Awb heeft de korpschef van politie -gelet op de uitspraak van de Afdeling bestuursrechtspraak van 28 april 2021 [ECLI:NL:RVS:2021:911]- geoordeeld dat artikel 68 van de Grondwet niet aangemerkt kan worden als een bijzondere openbaarmakingsregeling die voorgaat op de Wob als algemene openbaarmakingsregeling.

Hieruit vloeit voort, dat er reden is om -voorafgaand aan het besluit op bezwaar- het besluit van 5 november 2019 onder B. in te trekken en een nieuw primair besluit op het informatieverzoek van 5 juni 2019 onder punt 2. tot en met punt 6 te nemen.

III. Beslissing op het informatieverzoek van 5 juni 2019 onder punt 2., punt 3. en punt 5. met betrekking tot overzichtslijsten van leveranciers van hacksoftware.

Bij de NP berust geen informatie als omschreven in het verzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 5 met betrekking tot overzichtslijsten van leveranciers van hacksoftware. De Wob is niet van toepassing op niet bestaande informatie en de Wob bevat geen verplichting om niet bestaande informatie te vervaardigen, ongeacht de mate van inspanning.

IV. Beslissing op het informatieverzoek van 5 juni 2019 onder punt 4. met betrekking tot documenten en communicatie die betrekking hebben op [redacted] en onder punt 6. met betrekking tot documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

Bij de NP berust informatie als omschreven in het verzoek van 5 juni 2019 onder punt 4 en 6. De openbaarmaking hiervan wordt integraal geweigerd omdat:

I. Dit het belang van de veiligheid van de Staat zou kunnen schaden, als bedoeld in artikel 10, eerste lid onder b van de Wob en/of;
II. Dit bedrijfs- en fabricagegegevens betreffen, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld, als bedoeld in artikel 10, eerste lid onder c. van de Wob en/of;
III. Het belang van openbaarmaking daarvan niet opweegt tegen het belang van: (1.) de betrekkingen van Nederland met andere staten en met internationale organisaties, als bedoeld in artikel 10, tweede lid onder a. van de Wob en/of (2.) de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen, als bedoeld in artikel 10, tweede lid onder b. van de Wob en/of (3.) de opsporing en vervolging van strafbare feiten als bedoeld in artikel 10, tweede lid onder c. van de Wob en/of (d.) inspectie, controle en toezicht door bestuursorganen, als bedoeld in artikel 10, tweede lid onder d. van de Wob en/of (4.) de eerbiediging van de persoonlijke levenssfeer, als bedoeld in artikel 10, tweede lid onder e. van de Wob en/of (5.) het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, als bedoeld in artikel 10, tweede lid onder g. van de Wob en/of (6.) het intern beraad, waarin persoonlijke beleidsopvattingen zijn opgenomen, als bedoeld in artikel 11 van de Wob.

In een Wob-besluit dient de uitkomst van de belangenafweging in beginsel per informatiedrager of per onderdeel daarvan te worden gemotiveerd waarom die informatie of (onder)deel daarvan niet openbaar kan worden gemaakt, zie onder meer ECLI:NL:RVS:2018:666. Bij de onderhavige beslissing kan een andere dan een 'kale' motivering niet worden gegeven zonder zicht te bieden op de aard of de inhoud van de informatie, zie uitspraak ABRvS van 28 december 1999 inzake no. 199901860/1 en 199901860/2, ECLI:NL:RVS:2003:AF2889 en ECLI:NL:RVS:2013:1209.

Hieruit vloeit voort, dat de afweging van de bovenvermelde onder I. en/of II. en/of III. omschreven belang(en) niet verder te motiveren is (zijn), zonder prijs te geven wat met toepassing van de onder I. en/of II. en/of III. omschreven artikel(en) van de Wob aan de openbaarheid wordt onthouden. Daarom kan niet meer specifiek op de weigering van de informatie worden ingegaan.

In bovenvermelde context wordt opgemerkt, dat binnen het kader van de in artikel 8:29 van de Algemene wet bestuursrecht (Awb) opgenomen procedure de rechter kan beoordelen of een bestuursorgaan met betrekking tot de stukken tot een juiste beslissing inzake de niet openbaarmaking is gekomen. Op die wijze vindt een controle plaats op de beoordeling door het bestuursorgaan van de in de Wob omschreven beperkingen en uitzonderingen.

Besluit

I. Het besluit van 5 november 2019 onder B. wordt ingetrokken.
II. De Wob is niet van toepassing op niet bestaande informatie en de Wob bevat geen verplichting om niet bestaande informatie te vervaardigen, ongeacht de mate van inspanning.
III. De in het verzoek van 5 juni 2019 onder punt 4. en punt 6. gevraagde informatie wordt integraal geweigerd / wordt niet openbaar gemaakt.

Hoogachtend,

De korpschef van politie,
namens deze,
De politiechef van de Landelijke Eenheid,
namens deze,

art. 5.1. 2e lid onder e Woo

Rechtsbescherming
Ingevolge artikel 6:19, eerste lid van de Awb heeft het bezwaar van 12 december 2019 gericht tegen het besluit van 5 november 2019 van rechtswege mede betrekking op het besluit van 28 maart 2022 onder I. tot intrekking van het besluit van 5 november 2019 onder B. Indien u zich niet kunt verenigen met het besluit van 28 maart 2022 onder II. en/of III., kunt u binnen een termijn van zes weken na bekendmaking van dit besluit schriftelijk bezwaar maken. Het bezwaarschrift dient te worden gericht aan de Nationale Politie, Landelijke Eenheid, postbus 100, 3970 AC Driebergen-Rijsenburg, onder vermelding van het kenmerk van de politie zoals deze is vermeld in het colofon van het besluit. Het bezwaarschrift moet ondertekend zijn en ten minste bevatten: naam en adres, dagtekening, omschrijving van het besluit waartegen het bezwaarschrift is gericht en de gronden van bezwaar. Er dient een volmacht te worden verstrekt, indien het bezwaarschrift niet door de belanghebbende zelf, maar namens deze wordt ingediend. De elektronische weg voor het indienen van een bezwaarschrift is niet geopend.

Onderwerp
Beslissing op het bezwaarschrift
van 12-12-2019

AANTEKENEN
De Volkskrant B.V.
T.a.v. art. 5.1. 2e lid onder e Woo
Postbus 1002
1000 BA AMSTERDAM

Organisatieonderdeel
Landelijke Eenheid
Staf
Team Juridische Zaken

Behandeld door
art. 5.1. 2e lid onder e

Functie
Bedrijfsvoeringspecialist

Telefoon

E-mail
art. @politie.nl

Ons kenmerk
2019-0033028
5992

Uw kenmerk
2018054721

In afschrift aan

Datum
11 april 2022

Bijlage(n)
Besluit van 28 maart 2022

Geachte art. 5.1. 2e lid onder e Woo

I. Informatieverzoek / procesverloop

Bij brief van 5 juni 2019[1] is een informatieverzoek ingediend op grond van de Wet openbaarheid van bestuur (Wob).[2]

Hierop is bij besluit van 5 november 2019[3] kenmerk 2019-00330285992 beslist.[4]

Bij brief van 12 december 2019[5] is een bezwaarschrift ingediend gericht tegen het besluit van 5 november 2019 onder B. onder punt 2 tot en met punt 6.[6]

Bij brief van 7 januari 2020 kenmerk 2019-0033028 7207 is de (voorbereiding op de) besluitvorming in het voorliggende bezwaar ingevolge artikel 7:10, vierde lid onder c. van de Algemene wet bestuursrecht (Awb) uitgesteld tot na de uitspraak van de hoger beroepsprocedure, zaaknummer 201708552/1/A3.

Bij brief van 9 januari 2020[7] is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019. Hierop heeft de rechtbank Amsterdam in de uitspraak van 19 november 2020, zaaknummer AMS 20 / 238 WOB beslist.[8]

Bij brief van 6 februari 2020[9] is een ingebrekestelling ingediend wegens het niet tijdig nemen van een beslissing op het bezwaar van 12 december 2019.

Bij brief van 7 juni 2021[10] is een ingebrekestelling ingediend wegens het niet tijdig nemen van een beslissing op het bezwaar van 12 december 2019.

In de uitspraak van 28 april 2021 (ECLI:NL:RVS:2021:911) heeft de Afdeling bestuursrechtspraak van de Raad van State zaaknummer 201708552/1/A3 beslist.[11]

Bij brief van 24 juli 2021[12] is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019. Hierop heeft de rechtbank Amsterdam in de uitspraak van 20 augustus 2021, zaaknummer AWB 21/3394 beslist.[13]

Bij brief van 17 februari 2022[14] is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019. Hierop heeft de rechtbank Amsterdam nog niet beslist.

II. Overwegingen

In de uitspraak van de Afdeling bestuursrechtspraak van 28 april 2021 [ECLI:NL:RVS:2021:911] heeft de Afdeling in rechtsoverweging 5.3. geoordeeld dat artikel 68 van de Grondwet niet aangemerkt kan worden als een bijzondere openbaarmakingsregeling die voorgaat op de Wob als algemene openbaarmakingsregeling.

Op grondslag van en onder verwijzing naar deze uitspraak is bij besluit van 28 maart 2022[15] onder:

II. Het besluit van 5 november 2019 onder B met betrekking tot het informatieverzoek van 5 juni 2019 onder punt 2.[16], onder punt 3.[17], onder punt 4.[18], onder punt 5.[19] en onder punt 6.[20] ingetrokken.
III. Een nieuw primair besluit genomen op het informatieverzoek van 5 juni 2019 onder punt 2. onder punt 3. en onder punt 5.[21]
IV. Een nieuw primair besluit genomen op het informatieverzoek van 5 juni 2019 onder punt 4. en onder punt 6.[22]

Ingevolge artikel 7:2, eerste lid van de Awb stelt een bestuursorgaan, voordat op het bezwaar van 12 december 2019 wordt beslist, belanghebbenden in de gelegenheid te worden gehoord. Ingevolge het tweede lid van dit artikel stelt het bestuursorgaan daarvan in ieder geval de indiener van het bezwaarschrift op de hoogte alsmede de belanghebbenden die bij de voorbereiding van het besluit hun zienswijze naar voren hebben gebracht.

Ingevolge artikel 7:3, aanhef en onder e. van de Awb kan van het horen van een belanghebbende worden afgezien indien aan het bezwaar volledig tegemoet wordt gekomen en andere belanghebbenden daardoor niet in hun belangen kunnen worden geschaad.

Omdat en de korpschef van politie (a.) over alle feiten en omstandigheden beschikt om een volledige heroverweging van het bestreden besluit van 5 november 2019 onder B., onder punt 2 tot en onder punt 6. te kunnen verrichten, (b.) voor de beslissing op bezwaar geen nader onderzoek dient te worden verricht en (c.) volledig aan het bezwaar volledig is tegemoet gekomen en (d.) het feit dat onder deze omstandigheden een hoorzitting niets zal (kunnen) toevoegen aan de informatie die nodig is voor een juiste beslissing op bezwaar, stelt de korpschef van politie zich op het standpunt dat er op voorhand redelijkerwijs geen twijfel over mogelijk is dat de bezwaargronden niet kunnen leiden tot een andersluidend standpunt dan intrekking van het in bezwaar bestreden primaire besluit van 5 november 2019 onder B., onder punt 2 tot en met onder punt 6.

III. Besluit

I. Het bezwaar van 12 december 2019, gericht tegen het primaire besluit van 5 november 2019 onder B., onder punt 2 tot en met onder punt 6. wordt ontvankelijk en gegrond verklaard.

Hoogachtend,

De korpschef van politie,
Voor deze,
art. 5.1 2e lid onder e WOO

Rechtsbescherming
Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit beroep instellen bij de rechtbank, binnen het rechtsgebied waarvan de indiener van het beroepschrift zijn woonplaats in Nederland heeft. Indien de indiener van het beroep geen woonplaats in Nederland heeft, is de rechtbank binnen het rechtsgebied waarvan het bestuursorgaan zijn zetel heeft bevoegd. Het beroepschrift moet op grond van artikel 6:5 van de Awb zijn ondertekend en ten minste bevatten: de naam en het adres van de indiener, de dagtekening, de omschrijving van het besluit waartegen het beroep is gericht, zo mogelijk een afschrift van dit besluit, en de gronden waarop het beroepschrift rust. Nadere informatie over de hoogte van het griffierecht en de wijze van betalen wordt door de griffie van de rechtbank verstrekt.

U kunt ook digitaal beroep instellen bij de rechtbank via http://loket.rechtspraak.nl/bestuursrecht. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). U kunt op de genoemde site de precieze voorwaarden vinden

[1] Ontvangen op 7 juni 2019.
[2] Hierin wordt op grond van de Wet openbaarheid van bestuur (Wob) verzocht tot openbaarmaking van de navolgende documenten:
1. Documenten betreffende het beleid ten aanzien screening van leveranciers van hacksoftware. Dit omvat het beleid waarin staat hoe wordt getoetst of een leverancier levert aan dubieuze regimes en, wanneer een overeenkomst tot stand is gekomen, hoe gecontroleerd wordt of een leverancier aan dubieuze regimes is gaan leveren.
2. Een overzicht van leveranciers van hacksoftware, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop een overeenkomst met het bedrijf is aangegaan, en (eventueel) gevolgd door een datum waarop de overeenkomst is beëindigd. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
3. Een overzicht van leveranciers waarvan expliciet niet hacksoftware afgenomen mag worden, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop de leverancier op de lijst terecht is gekomen, eventueel gevolgd door een datum waarop de leverancier van de lijst is afgehaald. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
4. Documenten en communicatie die betrekking hebben op [naam bedrijf art. 5.1 2e lid onder c. WOB], zoals overeenkomsten, nota's en e-mails over de screening van deze leverancier en de afwegingen van het aangaan, het afzien en het verbreken van een overeenkomst met deze leverancier.
5. Een overzicht van de onderzoeken naar leveranciers van hacksoftware. Hier wordt gevraagd om een lijst waarin duidelijk wordt naar wie het onderzoek is ingesteld, wanneer het onderzoek is gestart, wanneer het is afgerond, en wat de conclusie en adviezen voortkomend uit het onderzoek zijn. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan die documenten zelf een overzicht gemaakt kan worden.
6. Documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.
[3] Ontvangen op 12 november 2021.
[4] Hierin is onder A. m.b.t. het informatieverzoek onder punt 1. als volgt beslist:
Betreffende het informatieverzoek onder punt 1. zijn na onderzoek drie (concept) beleidsnota's en acht e-mails aangetroffen. Na toetsing aan de uitzonderingsgronden en beperkingen omschreven in artikel 10 en 11 van de Wob worden deze documenten deels openbaar gemaakt. De in documenten vervatte informatie waarvan de openbaarmaking geheel dan wel deels is geweigerd, zijn voorzien van een cijfercode' die correspondeert met de (algemene) motivering, omschreven in de bij dit besluit behorende bijlage.
Hierin is onder B. m.b.t. het informatieverzoek onder punt 2. tot en met punt 6. als volgt beslist:
Betreffende het informatieverzoek onder punt 2. tot en met punt 6. neem ik het standpunt in om (in het geheel) geen mededeling(en) te doen over: (a.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers van hacksoftware, (b.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) leveranciers waarvan expliciet geen hacksoftware afgenomen mag worden, (c.) al dan niet bij de politie berustend(e) (communicatie)document(en) van [naam bedrijf art. 5.1 2e lid onder c. WOB], (d.) al dan niet bij de politie berustend(e) overzicht(en) van een of meer(dere) onderzoek(en) naar een of meer leveranciers van hacksoftware en (e.) (communicatie)documenten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over een of meer de leverancier(s) van hacksoftware. Voor dit standpunt wordt verwezen naar, c.q. een beroep gedaan op: (1.) de parlementaire geschiedenis van de reikwijdte van het verschoningsgrond bedoeld in artikel 68 Grondwet (Grw) inzake het geven van inlichtingen door de ministers en staatssecretarissen en (2.) de parlementaire geschiedenis van de Wet openbaarheid van bestuur, (mede) gelet op dan wel in samenhang bezien met artikel 10, eerste lid onder b. en/of onder c. van de Wob en/of artikel 11 van de Wob en/of artikel 10, tweede lid onder c. en/of onder d. en/of onder e. en/of onder g. van de Wob en artikel 3 van de Politiewet 2012. Hieruit vloeit voort, dat in het onderhavige geval de Wob als algemene openbaarmakingsregeling dient te wijken voor de bijzondere openbaarmakingsregeling met een uitputtend karakter, bedoeld in artikel 68 Grw en daarom niet wordt (kan worden) toegekomen aan een beoordeling op grond van de Wob. De motivering is omschreven in de bij dit besluit behorende bijlage.
[5] Ontvangen op 16 december 2019.
[6] Hierin is bezwaar gemaakt tegen het besluit van 5 november 2019 onder B. m.b.t. het informatieverzoek onder punt 2. tot en met punt 6. Hierin is omschreven dat de Wob als algemene openbaarmakingsregeling dient te wijken voor de bijzondere openbaarmakingsregeling met een uitputtend karakter, bedoeld in artikel 68 Grw en daarom niet wordt (kan worden) toegekomen aan een beoordeling op grond van de Wob de bijzondere openbaarmakingsregeling bedoeld in artikel 68 van de Grondwet (Grw) voorgaat op de Wob.
[7] Ontvangen op 23 januari 2020.
[8] Hierin verklaart de rechtbank het beroep niet-ontvankelijk.
[9] Ontvangen op 6 februari 2020.
[10] Ontvangen op 8 juni 2021.
[11] In r.o. 5.3 overweegt de Afdeling dat artikel 68 van de Grw niet aangemerkt kan worden als een bijzondere openbaarmakingsregeling die voorgaat op de Wob als algemene openbaarmakings-regeling.
[12] Ontvangen op 30 juni 2021.
[13] Hierin verklaart de rechtbank het beroep gegrond en draagt aan de korpschef van politie op om binnen twee weken na de dag van verzending van deze uitspraak een besluit op het bezwaar te nemen en bepaalt dat de korpschef van politie een dwangsom van € 100,- verbeurt voor elke dag waarmee hij de hiervoor genoemde termijn overschrijdt, met een maximum van €15.000,-.

[14] Ontvangen op 22 februari 2022.
[15] Ontvangen op 30 maart 2022.
[16] 2. Een overzicht van leveranciers van hacksoftware, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop een overeenkomst met het bedrijf is aangegaan, en (eventueel) gevolgd door een datum waarop de overeenkomst is beëindigd. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
[17] 3. Een overzicht van leveranciers waarvan expliciet niet hacksoftware afgenomen mag worden, inclusief wijzigingen in die lijst met het moment waarop die wijziging is ingetreden, zoals de naam van de leverancier, gevolgd door de datum waarop de leverancier op de lijst terecht is gekomen, eventueel gevolgd door een datum waarop de leverancier van de lijst is afgehaald. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden.
[18] 4. Documenten en communicatie die betrekking hebben op [naam bedrijf] art. 5.1 2e lid onder c. WOO , zoals overeenkomsten, nota's en e-mails over de screening van deze leverancier en de afwegingen van het aangaan, het afzien en het verbreken van een overeenkomst met deze leverancier.
[19] 5. Een overzicht van de onderzoeken naar leveranciers van hacksoftware. Hier wordt gevraagd om een lijst waarin duidelijk wordt naar wie het onderzoek is ingesteld, wanneer het onderzoek is gestart, wanneer het is afgerond, en wat de conclusie en adviezen voortkomend uit het onderzoek zijn. Indien een dergelijk overzicht niet bestaat, de brondocumenten op basis waarvan die documenten zelf een overzicht gemaakt kan worden.
[20] 6. Documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.
[21] III. Beslissing op het informatieverzoek van 5 juni 2019 onder punt 2, punt 3. en punt 5. met betrekking tot overzichtslijsten van leveranciers van hacksoftware. Bij de NP berust geen informatie als omschreven in het verzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 5 met betrekking tot overzichtslijsten van leveranciers van hacksoftware. De Wob is niet van toepassing op niet bestaande informatie en de Wob bevat geen verplichting om niet bestaande informatie te vervaardigen, ongeacht de mate van inspanning.
[22] IV. Beslissing op het informatieverzoek van 5 juni 2019 onder punt 4. met betrekking tot documenten en communicatie die betrekking hebben op [naam bedrijf] art. 5.1 2e lid onder c. WOO en onder punt 6. met betrekking tot documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware. Bij de NP berust informatie als omschreven in het verzoek van 5 juni 2019 onder punt 4 en 6. De openbaarmaking hiervan wordt integraal geweigerd omdat:
I. Dit het belang van de veiligheid van de Staat zou kunnen schaden, als bedoeld in artikel 10, eerste lid onder b van de Wob en/of;
II. Dit bedrijfs- en fabricagegegevens betreffen, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld, als bedoeld in artikel 10, eerste lid onder c. van de Wob en/of;
III. Het belang van openbaarmaking daarvan niet opweegt tegen het belang van: (1.) de betrekkingen van Nederland met andere staten en met internationale organisaties, als bedoeld in artikel 10, tweede lid onder a. van de Wob en/of (2.) de economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen, als bedoeld in artikel 10, tweede lid onder b. van de Wob en/of (3.) de opsporing en vervolging van strafbare feiten als bedoeld in artikel 10, tweede lid onder c. van de Wob en/of (d.) inspectie, controle en toezicht door bestuursorganen, als bedoeld in artikel 10, tweede lid onder d. van de Wob en/of (4.) de eerbiediging van de persoonlijke levenssfeer, als bedoeld in artikel 10, tweede lid onder e. van de Wob en/of (5.) het voorkomen van onevenredige bevoordeling of benadeling van bij de aangelegenheid betrokken natuurlijke personen of rechtspersonen dan wel van derden, als bedoeld in artikel 10, tweede lid onder g. van de Wob en/of (6.) het intern beraad, waarin persoonlijke beleidsopvattingen zijn opgenomen, als bedoeld in artikel 11 van de Wob.

Onderwerp
1.Aanvulling besluit van 28 maart 2022 onder III. punt 2., punt 3. en punt 5.
2. Wijziging besluit van 28 maart 2022 onder IV. punt 6.

AANTEKENEN
De Volkskrant B.V.
T.a.v art. 5.1. 2e lid onder e Woo
Postbus 1002
1000 BA AMSTERDAM

Organisatieonderdeel
Landelijke Eenheid
Staf
Afdeling Bestuursondersteuning
Juridische Zaken

Behandeld door
art. 5.1. 2e lid onder e Woo

Functie
Bedrijfsvoeringspecialist

Telefoon

E-mail
art. 5.1. 2e lid onder e Woo
art. 5.1. 2e lid politie.nl

Ons kenmerk
2019-0033028
5992

Uw kenmerk
2018054721

In afschrift aan

Datum
19 september 2022

Bijlage(n)
Besluit van 28 maart 2022

Pagina
1

Geachte art. 5.1. 2e lid onder e Woo

Gelet op en onder inhoudelijke verwijzing naar (1.) het informatieverzoek van 5 juni 2019, (2.) de besluitvorming van 28 maart 2022 en 11 april 2002, (3.) de op 26 april 2022 ingediende beroepsgronden en (4.) het gestelde tijdens de behandeling ter zitting van 3 augustus 2022 in de beroepsprocedure zaaknummer AMS 2022/1010, deel ik u het navolgende mede.

In het besluit van 28 maart 2022 onder III. is omschreven dat bij de Nationale Politie geen informatie berust als omschreven in het informatieverzoek van 5 juni 2019 onder punt 2. en/of punt 3. en/of punt 5 met betrekking tot overzichtslijsten van leveranciers van hacksoftware, de Wob niet van toepassing is op niet bestaande informatie en de Wob bevat geen verplichting om niet bestaande informatie te vervaardigen, ongeacht de mate van inspanning.

In het besluit van 28 maart 2022 onder IV. is omschreven dat bij de Nationale Politie informatie berust als omschreven in het informatieverzoek van 5 juni 2019 onder punt 4. met betrekking tot documenten en communicatie die betrekking hebben op [naam bedrijf] art. 5.1 2e lid onder c. WOO en onder punt 6. met betrekking tot documenten en communicatie tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware.

Hieromtrent overweeg ik als volgt met betrekking tot:

Het besluit van 28 maart 2022 onder III onder punt 2.

In het besluit van 28 maart 2022 onder III is, in zoverre het informatieverzoek onder punt 2. betreft, niet onderkend dat indien een overzichtslijst niet bestaat, verzocht is tot openbaarmaking van de brondocumenten met betrekking tot leveranciers van hacksoftware, op basis waarvan zelf een overzicht gemaakt kan worden.

Bij de Nationale Politie berusten (bron)documenten van een leverancier van hacksoftware. De openbaarmaking van deze (bron)documenten wordt integraal geweigerd.

Het besluit van 28 maart 2022 onder III onder punt 3.

In het besluit van 28 maart 2022 onder III is, in zoverre het informatieverzoek onder punt 3. betreft, niet onderkend dat indien een overzichtslijst met betrekking tot leveranciers waarvan expliciet geen hacksoftware afgenomen mag worden niet bestaat, verzocht is tot openbaarmaking van de brondocumenten met betrekking tot leveranciers waarvan expliciet geen hacksoftware afgenomen mag worden.

In het antwoord op vraag 12 van de leden Omtzigt (Omtzigt) en Jasper van Dijk (SP) heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Justitie en Veiligheid[1] omschreven: *"In het Regeerakkoord 2017-2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. Zoals aangegeven in de beantwoording van Kamervragen gaat het om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[2] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning".[3]*

De Woo is niet van toepassing op:

1. Al openbaar gemaakte documenten, zoals bovenvermeld document, waaruit zelf kan worden afgeleid van welke leverancier(s) en onder welke voorwaarde(n) (geen) hacksoftware afgenomen mag worden en
2. Op niet bestaande documenten.

Het besluit van 28 maart 2022 onder III onder punt 5.

In het besluit van 28 maart 2022 onder III is, in zoverre het informatieverzoek onder punt 5. betreft, niet onderkend dat indien een overzichtslijst met betrekking tot onderzoeken naar leveranciers van hacksoftware niet bestaat, verzocht is tot openbaarmaking van de brondocumenten met betrekking tot onderzoeken naar leveranciers van hacksoftware.

Bij de Nationale Politie berusten (bron)documenten met betrekking tot een verzoek tot screening van een leverancier van hacksoftware. De openbaarmaking van deze (bron)documenten wordt integraal geweigerd.

Het besluit van 28 maart 2022 onder IV. onder punt 6.

In het besluit van 28 maart 2022 onder IV. is, in zoverre het informatieverzoek onder punt 6. betreft, zoals reeds op zitting d.d. 3 augustus 2022 is aangegeven, abusievelijk vermeld dat bij de Nationale Politie documenten berusten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware. Er berusten geen documenten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware. De Woo is niet van toepassing op niet bestaande documenten. Het besluit van 28 maart 2022 onder punt 6 wordt in zoverre gewijzigd.

Besluit

I. Het besluit van 28 maart 2022 onder III. wordt, in zoverre het informatieverzoek van 5 juni 2019 onder punt 2. en 5. betreft aangevuld. De openbaarmaking van de (bron)documenten omschreven in het informatieverzoek van 5 juni 2019 onder punt 2. en punt 5. wordt integraal geweigerd omdat:

A. Dit het belang van de veiligheid van de Staat zou kunnen schaden, als bedoeld in artikel 5.1, eerste lid onder b van de Woo en/of;

B. Dit bedrijfs- en fabricagegegevens betreffen, die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld, als bedoeld in artikel 5.1, eerste lid onder c. van de Woo en/of;

C. Het belang van openbaarmaking daarvan niet opweegt tegen het belang van: (1.) De betrekkingen van Nederland met andere staten en met internationale organisaties, als bedoeld in artikel 5.2, tweede lid onder a. van de Woo en/of (2.) De economische of financiële belangen van de Staat, de andere publiekrechtelijke lichamen of de in artikel 1a, onder c en d, bedoelde bestuursorganen, als bedoeld in artikel 5.1, tweede lid onder b. van de Woo en/of (3.) De opsporing en vervolging van strafbare feiten als bedoeld in artikel 5.1, tweede lid onder c. van de Woo en/of (4.) Inspectie, controle en toezicht door bestuursorganen, als bedoeld in artikel 5.2, tweede lid onder d. van de Woo en/of (5.) De eerbiediging van de persoonlijke levenssfeer, als bedoeld in artikel 5.1, tweede lid onder e. van de Woo en/of (6.) de bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens, als bedoeld in artikel 5.1, tweede lid onder f. van de Woo (7.) de beveiliging van personen en bedrijven en het voorkomen van sabotage, als bedoeld in artikel 5.1, tweede lid onder h. van de Woo en/of (8.) Het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen als bedoeld in artikel 5.1, tweede lid onder i. van de Woo en/of (9.) Het intern beraad, waarin persoonlijke beleidsopvattingen zijn opgenomen, als bedoeld in artikel 5.2, eerste lid van de Woo.

In een Woo-besluit dient de uitkomst van de belangenafweging in beginsel per informatiedrager of per onderdeel daarvan te worden gemotiveerd waarom die informatie of (onder)deel daarvan niet openbaar kan worden gemaakt, zie onder meer ECLI:NL:RVS:2018:666. Bij de onderhavige beslissing kan een andere dan een 'kale' motivering niet worden gegeven zonder zicht te bieden op de aard of de inhoud van de informatie, zie uitspraak ABRvS van 28 december 1999 inzake no. 199901860/1 en 199901860/2, ECLI:NL:RVS:2003:AF2889 en ECLI:NL:RVS:2013:1209.

Hieruit vloeit voort, dat de afweging van de bovenvermelde onder II. omschreven belang(en) niet verder te motiveren is (zijn), zonder prijs te geven wat met toepassing van de onder II. omschreven artikel(en) van de Wob aan de openbaarheid wordt onthouden. Daarom kan niet meer specifiek op de weigering van de informatie worden ingegaan.

In bovenvermelde context wordt opgemerkt, dat binnen het kader van de in artikel 8:29 van de Algemene wet bestuursrecht (Awb) opgenomen procedure de rechter kan beoordelen of een bestuursorgaan met betrekking tot de stukken tot een juiste beslissing inzake de niet openbaarmaking is gekomen. Op die wijze vindt een controle plaats op de beoordeling door het bestuursorgaan van de in de Wob omschreven beperkingen en uitzonderingen.

II. Het besluit van 28 maart 2022 onder III. wordt, in zoverre het informatieverzoek van 5 juni 2019 onder punt 3. betreft, aangevuld. De Woo is niet van toepassing op (1.) al openbaar gemaakte documenten waaruit zelf kan worden afgeleid van welke leverancier(s) en onder welke voorwaarde(n) (geen) hacksoftware afgenomen mag worden en (2.) op niet bestaande documenten.

III. Het besluit van 28 maart 2022 onder IV. wordt, in zoverre het informatieverzoek van 5 juni 2019 onder punt 6. betreft, gewijzigd. Bij de Nationale Politie berusten geen documenten tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware. De Woo is niet van toepassing op niet bestaande documenten.

Hoogachtend,

De korpschef van politie,
namens deze,
De politiechef van de Landelijke Eenheid,
namens deze,

art. 5.1. 2e lid onder e Woo

Rechtsbescherming

Ingevolge artikel 6:19, eerste lid van de Awb heeft het bezwaar van 12 december 2019 gericht tegen het besluit van 5 november 2019 van rechtswege mede betrekking op het besluit van 28 maart 2022 en het besluit van 19 september 2022. Het besluit van 19 september 2022 is overeenkomstig artikel 6:19, derde lid van de Awb onverwijld ter beschikking gesteld aan de rechtbank Amsterdam, afdeling bestuursrecht, zaaknummer AMS 22 /1010.

[1] Kamerstukken, TK, 2021/2022, Aanhangsel Handelingen, vergaderjaar 2021-2022, nr. 3537.
[2] Handelingen I 2017-2018, 34, item 5, p. 29.
[3] Kamerstukken, TK, 2018/2019, Aanhangsel Handelingen, vergaderjaar 2018-2019, nr. 3537.

POLITIE

Afzender
Staf Bestuursondersteuning
woo.team-bestuursondersteuning.
Landelijke-Eenheid@politie.nl
+31 [redacted]

AANTEKENEN
De Volkskrant B.V.
T.a.v. [redacted]
Postbus 1002
1000 BA AMSTERDAM

Rubricering
-

Datum	26 januari 2023	**Behandeld door**	[redacted]
Ons kenmerk	2019-0033028 7207	**Kopie aan**	--
Uw kenmerk	2018054721	**Bijlage(n)**	Concept nota leveranciers binnendringsoftware Document 01 t/m 82

Onderwerp Beslissing op bezwaar

Geachte [redacted],

I. Informatieverzoek / procesverloop

Bij brief van 5 juni 2019 is een informatieverzoek ingediend op grond van de Wet openbaarheid van bestuur (Wob).

Hierop is bij besluit van 5 november 2019 kenmerk 2019-00330285992 beslist.

~~Bij brief van 12 december 2019 is een bezwaarschrift ingediend gericht tegen het besluit van 5~~ november 2019.

Bij brief van 7 januari 2020 kenmerk 2019-0033028 7207 is de (voorbereiding op de) besluitvorming in het voorliggende bezwaar uitgesteld tot na de uitspraak van de hoger beroepsprocedure, zaaknummer 201708552/1/A3.

Bij brief van 9 januari 2020 is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019.

Bij brief van 6 februari 2020 is een ingebrekestelling ingediend wegens het niet tijdig nemen van een beslissing op het bezwaar van 12 december 2019.

In de uitspraak van 28 april 2021 (ECLI:NL:RVS:2021:911) heeft de Afdeling bestuursrechtspraak van de Raad van State zaaknummer 201708552/1/A3 beslist.

Bij brief van 7 juni 2021 is een ingebrekestelling ingediend wegens het niet tijdig nemen van een beslissing op het bezwaar van 12 december 2019.

Bij brief van 24 juli 2021 is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019.

Op 20 augustus 2021 heeft de rechtbank Amsterdam in zaaknummer AMS 21 / 238 WOB beslist op het bij brief van 9 januari 2020 ingestelde beroep wegens niet tijdig beslissen op het bezwaar van 12 december 2019.[1]

Op 19 november 2021 heeft de rechtbank Amsterdam in zaaknummer AMS 21 / 3394 WOB beslist op het bij brief van 24 juli 2021 ingestelde beroep wegens niet tijdig beslissen op het bezwaar van 12 december 2019.[2]

Bij brief van 17 februari 2022 is beroep ingesteld wegens niet tijdig beslissen op het bezwaar van 12 december 2019.

Bij besluit van 28 maart 2022 is beslist dat:

I. Het primaire besluit van 5 november 2019 wordt ingetrokken voor zover het onderdeel B betreft,
II. Voor wat de punten 2, 3 en 5 van het Wob-verzoek betreft niet wordt beschikt over overzichtslijsten van leveranciers van hacksoftware en de Wob niet verplicht om niet-bestaande informatie te vervaardigen,
III. Voor wat punt 4 en punt 6 van het Wob-verzoek betreft, de aangetroffen documenten integraal worden geweigerd.

Bij besluit van 11 april 2022 is het bezwaar van 12 december 2019 gegrond verklaard en verwezen naar de motivering in het besluit van 28 maart 2022.

Bij besluit van 19 september 2022 is beslist dat:

I. In het besluit van 28 maart 2022 onder III, in zoverre het informatieverzoek onder punt 2. betreft, niet onderkend is dat indien een overzichtslijst met betrekking tot leveranciers van hacksoftware niet bestaat, verzocht is tot openbaarmaking van de brondocumenten op basis waarvan zelf een overzicht gemaakt kan worden,
II. Openbaarmaking van de bij de Nationale Politie berustende (bron)document(en) van een leverancier van hacksoftware integraal wordt (worden) geweigerd,
III. Bij de Nationale Politie geen documenten berusten die zijn verzonden tussen de Nationale Politie en het Ministerie van Buitenlandse Zaken aangaande adviezen over leveranciers van hacksoftware,
IV. De Woo niet van toepassing is op niet bestaande en op al openbaar gemaakte documenten.

Op 1 december 2022 heeft de rechtbank Amsterdam in zaaknummer AMS 22 / 1010 beslist op het bij brief van 17 februari 2022 ingestelde beroep wegens niet tijdig beslissen op het bezwaar van 12 december 2019.[3]

II. Overwegingen

Bij de Nationale Politie berusten twee conceptnota's Leveranciers binnendringsoftware versie 13 maart 2019 (hierna: conceptnota) zijnde één conceptnota zonder opmerkingen in de kantlijn en één conceptnota voorzien van opmerkingen in de kantlijn.

Bij het bestreden besluit van 5 november 2019 zijn bovenvermelde conceptnota's deels openbaar en deels niet openbaar gemaakt.

A. Ten aanzien van de conceptnota Leveranciers binnendringsoftware versie 13 maart 2019

De verstrekking van informatie aan de Tweede Kamer met betrekking tot het beleid dat wordt gevoerd ten aanzien van aanschaf van binnendringsoftware[4] heeft invloed op de thans voorliggende besluitvorming om bepaalde (onder)delen van de conceptnota's al dan niet openbaar te maken.

1. Ten aanzien van de niet openbaarmaking van (onder)delen van de conceptnota

In de ten behoeve van intern beraad opgestelde conceptnota is met betrekking tot de aanschaf van binnendringsoftware een onderscheid gemaakt tussen leveranciers binnen de Europese Unie en leveranciers buiten de Europese Unie. Hierin is onder meer omschreven dat in de periode tussen de implementatie van de conceptverordening 2016/0295 en de inwerkingtreding van het beleid inzake binnendringsoftware het regime voor leveranciers buiten de Europese Unie (waarvoor het exportcontrole regime niet geldt) zal worden gevolgd, tenzij een leverancier alleen zaken doet met lidstaten.

In de conceptnota zijn met betrekking tot leveranciers buiten de Europese Unie visies en/of standpunten en/of overwegingen ten behoeve van intern beraad omschreven, waaraan dient te zijn voldaan voordat over wordt gegaan tot de aanschaf van binnendringsoftware.

Op 26 juli 2019 is door de verstrekking van informatie aan de Tweede Kamer het beleid ten aanzien van aanschaf van binnendringsoftware openbaar gemaakt.[5]

Op grond hiervan (1.) worden leveranciers van binnendringsoftware gescreend door de AIVD, (2.) mogen leveranciers van binnendringsoftware die wordt ingekocht door opsporingsdiensten niet leveren aan dubieuze regimes [6] en (3.) om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware, waarin (a.) de leverancier wordt gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en (b.) wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.

Hieruit volgt, dat op 26 juli 2019, het moment van openbaarmaking van het beleid ten aanzien van de aanschaf van binnendringsoftware in de conceptnota (1.) concept beleidsteksten en/of (2.) persoonlijke beleidsopvattingen, zoals visies en/of standpunten en/of overwegingen ten behoeve van intern beraad zijn opgenomen / omschreven, die afwijken van het op 26 juli 2019 openbaar gemaakte beleid ten aanzien van de aanschaf van binnendringsoftware.

In bovenvermelde context wordt vermeld, dat in de kantlijn van de conceptnota door een beperkte kring van) de betrokken ambtena(a)r(en) achter het woord 'Met opmerkingen' visies en/of standpunten en/of overwegingen ten behoeve van intern beraad zijn omschreven, waarin diens (hun) visie en/of standpunt over bepaalde (onder)delen van de conceptnota kenbaar wordt (worden) gemaakt.

Hieruit volgt, dat

a. In de conceptnota concept beleidsteksten zijn opgenomen die (mogen) worden geweigerd op grond van artikel 5.2. eerste lid van de Woo[7],
b. In de conceptnota visies en/of standpunten en/of overwegingen ten behoeve van intern beraad zijn opgenomen die afwijken van het vastgestelde beleid tot de aanschaf van binnendringsoftware, die (mogen) worden geweigerd op grond van artikel 5.2. eerste lid van de Woo en
c. In de kantlijn van de conceptnota achter het woord 'Met opmerkingen' visies en/of standpunten en/of overwegingen ten behoeve van intern beraad zijn opgenomen die persoonlijke beleidsopvattingen bevatten bedoeld in artikel 5.2. eerste lid van de Woo en
d. Verstrekking van de hiervoor onder (c.) omschreven persoonlijke beleidsopvattingen in een niet tot personen te herleiden vorm niet in het belang is van een goede en democratische bestuursvoering, omdat hierin door de betrokken ambtena(a)r(en) diens (hun) visie(s) en/of standpunt(en) over bepaalde (onder)delen van de conceptnota kenbaar wordt (worden) gemaakt en om die reden (mogen) worden geweigerd op grond van artikel 5.2., tweede lid van de Woo.

In bovenvermelde context wordt ten overvloede vermeld, dat de conceptnota niet ouder is dan vijf jaar, zodat hierop artikel 5.3 van de Woo niet van toepassing is.

Conclusie

1. De in de conceptnota opgenomen concept beleidsteksten en persoonlijke beleidsopvattingen worden niet openbaar gemaakt;
2. De in de conceptnota in de kantlijn opgenomen persoonlijke beleidsopvattingen worden niet (in een niet tot personen herleidbare vorm) openbaar gemaakt;
3. Artikel 5.3 van de Woo is niet van toepassing op de conceptnota.

In zoverre het dit onderdeel betreft, is het bezwaar ongegrond.

2. Ten aanzien van de openbaarmaking van (onder)delen van de conceptnota

Bij het onderhavige besluit worden de navolgende in de conceptnota opgenomen feiten en/of andere in de concept nota opgenomen (onder)delen met een overwegend objectief karakter, niet zijnde persoonlijke beleidsopvattingen, openbaar gemaakt:

1. Onder het kopje 'Screening AIVD':
   De zin in de 1e alinea beginnende met het woord 'De' tot en met het woord 'veiligheid', het woord 'Het' tot en met het woord 'AIVD' en het woord 'Wanneer' tot en met het woord 'screening'.
2. Onder het kopje 'Levering van binnendringsoftware aan dubieuze regimes':
   De zin in de 2e alinea beginnende met het woord 'Er' tot en met het woord 'gehandeld' en de zin in de 3e alinea beginnende met het woord 'Bestaande ' tot en met het woord 'technologie'.
3. Onder het kopje Leveranciers binnen de Europese Unie:
   De zin in de 2e alinea beginnende met het woord 'In' tot en met het woord 'lidstaten'.
4. Onder het kopje 'Leveranciers buiten de Europese Unie':
   De zin in de 1e alinea beginnende met het woord 'Voor' tot en met het woord 'verordening' en de zin beginnende met het woord 'Het' tot en met het woord 'schaffen'.
   Het kopje 'Stap 1' en de zin onder Stap 1 beginnende met het woord 'Het' tot en met het woord 'raadplegen'.
   Het kopje 'Stap 2' en in de 2e alinea de zin beginnende met het woord 'De' tot en met het woord 'recht'.
5. De zin 'Zie bijlage 2 voor de uitwerking van deze vragen'.

6. Het kopje 'Stap 3'.
7. Het kopje 'Rol van de overheid'.
8. Het kopje 'Toekomstig handelen van een leverancier' en in de 1e alinea de zin beginnende met het woord 'Een' tot en met het woord 'doorlopen', de zin beginnende met het woord 'Een' tot en met het woord 'mogelijk' en de zin beginnende met 'Deze' tot en met '3'.
9. Het kopje 'Bijlage 2'
   De zin achter 1. beginnende met het woord '[een' tot en met het woord 'verbintenissen' en de zinsnede achter de bullet • beginnende met het woord 'aan' tot en met het woord Unie'.
   De zin achter 2. beginnende met het woord 'Criterium' tot en met het woord 'land', de zin achter de eerste bullet • beginnende met het woord 'In tot en met het woord 'beginselen' en de zin achter de derde bullet o beginnende met het woord 'Heeft' tot en met het woord 'geconstateerd'.
10. De tekst achter voetnoot 4, 5 en 11 tot en met 17.

Conclusie

1. De Woo is niet van toepassing op de bij besluit van 5 november 2019 al openbaar gemaakte informatie.
2. De bovenvermelde onder 1. tot en met 10. vermelde feiten en/of andere (onder)delen met een overwegend objectief karakter, niet zijnde persoonlijke beleidsopvattingen bedoeld in artikel 5.2, eerste lid van de Woo, worden openbaar worden gemaakt.

In zoverre het bovenvermelde onder 1. betreft, is het bezwaar ongegrond.
In zoverre het bovenvermelde onder 2. betreft, is het bezwaar gegrond.

Met inachtneming van en onder verwijzing naar de uitspraak van de rechtbank Amsterdam van 1 december 2022 in zaaknummer 22 / 1010 wordt als volgt besloten.

3. Ten aanzien van de deels (niet) openbaarmaking van niet-inhoudelijke e-mail.

De rechtbank Amsterdam overweegt in de uitspraak van 1 december 2022 in zaaknummer AMS 22/1010 dat (1.) een beperkt deel van de documenten ziet op correspondentie tussen personen waarbij geen sprake is van zaaksinhoudelijke mededelingen, (2.) deze documenten met het lakken van persoonsgegevens, mailadressen, data en locatievermeldingen openbaar gemaakt kunnen worden en (3.) de korpschef bij de nieuw te nemen beslissing op bezwaar met inachtneming van deze overwegingen van de rechtbank zelf een selectie moeten maken van de documenten die wel deels openbaar kunnen worden gemaakt. Op grondslag hiervan is een selectie gemaakt van 82 documenten.

Conclusie

De documenten voorzien het nummer 01 tot en met 82 worden, behoudens de daarin vermelde persoonsgegevens, mailadressen, data en locatievermeldingen, deels openbaar gemaakt.

III. Besluit

A. Het bezwaar van 12 december 2019 gericht tegen het bij besluit van 5 november 2019 onder A. waarin de conceptnota deels (niet) openbaar is gemaakt, wordt deels (on)gegrond verklaard.
B. Het bezwaar van 12 december 2019 gericht tegen het besluit van 11 april 2022 niet inhoudelijk beslissen op het bezwaar van 12 december 2019 onder A., wordt gegrond verklaard.
C. Het bezwaar van 12 december 2019 gericht tegen (1.) het besluit van 5 november 2019 onder B., (2.) het besluit van 28 maart 2022 onder I., II en II en (3.) het besluit van 19 september 2022 wordt deels (on)gegrond verklaard.
D. De conceptnota wordt, behoudens de daarin opgenomen persoonsgegevens, bedoeld in artikel 5.1 tweede lid onder e. van de Woo en behoudens de daarin persoonlijke beleidsopvattingen, bedoeld in artikel 5.2, eerste lid van de Woo, deels openbaar gemaakt.
E. De in de kantlijn van de conceptnota achter het woord 'opmerkingen' opgenomen persoonlijke beleidsopvattingen, bedoeld in artikel 5.2. eerste lid van de Woo, worden niet (in een niet tot personen te herleiden vorm) openbaar gemaakt.
F. De documenten (e-mails) voorzien van het nummer 1 tot en met 82 die betrekking hebben op correspondentie tussen personen waarbij geen sprake is van zaaksinhoudelijke mededelingen, worden behoudens de daarin vermelde persoonsgegevens, mailadressen, data en locatievermeldingen, bedoeld in artikel 5.1 tweede lid onder e. van de Woo deels openbaar gemaakt.
G. De Woo is niet van toepassing op al openbaar gemaakte informatie dan wel op informatie die zelf uit al openbaar gemaakte informatie kan worden afgeleid.

De korpschef van politie,
Voor deze,
De Politiechef Landelijke Eenheid

art 5.1, 2e lid onder e. WOO

O.R. Dros

Rechtsbescherming

Belanghebbenden kunnen binnen zes weken na bekendmaking van dit besluit beroep instellen bij de rechtbank, binnen het rechtsgebied waarvan de indiener van het beroepschrift zijn woonplaats in Nederland heeft. Indien de indiener van het beroep geen woonplaats in Nederland heeft, is de rechtbank binnen het rechtsgebied waarvan het bestuursorgaan zijn zetel heeft bevoegd. Het beroepschrift moet op grond van artikel 6:5 van de Awb zijn ondertekend en ten minste bevatten: de naam en het adres van de indiener, de dagtekening, de omschrijving van het besluit waartegen het beroep is gericht, zo mogelijk een afschrift van dit besluit, en de gronden waarop het beroepschrift rust. Nadere informatie over de hoogte van het griffierecht en de wijze van betalen wordt door de griffie van de rechtbank verstrekt.

U kunt ook digitaal beroep instellen bij de rechtbank via http://loket.rechtspraak.nl/ bestuursrecht. Daarvoor moet u wel beschikken over een elektronische handtekening (DigiD). U kunt op de genoemde site de precieze voorwaarden vinden.

[1] In de uitspraak van 20 augustus 2021 verklaart de rechtbank het beroep gegrond; draagt verweerder op binnen twee weken na de dag van verzending van deze uitspraak een besluit op het bezwaar te nemen; bepaalt dat verweerder aan eiseres een dwangsom van €100, - verbeurt voor elke dag waarmee hij de hiervoor genoemde termijn overschrijdt, met een maximum van € 15.000, - en draagt verweerder op het betaalde griffierecht van 360, - aan eiseres te vergoeden.

[2] In de uitspraak van 19 november 2021 verklaart de rechtbank het beroep niet-ontvankelijk.

[3] In de uitspraak van 1 december 2022 verklaart de rechtbank het beroep tegen het bestreden besluit gegrond voor zover daarbij de Nota Leveranciers binnendringsoftware versie 13 maart 2019, behoudens persoonsgegevens en persoonlijke beleidsopvattingen, niet volledig is geopenbaard; vernietigt het bestreden besluit voor zover daarbij de Nota Leveranciers binnendringsoftware versie 13 maart 2019, behoudens de persoonsgegevens en persoonlijke beleidsopvattingen, niet volledig is geopenbaard; draagt de korpschef op de Nota Leveranciers binnendringsoftware versie 13 maart 2019, behoudens persoonsgegevens en persoonlijke beleidsopvattingen, openbaar te maken; bepaalt dat deze uitspraak in zoverre in de plaats treedt van het vernietigde gedeelte van het bestreden besluit; verklaart het beroep tegen het bestreden besluit van 19 september 2022 gegrond en draagt de korpschef op om met inachtneming van wat de rechtbank heeft geoordeeld in overweging 13 van deze uitspraak binnen zes weken een nieuwe beslissing op bezwaar te nemen en draagt de korpschef op het betaalde griffierecht van € 365, - aan eiseres te vergoeden.

[4] **Vergaderjaar 2018–2019 Aanhangsel van de Handelingen 3537 (d.d. 26-07-2019)**
Antwoord 6:
Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en leveren niet aan dubieuze regimes. [voetnoot 7 Regeerakkoord 2017–2021 Vertrouwen in de Toekomst] Het gaat dan om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[voetnoot 8: Handelingen I 2017/18, 34, item 5, p. 29] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.
Vergaderjaar 2021–2022 Aanhangsel van de Handelingen 3252 (d.d.22-06-2022)
Antwoord 12:
In het Regeerakkoord 2017–2021 is vastgelegd dat leveranciers van hacksoftware die wordt ingekocht door opsporingsdiensten niet mogen leveren aan dubieuze regimes. Zoals aangegeven in de beantwoording van Kamervragen gaat het om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[voetnoot 3 Handelingen I 2017/18, 34, item 5, p. 29.] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.[voetnoot 4 Kamerstukken, TK, 2018/2019, Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3537.] De politie past dit beleid toe en eist van leveranciers een bevestiging dat niet aan zulke dubieuze regimes wordt geleverd. Aanvullend hierop wordt door de politie deze toets periodiek herhaald.
Vergaderjaar 2022–2023 Aanhangsel van de Handelingen 1171 (d.d. 23-12-2022)
Antwoord 4
Zoals aangegeven in de Kamervragen van de leden Omtzigt (CDA) en van Dijk (SP) (Aanhangsel Handelingen, vergaderjaar 2021–2022, nr. 3252) mogen leveranciers van binnendringsoftware die wordt ingekocht door opsporingsdiensten niet leveren aan dubieuze regimes. Het gaat om landen die zich schuldig maken aan ernstige schendingen van mensenrechten of internationaal humanitair recht.[voetnoot 5 Handelingen I 2017/18, 34, item 5, p. 29.] Om deze reden voert de politie een toets uit voordat over wordt gegaan tot de aanschaf van binnendringsoftware. In deze toets wordt de leverancier gevraagd niet te hebben geleverd aan landen waartegen vanuit de EU of de VN restrictieve sancties bestaan en wordt gecontroleerd of in het land waar de leverancier is gevestigd een exportcontroleregime bestaat waar het respecteren van mensenrechten een onderdeel is in de beoordeling voor het verstrekken van een exportvergunning.[voetnoot 6 Kamerstukken, TK, 2018/2019, Aanhangsel Handelingen, vergaderjaar 2018–2019, nr. 3537.] De politie past dit beleid toe en eist van leveranciers een bevestiging dat niet aan dergelijke landen wordt geleverd. Aanvullend hierop wordt door de politie deze toets periodiek herhaald.

[5] Zie onder meer Vergaderjaar 2018–2019 Aanhangsel van de Handelingen 3537. (d.d. 26-07-2019)

[6] Een dubieus regime is aan de Eerste Kamer omschreven als een land dat zich schuldig maakt aan ernstige schendingen van mensenrechten of internationaal humanitair recht. Handelingen EK 34, p.29.

[7] Zie onder meer de uitspraak van de Afdeling bestuursrechtspraak van de Raad van State van 1 september 2010 (ECLI:NL:RVS:2010:BN5699) en de uitspraak van de rechtbank Amsterdam van 5 augustus 2019 (ECLI:NL:RBAMS:2019:5720).

Ministerie van Justitie en Veiligheid

Dep. VERTROUWELIJK
Beleidsnota

Versie **13 maart 2019**

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e

T 070 5.1.2.e
F 070 5.1.2.e

Datum

Ons kenmerk

nota

Leveranciers binnendringsoftware

Aanleiding

In het regeerakkoord 'Vertrouwen in de Toekomst' van het kabinet Rutte III staat de volgende passage over het wetsvoorstel Computercriminaliteit III:

"Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen." [1]

Deze beleidsnota zet uiteen welk beleid wordt gevoerd binnen de opsporing ten aanzien van aanschaf van binnendringsoftware van particuliere leveranciers.

Beleid

Het regeerakkoord vereist dat leveranciers van binnendringsoftware worden gescreend door de AIVD en dat deze leverancier niet aan dubieuze regimes verkopen. Commerciële binnendringsoftware is prominent onderwerp geweest in het debat over de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Commerciële binnendringsoftware maakt (mogelijk) gebruik van onbekende kwetsbaarheden in software. In plaats dat deze kwetsbaarheid wordt gemeld waardoor de software veiliger wordt, wordt deze kwetsbaarheid commercieel geëxploiteerd. Daarnaast kunnen leveranciers van deze software ook leveren aan regimes die de producten kunnen gebruiken voor het (ernstig) schenden van mensenrechten. Om de markt van binnendringsoftware niet meer dan strikt noodzakelijk te betreden is de aanschaf beperkt tot een specifieke zaak en worden aanvullende eisen gesteld aan leveranciers. Deze eisen betreffen 1) screening door de AIVD, 2) beoordeling of een bedrijf heeft geleverd aan dubieuze regimes.

Wat is binnendringsoftware?
Voor binnendring software wordt de definitie van de concept-verordening 2016/0295, annex I als uitgangspunt gebruikt.

[1] Regeerakkoord 2017-2021 'Vertrouwen in de toekomst'.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

De actualisering van de verordening is nog gaande daarmee staat de definitie nog niet vast.

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht:

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Zie bijlage 1 voor de (technische) noten die horen bij deze definitie.

Binnen de wet Computercriminaliteit III is onderscheid gemaakt tussen het technisch hulpmiddel dat bewijs vergaart en binnendringsoftware die de beveiliging van een geautomatiseerd werk doorbreekt. Het technisch hulpmiddel wordt geïnstalleerd nadat toegang is verkregen tot een geautomatiseerd werk. Binnendringsoftware omzeilt de beschermende tegenmaatregelen van een computer of apparaat met netwerkcapaciteit. Het beleid in deze nota zich op binnendringsoftware.

Screening AIVD
De screening van de AIVD ziet op de eventuele dreiging die een leverancier vormt voor de nationale veiligheid. Het beoordelen met het oog op mensenrechtenschendingen is geen onderdeel van de wettelijke taak van de AIVD. Wanneer een onderhandeling met een bedrijf zich in de slotfase bevindt kan de politie contact zoeken met het ministerie van Justitie en Veiligheid om een verzoek richting het Ministerie van Binnenlandse Zaken te doen uitgaan voor een dergelijke screening.

Levering van binnendringsoftware aan dubieuze regimes
Binnendringsoftware kan een essentieel middel zijn in de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk, maar kan ook worden misbruikt door repressieve regimes. Het is een zogenaamd product voor tweeërlei gebruik[2], oftewel een dual-use goed. In de kamerbrief over kwetsbaarheden in hard- en software van november 2016 staat dat de regering hecht aan beperking van uitvoer van ICT-goederen en –software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] In onderstaand beleid wordt uiteengezet hoe hier in het kader van de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk vorm aan wordt gegeven.

[2] COM(2016), 2016/0295
[3] Kamerstukken TK, 2016/17, 26 643, nr. 428

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

Binnen het recht of beleid bestaat geen eenduidige definitie van een dubieus regime. Er wordt daarom zoveel mogelijk aangesloten bij bestaande regelgeving die ziet op soortgelijke materie of in de geest van toekomstige regelgeving, zoals verordening 2016/0295, gehandeld.

Bestaande regelgeving die dient als inspiratie voor het beleid zijn onder andere The Wassenaar Arrangement het beleid in omringende landen[4], en het beleid rond controle op de uitvoer van militaire goederen en technologie.[5].

Bij The Wassenaar Arrangement wordt de reikwijdte van de export controle bepaald door de lijsten die zijn opgesteld onder het arrangement, de praktische implementatie varieert van land tot land.[6] Er zijn ook zogenaamde 'best practices' gepubliceerd. De bescherming van mensenrechten speelt in deze best practices een rol bij de uitvoer van conventionele wapens, handvuurwapens en lichte wapens, maar nog niet bij 'intrusion software'. Deze software wordt wel genoemd in de lijst met dual-use items. In de categorie computers (p. 79) wordt *software* die speciaal ontwikkeld of aangepast is voor de ontwikkeling, controle, of aflevering van 'intrusion software' op de dual-use lijst geplaatst, alsook de *technologie* voor de ontwikkeling van 'intrusion software' (p. 80).[7] [Nota bene, het arrangement reguleert niet de binnendringsoftware zelf, maar software of technologie die deze software ontwikkelt, controleert of aflevert.] De definitie van 'intrusion software' komt overeen met die uit de concept-verordening 2016/0295 (p. 221)[8] [9] . 5.2. 1 [redacted]. Het staat Nederland vrij om een strikter regime te creëren.

Leveranciers binnen de Europese Unie

In de Europese Unie bestaat sinds 2009 een verordening die een exportcontrole regime vereist op dual-use goederen[10]. Een dergelijk regime stelt voorwaarden aan exporteurs van dual-use goederen om misbruik te voorkomen. 5.2. 1 [redacted]. 5.2. 1 [redacted]. De Europese Commissie is bezig deze te actualiseren en heeft in haar ontwerpverordening voorgesteld om

[4] UK Department of Business Innovation and Skills, Export Control Organisation, Notice to Exporters 2015/24 : Intrusion Software Tools and Export Control , 10082015

[5] GEMEENSCHAPPELIJK STANDPUNT 2008/944/GBVB VAN DE RAAD

[6] https://www.wassenaar.org/about-us/#faq

[7] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public documents Volume II List of Dual-Use Goods and Technologies And Munitions List (December 2018)

[8] Idem.

[9] Annex I, COM(2016, 2016/0295: p. 2, p.15

[10] VERORDENING (EG) Nr. 428/2009 VAN DE RAAD

[11] Publicatieblad van de Europese Unie Nr. L 335 van 13-12-2008 vanaf pag.99 (directe link http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:nl:PDF)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

'technologieën voor cybertoezicht' onder het exportcontrole regime te brengen[12]. "Inbraakprogrammatuur" (intrusion software)is onderdeel van deze technologieën voor cybertoezicht en zoals in tabel 1 aangegeven is binnendringsoftware een onderdeel van deze definitie .[13] Het Europees Parlement heeft op het moment van het schrijven van deze nota reeds haar amendementen aangenomen[14], de Raad poogt om voor de Europese verkiezingen een algemene oriëntatie aan te nemen[15].

Wanneer deze verordening in werking treedt moeten Europese producenten voldoen aan de eisen in de verordering, waaronder de controle op het mogelijke schenden van mensenrechten door de software. Europese leveranciers dienen dan daarmee aan de eisen uit het regeerakkoord 2017-2021 'Vertrouwen in de Toekomst' te voldoen. In de periode tussen de implementatie van de concept-verordening 2016/0295 en de inwerkingtreding van het beleid inzake binnendringsoftware zal het regime voor leveranciers buiten de Europese Unie worden gevolgd, tenzij een leverancier alleen zaken doet met lidstaten.

Leveranciers buiten de Europese Unie

Voor leveranciers buiten de Europese Unie geldt het exportcontrole regime niet en zij bevinden zich niet in een lidstaat die middels de Unie werkt aan een ruimte van vrijheid, veiligheid en recht (art. 67 VWEU). Voor een invulling van het begrip van 'dubieuze regimes' wordt aangesloten bij bestaande instrumenten, zoals The Wassennaar arrangenment, en toekomstige instrumenten zoals de actualisering van de dual-use verordening. 5.2. 1 . 5.2. 1 . Het klantenbestand van een bedrijf is veelal om legitieme redenen commercieel vertrouwelijk. Om het risico dat zaken worden gedaan met een leverancier die zaken doet met een dubieus regime zoveel mogelijk uit te sluiten worden leveranciers op drie wijzen getoetst alvorens binnendringsoftware aan te schaffen.

Stap 1

Het bedrijf wordt gevraagd om uit te sluiten dat het producten levert aan landen waartegen de Europese Unie restrictieve sancties heeft ingesteld. Binnen de Raad van de Europese Unie wordt hiervoor een lijst bijgehouden van EU en VN sancties: https://www.sanctionsmap.eu/#/main[16]. Deze lijsten zijn openbaar en voor een bedrijf gemakkelijk te raadplegen.

Stap 2

5.2. 1 . 5.2. 1

[12] COM(2016), 2016/0295

[13] COM(2016), 2016/0295, hoofdstuk II

[14] P8_TA(2018)0006

[15] TK 2018/2019, 21 501-02, 1934

[16] NB men ziet de VS op deze lijst staan, maar geen restrictieve sancties vermeld staan. De VS is daarom geen land dat wordt uitgesloten.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

5.2. 1

De vragen die moeten worden beantwoord zien 1) op de naleving van de internationale verplichtingen en verbintenissen van het land van bestemming, 2) de eerbiediging van mensenrechten en de naleving van het internationaal humanitair recht, 3) 5.2. 1
4) 5.2. 1
5) 5.2. 1
en 6)

Zie bijlage 2 voor de uitwerking van deze vragen.

Stap 3

5.2. 1

17
https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/richtlijnen/2018/02/21/richtlijnen-voor-het-opstellen-van-een-internal-compliance-programme-icp/Richtlijnen+voor+het+opstellen+van+een+Internal+Compliance+Programme.pdf

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

5.2. 1 [redacted]

Rol overheid

5.2. 1 [redacted]

Toekomstig handelen van een leverancier

Een toets is een momentopname in het specifieke geval. Doet de mogelijkheid zich voor dat wederom software van een eerder getoetste leverancier moet worden aangeschaft worden de stappen 1,2 en 3 wederom doorlopen. Een verkorte procedure is mogelijk 5.2. 1 [redacted] . 5.2. 1 [redacted] . Deze verkorte procedure bestaat uit een verklaring dat er geen wijzigingen zijn in de eerder gegeven beantwoording bij stap 1,2 en 3.

Bijlage 1 Definitie Inbraakprogrammatuur

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: .

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Noten:

1."Inbraakprogrammatuur" omvat niet het volgende: .
a.‹hypervisors›, ‹debuggers› of hulpmiddelen voor de reverse engineering van programmatuur (SRE); .
b."programmatuur" voor het beheer van digitale rechten (DRM); of .
c."programmatuur" die is ontworpen voor installatie door de fabrikanten, beheerders of gebruikers met het oog op goederenbewaking of -herstel. .
2.Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters.

Technische noten:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1.'Bewakingshulpmiddelen': "programmatuur" of hardwareapparaten die het systeemgedrag of de processen die op een apparaat worden uitgevoerd, bewaken. Dit omvat antivirus (AV)-producten, producten voor eindpuntbeveiliging, producten voor persoonlijke veiligheid (PSP: Personal Security Products), inbraakdetectiesystemen (IDS: Intrusion Detection Systems), inbraakpreventiesystemen (IPS: Intrusion Prevention Systems) of firewalls. .

2.'Beschermende tegenmaatregelen': technieken die zijn ontworpen om te zorgen voor de veilige uitvoering van programmacode, zoals preventie van gegevensuitvoering, (DEP: Data Execution Prevention DEP), willekeurige adresruimte-indeling (ASLR: Address Space Layout Randomisation) of ‹sandboxing›.

Bijlage 2

1. [een bevestiging van Stap 1] Criterium één ziet op de naleving van internationale verplichtingen en verbintenissen.

- 5.2. 1 aan landen gesanctioneerd door de VN-Veiligheidsraad of de Europese Unie?

2. Criterium twee ziet op de eerbiediging van de mensenrechten in het land van eindbestemming en de naleving van het internationaal humanitair recht door dat land.

- In het kader van de houding van het ontvangende land ten opzichte van belangrijk, in internationale mensenrechteninstrumenten vastgelegde beginselen;
  - 5.2. 1 [18]
  - Heeft u een product/producten geleverd aan landen waar door de ter zake bevoegde instanties van de Verenigde Naties, de Europese Unie of de Raad van Europa ernstige schendingen van de mensenrechten zijn geconstateerd?
- 5.2. 1

[18] 5.2. 1 .

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

- 5.2. 1

3. 5.2. 1
.
5.2. 1

4. 5.2. 1
.

- 5.2. 1
  - 5.2. 1
  - 5.2. 1
  - 5.2. 1
  - 5.2. 1
.
- 5.2. 1

5. 5.2. 1

- 5.2. 1

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

- 5.2. 1
- 5.2. 1
- 5.2. 1

6. 5.2. 1

- 5.2. 1
  - 5.2. 1
  - 5.2. 1

Ministerie van Justitie en Veiligheid

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Contactpersoon
5.1.2.e
T 070 5.1.2.e
F 070 5.1.2.e

Datum

Ons kenmerk

Dep. VERTROUWELIJK
Beleidsnota

Versie **13 maart 2019**

nota

Leveranciers binnendringsoftware

Aanleiding

In het regeerakkoord 'Vertrouwen in de Toekomst' van het kabinet Rutte III staat de volgende passage over het wetsvoorstel Computercriminaliteit III:

"Voor de uitvoering van de Wet Computercriminaliteit III komt 10 miljoen euro extra beschikbaar. Daarbij zal slechts in een specifieke zaak hacksoftware worden ingekocht door opsporingsdiensten. Leveranciers van dergelijke software worden gescreend door de AIVD en verkopen niet aan dubieuze regimes. Statistieken over het gebruik van hacksoftware worden jaarlijks openbaar gemaakt. Bij de evaluatie van de wet na twee jaar wordt bezien in hoeverre deze regeling de effectiviteit van de wet ernstig aantast. In dat geval wordt alsnog de aanschaf van hacksoftware voor algemeen gebruik overwogen." [1]

Deze beleidsnota zet uiteen welk beleid wordt gevoerd binnen de opsporing ten aanzien van aanschaf van binnendringsoftware van particuliere leveranciers.

Beleid

Het regeerakkoord vereist dat leveranciers van binnendringsoftware worden gescreend door de AIVD en dat deze leverancier niet aan dubieuze regimes verkopen. Commerciële binnendringsoftware is prominent onderwerp geweest in het debat over de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk. Commerciële binnendringsoftware maakt (mogelijk) gebruik van onbekende kwetsbaarheden in software. In plaats dat deze kwetsbaarheid wordt gemeld waardoor de software veiliger wordt, wordt deze kwetsbaarheid commercieel geëxploiteerd. Daarnaast kunnen leveranciers van deze software ook leveren aan regimes die de producten kunnen gebruiken voor het (ernstig) schenden van mensenrechten. Om de markt van binnendringsoftware niet meer dan strikt noodzakelijk te betreden is de aanschaf beperkt tot een specifieke zaak en worden aanvullende eisen gesteld aan leveranciers. Deze eisen betreffen 1) screening door de AIVD, 2) beoordeling of een bedrijf heeft geleverd aan dubieuze regimes.

Met opmerkingen 5.1.2.e 5.2.1

Wat is binnendringsoftware?
Voor binnendring software wordt de definitie van de concept-verordening 2016/0295, annex I als uitgangspunt gebruikt.

[1] Regeerakkoord 2017-2021 'Vertrouwen in de toekomst'.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

De actualisering van de verordening is nog gaande daarmee staat de definitie nog niet vast.

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht:

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Zie bijlage 1 voor de (technische) noten die horen bij deze definitie.

Binnen de wet Computercriminaliteit III is onderscheid gemaakt tussen het technisch hulpmiddel dat bewijs vergaart en binnendringsoftware die de beveiliging van een geautomatiseerd werk doorbreekt. Het technisch hulpmiddel wordt geïnstalleerd nadat toegang is verkregen tot een geautomatiseerd werk. Binnendringsoftware omzeilt de beschermende tegenmaatregelen van een computer of apparaat met netwerkcapaciteit. Het beleid in deze nota zich op binnendringsoftware.

Met opmerkingen 5.1. 2. e 5.2. 1

Screening AIVD
De screening van de AIVD ziet op de eventuele dreiging die een leverancier vormt voor de nationale veiligheid. Het beoordelen met het oog op mensenrechtenschendingen is geen onderdeel van de wettelijke taak van de AIVD. Wanneer een onderhandeling met een bedrijf zich in de slotfase bevindt kan de politie contact zoeken met het ministerie van Justitie en Veiligheid om een verzoek richting het Ministerie van Binnenlandse Zaken te doen uitgaan voor een dergelijke screening.

Levering van binnendringsoftware aan dubieuze regimes
Binnendringsoftware kan een essentieel middel zijn in de inzet van de bevoegdheid tot binnendringen in een geautomatiseerd werk, maar kan ook worden misbruikt door repressieve regimes. Het is een zogenaamd product voor tweeërlei gebruik[2], oftewel een dual-use goed. In de kamerbrief over kwetsbaarheden in hard- en software van november 2016 staat dat de regering hecht aan beperking van uitvoer van ICT-goederen en –software naar regimes met een slechte staat van dienst op het gebied van mensenrechten.[3] In onderstaand beleid wordt uiteengezet hoe hier in het kader van de uitvoering van de bevoegdheid tot het heimelijk en op afstand binnendringen in een geautomatiseerd werk vorm aan wordt gegeven.

[2] COM(2016), 2016/0295
[3] Kamerstukken TK, 2016/17, 26 643, nr. 428

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

Binnen het recht of beleid bestaat geen eenduidige definitie van een dubieus regime. Er wordt daarom zoveel mogelijk aangesloten bij bestaande regelgeving die ziet op soortgelijke materie of in de geest van toekomstige regelgeving, zoals verordening 2016/0295, gehandeld.

Bestaande regelgeving die dient als inspiratie voor het beleid zijn onder andere The Wassenaar Arrangement het beleid in omringende landen[4], en het beleid rond controle op de uitvoer van militaire goederen en technologie.[5].

Bij The Wassenaar Arrangement wordt de reikwijdte van de export controle bepaald door de lijsten die zijn opgesteld onder het arrangement, de praktische implementatie varieert van land tot land.[6] Er zijn ook zogenaamde 'best practices' gepubliceerd. De bescherming van mensenrechten speelt in deze best practices een rol bij de uitvoer van conventionele wapens, handvuurwapens en lichte wapens, maar nog niet bij 'intrusion software'. Deze software wordt wel genoemd in de lijst met dual-use items. In de categorie computers (p. 79) wordt *software* die speciaal ontwikkeld of aangepast is voor de ontwikkeling, controle, of aflevering van 'intrusion software' op de dual-use lijst geplaatst, alsook de *technologie* voor de ontwikkeling van 'intrusion software' (p. 80).[7] [Nota bene, het arrangement reguleert niet de binnendringsoftware zelf, maar software of technologie die deze software ontwikkelt, controleert of aflevert.] De definitie van 'intrusion software' komt overeen met die uit de concept-verordening 2016/0295 (p. 221)[8] [9] . 5.2.1 [redacted] Het staat Nederland vrij om een strikter regime te creëren.

Leveranciers binnen de Europese Unie

In de Europese Unie bestaat sinds 2009 een verordening die een exportcontrole regime vereist op dual-use goederen[10]. Een dergelijk regime stelt voorwaarden aan exporteurs van dual-use goederen om misbruik te voorkomen. 5.2.1 [redacted] . 5.2.1 [redacted] . De Europese Commissie is bezig

[4] UK Department of Business Innovation and Skills, Export Control Organisation, Notice to Exporters 2015/24 : Intrusion Software Tools and Exort Control , 10082015

[5] GEMEENSCHAPPELIJK STANDPUNT 2008/944/GBVB VAN DE RAAD

[6] https://www.wassenaar.org/about-us/#faq

[7] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public documents Volume II List of Dual-Use Goods and Technologies And Munitions List (December 2018)

[8] Idem.

[9] Annex I, COM(2016, 2016/0295: p. 2, p.15

[10] VERORDENING (EG) Nr. 428/2009 VAN DE RAAD

[11] Publicatieblad van de Europese Unie Nr. L 335 van 13-12-2008 vanaf pag.99 (directe link http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:335:0099:0103:nl:PDF)

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

deze te actualiseren en heeft in haar ontwerpverordening voorgesteld om 'technologieën voor cybertoezicht' onder het exportcontrole regime te brengen[12]. "Inbraakprogrammatuur" (intrusion software)is onderdeel van deze technologieën voor cybertoezicht en zoals in tabel 1 aangegeven is binnendringsoftware een onderdeel van deze definitie .[13] Het Europees Parlement heeft op het moment van het schrijven van deze nota reeds haar amendementen aangenomen[14], de Raad poogt om voor de Europese verkiezingen een algemene oriëntatie aan te nemen[15].

Wanneer deze verordening in werking treedt moeten Europese producenten voldoen aan de eisen in de verordering, waaronder de controle op het mogelijke schenden van mensenrechten door de software. Europese leveranciers dienen dan daarmee aan de eisen uit het regeerakkoord 2017-2021 'Vertrouwen in de Toekomst' te voldoen. In de periode tussen de implementatie van de concept-verordening 2016/0295 en de inwerkingtreding van het beleid inzake binnendringsoftware zal het regime voor leveranciers buiten de Europese Unie worden gevolgd, tenzij een leverancier alleen zaken doet met lidstaten.

Met opmerkingen 5.1. 2. e 5.2. 1

Leveranciers buiten de Europese Unie

Voor leveranciers buiten de Europese Unie geldt het exportcontrole regime niet en zij bevinden zich niet in een lidstaat die middels de Unie werkt aan een ruimte van vrijheid, veiligheid en recht (art. 67 VWEU). Voor een invulling van het begrip van 'dubieuze regimes' wordt aangesloten bij bestaande instrumenten, zoals The Wassennaar arrangement, en toekomstige instrumenten zoals de actualisering van de dual-use verordening. 5.2. 1 . 5.2. 1 . 5.2. 1 . Om het risico dat zaken worden gedaan met een leverancier die zaken doet met een dubieus regime zoveel mogelijk uit te sluiten worden leveranciers op drie wijzen getoetst alvorens binnendringsoftware aan te schaffen.

Stap 1

Het bedrijf wordt gevraagd om uit te sluiten dat het producten levert aan landen waartegen de Europese Unie restrictieve sancties heeft ingesteld. Binnen de Raad van de Europese Unie wordt hiervoor een lijst bijgehouden van EU en VN sancties: https://www.sanctionsmap.eu/#/main[16]. Deze lijsten zijn openbaar en voor een bedrijf gemakkelijk te raadplegen.

Met opmerkingen 5.1. 2. e 5.2. 1

Stap 2

5.2. 1 5.2. 1

[12] COM(2016), 2016/0295

[13] COM(2016), 2016/0295, hoofdstuk II

[14] P8_TA(2018)0006

[15] TK 2018/2019, 21 501-02, 1934

[16] NB men ziet de VS op deze lijst staan, maar geen restrictieve sancties vermeld staan. De VS is daarom geen land dat wordt uitgesloten.

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

5.2. 1

De vragen die moeten worden beantwoord zien 1) op de naleving van de internationale verplichtingen en verbintenissen van het land van bestemming, 2) de eerbiediging van mensenrechten en de naleving van het internationaal humanitair recht, 3) 5.2. 1
4) 5.2. 1
5) 5.2. 1
en 6) 5.2
5.2. 1

Zie bijlage 2 voor de uitwerking van deze vragen.

Stap 3

5.2. 1

Met opmerkingen 5.1. 2. e 5.2. 1

[17] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/richtlijnen/2018/02/21/richtlijnen-voor-het-opstellen-van-een-internal-compliance-programme-icp/Richtlijnen+voor+het+opstellen+van+een+Internal+Compliance+Programme.pdf

Directoraat-Generaal
Rechtspleging en
Rechtshandhaving
Directie Rechtshandhaving en
Criminaliteitsbestrijding

Datum

Ons kenmerk

5.2. 1

Rol overheid

5.2. 1

Met opmerkingen 5.1. 2. e 5.2. 1

Met opmerkingen 5.1. 2. e 5.2. 1

Toekomstig handelen van een leverancier

Een toets is een momentopname in het specifieke geval. Doet de mogelijkheid zich voor dat wederom software van een eerder getoetste leverancier moet worden aangeschaft worden de stappen 1,2 en 3 wederom doorlopen. Een verkorte procedure is mogelijk 5.2. 1

Met opmerkingen 5.1. 2. e 5.2. 1

. 5.2. 1

. Deze verkorte procedure bestaat uit een verklaring dat er geen wijzigingen zijn in de eerder gegeven beantwoording bij stap 1,2 en 3.

Bijlage 1 Definitie Inbraakprogrammatuur

"Inbraakprogrammatuur" (intrusion software), "programmatuur" die speciaal is ontworpen of aangepast om opsporing [detectie] door 'bewakingshulpmiddelen' te voorkomen of om 'beschermende tegenmaatregelen' van een computer of apparaat met netwerkcapaciteit te omzeilen en die een van de volgende functies verricht: .

a.het onttrekken van gegevens of informatie uit een computer of apparaat met netwerkcapaciteit of het wijzigen van systeem- of gebruikersgegevens; of .

b.het wijzigen het normale executiepad van een programma of proces om de uitvoering van buitenaf geleverde instructies mogelijk te maken.

Noten:

1."Inbraakprogrammatuur" omvat niet het volgende: .
a.‹hypervisors›, ‹debuggers› of hulpmiddelen voor de reverse engineering van programmatuur (SRE); .
b."programmatuur" voor het beheer van digitale rechten (DRM); of .
c."programmatuur" die is ontworpen voor installatie door de fabrikanten, beheerders of gebruikers met het oog op goederenbewaking of -herstel. .
2.Apparaten met netwerkcapaciteit omvatten mobiele apparaten en slimme meters.

Technische noten:

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

1.'Bewakingshulpmiddelen': "programmatuur" of hardwareapparaten die het systeemgedrag of de processen die op een apparaat worden uitgevoerd, bewaken. Dit omvat antivirus (AV)-producten, producten voor eindpuntbeveiliging, producten voor persoonlijke veiligheid (PSP: Personal Security Products), inbraakdetectiesystemen (IDS: Intrusion Detection Systems), inbraakpreventiesystemen (IPS: Intrusion Prevention Systems) of firewalls. .

2.'Beschermende tegenmaatregelen': technieken die zijn ontworpen om te zorgen voor de veilige uitvoering van programmacode, zoals preventie van gegevensuitvoering, (DEP: Data Execution Prevention DEP), willekeurige adresruimte-indeling (ASLR: Address Space Layout Randomisation) of ‹sandboxing›.

Bijlage 2

1. [een bevestiging van Stap 1] Criterium één ziet op de naleving van internationale verplichtingen en verbintenissen.

- 5.2. 1 aan landen gesanctioneerd door de VN-Veiligheidsraad of de Europese Unie?

2. Criterium twee ziet op de eerbiediging van de mensenrechten in het land van eindbestemming en de naleving van het internationaal humanitair recht door dat land.

- In het kader van de houding van het ontvangende land ten opzichte van belangrijk, in internationale mensenrechteninstrumenten vastgelegde beginselen;
  - 5.2. 1 [18]
  - Heeft u een product/producten geleverd aan landen waar door de ter zake bevoegde instanties van de Verenigde Naties, de Europese Unie of de Raad van Europa ernstige schendingen van de mensenrechten zijn geconstateerd?
- 5.2. 1

[18] 5.2. 1

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

- 5.2. 1

3. 5.2. 1
5.2. 1

4. 5.2. 1
   - 5.2. 1
     - 5.2. 1
     - 5.2. 1
     - 5.2. 1
     - 5.2. 1
   - 5.2. 1

5. 5.2. 1
   - 5.2. 1

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding

Datum

Ons kenmerk

- 5.2. 1
- 5.2. 1
- 5.2. 1

6. 5.2. 1 .
   - 5.2. 1
     - 5.2. 1 ;
     - 5.2. 1

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

Hi,
I am on vacation and just arrived airport [redacted] this minute - will check on Monday.

Best regards,

[redacted]

From [redacted]
Subject
To
Date

Couldn't open it.
Is your key the same like yesterday?

From [redacted]
Subject
To
Date

Perfect.
Thank you!

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

...you will get it today...!

Best regards,

[redacted]

From [redacted]
Subject
To
Date

Dear [redacted]

Thanx for your response, I will inform the operational team with your answer.

[redacted]

Document 06

From [redacted]
Subject
To
Date

Dear [redacted]

How are you?
Hope all is good considering the crazy times...
Any news or timeframe regarding our part?

Best,
[redacted]

[redacted]

> Dear [redacted]

>

> Hope you feel better now :)

> I am fine, travelling a lot, end of the year...

> Using this opportunity, I wish you and your colleagues a Merry Christmas and a good and successful New Year from all of us here [redacted]

>

> [redacted]

From [redacted]
Subject [redacted]
To [redacted]
Date [redacted]

Dear [redacted]

Thanx for your email, I will discuss it with my colleagues next year ;-)
I couldn't open the attachments, double pgp gpg?

For you and your colleagues also best wishes and a healthy [redacted]

[redacted]

Document 09

From [redacted]
Subject
To
Date

Dear [redacted],
I will try to resend it next week.
I just attached the files :(
Enjoy your holidays!!!
[redacted]

Document 10

From [redacted]
Subject
To
Date

Dear [redacted]

I understand your work frame and appreciate the update.
If there is anything that I can do to help the process, please let me know.

p.s. Does [redacted] still have the same phone number like when we met?

Best regards,
[redacted]

-----Original Message-----
From: [redacted]
Sent: [redacted]
To [redacted]
Subject: [redacted]

Hello,

As discussed during our telephone call, this is my e-mail address.
Please find my attached public key for your response.

Grz

[redacted]

Document 12

From [redacted]
Subject
To
Date

Hi,

Please find enclosed my key.

Regards,

[redacted]

From [redacted]
Subject
To
Date

Hello [redacted]

That sounds great, but that's still in the [redacted] holiday :-(
So I will focus on the second part of [redacted]
Enjoy your [redacted] day and I will come back to you asap!

[redacted]

Document 14

From [redacted]
Subject
To
Date

Dear [redacted]

Could we meet in [redacted]

All the best,
[redacted]

[redacted]

> Just noticed that my PGP didn't function properly, I hope that the email arrived.

> Resending it just in case.

Document 16

From [redacted]
Subject
To
Date

Dear [redacted]

How are you?
Any news on your visit?

Best,
[redacted]

From [redacted]
Subject
To
Date

Currently it is fine but I need final confirmation from you - we travel a lot and it is better to know in advance.
Let me know how much time will you have with us :)
Hope to see you!!!

[redacted]

From [redacted]
Subject
To
Date

Dear [redacted]

Sounds like a good plan - just let me know to which train station to arrive…

My phone number is [redacted]

Looking forward to seeing you tomorrow.

All the best,
[redacted]

Document 19

From [redacted]
Subject
To
Date

Dear [redacted]

Please send me all the following details:

Full Names of all
Flight details
Hotel

Looking forward to seeing you,
[redacted]

From [redacted]
Subject
To
Date

BTW, this hotel is [redacted]
Just to make sure.

Document 21

From [redacted]
Subject
To
Date

I am sorry for [redacted] but yet sounds like a great team :)
Have a safe flight!

Document 22

From [redacted]
Subject
To
Date

Thanks [redacted]

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

H[redacted]

Thanks for the agenda. I will discuss it with [redacted] and come back with an answer.

Good weekend,

From [redacted]
Subject
To
Date

Hi,

Hope all is good.
Any news?

Best regards,
[redacted]

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

perfect

All booked here

[redacted]

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

hello

our mails crossed.

all info in the other mail :-)

i wish you a successful day tomorrow. Our office is yours

[redacted]

Best Regards

[redacted]

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

Hi,

All fine here, thanks.
The starting time of 9.30am is fine.
We are pleased to meet [redacted],

Regards,
[redacted]

>

From [redacted]
Subject
To
Date

Hoi [redacted]

Ik zal deze info doorgeven aan projectleiding en om akkoord vragen.
Zodra ik dat heb kom ik terug op de lijn, ook over je andere vragen.

Bedankt,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Ik heb de bijlagen wel correct ontvangen, bedankt, maar de inhoud van de mail kan ik niet ontcijferen. Mogelijk gaat hierbij iets mis met pgp.

Zou je de inhoud van de mail nog een keer kunnen sturen?

Groet,
[redacted]

Van:
Verzonden:
Aan:
Onderwerp:

[redacted]

Hi [redacted]

Please give me a short notice you received the attachments correctly from the previous email. Otherwise I will resend them Good weekend, [redacted]

->>

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

Hi [redacted]

I missed the deadline date, could you please regenerate the download link for us,

Regards,
[redacted]

Van: [redacted]
Verzonden:
Aan:
Onderwerp:

Hi [redacted]

Thanks, you can remove the link now, the download succeeded.

Regards,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Zou je me eventueel kunnen bellen ivm programma op [redacted]

Alvast bedankt,

[redacted]

From [redacted]
Subject
To
Date

Good luck!
Let me know as soon as possible!

[redacted]
> Please confirm that you got my email.
>

From [redacted]
Subject
To
Date

Hi [redacted]

Thanks, yes I received your message. We will study it and reply asap.

Please be informed that the previous mail was in clear text (not encrypted), with so far I see the same content.

Regards,
[redacted]

Document 37

From [redacted]
Subject
To
Date

Yes, I noticed. Sorry for that.

From [redacted]
Subject
To
Date

Hallo [redacted],

Bedankt voor het antwoord. Goed te horen dat het kan.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted],

Mooi om te horen.

Bedankt,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Heb navraag gedaan en heb als bindende factor op dit onderwerp [redacted] gevonden. Je kunt met hem contact opnemen, heb hem hiervan op de hoogte gebracht. Hij kan mensen die hiermee bezig zijn bij elkaar brengen.

Groet, [redacted]

From [redacted]
Subject
To
Date

Beste [redacted]

Ik heb inmiddels een email gestuurd naar [redacted]

Onzettend bedankt voor het meedenken!

Met vriendelijke groet,

[redacted].

From [redacted]
Subject
To
Date

Hi [redacted]

We planned to arrive the day before [redacted] and to fly back [redacted] evening.

Is it possible to arrange an appointment earlier that day so we can fly back that same evening?

Regards, [redacted]

Document 43

From [redacted]
Subject
To
Date

Hi [redacted],

Great we can arrange a meeting at 9:30 in the morning. The journey is waiting approval. I'll let you know when it passed definitely our management team.

Thanks,
[redacted]

From [redacted]
Subject
To
Date

No worries - I added it to our schedule and we all will be there starting at 9:00
Hope to see you!

From [redacted]
Subject
To
Date

Dear [redacted]

Hope you all are fine,
Have you gotten the approval yet for the visit?

Hope yes :)

From [redacted]
Subject
To
Date

Hi [redacted]

Yes, we got the approval, all fine.

See you [redacted] at 9:30

Thanks,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Bedankt voor je reactie.

Ik heb nog niets gehoord van je collega maar hij is van harte welkom op vrijdag middag.

Met vriendelijke groet,

[redacted]

Document 48

From [redacted]
Subject
To
Date

Hoi [redacted]

Heb je al iets gehoord?

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted],

Bedankt voor je reactie! Ik hoor het graag als je meer weet.

Met vriendelijke groet,

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Deze dagen hebben bij ons de voorkeur, omdat een week later herfstvakantie is en we liever niet verder willen doorschuiven om zo snel mogelijk de beslissers van antwoorden kunnen voorzien.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Geen probleem.

Zal ik dan [redacted] vastleggen voor de meeting?

Willen jullie twee dagen afspreken of 1 van deze dagen kiezen?

Ik hoor het graag zodat ik het kan gaan organiseren.

Groet!

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Een van die twee dagen is voldoende, denk ik.
Zullen we uitgaan van woensdag [redacted]

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hi [redacted]

Is it ok to meet Tuesday [redacted]

With kind regards,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Woensdag de [redacted] is prima

k ga dit doorgeven en ook zelf mijn reis boeken/plannen

Groet

[redacted]

From [redacted]
Subject
To
Date

Goede morgen [redacted]

Misschien is het verstandig even te wachten met je reis boeken, totdat onze dienstreis goedgekeurd is.

Ik geef je een seintje zodra dit het geval is.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Helemaal goed k wacht op jouw bericht en zal dan ook mijn vlucht/hotel boeken

Groet

[redacted]

Document 57

From [redacted]
Subject
To
Date

Hoi [redacted]

Onze dienstreis is goedgekeurd. Wij gaan nu vlucht en hotel boeken.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Helemaal goed.

Dan zien we elkaar [redacted]

Groet,

[redacted]

Document 59

From [redacted]
Subject
To
Date

Hoi[redacted].

1 vraagje nog. Met hoeveel zijn jullie? Dan kunnen we daar op voorbereiden.

Goed weekend alvast.

Groet,

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

We komen met [redacted] personen,

Groet, [redacted]

[redacted]

> Hi [redacted]
>
> Our hotel will be booked, in case we need any help, we let you know,
> thanx for the offer to help.
>
> We will hire a car at the airport, so transportation should not be a
> problem.
>
> We don't have the time schedule of our flight [redacted] yet. As soon
> as I know our arrival time I will let you know, so we can plan for
> dinner. [redacted]
>
> See you soon,
> [redacted]

From [redacted]
Subject
To
Date

Hi [redacted]

We will arrive at [redacted] So we should be able to meet at [redacted] that evening. Is that OK?

Could you provide us a phone number to contact in case of any changes?

With kind regards,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Goede vragen ;-)
Onze vlucht gaat diezelfde dag [redacted] terug. We wilden dus graag 's ochtends bij elkaar komen. Is [redacted] uur een goede tijd? Verder hebben we een huurauto. Naar welk adres moeten we rijden?

Ik neem aan dat we jou als contact kunnen houden. Heb je een telefoonnummer waaronder we je kunnen bereiken [redacted]

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

We zullen de [redacted] bij jullie zijn,

Tot dan,
[redacted]

From [redacted]
Subject
To
Date

Sure, I have [redacted] number [redacted]
Will let you know!

From [redacted]
Subject
To
Date

Hi guys,
For [redacted] I booked us a table [redacted]

have a safe trip!
[redacted]

From [redacted]
Subject
To
Date

Hi [redacted]

Thank you, very nice.

My phone number [redacted]

See you at [redacted]

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Ok, goed om te horen,

Ik ben bereikbaar [redacted]

Gaan straks vliegen.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hallo [redacted]

Hierbij de bevestiging voor de afspraak komende dinsdag [redacted]
uur in [redacted]

Tot dan,
[redacted]

Document 70

From [redacted]
Subject
To
Date

Hoi [redacted]

Sorry, deze had ik even over het hoofd gezien.
Ik hoorde [redacted] dat jullie al contact gehad hebben.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hallo [redacted]

Bedankt,
Ik zal deze [redacted] delen en doornemen.
Zie jullie woensdag,

Tot dan,
[redacted]

From [redacted]
Subject
To
Date

Dank e we [redacted] Tot woensdag!

[redacted]

From [redacted]
Subject
To
Date

Goedemorgen [redacted]

Ik zal alle doorgestuurde informatie [redacted] doorgeven.

Alvast bedankt,

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Heb het document in goede orde ontvangen, bedankt.

Ik zal met het team overleggen of het mogelijk is iets in [redacted] te plannen. Kom hier zo spoedig mogelijk op terug.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Begin [redacted] gaan we [redacted] Hierdoor gaan we het niet redden om iets in de tweede week van [redacted] af te spreken. De vierde week zou voor ons beter uitkomen.

Met vriendelijke groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Ja helemaal goed.

Tot in [redacted]

Met vriendelijke groet,

[redacted]

From [redacted]
Subject [redacted]
To [redacted]
Date [redacted]

Hoi [redacted]

Ik zal het hier intern bespreken hoe we verder gaan. Ik kom hierover nog op de lijn.

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Bedankt voor je reactie.

Ik wacht geduldig af :)

Groet,

[redacted]

From [redacted]
Subject [redacted]
To [redacted]
Date [redacted]

Hoi [redacted]

Wij zouden maandag middag [redacted] of dinsdag [redacted] kunnen.
Heb je een voorstel voor een tijd en dag?

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Top. Staat in onze agenda. Jullie zijn hier van harte welkom. Wij zitten tegenwoordig [redacted].

Groet,
[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Excuses, ik zag dat ik nog niet gereageerd had. Maar dank voor het vrijmaken van jullie tijd en wij zullen er om [redacted] zijn op maandag [redacted]

Groet,

[redacted]

From [redacted]
Subject
To
Date

Hoi [redacted]

Ik hoop dat [redacted] nuttig/goed geweest is voor jullie!

Ik heb je vraag inmiddels neergelegd en hoop je zsm een antwoord te sturen.

Met vriendelijke groet,

[redacted]