Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

32 761 Verwerking en bescherming persoonsgegevens

Nr. 182 **BRIEF VAN DE MINISTER VAN DEFENSIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 mei 2021

Hierbij ontvangt u het onderzoeksrapport van de Functionaris Gegevensbescherming Defensie over de naleving van de Algemene Verordening Gegevensbescherming (AVG) door het experimentele Land Information Manoeuvre Centre (LIMC)[1]. In mijn brief van 27 november met mijn eerste reactie op de berichtgeving over LIMC zegde ik toe deze samen met mijn beoordeling van de activiteiten van het LIMC aan te bieden.[2] Gelijktijdig met deze brief ontvangt u, zoals toegezegd in mijn brief van 15 december[3], de antwoorden op de Kamervragen van 24 november 2020 van de leden Belhaj (D66) en Karabulut (SP) «over LIMC, JISTARC en andere inlichtingenwerkzaamheden door de krijgsmacht».[4] Verder heeft het lid Verhoeven op 15 januari 2021 vragen gesteld over «grootschalige en onrechtmatige verzameling van data van burgers door de krijgsmacht, de politie, de Belastingdienst, de Inlichtingen- en Veiligheidsdiensten en andere overheidsorganisaties».[5] In de kabinetsreactie hierop van 9 april is over de defensiegerelateerde vragen 7–13 gesteld dat die in voorliggende brief worden beantwoord als het rapport van de Functionaris Gegevensbescherming gereed was.[6] Desbetreffende antwoorden zijn als bijlage 3 bij deze brief gevoegd[7].

De Functionaris Gegevensbescherming heeft in korte tijd een onderzoek uitgevoerd naar de naleving van de AVG door het experimentele LIMC. Dit onderzoek heeft mij de aanvullende informatie geleverd om een integraal oordeel over de activiteiten van het LIMC te kunnen geven. Ik ben de Functionaris erkentelijk voor het werk dat ze in korte tijd met haar team heeft verricht. Zoals ik in mijn brief van november zei, is zij de wettelijke,

[1] Raadpleegbaar via www.tweedekamer.nl
[2] Kamerstuk 32 761, nr. 175.
[3] Aanhangsel Handelingen II 2020/21, nr. 1099.
[4] Aanhangsel Handelingen II 2020/21, nr. 2623
[5] Aanhangsel Handelingen II 2020/21, nr. 2287
[6] Aanhangsel Handelingen II 2020/21, nr. 2652
[7] Raadpleegbaar via www.tweedekamer.nl

kst-32761-182
ISSN 0921 - 7371
's-Gravenhage 2021

onafhankelijke, interne toezichthouder van Defensie op het gebied van gegevensbescherming.[8] Ik onderschrijf de conclusies uit het rapport en neem de aanbevelingen over. Voordat ik daar nader op reageer, ga ik eerst kort in op het belang om verantwoord te experimenteren met informatiegestuurd optreden en op de achtergrond waartegen de experimenteeromgeving LIMC werd opgericht, namelijk de COVID-19 crisis.

Het belang van experimenteren met Informatie Gestuurd Optreden

Zoals ik in mijn eerste reactie van 27 november over het LIMC schreef, hebben de razendsnelle IT-ontwikkelingen grote operationele gevolgen voor de krijgsmacht. Uit de dreigings- en probleemanalyse van de Defensievisie-2035 die het kabinet vorig jaar oktober naar het parlement stuurde, komt naar voren dat Defensie nu onvoldoende is toegerust voor het opereren in de informatie-omgeving. Daarom is informatiegestuurd optreden een van de drie eigenschappen in de Defensievisie die helpen koersvast te blijven bij keuzes over de inrichting en samenstelling van de defensieorganisatie in 2035.[9]

Statelijke actoren en terroristische organisaties gebruiken informatie nu al als wapen. Bijvoorbeeld door voordeel te halen uit het verspreiden van valse of onvolledige informatie en daarmee onze manier van leven en denken te beïnvloeden. Met cyber kunnen ook fysieke effecten worden bereikt, zoals het aanvallen of saboteren van vitale sectoren waarvan ook Defensie afhankelijk is. De Defensievisie zegt hierover dat Defensie haar bijdrage moet leveren aan het vergroten van de weerbaarheid van de samenleving hiertegen. Indien nodig moet Defensie ook terug kunnen slaan. Uiteraard moet Defensie zich daarbij houden aan de geldende juridische en ethische kaders. Dit onderscheidt ons van onze tegenstanders.[10]

Binnen die kaders moet de krijgsmacht in de informatie-omgeving kunnen opleiden en trainen, anticiperen en zichzelf beschermen, zodat onze militairen operationeel gereed zijn voor inzet in Nederland en daarbuiten. De bestaande juridische mogelijkheden moeten daarbij optimaal worden gebruikt en het toezicht daarop moet goed zijn ingericht. Dit principe is voor de verzameling en verwerking van data waaronder persoonsgegevens niet anders dan bij wapengebruik.

De «digitalisering van het slagveld» is een van de grootste veranderopgaven van de krijgsmacht. In de brief van 27 november verwees ik al naar het belang om hierbij ook te leren door te experimenteren. De organisatie moet zich kunnen blijven ontwikkelen. Hiervoor is het ook door de NAVO gebruikte instrument voor capaciteitenontwikkeling van *Concept Development & Experimentation* gehanteerd. Het gaat hierbij om leren door experimenteren, vallen en opstaan en voortdurend herhalen en evalueren van dit proces.

De noodzakelijke veranderingen die de komende jaren nodig zijn voor de verdere invoering van Informatie Gestuurde Optreden (IGO) laten zich niet enkel van bovenaf met blauwdrukken opleggen. Dit vergt ook dat op de werkvloer wordt geëxperimenteerd met innovatieve concepten. De in de praktijk geleerde lessen zijn essentieel om de toekomstige organisatie in te richten en te betrekken bij grote investeringsplannen die nodig zijn om

---

[8] Staatscourant, nr. 28291, 22 mei 2018.
[9] Defensievisie-2035, 15 oktober 2020, Kamerstuk 34 919, nr. 7.
[10] Zie ook *From Blurred Lines to Red Lines, How Countermeasures and Norms Shape Hybrid Conflict,* HCSS, september 2020.

de grondwettelijke taken van Defensie nu en in de toekomst uit te kunnen voeren.

COVID-19 en het experimentele LIMC

In maart 2020 brak in Nederland COVID-19 uit, de grootste nationale crisis sinds de Tweede Wereldoorlog.[11] De krijgsmacht stond en staat beschikbaar voor de ondersteuning van de civiele autoriteiten bij de bestrijding van COVID-19. Het Commando Landstrijdkrachten was door de CDS aangewezen als het uitvoerend Operationeel Commando voor alle land gerelateerde steunverlening tijdens deze operatie. De steun aan ziekenhuizen en verpleeg- en verzorgingshuizen is de meest in het oog springende.

Het gevoel van urgentie om de civiele autoriteiten bij deze nationale COVID-crisis te hulp te schieten, gecombineerd met het belang om te experimenteren met informatiegestuurd optreden, verklaart dat de landmacht deze crisis aangreep om in een experimenteeromgeving het LIMC op te richten. Het doel van het LIMC was om in een experimenteeromgeving met moderne data-analyse van open bronnen militaire en civiele besluitvorming te voeden met inzicht en handelingsperspectief. Uiteraard gelden ook voor experimenteer projecten altijd de juridische en ethische kaders. Dit kwam tot uiting door in alle opdrachten die het Commando Landstrijdkrachten hiertoe verstrekte, te vermelden dat het LIMC binnen de vigerende regelgeving moest opereren.

Het AVG-rapport van de Functionaris Gegevensbescherming Defensie

Het experimentele LIMC gaf uitvoering aan de opdracht van het Commando Landstrijdkrachten tot het opstellen van een omgevingsbeeld over COVID-19 gerelateerde maatschappelijke ontwikkelingen als fenomeen door data uit algemeen toegankelijke bronnen te verzamelen, te verwerken en te analyseren. Het uitgangspunt hierbij was dat hier geen aparte grondslag of mandaat voor nodig was. Dit uitgangspunt was juist voor zover het verrichten van dergelijke activiteiten tot de gereedstellings- en instandhoudingstaak van de krijgsmacht behoort. Voor activiteiten die niet tot deze taak behoren, zoals het inschatten van effecten in de maatschappij en het opstellen en verspreiden van rapporten hierover, geldt dat dit inzet betreft waarvoor altijd een grondslag vereist is. In geval van inzet voor nationale taken is dat – afgezien van enkele structurele taken die zijn vastgelegd in wet- en regelgeving, of in geval van structurele ondersteuning van civiel gezag – alleen mogelijk op basis van bijstand of Militaire Steunverlening in het Openbaar Belang (MSOB). Zoals ik op 27 november in mijn brief aan u al schreef, heeft het civiele gezag geen verzoek tot bijstand aan het LIMC gedaan.

Daarnaast was het uitgangspunt dat bij dergelijke activiteiten geen persoonsgegevens mochten worden verwerkt. Om dat laatste te voorkomen, had het LIMC een reeks aan organisatorische en technische maatregelen getroffen.

De Functionaris Gegevensbescherming stelt in de eindconclusie van haar AVG-onderzoek naar de experimenteeromgeving LIMC dat *«[...] Het LIMC had niet de intentie om (grootschalig) persoonsgegevens te verwerken, maar is hierin niet volledig geslaagd. Persoonsgegevens kwamen mee als «bijvangst». Voor deze verwerking bestond geen wettelijke grondslag en*

[11] Minister-President Rutte tijdens persconferentie op 20 maart 2020.

is niet voldaan aan de verantwoordingsplicht waardoor de AVG onvoldoende is nageleefd.»[12]

Ik neem deze eindconclusie en de onderliggende deelconclusies van de Functionaris Gegevensbescherming over. De interne AVG-organisatie moet worden verbeterd om herhaling te voorkomen en Defensie moet op dit vlak ook meer toekomstgericht worden. De Functionaris doet hiervoor zes aanbevelingen die ik allemaal overneem. In het vervolg ga ik kort op de aanbevelingen in.

Aanbeveling 1) Stel een (beleids-)gegevensbeschermings-effectbeoordeling (DPIA) op voor Informatiegestuurd optreden

Terecht merkt de Functionaris Gegevensbescherming op dat informatie gestuurd optreden de basis voor de toekomstige defensieorganisatie is. Bij zijn optreden bestudeert Defensie van oudsher altijd al weer en terrein, omdat die bepalend zijn voor de wijze waarop fysieke capaciteiten worden ingezet. Dit is het zogeheten fysieke landschap. Maar het moderne militaire optreden speelt zich voor een groot deel ook af in het virtuele (cyber) en in het menselijk of cognitieve landschap.[13] Dit geldt voor alle drie de hoofdtaken van de krijgsmacht. Bij informatiegestuurd optreden is het verwerken van persoonsgegevens dan onvermijdelijk, zoals de Functionaris Gegevensbescherming in haar rapport vaststelt. Cruciaal hierbij is dat Defensie zich daarbij steeds aan de AVG houdt. Hiermee moet aan de voorkant, bij het opstellen van het beleid, al rekening worden gehouden. Defensie zal in het op te stellen beleidskader «Informatie gestuurd optreden» op advies van de Functionaris Gegevensbescherming expliciet de principes van gegevensbescherming toepassen en een gegevensbeschermingseffectbeoordeling (*Data Protection Impact Assessment*, DPIA) opstellen.[14] De vraag of er een grondslag is om persoonsgegevens te verwerken, valt hier altijd onder.

Aanbeveling 2) Actualiseer de Catalogus Nationale Operaties 2018

Op dit moment wordt de catalogus Nationale Operaties herijkt. Daarin worden naast de militaire capaciteiten waarop civiele autoriteiten in het kader van de eerste en derde hoofdtaak een beroep kunnen doen, ook civiele capaciteiten opgenomen waarop Defensie in voorkomend geval een beroep kan doen. De nieuwe catalogus zal de beschikbare capaciteiten meer in termen van te bereiken effecten beschrijven, dan in termen van kwantitatieve toezeggingen.

De Functionaris Gegevensbescherming adviseert in deze catalogus een omschrijving van de taken, verantwoordelijkheden, bevoegdheden en mogelijkheden van de krijgsmacht op het gebied van *information manoeuvre* en andere militaire analysecapaciteit op te nemen, waarop civiele autoriteiten in voorkomend geval een beroep kunnen doen. De mogelijkheden en beperkingen hiervan worden in de volgende versie van de catalogus opgenomen. Daarbij wordt ook de rol die de inlichtingendiensten MIVD en AIVD hierbij vervullen meegenomen. De vaststelling van de herijkte catalogus is mede afhankelijk van de bijdragen van de

---

[12] Zie p.9 van het rapport.

[13] Defensievisie-2035. Rupert Smith heeft het bijvoorbeeld over «War amongst the people» in zijn bekende boek *The Utility of Force: the Art of War in the Modern World*, 2005.

[14] Zie het model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA), www.rijksoverheid.nl. Dit is niet nodig bij de verwerking van persoonsgegevens onder de Wet inlichtingen- en veiligheidsdiensten 2017, de Wet politiegegevens of als een uitzondering voor inzet van de krijgsmacht aan de orde is waardoor de AVG materieel niet van toepassing is.

civiele autoriteiten en loopt door COVID-19 vertraging op. De militaire bijdrage aan de catalogus Nationale Operaties zal voor het eind van dit jaar gereed zijn.

Aanbeveling 3) Hanteer willen, mogen en kunnen in de juiste volgorde

De Functionaris Gegevensbescherming snijdt hier een actueel thema aan waarop ook de Defensievisie ingaat, namelijk dat Nederland dagelijks wordt aangevallen in het cyberdomein en blootstaat aan beïnvloedings-campagnes van statelijke actoren.[15] De Defensievisie constateert tevens dat met de bescherming van het eigen en bondgenootschappelijk grondgebied (eerste hoofdtaak) allang niet meer alleen het territoriale grondgebied wordt bedoeld, maar net zo goed het digitale- en cognitieve grondgebied. Tegelijk raken de drie hoofdtaken ook meer en meer met elkaar verweven.

Gezien deze ontwikkelingen is de vraag relevant of «willen, mogen en kunnen» voor Defensie in de informatie-omgeving nog steeds met elkaar in evenwicht zijn. De Functionaris Gegevensbescherming stelt hierover dat als bij Defensie een behoefte bestaat om op dit vlak meer te «mogen», bijvoorbeeld door ontwikkelingen in de informatie-omgeving, daarvoor wetgeving vereist is. Voordat deze behoefte wordt overwogen is het antwoord op de «willen» vraag noodzakelijk, aldus de Functionaris Gegevensbescherming. Hiermee ben ik het uiteraard eens. Dit gaat Defensie de komende tijd onderzoeken. Hiertoe worden verschillende werkgroepen georganiseerd waarin militair juristen, AVG-functionarissen, ethisch experts en operationele eenheden die in de informatie-omgeving actief zijn, bijeenkomen om aan de hand van praktijkvoorbeelden volgens de trits «willen, mogen, kunnen» te onderzoeken wat de mogelijkheden en beperkingen in het informatiedomein zijn en hoe Defensie de juridische mogelijkheden optimaal kan gebruiken bij gereedstelling en inzet.

Hiernaast maakt TNO in opdracht van Defensie een dilemmagame over de juridische en ethische kaders in de informatie-omgeving en betrekt daarbij ook de discussies uit de werkgroepen. Deze dilemmagame zal voor het eind van dit jaar gereed zijn. Deze game kan en moet op alle niveaus van de organisatie worden gespeeld.

Uit die discussie en uit het externe onderzoek (zie aanbeveling 5) zal moeten blijken of er een inderdaad een operationele noodzaak is om in antwoord op de «willen» vraag ook de wet- en regelgeving aan te passen. Daarbij kijkt Defensie ook naar hoe bij Europese partnerlanden de verhouding «krijgsmacht-AVG» is ingevuld. Ook het advies van de externe toezichthouder, de Autoriteit Persoonsgegevens, maakt hier deel van uit.

Aanbeveling 4) Versterk de poortwachtersfunctie op het gebied van gegevensverwerking

Deze aanbeveling beoogt het risicobewustzijn bij de (mogelijke) verwerking van persoonsgegevens bij behoeftestellers en inkopers te verhogen door bij de verwerving van *webbased* producten en diensten ten behoeve van het informatiedomein een controle-vraag te stellen: waarvoor gaan jullie dit eigenlijk gebruiken? Zoals de Functionaris Gegevensbescherming stelt, kan daarbij gebruik worden gemaakt van de

[15] Zie bijvoorbeeld het openbare Dreigingsbeeld Statelijke Actoren van de MIVD, AIVD en NCTV, 3 februari 2021, Kamerstuk 30 821, nr, 124.

voorgeschreven model AVG-verwerkersovereenkomsten. Overigens blijft hierbij de eindverantwoordelijkheid dan bij de behoeftesteller of gebruiker liggen.

Aanbeveling 5) Inventariseer risicovolle verwerkingen van persoonsgegevens

Zoals ik u in antwoord op de vragen van het lid Verhoeven van 15 januari informeerde[16], was het AVG-onderzoek bij het LIMC aanleiding om bij alle defensieonderdelen nadrukkelijk aandacht te besteden aan de informatie-activiteiten en de naleving van de AVG bij de verwerking van persoonsgegevens. We hebben daarvoor in november en december een *quick scan* uitgevoerd. Naar aanleiding hiervan heeft de CDS in januari in afwachting van nader onderzoek uit voorzorg een beperkt aantal activiteiten aangepast of stilgelegd en ben ik hierover geïnformeerd. Het betrof activiteiten van eenheden van het Commando Zeestrijdkrachten (CZSK) en het Commando Luchtstrijdkrachten (CLSK).

De komende tijd gaat een extern bureau nader onderzoek doen naar de naleving van de AVG bij de informatieactiviteiten van verschillende defensie-onderdelen. Dit bureau zal ook nader onderzoek verrichten naar de activiteiten die nu uit voorzorg zijn aangepast of stopgezet.

Dit externe bureau wordt tevens gevraagd om de door de onderdelen gesignaleerde knelpunten voor de uitvoering van hun taken te inventariseren en aanbevelingen te doen voor het oplossen of mitigeren van deze knelpunten. Dit betrekt Defensie bij de uitkomsten van de werkgroepen onder aanbeveling 3.

Aanbeveling 6) Versterk en professionaliseer de AVG organisatie

Mede aan de hand van het onderzoeksrapport van de Functionaris Gegevensbescherming heeft Defensie een algemeen overzicht gemaakt van de meest relevante juridische bepalingen die van toepassing zijn op operationele activiteiten in de informatie-omgeving. Dit overzicht is als bijlage bij deze brief gevoegd. Alle commandanten van organisatieonderdelen die in de informatie-omgeving actief zijn, hebben hierover een gesprek met hun juridische adviseur en/of AVG-functionaris. Dit draagt bij aan de gewenste versterking van de samenwerking tussen de juridische en operationele lijn waar de Functionaris Gegevensbescherming op wijst. Het streven is deze gesprekken voor het zomerreces te hebben voltooid.

Verder neem ik het advies van de Functionaris Gegevensbescherming over om vanuit het oogpunt van een risicogerichte invulling van de AVG-organisatie als eerste een extra AVG-coördinator toe te voegen aan het Operationeel Ondersteuningscommando Land (OOCL). Daar bevindt zich het merendeel van de militaire analysecapaciteit van de landmacht waaronder het *Joint Intelligence, Surveillance, Target Acquisition & Reconnaissance Commando* (JISTARC) waar de Functionaris Gegevensbescherming op wijst. Ook gaat Defensie conform de aanbeveling in gesprek met de Functionaris Gegevensbescherming hoe zij invulling kan geven aan de functie van een *Chief Privacy Officer (CPO)* om de beleidscapaciteit op het gebied van de AVG te versterken.

Vervolg

De komende maanden krijgen deze maatregelen hun beslag en wordt aanvullend onderzoek uitgevoerd. Eind dit jaar zal ik u over de voortgang

[16] Aanhangsel Handelingen II 2020/21, nr. 2287

en de bevindingen hiervan informeren. Als daar in uw Kamer behoefte aan bestaat, ben ik graag bereid te voorzien in een Technische Briefing over het rapport en de manier waarop de aanbevelingen worden uitgewerkt.

De Minister van Defensie,
A.Th.B. Bijleveld-Schouten