VAST COMITÉ VAN TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Notitienummer 2020. 279

Toezichtonderzoek naar de manier waarop de Belgische inlichtingendiensten communiceren met een private of publieke werkgever over een werknemer

7 april 2021

I. INTRODUCTIE

I.1. CONTEXT EN VOORWERP VAN ONDERZOEK

In augustus 2019 ontving het Vast Comité I een klacht van een persoon die werkzaam was voor een publieke instelling. Deze persoon beklaagde zich over het feit dat zijn werkgever informatie had opgevraagd over hem bij een inlichtingendienst en op basis daarvan disciplinaire stappen wou ondernemen.

Het Comité besloot in de loop van de behandeling van de klacht om vooreerst een juridische analyse te voeren naar de meer algemene vraag in welke gevallen en onder welke voorwaarden een private of publieke instantie een vraag kan richten tot een of beide inlichtingendiensten over een (kandidaat-)werknemer én – nog belangrijker - in welke gevallen de betrokken inlichtingendienst hierop een antwoord mag of moet formuleren en aan welke vereisten dit antwoord vervolgens moet voldoen.

I.2. BEVOEGDHEDEN VAN HET VAST COMITÉ IPERMANENT R

Artikel 33 van de Toezichtswet van 18 juli 1991 stelt dat het Vast Comité I onderzoeken doet naar de activiteiten en de methoden van de inlichtingendiensten en naar wijze waarop zij hun opdrachten uitvoeren (wettelijkheid, efficiëntie en effectiviteit). De vraagstelling van voorliggend onderzoek betreft uitsluitend de vraag naar de wettelijkheid van het optreden van een inlichtingendienst.

Op 16 december 2019 heeft het Comité een extern juridisch advies gevraagd. Het advies handelt over de eerbiediging van de privacyrechten van werknemers in het kader van eventuele uitwisselingen tussen werkgevers en inlichtingendiensten. Het juridisch advies werd op 14 april 2020 aan het Vast Comité I toegezonden.

In voorliggend verslag worden de bevindingen van de experten samengevoegd met de analyse van het Comité. De citaten doorheen de tekst zijn afkomstig van het expertenadvies.

Bij brief van 26 februari 2021 formuleerde de ADIV enkele opmerkingen bij dit toezichtonderzoek. Daar waar nodig werden die bemerkingen in voorliggend verslag geïntegreerd.

Bij mail van 29 maart 2021 liet de VSSE weten geen bemerkingen te hebben bij de tekst. De dienst kondigde wel aan om werk te maken van een interne richtlijn aangaande de besproken problematiek.

II. HET ALGEMENE KADER

Of een inlichtingendienst nu op eigen initiatief of op vraag van een werkgever informatie verschaft over een (kandidaat-)werknemer, in beide gevallen betreft het een inmenging in de privacy en in het recht op de bescherming van persoonsgegevens, ook al betreft het een arbeidsrelatie. Dergelijke inmenging is slechts toegelaten indien er een duidelijke wettelijke basis is, indien de inmenging een legitiem doel nastreeft en proportioneel is (art. 8 EVRM, Conventie 108 en 108+ en art. 22 Grondwet).

Er dient in dit kader ook verwezen te worden naar artikel 2 §1, tweede lid, W.I&V dat stelt dat de inlichtingendiensten '*bij het vervullen van hun opdrachten zorgen (…) voor de naleving*

van, en (bij)dragen (…) tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij'.

De experten, die door het Comité waren aangesteld, verwoordden het als volgt:

> *«* Un employeur (du service public) peut-il interroger un des services de renseignement belges aux fins de savoir si un de ses travailleurs (agents) est connu de ces services ?
>
> *1. Cette première question met au centre **l'employeur et la relation de travail** entre l'agent et l'employeur. Selon que l'employeur relève du secteur privé ou du secteur public, selon les législations et réglementations spécifiquement applicables à tel ou tel secteur, à tel ou tel employeur, des nuances peuvent infléchir la portée des restrictions ou ingérences autorisées.*
>
> *Dans tous les cas cependant, l'employeur devra justifier, s'il sollicite des informations à propos d'un agent et le contrôle à son insu, que son initiative est prévue par la loi, poursuit un but légitime et est proportionnée.*
>
> *En droit belge et dans le droit européen des droits humains, la seule qualité d'employeur invoqué sans autre justification légitime ne permet pas de rencontrer ces trois exigences. La relation de travail implique le respect au droit à la vie privée et non des restrictions ou ingérences dans celui-ci.*
>
> *Il en résulte que l'appréciation de la conformité au droit positif du comportement d'un tel employeur relève avant tout du contentieux de la relation de travail, dès lors que l'agent en est averti ou en prend connaissance, et des remédiations ou sanctions propres à ce contentieux. »*
>
> *« 2. On peut toutefois en inférer qu'**un service de renseignement** à qui une telle question serait adressée et qui envisagerait d'y répondre **veillera à ce que sa saisine soit régulière**, c'est à dire fondée sur une compétence légale pertinente, poursuivant un but légitime et enclose dans le principe de proportionnalité.* [1] *»*
>
> *« 3. Certes l'agent public voit sa position caractérisée par un **devoir de réserve et de dignité** et ceci peut commander des restrictions plus larges que pour les travailleurs ordinaires. Il n'en reste pas moins que la possibilité d'exercer un contrôle secret portant sur la vie privée d'un agent répond aux principes rappelés ci-dessus et détaillés comme suit dans la jurisprudence :*
>
> - *existence de dispositions légales habilitant à procéder à un contrôle secret à l'égard de l'intéressé ;*
> - *accessibilité et prévisibilité de ces dispositions, notamment la question de savoir si l'intéressé savait, au moment où il a été engagé, qu'il pouvait être exposé à un contrôle secret de ses activités ne relevant pas directement de sa mission ;*
> - *précision de ces dispositions (cas dans lequel un contrôle secret peut être pratiqué, type de mesures pouvant être pratiquées, conditions dans lesquelles ces mesures peuvent être opérées…) ;*
> - *étendue du contrôle pratiqué ;*
> - *garanties procédurales offertes par ces dispositions pour éviter tout arbitraire. »*

Voor alle duidelijkheid: geen enkele bepaling uit de Inlichtingenwet verbiedt dat een private of publieke instantie een vraag zou richten tot een van de Belgische inlichtingendiensten.

---

[1] De ADIV stelde in dit kader het volgende: « *En principe, Le SGRS demande la base légale qui fonde la demande de 'screening'. Néanmoins, il n'appartient pas au SGRS de vérifier que l'autorité qui pose la question respecte bien son cadre légal. C'est d'autant plus vrai lorsqu'elle transmet au SGRS des informations sur une menace potentielle. Le SGRS va traiter toute information pertinente qu'il reçoit, peu importe si l'autorité a, par exemple, violé son secret professionnel pour transmettre l'information. C'est la même chose pour une source ou un service partenaire. Il n'appartient pas au SGRS de 'contrôler' ses sources au sens large. Par contre il est évident qu'il ne transmettra des informations que si son cadre légal propre le lui permet.* »

Indien een werkgever informatie opvraagt bij een inlichtingendienst, betekent dit onvermijdelijk dat hij ook persoonsgegevens meedeelt aan deze dienst, zeker indien hij zijn vraag om informatie contextualiseert. Ook dit vormt een inmenging in het privéleven die slechts mogelijk is indien er een duidelijke wettelijke basis voorhanden is. De Inlichtingenwet laat dit toe in de mate waarin de werkgever met rede van oordeel is dat de inlichtingen nuttig kunnen zijn voor de uitvoering van de opdrachten van de betrokken inlichtingendienst (art. 14 W.I&V m.b.t. publieke actoren; art. 16 W.I&V m.b.t. private actoren).

Bij het beantwoorden van de vraag of er informatie van een inlichtingendienst mag doorstromen naar een private of publieke werkgever, is het ook van belang te wijzen op het specifieke en strafrechtelijk gesanctioneerde beroepsgeheim waaraan de leden van de inlichtingendiensten onderworpen zijn (art. 36 W.I&V). Ook deze bepaling maakt duidelijk dat dergelijke informatiestromen alleen kunnen als de wet dit expliciet toelaat. Daarbij moet opgemerkt worden dat de loutere bevestiging dat een persoon al dan niet 'gekend' is door een inlichtingendienst, zonder hierover in detail te treden, ook onder deze regeling valt.

De Belgische wetgever heeft slechts in twee gevallen voorzien dat een werkgever (op eigen verzoek of op initiatief van de inlichtingendienst) rechtstreeks of onrechtstreeks informatie kan bekomen over een (kandidaat-)werknemer: in geval van een veiligheidsscreening of in geval van een dreiging. Ook de loutere vraag of een (kandidaat-)werknemer[2] al dan niet 'gekend' is bij één van de twee Belgische inlichtingendiensten, moet kunnen aangeknoopt worden bij een van deze twee regelingen.

III. DE WERKGEVER WIL EEN VEILIGHEIDSSCREENING

III.1. DE WETTELIJKE BASIS VOOR VEILIGHEIDSSCREENINGS

Met veiligheidsscreenings worden situaties bedoeld waarbij een werkgever, los van een voorafgaandelijk element, alle personen wil laten *screenen* die een bepaalde toelating of vergunning behoeven. De meest klassieke voorbeelden zijn deze van een veiligheidsmachtiging om toegang te krijgen tot geclassificeerde informatie, het veiligheidsattest om toegang te krijgen tot een bepaald locatie of een bepaald evenement, of nog, het veiligheidsadvies dan kan aangevraagd worden voor tientallen verschillende toelatingen. Een private of publieke werkgever kan van deze mogelijkheden gebruik maken onder de voorwaarden bepaald in de Classificatiewet van 11 december 1998 en haar verschillende uitvoeringsbesluiten. Algemeen gesproken is het gebruik van deze instrumenten alleen toegelaten indien het niet-geëigend gebruik van een toelating of vergunning (door bijv. een werknemer) schade kan toebrengen aan fundamentele staatsbelangen.

In principe zal de werkgever zelf hier niet in kennis worden gesteld van de persoonsgegevens die naar aanleiding van de verificatie of het onderzoek naar boven komen. Hij krijgt meestal alleen het resultaat van de *screening*: de veiligheidsmachtiging of het –attest worden wel/niet toegekend; het veiligheidsadvies is positief/negatief. Het is de veiligheidsofficier[3] die op de hoogte zal zijn van de concrete elementen van het dossier. Maar

---

2 Voor alle duidelijkheid: de onderstaande analyse geldt onverkort het eventuele 'beschermde' statuut dat op een werknemer van toepassing zou zijn.

3 De veiligheidsofficier is de persoon aangeduid binnen een private of publieke instantie, die instaat voor de naleving van de classificatieregels. Hij is ook de contactpersoon tussen de instantie, de betrokkene en de bevoegde veiligheidsoverheid.

deze veiligheidsofficier is op zijn beurt onderworpen aan een specifiek en strafrechtelijk gesanctioneerd beroepsgeheim (artt. 23 en 24 Classificatiewet) Hij kan de elementen waarover hij beschikt niet zomaar meedelen aan de werkgever.

De Classificatiewet voorziet niet enkel in een *screening* en mededeling van informatie bij de initiële toelating of vergunning. In bepaalde gevallen (bijv. bij een veiligheidsmachtiging) is de werknemer onderworpen aan een vorm van een 'permanente s*creening*'. Hij moet m.a.w. gedurende de hele looptijd van zijn machtiging voldoen aan de vereisten om die machtiging te bekomen. Indien een werkgever op een gegeven ogenblik twijfelt aan die voorwaarde, kan hij hierover zijn veiligheidsofficier raadplegen. Deze kan op zijn beurt de veiligheidsoverheid en/of de onderzoekende inlichtingendienst vatten. Maar niets belet dat de werkgever rechtreeks contact opneemt met een inlichtingendienst indien hij van oordeel is dat hij over informatie beschikt die nuttig is voor de uitoefening van hun opdrachten (artt. 14 of 16 W.I&V).

Wat betreft de veiligheidsscreenings is het dus van belang te onderlijnen dat de wettelijke regeling duidelijk bepaalt welke persoonsgegevens (bijv. de gegevens opgesomd in art. 22*sexies* Classificatiewet en in het ter uitvoering van deze bepaling genomen KB van 8 mei 2018), onder welke vorm (bijv. een onderzoeksverslag) aan welke bestemmeling (meestal een veiligheidsoverheid) kan worden overgezonden.

III.2. ARTIKEL 19, EERSTE LID, EERSTE ZINSNEDE W.I&V[4]

Tot slot wijst het Comité er andermaal op dat artikel 19 van de Inlichtingenwet geen grondslag biedt voor het systematisch doorgeven van informatie aan werkgevers die hierom verzoeken in het kader van de door hen te verlenen toelatingen of vergunningen.[5]

IV. DE WERKGEVER IS HET VOORWERP VAN EEN (VERMEENDE) DREIGING

IV.1. ARTIKEL 19, EERSTE LID, LAATSTE ZINSNEDE W.I&V

Artikel 19 W.I&V luidt als volgt: '*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee (…) aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11*.'

---

[4] Het volledige eerste lid van art. 19 luidt als volgt: "*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een [dreiging] bedoeld in de artikelen 7 en 11*."

[5] Uit onderzoek bleek dat de Dienst Veiligheidsverificaties van de VSSE *screenings* uitvoert zonder dat daarbij de wettelijke basis duidelijk kan aangegeven worden (*supra*). In bepaalde gevallen is het daarbij niet duidelijk wat de precieze finaliteit is van de vraag, m.a.w. of het om een veiligheidsscreening gaat of om een andere controle in de databank van de VSSE. Hiervoor verwees de VSSE (verkeerdelijk, *supra*) systematisch naar artikel 19 W.I&V. Alhoewel het nuttig en raadzaam kan zijn dat de Belgische diensten worden geconsulteerd met betrekking tot Belgische ingezetenen aan wie eventueel toegang zou worden verschaft tot de installaties van in België gevestigde internationale instellingen, is hiervoor een wettelijk mandaat vereist (VAST COMITÉ I, *Activiteitenverslag 2019*, 2 e.v.).

Deze bepaling vormt een duidelijke wettelijke basis voor een inlichtingendienst om (persoons)gegevens mee te delen aan publieke of private[6] personen en instanties, en dus desgevallend ook aan een werkgever wiens werknemer een dreiging vormt die wettelijk gezien moet worden opgevolgd door de VSSE of de ADIV.

Deze bepaling vormt, in samenlezing met artikel 14 of 16 W.I&V, ook de wettelijke grondslag voor een verontruste publieke of private werkgever die een inlichtingendienst bevraagt over zijn werknemer omdat die naar het oordeel van de werkgever een (mogelijke) dreiging vormt in de zin van de Inlichtingenwet. Deze bepalingen vormen ook de wettelijke basis om naar aanleiding van deze vraag desgevallend concrete elementen mee te delen over de werknemer die die (vermeende) dreiging aannemelijk kunnen maken.[7]

Deze mededeling/vraag kan voor een inlichtingendienst uiteraard de aanleiding vormen om een inlichtingenonderzoek op te starten. Het al dan niet opstarten van een dergelijk onderzoek alsook de diepgang ervan, staat juridisch gezien los van de vraag of en wat een inlichtingendienst aan een werkgever mag meedelen.[8]

IV.2. TWEE EERDERE TOEZICHTONDERZOEKEN VAN HET COMITÉ

In 2014-2015 voerde het Comité een klachtonderzoek waarbij de toepassing van de laatste zinsnede van artikel 19, eerste lid, W.I&V centraal stond.[9] De resultaten worden hieronder samengevat weergeven. Verschillende aspecten van deze samenvatting komen verder diepgaander aan bod.

Volgens de klager die zich in 2014 bij het Comité had aangemeld, zou de inhoud van persoonlijke e-mails die hij had verzonden naar een lid van het ministerie van Defensie, via de militaire inlichtingendienst bij zijn werkgever zijn beland. Kort daarop werd hij ontslagen. Daarbij verwees de werkgever expliciet naar het feit dat hij in het bezit was gesteld van een kopie van de bewuste e-mails door een personeelslid van de ADIV. Het onderzoek moest duidelijk maken op welke wijze het dossier werd behandeld door de ADIV, of de dienst zich daarbij hield aan de vigerende regelgeving en of er inderdaad informatie was doorgegeven aan een derde. De e-mails in kwestie waren bij de ADIV terecht gekomen via het lid van het ministerie van Defensie. De klager had in zijn berichten immers – bij wijze van grap, zo bleek achteraf – gemeld dat hij een computervirus had doorgezonden. De ADIV is de aangewezen dienst om dergelijke potentiële dreiging te onderzoeken; dit behoort tot zijn wettelijke

---

6 De wet verwijst alleen naar 'instanties en personen'. Er is geen reden om aan te nemen dat deze regeling, anders dan de eerste zinssnede van artikel 19, eerste lid, W.I&V, beperkt zou zijn tot publieke (rechts)personen.

7 Geen enkele bepaling uit de W.I&V verbiedt een werkgever om vragen te stellen aan een inlichtingendienst. Integendeel, indien een overheidsdienst van oordeel is dat gevoelige informatie gevaar loopt te worden gecompromitteerd of dat er sprake kan zijn van spionagedreiging of inmenging in besluitvormingsprocessen, belet niets de ambtenaren van die overheidsdienst zich te wenden tot de meest bevoegde inlichtingendienst. Niets belet een werkgever van een openbare dienst dus om informatie te verstrekken of vragen te stellen over een van zijn personeelsleden. Dit betekent echter niet dat de inlichtingendiensten de gestelde vraag kunnen of moeten beantwoorden. Het feit dat de inlichtingendienst een vraag niet kan (of wil) beantwoorden, betekent niet dat het onwettig of onrechtmatig is om de vraag te stellen.

8 Uiteraard is het niet legitiem een (per definitie privacyschendend) onderzoek te starten indien er geen enkele aanwijzing is van een potentiële of concrete dreiging tegen fundamentele staatsbelangen.

9 VAST COMITÉ I, *Activiteitenverslag 2015*, 41 e.v. ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde').

opdrachten. Naast het informaticaonderzoek, won de ADIV ook inlichtingen in over de klager zelf om zo de eventuele bedreiging te kunnen beoordelen. Ook dit behoort tot zijn bevoegdheden. Het resultaat van dit technisch onderzoek (waaruit bleek dat er geen bedreiging was) werd in algemene bewoordingen ter kennis gebracht van de veiligheidsofficier van de onderneming waar de klager werkte. Deze mededeling – zo oordeelde het Comité destijds vond haar wettelijke grondslag in artikel 19 W.I&V.

Ook in een eerder toezichtonderzoek[10] sprak het Vast Comité I zich uit over de toepasbaarheid van deze bepaling. Het Comité stelde zich de vraag welke 'tegenmaatregelen' kunnen genomen worden indien buitenlandse inlichtingendiensten over hun diaspora heimelijk inlichtingen verzamelen op Belgisch grondgebied: *'Duidelijk is alleszins dat zij niet 'actief' kunnen optreden om de loop van gebeurtenissen te beïnvloeden. Het wettelijk kader laat de mogelijkheden tot rechtstreekse interventies slechts beperkt toe. Het hoofd van de VSSE of de ADIV kan zijn buitenlandse collega slechts mondeling interpelleren of de diaspora inlichten van de activiteiten die een buitenlandse inlichtingendienst ten aanzien van die gemeenschap onderneemt'* en dit op basis van de bewuste zinsnede van artikel 19 WI&V.

IV.3. EEN NADERE UITWERKING VAN DEZE REGELING IN EEN RICHTLIJN?

Alhoewel het Comité van oordeel is dat de laatste zinsnede van artikel 19, eerste lid W.I&V voldoende duidelijk is als de wettelijke basis voor informatieoverdracht naar publieke en private instanties[11], is er wél een verplichting om de modaliteiten van deze mogelijkheid regeling nader uit te werken.

Ingevolge artikel 20 §3 W.I&V dient de Nationale Veiligheidsraad (NVR) in een richtlijn de voorwaarden te bepalen waaronder inlichtingen kunnen worden meegedeeld aan private of publieke instanties of personen. Voor zover het Comité kon nagaan, werd tot op heden niet voldaan aan deze verplichting wat betreft de situatie van personen en instanties die het voorwerp zijn van een dreiging. Het Comité had in het kader van een onderzoek m.b.t. de strijd tegen terrorisme en extremisme reeds aangedrongen op zo'n richtlijn.[12] Het herhaalt zijn aanbeveling met klem. De richtlijn moet de inlichtingendiensten houvast bieden in deze delicate materie waar de gevolgen van het al dan niet meedelen van informatie ernstig kunnen zijn voor algemene én private belangen.

---

10 VAST COMITÉ I, *Activiteitenverslag 2012*, 14 e.v. ('II.2. De opvolging van buitenlandse inlichtingendiensten ten aanzien van hun diapsora in België').

11 M.b.t de mogelijkheid voorzien in artikel 19 eerste lid om inlichtingen door te zenden naar gerechtelijke overheden stelde het Comité zich vragen bij de kwaliteit van deze regeling: *"Is deze regeling dermate opgesteld dat ze beantwoordt aan de eis van voorzienbaarheid [zoals vervat in art. 8 EVRM en art. 22 Grondwet, nvda]? Weet een burger dat de gegevens die een inlichtingendienst over hem zou kunnen hebben voor doel A, naar een andere overheid kunnen doorgespeeld worden voor doel B? En is dit doel B steeds een legitiem doel in de zin van artikel 8 EVRM? En wat met de proportionaliteit? Al speelt deze problematiek minder bij de overdracht van informatie naar het gerecht, toch is het Vast Comité I is van oordeel dat de regeling uit artikel 19 nader moet worden uitgewerkt via een publiek te maken richtlijn, die het Ministerieel Comité voor inlichting en veiligheid ter uitvoering van artikel 20 moet nemen.'* (VAST COMITÉ I, *Activiteitenverslag 2004*, 120).

12 *"De inlichtingendiensten moeten criteria uitwerken voor het in kennis stellen van personen die het voorwerp zijn van een dreiging (art. 19 W.I&V)."* Het Comité beval aan dat beide inlichtingendiensten criteria zouden uitwerken inzake de toepassing van deze bepaling (VAST COMITÉ I, Activiteitenverslag 2012, 92).

Ook op het niveau van de inlichtingendiensten werd ter zake geen nadere regeling uitgewerkt.

De ADIV deelde mee over geen interne richtlijn/SOP te beschikken die omschrijft hoe haar personeel dient om te springen met deze problematiek.[13]

Wat betreft de VSSE kan verwezen worden naar twee richtlijnen. Vooreerst is er de als vertrouwelijk geclassificeerde instructie van 10 oktober 2016 die handelt over de wijze waarop dient gereageerd te worden in geval van een vraag vanuit een publieke overheid om verificatie van een bepaalde persoon. Deze richtlijn verduidelijkt niet op basis van welke wettelijke regeling bepaalde antwoorden moeten worden verschaft. De richtlijn lijkt niet van toepassing op de situatie voorzien in de laatste zinsnede van artikel 19, eerste lid, W.I&V. Alleszins regelt zij niet de verhouding met private actoren. Het Comité plaatst overigens vraagtekens bij de wettelijkheid van sommige passages van deze richtlijn, omdat ze schijnbaar ingaan tegen de wettelijke regeling inzake veiligheidsscreenings. Daarnaast stelde de VSSE in 2018 ook een vertrouwelijk geclassificeerde richtlijn op over disruptief optreden of verstoren. Dit is het dermate hinderen van dreigingen opdat deze niet langer plaatsvinden of dat de schadelijkheid ervan aanzienlijk wordt teruggebracht. Alhoewel het meedelen van informatie aan een persoon of instantie die het voorwerp is van een dreiging, perfect onder die definitie te brengen is, wordt in die richtlijn nergens verwezen naar artikel 19 W.I&V, noch naar enige andere wettelijke bepaling.

Het Comité dringt dan ook aan op een algemene, omvattende richtlijn van de Nationale Veiligheidsraad. Die richtlijn zou alleszins een antwoord moeten bieden op onderstaande vragen en aandachtspunten.

IV.4. LIMIETEN GESTELD DOOR DE INLICHTINGENWET

In welke gevallen en binnen welke limieten mag nu toepassing worden gemaakt van de mogelijkheid voor een inlichtingendienst om een (publieke of private) derde op de hoogte te brengen van inlichtingen waarover ze beschikt?

De dreigingen die bedoeld worden in artikel 19 W.I&V zijn wat betreft de VSSE, elke activiteit van spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land in het gedrang kan brengen (art. 7 W.I&V). Er moet dus niet alleen een bepaalde activiteit zijn van de werknemer (bijv. extremisme), deze moet ook een gevaar inhouden voor een of meerdere fundamentele staatsbelangen. En in de context van artikel 19 W.I&V moet die private of publieke instantie ook het voorwerp zijn van de dreiging. Een werkgever mag dus niet geïnformeerd worden over bijv. de extremistische activiteiten van zijn werknemer, indien die werkgever op geen enkele wijze zelf het voorwerp is van een dreiging.

Het weze ook duidelijk dat er geen toepassing mag gemaakt worden van artikel 19 W.I&V wanneer er op geen enkele wijze fundamentele staatsbelangen op het spel staan zoals bijv. imagoschade voor een privébedrijf (tenzij dit bijv. het verlies van het vertrouwen in bepaalde

---

13 De ADIV wijst er op dat het zich in dit kader baseert op de bestaande wettelijke regelingen (Classificatiewet van 11 december 1998 voor verificaties; artikel 19 Inlichtingenwet voor mededeling info aan werkgevers i.g.v. een dreiging; andere wettelijke bepalingen).

instellingen betekent), een slechte werkssfeer of een financieel verlies (tenzij deze financiële belangen die individuele belangen van de onderneming overstijgen en als fundamenteel voor het land kunnen aanzien worden).

De dreigingen die voor de ADIV een aanleiding kunnen zijn om publieke of private instanties of personen te verwittigen, moeten gevonden worden in artikel 11 W.I&V. Het betreft bijvoorbeeld elke activiteit die een bedreiging betekent voor de onschendbaarheid van het nationaal grondgebied of de bevolking, de militaire defensieplannen, het wetenschappelijk en economisch potentieel met betrekking tot bepaalde bedrijvenactief in defensie-gerelateerde sectoren, de vervulling van de opdrachten van de strijdkrachten, de veiligheid van de Belgische onderdanen in het buitenland, de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert, …

Aangezien de mededeling van gegevens op basis de laatste zinsnede van artikel 19, eerste lid, W.I&V een duidelijke finaliteit heeft (vrijwaren van fundamentele staatsbelangen tegen bepaalde activiteiten waarvan de betrokken instantie of persoon het voorwerp is), moet de mededeling van (persoons)gegevens ook beperkt zijn tot die informatie die bijdraagt tot het opvolgen of – indien nodig - neutraliseren van de dreiging.

> *« Avant de répondre et en vue de répondre, les services de renseignement s'assureront en conséquence du fondement, de la motivation et de la pertinence de la question relative à un agent qui leur est adressée. Nul doute que s'ils réservent une réponse aux questions qui leur sont posées (ceci relève davantage de la deuxième question ci-après), ils engagent leur responsabilité. Nous visons bien ici le fait* ***de répondre*** *aux questions posées par un employeur, et non le fait de diligenter une enquête pour les bes oins propres des services, à la suite des questions posées, sans répondre à ces dernières. »*
>
> *« 4. Tout employeur normalement prudent et diligent veillera donc à cadrer sa demande dans le respect de ces principes. Il sera prudent, pour les services, de veiller à ne répondre le cas échéant qu'à des demandes satisfaisant à ces exigences. À défaut, la communication des informations par les services pourrait constituer une violation du droit à la protection de la vie privée dans les organes juridictionnels et non juridictionnels de contrôle pourront être saisis : c'est tout l'objet de la deuxième question. »*
>
> *« La question est de savoir si le service de renseignement est tenu de répondre, s'il peut répondre ou si, au contraire, il lui est interdit de répondre.*
>
> *5. La réponse à cette question doit être analysée au regard des* ***missions assignées au service de renseignement*** *: le principe de finalité commande la réponse. Le service doit n'avoir en vue que l'accomplissement de sa mission propre ; il ne peut accepter d'être instrumentalisé. En d'autres termes, il n'a aucune obligation de répondre, voir même il lui est interdit de répondre sauf dans la mesure où la bonne fin des missions propres qui lui sont confiées commande de répondre.*
>
> *L'éventuelle obligation de répondre ne peut venir que d'une* ***législation spécifique*** *conférant au service de renseignement* ***une mission*** *dont découle cette obligation, et non de la demande qui lui est adressée par un employeur. Une telle obligation éventuelle aura toujours le statut d'une exception à la règle : le respect au droit de la vie privée des agents. »*

De eerste verplichting van een inlichtingendienst die wordt geconfronteerd met een verzoek om informatie is dan ook na te gaan om welk probleem, welk incident, welke dreiging het zou kunnen gaan. In dit verband zou de inlichtingendienst zijn databanken kunnen raadplegen om de aan hem meegedeelde naam of namen te verifiëren.[14] Het lijkt ook voor de hand te liggen

[14] Dit is ook wat de richtlijn van de VSSE van 10 oktober 2016 (VERTROUWELIJK) voorschrijft bij een vraag van een publieke overheid om een persoon te verifiëren.

dat de inlichtingendienst contact opneemt met de werkgever om het verzoek in de juiste context te plaatsen. Daartoe zal met name moeten worden nagegaan waarom de werkgever wil weten of zijn werknemer bekend is bij de inlichtingendiensten, wat het probleem en de dreiging is, of er een veiligheids- of ander incident is geweest, of er sprake is van een noodsituatie…

Indien die gegevens geen uitsluitsel geven in de ene of de andere richting, kan verder onderzoek door de dienst aangewezen zijn. De reikwijdte van dit onderzoek kan niet in abstracto worden bepaald. Dit zal afhangen van de aard van de bedreiging en van de informatie die in de loop van het onderzoek naar voren komt. Bij dergelijk onderzoek zal de dienst alleszins rekening moeten houden met de proportionaliteits- en subsidiairiteitsprincipes.

De antwoorden op deze vragen en de resultaten van het bijkomende onderzoek moeten de inlichtingendienst toelaten te beoordelen of ze in deze bevoegd is en desgevallend toepassing kan maken van artikel 19 W.I&V en wat ze, gelet op de dreiging, al dan niet kan meedelen aan de werkgever.

IV.5. WAT MAG OF MOET WORDEN MEEGEDEELD?

Eerst wordt kort de hypothese aangehaald waarbij de inlichtingendienst in hoofde van de werknemer (eventueel na een eerste bevraging of na een grondiger inlichtingenonderzoek) *geen enkele* dreiging in de zin van de Inlichtingenwet vaststelt. Op dat ogenblik maakt de werkgever per definitie niet het voorwerp uit van een dreiging en kan strikt genomen geen toepassing gemaakt worden van artikel 19 W.I&V. Het Comité is echter van oordeel dat in deze gevallen aan de inlichtingendienst de mogelijkheid moet gelaten worden om de werkgever mee te delen dat er geen sprake is van een dreiging in de zin van de Inlichtingenwet (hetgeen uiteraard niet betekent dat er geen andersoortige dreiging kan zijn voor de werkgever). Het Comité oordeelde reeds in die zin in het in 2014-2015 gevoerde klachtonderzoek (zie IV.2.).

In wat volgt, wordt er van uit gegaan dat er effectief sprake is van een dreiging. De vraag stelt zich vervolgens wat op welke wijze kan meegedeeld worden.

IV.5.1. Het proportionaliteits- en subsidiariteitsbeginsel

> *« 6. Les limites de la réponse éventuelle sont circonscrites* ***par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, qui doit être mise en œuvre en combinaison avec l'article 74 de la loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel.***
>
> *On voit que le traitement des données impliquant la communication de celle-ci à l'employeur est licite :*
> *– lorsqu'il est "utile" au respect des obligations incombant au service de renseignement ;*
> – *ou lorsqu'il est "nécessaire" (et non seulement "utile" ; on retrouve ici le principe de nécessité qui est au cœur du principe de proportionnalité) à la mission dont est investie de l'autorité publique destinataire des informations communiquées par le service de renseignement. »*
>
> *« 7. On mesure donc les limites très strictes dans lesquelles doit être contenue une réponse éventuelle du service de renseignement. Pour que le service puisse répondre, il faut qu'il ait à transmettre des informations résultant du traitement de données à caractère personnel qui soit* ***« nécessaire » à la mission dont est investie l'autorité publique destinataire*** *des informations communiquées.*
> *En d'autres termes, s'il est toujours licite que le service de renseignement puisse procéder au traitement de données consistant en une collecte de données pertinentes et à jour lorsque celui-ci est simplement*

***« utile » à l'accomplissement de ses obligations propres**, ceci ne lui donne pas pour autant l'autorisation de communiquer ces informations et de répondre ainsi à la demande qui lui a été adressée. Elle ne le pourra que si le résultat du traitement se révèle nécessaire à la bonne fin de la mission de l'autorité qui l'aura interrogée. »*

*« 8. Pour rappel, **ce rapport de nécessité s'interprète restrictivement** dès lors que l'on est dans le domaine des ingérences et restrictions aux droits au respect de la vie privée.*
La seule existence d'un lien d'emploi non autrement qualifié n'est pas de nature à justifier cette nécessité. Il faudrait encore que l'autorité ayant interrogé la sûreté ait été en mesure de décrire et de justifier les faits spécifiques pertinents (responsabilité spécifique de l'agent, dimension opérationnelle propre de son emploi…) qui justifieraient la communication des données « nécessaires » pour la bonne fin de la mission propre de cette autorité.

– *À défaut, la demande comme l'éventuelle réponse que cette demande aura appelée constitueront une violation du droit à la protection de la vie privée dont les organes juridictionnels ou non juridictionnels de contrôle pourront être saisis. »*

Gelet op de eisen van de proportionaliteit en de subsidiariteit moet de eerste vraag zijn of de werkgever *überhaupt* in kennis mag gesteld worden. Indien de dreiging zeer vaag en weinig ernstig is, of indien de dienst de evaluatie van de dreiging zelf kan opvolgen of de dreiging kan counteren op een andere wijze (bijv. door de werknemer zelf aan te spreken zodat die zich realiseert dat hij wordt opgevolgd), dan is een mededeling van persoonsgegevens aan een werkgever mogelijk disproportioneel en niet subsidiair.

Indien dit niet volstaat en de dreiging is voldoende ernstig, dan dient de mogelijkheid zich aan om de werkgever in kennis te stellen. Ook hier moet worden afgewogen hoeveel en welke informatie wordt gegeven. De regel hierbij is opnieuw dat er, gegeven de aard en de ernst van de dreiging en nood en de mogelijkheden om deze te counteren, gestreefd wordt naar een de minimale inmenging in het privéleven.

Indien de dreiging echter dermate ernstig is dat deze alleen door een tussenkomst van de werkgever kan gecounterd worden, kan méér en concretere informatie worden meegedeeld die bijvoorbeeld kan dienen om een administratieve of private beslissing (bijv. disciplinaire sanctie, overplaatsing, ontslag…), te onderbouwen. Het weze duidelijk dat het uiteindelijke doel van de inlichtingendienst hier het neutraliseren of verkleinen van een dreiging moet zijn.

Aansluitend bij de vraag naar een proportionele informatieverstrekking, rijst de vraag of een inlichtingendienst in zijn mededeling zelf een oplossing mag suggereren aan de bedreigde publieke of private instantie[15] of – sterker nog – mag deelnemen aan de besluitvorming over het handelen door de bedreigde instantie of persoon. Bedoeld wordt bijvoorbeeld de suggestie om iemand te ontslaan. Het Comité is van oordeel dat dit niet onwettelijk is in de mate waarin de gesuggereerde oplossing zelf wettelijk en proportioneel is.

Tot slot stelt zich de vraag of uit artikel 19 W.I&V een *verplichting* blijkt om te antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. De bepaling stelt dat de inlichtingen- en veiligheidsdiensten hun inlichtingen *'slechts meedelen'* aan instanties en personen die het voorwerp zijn van een dreiging. Alhoewel de bepaling op dit vlak niet erg duidelijk is, is het Comité van oordeel dat een inlichtingendienst verplicht is om gegevens mee te delen indien alleen hierdoor de realisatie van een ernstige dreiging tegen fundamentele staatsbelangen kan voorkomen worden. In de andere gevallen bepaalt zij autonoom wat de

[15] Dit is wat door de VSSE 'secundaire disruptie' wordt genoemd.

beste strategie vormt, gegeven de dreiging.[16] Het Comité beveelt aan dat deze onduidelijkheid wordt opgehelderd ofwel door een wetgevend initiatief ofwel door een regeling ter zake in de verplicht op te stellen richtlijn van de Nationale Veiligheidsraad.

Hierbij aansluitend suggereert het Comité om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in een Gemeenschappelijke gegevensbank Terrorist Fighters of Haatpredikers.

IV.5.2. Het zorgvuldigheidsbeginsel

Bij dit alles moet ook aandacht worden besteed aan de kwaliteit van de gegevensverstrekking. In een inlichtingencontext bestaan er weinig zekerheden, en dit gegeven moet mee de beslissing bepalen om en hoe een werkgever te informeren. Om over een rechtmatige informatievertrekking te kunnen spreken, moet de mededeling voldoende onderbouwd zijn door betrouwbare inlichtingen. Ze dient daarenboven zorgvuldig verwoord te zijn. Er mag bijvoorbeeld geen ongenuanceerd beeld wordt gegeven van de onderliggende inlichtingen, of een bepaald element mag niet als 'vaststaand' worden voorgesteld indien het om 'een visie over' of 'een aanvoelen van' gaat. De meegedeelde informatie moet in die zin ook 'eerlijk' zijn door een objectief beeld te bieden van de wijze waarop de inlichtingendienst de dreiging en de rol van de betrokkene daarin ziet, zonder 'manipulatief' te zijn in die zin dat ze de besluitvorming van private of publieke werkgever wil sturen.

IV.5.3. Geclassificeerde gegevens

Niet elke private en publieke instantie beschikt over een veiligheidsmachtiging. Dit betekent dat geclassificeerde informatie zal moeten gedeclassificeerd worden. Dit geldt des te meer indien de informatie moet dienen om een beslissing van de werkgever te schragen. Deze omslag dient uiteraard ook zorgvuldig te gebeuren. Enerzijds moet geheim blijven wat geheim moet blijven; anderzijds moet de informatie de werkgever (en mogelijks nadien de werknemer en zelfs een jurisdictionele instantie) toelaten de waarde van de informatie te beoordelen.

IV.5.4. Mondelinge of schriftelijke mededeling van informatie

Artikel 19 W.I&V bepaalt niet op welke wijze een bedreigde instantie in kennis moet worden gesteld. Het Comité is van oordeel is dat dit om redenen van rechtszekerheid, behoudens hoogdringendheid, schriftelijk dient te gebeuren. Dit om discussies achter te vermijden en een parlementaire of zelfs jurisdictionele controle toe te laten.

Het Comité heeft in dit verband reeds aanbevolen dat de VSSE elke analyse systematisch zou afsluiten met een (weze het beknopte of voorlopige) conclusie, teneinde vast te leggen óf

---

16 Ook m.b.t de informatieoverdracht naar gerechtelijke overheden (eerste zinsnede van art. 19, eerste lid, W.I&V) stelde het Comité eerder het volgende: "*Alhoewel dit niet zo duidelijk is, lezen wij in artikel 19 geen verplichting om gegevens over te maken. De bepaling is anders geredigeerd; ze houdt een verbod in ('slechts') om bepaalde gegevens mee te delen en dus een mogelijkheid voor de andere informatie. Wel zou de richtlijn die het Ministerieel Comité voor inlichting en veiligheid in uitvoering van artikel 20, § 3, zou moeten nemen, een verplichting in het leven kunnen roepen. Het Vast Comité I heeft geen kennis van dergelijke richtlijn.*" (VAST COMITÉ I, *Activiteitenverslag 2004*, 119).

en op welke wijze en met welke intensiteit het voorwerp van de analyse (een persoon, groepering, gebeurtenis of fenomeen) verder moet worden opgevolgd.[17]

V. CONCLUSIES EN AANBEVELINGEN

Voor de informatieverstrekking door de inlichtingendiensten aan een private of publieke werkgever gelden – terecht – strenge regels, omdat de mededeling grote gevolgen kan hebben voor de betrokken personen. Minimaal betekent dit een inbreuk op de privacy en in het uiterste geval kan het de basis vormen voor ingrijpende maatregelen die de betrokkenen in hun rechtspositie kunnen aantasten.

Indien de VSSE en de ADIV op eigen initiatief of op verzoek informatie verstrekken aan een publieke of private werkgever (en het loutere meedelen of een persoon 'gekend' is of niet valt daar ook onder), moet aan alle wettelijke vereisten voldaan zijn, te weten:

1. er moet een specifieke wettelijke grondslag zijn;
2. de dienst moet zorgvuldig tewerk gaan bij de interne totstandkoming van de te verstrekken gegevens en in de communicatie daarover naar de ontvanger;
3. de mededeling moet beantwoorden aan de eisen van de noodzakelijkheid; en
4. de mededeling moet proportionaliteit zijn.

Wat betreft de wettelijke basis, benadrukt het Comité dat het buiten de twee besproken situaties (m.n. de werkgever wil een veiligheidsscreening of de werkgever is voorwerp van dreiging) niet toegelaten is om informatie te verschaffen over een werknemer aan een publieke of private werkgever. Vanuit het oogpunt van de inlichtingenagent is dergelijke mededeling afhankelijk van de concrete situatie mogelijks zelfs strafbaar.

Het Comité beklemtoont tevens dat niets een werkgever uit de overheids- of de privésector belet om informatie mee te delen aan of vragen te stellen aan een Belgische inlichtingendienst over een mogelijke bedreiging in de zin van de Wet van 30 november 1998 waarvan een van zijn personeelsleden de 'oorzaak' zou zijn.

Het Comité nodigt spelers uit de publieke en private sector wel uit om te onderzoeken of bepaalde potentiële dreigingen niet preventief kunnen ondervangen worden door voor bepaalde functies, toelatingen of vergunningen een beroep te doen op het systeem van de veiligheidsscreenings uit de Classificatiewet. Het Comité benadrukt wel dat dit systeem oordeelkundig moet gebruikt worden en niet mag leiden tot een ongebreidelde toepassing.

Het Comité is van oordeel dat de VSSE en de ADIV binnen zes maanden na het afsluiten van deze studie een voorstel tot richtlijn ter uitvoering van de laatste zinsnede van artikel 19, eerste lid, moeten opstellen ten behoeve van respectievelijk de minister van Justitie en van Defensie met het verzoek het voorstel ter goedkeuring voor te leggen aan de Nationale Veiligheidsraad.

Tevens dient de VSSE zijn twee hierboven besproken richtlijnen te evalueren en aan te passen aan het wettelijke kader. Gelet op het belang van deze materie, dient deze aanpassong ook te gebeuren binnen een termijn van zes maanden.

Verder beveelt het Comité aan dat de wetgever zou verduidelijken of artikel 19, eerste lid, laatste zin W.I&V ook een verplichting inhoudt om onder bepaalde gevallen *verplicht* te

[17] VAST COMITE I, *Activiteitenverslag 2013*, 115.

antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. In afwachting van een wetgevend initiatief moet deze kwestie geregeld worden in de richtlijn van de Nationale Veiligheidsraad.

Hierbij aansluitend suggereert het Comité om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in een Gemeenschappelijke gegevensbank Terrorist Fighters of Haatpredikers.