Inspectie Justitie en Veiligheid
Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Griffier Tijdelijke Commissie Digitale Toekomst
van de Tweede Kamer der Staten-Generaal,
de heer R. Jansma
Postbus 20018
2500 EA DEN HAAG

Inspectie Justitie en Veiligheid

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.inspectie-jenv.nl

Ons kenmerk
2822514

Bijlagen
1

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 11 februari 2020
Onderwerp Beantwoording vragen tbv rondetafelgesprek 17/2.

Geachte heer Jansma,

In uw uitnodiging voor het rondetafelgesprek op maandag 17 februari 2020 heeft u mij verzocht om ter voorbereiding op dat gesprek vooraf een aantal vragen te beantwoorden. Hierbij stuur ik u de antwoorden toe.

Hoofdvraag I: Wie voert welk toezicht uit en in hoeverre is er sprake van overlappen dan wel leemtes in het huidige toezicht?

Deelvragen
1. Op grond van welke wettelijke bevoegdheden kunt u toezicht houden op de toepassing van digitale technologieën (zoals AI, gezichtsherkenning en Internet of Things) door de overheid, bedrijven en burgers? Houdt u hier ook toezicht op? Zo ja, hoe lang al en waaruit blijkt dat (activiteiten, toezichtsvisie)? Zo nee, waarom niet?
De Inspectie Justitie en Veiligheid (hierna: Inspectie JenV) houdt toezicht op de kwaliteit van de taakuitvoering op het terrein van justitie en veiligheid. Grondslag voor het toezicht vormen art. 57 eerste lid van de Wet veiligheidsregio's, de Jeugdwet, Politiewet 2012, Veiligheidswet BES, Wet forensische zorg en de Wet marktordening gezondheidszorg. Toezicht vindt verder plaats op grond van de Regeling toezicht terugkeer vreemdelingen en de Regeling Inspectie voor de Sanctietoepassing. Als bij die taakuitvoering digitale technologieën worden toegepast, dan kunnen die door de Inspectie JenV betrokken worden in het inspectieonderzoek. Het toezicht op digitale technologieën kan dan bestaan uit het beoordelen van de toegevoegde waarde van de technologie binnen de kwaliteit van de taakuitvoering van een organisatie, of uit het toetsen van de weerbaarheid van een systeem, waar een dergelijke techniek onderdeel van uitmaakt. Zo is tussen 2010 en 2015 toezicht uitgeoefend op het 'Verbetertraject C2000'. Hierin werd onder andere gekeken naar de dekking van het C2000 netwerk. Ook is het zaakvolgsysteem 'BOSZ' van de Politie onderdeel geweest van een onderzoek naar de betrouwbaarheid van politiecijfers. Bij een onderzoek naar informatieoverdracht in de asielketen (2019) is de toepassing van het informatieknooppunt SIGMA betrokken.

De Inspectie JenV heeft in haar meerjarenprogramma 2018-2020 al aangegeven dat zij het toezicht ook op cybersecurity gaat richten. In het werkprogramma 2020 heeft ze een aantal concrete onderzoeksthema's geagendeerd. Op dit moment zijn we bezig met de vraag hoe we het toezicht voor de jaren 2021-2024 willen inrichten. In het nieuwe in ontwikkeling zijnde meerjarenprogramma zijn de invloed van digitalisering en de noodzaak tot betere cybersecurity leidraden in het toezicht van de Inspectie JenV.

Tot nu toe heeft de Inspectie JenV nog geen onderzoek verricht naar kunstmatige intelligentie (AI), gezichtsherkenning en Internet of Things (IoT). Ze realiseert zich dat door de toename van de toepassing van deze digitale technologieën bij de organisaties waarop zij toezicht houdt, zoals bijvoorbeeld de politie en organisaties in de vreemdelingenketen, dit een steeds prominentere rol kan spelen in de kwaliteit van hun taakuitvoering. De Inspectie JenV wil op die veranderende beweging bij de organisaties inspelen en heeft de ambitie om haar toezicht de komende jaren daar nadrukkelijk op te richten. In 2020 zal ze hierin een eerste stap zetten door een inspectieonderzoek uit te voeren naar de toepassing van een nog nader te bepalen digitale technologie. Hierbij wordt getest of bestaande normenkaders volstaan voor het toetsen van de legitimiteit en de bijdrage van de inzet van deze technologie aan de kwaliteit van de taakuitvoering.

Bij het verder vormgeven van het toezicht op de inzet van digitale technologieën zal de Inspectie tevens de vraag betrekken of het gebruik van deze technologieën (zoals AI en algoritmes) niet leidt tot ethisch ongewenste effecten bij de taakuitvoering, zoals uitsluiting van mensen of discriminatie. Daarnaast wil de Inspectie de kwaliteit van de gebruikte algoritmes en de uitkomsten daarvan beoordelen. Dit vanuit het besef dat het inzetten van dit soort technologieën volledig transparant, veilig en betrouwbaar moet plaatsvinden omdat het ingrijpende gevolgen voor de burger kan hebben.

2. **In hoeverre overlappen de bevoegdheden van de toezichthouders elkaar? Zijn er gebieden waar u in de praktijk ook andere toezichthouders tegenkomt? Zo ja, worden werkzaamheden en beoordelingen dan op elkaar afgestemd?**
Toezichthouders opereren op basis van een eigen wettelijk kader. In de praktijk kan het zo zijn dat toezichthouders vanuit het eigen kader dezelfde situatie onderzoeken. De bevoegdheid van IJenV richt zich in algemene zin op de taakuitvoering door de onder toezicht staande organisaties op het terrein van justitie en veiligheid.

De Inspectie JenV komt bij het uitoefenen van haar toezicht meerdere andere toezichthouders tegen. Voor het uitvoeren van toezicht in het meldkamerdomein bijvoorbeeld bestaan afspraken met het Agentschap Telecom. Onderzoeken bij meldkamers worden veelal gezamenlijk en in afstemming uitgevoerd waarbij het Agentschap Telecom de technische invalshoek beoordeelt en de Inspectie JenV de processen en taakuitvoering onderzoekt. Voor het toezicht dat de Inspectie JenV gaat uitvoeren naar de inzet van algoritmes en AI zal zij voor de technische kant ervan kennis en expertise van het Agentschap Telecom betrekken.

Ook kan er in de toezichtpraktijk samenloop zijn met het toezicht door de Autoriteit Persoonsgegevens. Zo kunnen in toekomstige onderzoeken door de Inspectie JenV de inzet van algoritmes deel uitmaken van de taakuitvoering van een onderdeel waarop de Inspectie JenV toeziet. De algoritmes die onder

kunstmatige intelligentie geschaard kunnen worden, verwerken mogelijk persoonsgegevens. In dat geval oefenen zowel de Autoriteit Persoonsgegevens als de Inspectie JenV toezicht uit op deze algoritmes. In die situatie hebben de beide toezichthouders hun eigen perspectief, op basis van hun eigen wettelijke taken. Hier is wel enige overlap in te vinden. Deze overlap vindt plaats daar waar de Autoriteit Persoonsgegevens toetst of de persoonsgegevens conform de Algemene Verordening Gegevensbescherming worden verwerkt en waar de Inspectie JenV de legitimiteit en doelmatigheid van de inzet van een dergelijk algoritme binnen de taakuitvoering beoordeelt. Hoewel dergelijk toezicht nog niet heeft plaatsgevonden heeft de Inspectie JenV reeds oriënterende gesprekken gevoerd met de Autoriteit Persoonsgegevens met als doel om deze overlap te identificeren en daar in de toekomst afspraken over te maken. Ook heeft de Inspectie afspraken gemaakt met de Autoriteit Financiële Markten en met de Autoriteit Consument en Markt om kennis en ervaringen te delen rondom het toezicht op de inzet van algoritmes.

Daarnaast stemt de Inspectie JenV structureel af met andere toezichthouders die een rol hebben bij het toezicht op digitale vitale processen.[1] Deze afstemming vindt plaats in het kader van de versterking van de digitale weerbaarheid van vitale processen die door de minister van Justitie en Veiligheid in gang is gezet naar aanleiding van de zorgelijke uitkomst van het Cybersecuritybeeld Nederland 2019 (CSBN). Op zijn verzoek draagt de Inspectie JenV vanuit een coördinerende rol, er samen met die andere betrokken toezichthouders zorg voor dat er periodiek een samenhangend inspectiebeeld over de stand van de weerbaarheid van de digitale vitale processen wordt opgesteld. De systematiek van het inspectiebeeld wordt de komende tijd ontwikkeld.

3. Zijn er gebieden waar toezichthouders geen of ontoereikende bevoegdheden hebben en waar dat wel nodig zou zijn? Hoe wordt hier in de praktijk mee omgegaan?
De Inspectie JenV vindt het belangrijk dat zij effectief kan interveniëren indien zij ernstige tekortkomingen bij onder toezicht gestelde organisaties aantreft die directe maatregelen vereisen. De Inspectie moet bijvoorbeeld in staat kunnen zijn om in het kader van digitale ontwrichting de onder toezicht staande partij te dwingen om de beveiliging van netwerken en systemen onder de regie van de Inspectie te laten toetsen door externe deskundige partijen. Dit heeft zich tot nu toe in de praktijk nog niet voorgedaan maar zal in de toekomst zeker aan de orde kunnen zijn.

De Inspectie JenV heeft deze bevoegdheid nu niet. Het toekennen van deze bevoegdheid aan de Inspectie vereist aanvullende regelgeving met een concreet normenkader. Ook zal hierbij moeten worden bezien in hoeverre hier raakvlakken zijn met soortgelijke bevoegdheden van andere partijen.

4. **Hoe zorgt u ervoor dat uw organisatie voldoende geëquipeerd is om het toezicht op de toepassing van digitale technologieën door de overheid, bedrijven en burgers te kunnen uitvoeren? Beschikt u**

[1] De andere betrokken toezichthouders zijn de Autoriteit Nucleaire Veiligheid en Stralingsbescherming, Agentschap Telecom, De Nederlandsche Bank (DNB), Inspectie Gezondheidszorg en Jeugd en Inspectie Leefomgeving en Transport. Daarnaast wordt structureel afgestemd met de Autoriteit Persoonsgegevens.

momenteel over voldoende middelen, capaciteit en expertise? Zo nee, wat is er nodig om dat te hebben?
De Inspectie heeft het afgelopen jaar geïnvesteerd in de werving van medewerkers met kennis van het digitale domein en technologieën om dat toezicht goed te kunnen uitvoeren. Dit is nu in opbouw; de verwachting is dat de huidige nieuwe capaciteit binnen een aantal jaren zal moeten groeien. Door de steeds verdergaande digitalisering, de technologische ontwikkelingen en de toenemende risico's van verstoring van digitale processen die daarmee gepaard kunnen gaan, is het voor de Inspectie JenV belangrijk om over zowel kwantitatief als kwalitatief voldoende 'dedicated cybercollega's' te beschikken. Om beter in staat te zijn om onderzoek in dit domein te doen, zoekt de Inspectie expliciet naar verbinding met de wetenschap. Zo wordt een promotieonderzoek opgestart waarin in samenwerking met de TU Delft wordt gekeken naar het toezicht specifiek op de inzet van algoritmes.

Daarnaast wil de Inspectie JenV in het digitale domein de werking ervan in de praktijk kunnen toetsen. De Inspectie moet in staat kunnen zijn om testen uit te voeren of te laten uitvoeren op de netwerken en systemen van ketens waar toezicht op moet worden uitgevoerd. Het uitvoeren van deze testen vereist niet alleen specifieke expertise maar ook specifieke middelen (hardware, software). Het inrichten en onderhouden – al dan niet met andere toezichthouders – van zulke voorzieningen (bijv. een Cyberlab) en expertise vereist investeringen.

Een knelpunt dat de Inspectie wil benoemen, heeft betrekking op het algemene fenomeen van de achterblijvende aanwas van digitale specialisten. De komende jaren zal het een uitdaging blijven om dit soort mensen binnen te halen alsook in overheidsverband een marktconforme beloning aan te kunnen bieden. De ervaring met het werven van geschikte medewerkers voor het digitale domein leert dat het voor de overheid geldende Functiegebouw Rijk en de waardering van digitale specialisten daarin niet altijd goed aansluiten bij die in de private sector.

5. **Hoe zou volgens u het toezicht in Nederland er over tien jaar uit moeten zien? Zou het toezicht op digitalisering gecentraliseerd moeten worden? Zouden bepaalde toezichthouders een prominentere rol moeten krijgen?**
De Inspectie JenV geeft haar eerste ideeën bij deze vraag van de Commissie vanuit drie invalshoeken.

De kracht van toezicht op digitalisering zit volgens ons niet in zozeer in de gedachten met betrekking tot het centraliseren en/of decentraliseren. De kracht zit veel meer in te behalen flexibiliteit van de inzet van specialisten, waarbij toezichthouders de faciliteiten krijgen en gestimuleerd worden om specialisten (tijdelijk) met elkaar uit te wisselen.

Digitalisering en digitale technologieën manifesteren zich in alle geledingen van de samenleving. Digitalisering is daarmee steeds meer een onderdeel van de gewone processen, zoals gezondheidszorg, veiligheid, infrastructuur, communicatie, in het werk, in en om het huis et cetera. Door de inherente verwevenheid met die processen dient het toezicht op digitalisering daarbinnen plaats te vinden. Dus er zullen 'sectorale' toezichthouders blijven bestaan die binnen hun reguliere toezicht het toezicht op digitalisering daarin onderdeel laten zijn. De ordening van die toezichthouders zoals die nu is, kan onderwerp van discussie zijn. Mogelijk zullen

er nieuwe sectorale of functionele toezichthouders bij moeten komen om op bepaalde nieuwe thema's effectief toezicht te kunnen uitvoeren.

Het toezicht op digitalisering is op dit moment versnipperd. Daarom ziet de Inspectie JenV de noodzaak en de behoefte om, naast dit functioneel of sectoraal gerichte toezicht, op centraal niveau een gemeenschappelijke functionaliteit te creëren die ervoor zorgt dat er op het brede onderwerp digitalisering meer samenhang, regie en kennisontwikkeling en –deling is. Deze gemeenschappelijke functionaliteit oefent zelf geen toezicht uit maar dient wel voldoende mandaat te hebben om op overkoepelende digitale thema's adviserend, voorwaardenscheppend en stimulerend te zijn voor de toezichthouders. De positie van deze gemeenschappelijke functionaliteit dient zodanig belegd te worden dat de onafhankelijkheid ervan gewaarborgd is. In lijn met de coördinerende rol voor cyber van de minister van JenV zou het voor de hand liggen om de Inspectie JenV als de partij te positioneren om hierin het voortouw te nemen. Dit ligt logischerwijs in het verlengde van de coördinerende rol die de Inspectie JenV nu al vervult bij het toezicht op digitale vitale processen, zoals hiervoor bij de beantwoording van de tweede vraag van hoofdvraag I al is aangegeven. Deze rol vraagt wel om mensen en middelen.

De tweede invalshoek richt zich op het toezicht zelf. Wij zien ontwikkelingen waarbij het toezicht zelf steeds meer geautomatiseerd gaat plaatsvinden al dan niet ondersteund door bijvoorbeeld AI. In het cyberdomein zal de hoeveelheid data alleen maar toenemen. Er zullen nieuwe onderzoeksmethoden en -technieken geïntroduceerd worden, waarbij big-data analyse een steeds belangrijkere en nadrukkelijke rol krijgt in de toezichtfunctie. Ook deze big-data analyses zelf zullen steeds meer ondersteund gaan worden door geautomatiseerde data-algoritmes. Dit zal zijn uitwerking hebben op de vereiste samenstelling en diversiteit aan specialisten binnen de toezichtfunctie. Daarnaast zien wij dat toezichthouders en de wetenschap elkaar intensiever en pro-actiever opzoeken. Empirische wetenschap speelt een belangrijke rol in de totstandkoming van normenkaders in het cyberdomein.

De derde invalshoek die de Inspectie JenV wil meegeven is dat zij verwacht dat over een aantal jaar een sterke toename heeft plaatsgevonden van de inzet van digitale technologieën als hulpmiddel binnen de taakuitvoering van organisaties binnen het terrein van justitie en veiligheid. Digitale systemen zullen taken uitvoeren die nu nog worden uitgevoerd door mensen. De Inspectie JenV houdt daarmee in toenemende mate toezicht op de inzet van deze technieken. De Inspectie zal daarom zowel kennis over de taakuitvoering als over de technieken zelf in huis moeten hebben.

Hoofdvraag II: Welk normenkader hanteren toezichthouders bij het beoordelen van toepassingen van nieuwe technologie en hoe ontwikkelt dit normenkader zich?

Deelvragen:
1. **Kunt u een voorbeeld noemen van een situatie waarin de inzet van technologie (zoals AI, gezichtsherkenning en Internet of Things) leidde tot aanpassing van het normenkader dat u, impliciet of expliciet, hanteert bij uw toezicht?**
Het eerste voorbeeld gaat over het toezicht dat de Inspectie JenV houdt op de taakuitvoering door de politie. Vanaf 1 maart 2019 heeft de politie op grond van

de nieuwe Wet Computercriminaliteit III (Wet CCIII) de bevoegdheid om heimelijk en op afstand bij verdachten van zware misdrijven in hun computer, smartphone etc. binnen te dringen en daarin onderzoek te doen. De IJenV houdt sindsdien toezicht op de uitoefening van die bevoegdheid. Bij die bevoegdheid zet de politie nieuwe technologieën in (zoals hacksoftware etc) die voor de IJenV aanleiding zijn geweest om een specifiek hierop gericht normenkader op te stellen. Dat hanteren we nadrukkelijk bij ons toezicht.

Overigens is in dit verband afgestemd met de procureur-generaal bij de Hoge Raad en met de Autoriteit Persoonsgegevens omdat de Inspectie JenV tijdens haar toezicht in aanraking kan komen met mogelijke schendingen van de wettelijke voorschriften door of in opdracht van een officier van justitie of in aanraking kan komen met mogelijke schendingen van de regels rond de bescherming van persoonsgegevens. In dergelijke gevallen kan de Inspectie JenV de procureur-generaal bij de Hoge Raad respectievelijk de Autoriteit Persoonsgegevens informeren. Dit kan betrekking hebben op de inzet van digitale technologieën.

Een ander voorbeeld is het toezicht dat IJenV op grond van de Wet veiligheidsregio's uitvoert bij de meldkamers. In dat kader onderzoekt IJenV periodiek de continuïteit van de meldkamers. De Inspectie JenV heeft in haar meerjarenprogramma aangegeven dat zij de weerbaarheid tegen cyberdreigingen in haar toezicht opneemt. Door het toenemend belang van de inzet van technologie binnen de meldkamers heeft de IJenV in haar laatste onderzoek, dat zij samen met het Agentschap Telecom heeft uitgevoerd (Continuïteit van meldkamers, juli 2019), nieuwe elementen aan het normenkader toegevoegd die zijn gericht op het in kaart brengen van de weerbaarheid tegen cyberdreigingen.

2. **Kunt u, in dat voorbeeld, toelichten hoe dat normenkader zich ontwikkelde? Wie waren hierbij betrokken? Welke vragen werden gesteld? Welke publieke waarden spelen hierbij een rol?**
Bij deze vraag wordt nader ingegaan op het voorbeeld van de Wet CCIII. De IJenV realiseerde zich bij de voorbereiding op deze voor haar nieuwe toezichttaak dat de politie bij de uitoefening van die nieuwe bevoegdheid, gebruik ging maken van nieuwe technologie, zoals hacksoftware. Daaraan worden allerlei eisen gesteld, voor onder meer de keuring en de toepassing ervan. Deze eisen zijn vastgelegd in een nieuwe AMvB en onderliggende regels. De IJenV heeft op basis daarvan normen afgeleid en in een normenkader vastgelegd. Dit normenkader zal de komende tijd verder worden ontwikkeld omdat de ervaringen die de Inspectie met haar toezicht over het afgelopen eerste jaar heeft opgedaan, aanleiding kunnen zijn om een en ander nader te verfijnen.
De publieke waarden die hierbij uiteindelijk een rol spelen betreffen de bescherming van de persoonlijke levenssfeer van burgers en een veilige samenleving door effectieve opsporing.

3. **Biedt het huidige wettelijk kader voldoende houvast om het toezicht op nieuwe toepassingen van digitale technologieën te kunnen uitvoeren? Zo nee, wat is hiervoor nodig?**
We zien dat wetgeving voortdurend achterloopt op nieuwe en complexe technologische ontwikkelingen (zoals AI, Quantum Computing, Cloud, IoT, SDN, 5G-netwerken). Dit maakt dat er veelal sprake is van (achterhaalde) open normen die vaak moeilijk te interpreteren zijn voor uitvoerenden (en ook toezichthoudende partijen) in het cyberdomein.

Uit het grote aantal (internationale) standaarden en “best practices” in het cyberdomein (zoals ISO, NIST, ITIL, COBIT) is af te leiden dat het cyberdomein complex en divers is.

Daarnaast zal voor dit soort technologische ontwikkelingen een baseline beveiliging (zoals de BIO) veelal onvoldoende zijn als normering voor het toezicht op vitale processen, die nu en in de toekomst meer ingezet zullen worden in de verdere digitalisering van processen. Deze complexe technologische ontwikkelingen zijn zodanig “technology driven” dat in de praktijk maatwerk in de normering moet plaatsvinden. Een baseline beveiliging (zoals de BIO) geeft de onderzoeker te weinig grondslag om onderzoeken met voldoende diepgang uit te voeren.

Toezichthouders in het cyberdomein moeten in staat zijn op basis van o.a. wet- en regelgeving alsook op basis van (internationale) standaarden, bepalende en normatieve kaders te ontwikkelen en te hanteren in hun toezicht. Dit stelt (hoge) eisen aan de kwaliteit van de (cyber) inspecteurs. Daarnaast maakt de snelheid waarmee de technologische ontwikkelingen op dit gebied plaatsvinden, dat van inspecteurs wendbaarheid en flexibiliteit wordt vereist. Om dit goed te borgen zou een wettelijke verankering van deze beroepsgroep/deskundigheid met een aantal wettelijke bevoegdheden kunnen worden overwogen. Ook zou ingezet kunnen worden op een wettelijk verplichte opleiding tot gecertificeerd (cyber) inspecteur, waarbij na certificering, permanente educatie een vanzelfsprekendheid moet zijn.

Mocht u naar aanleiding van deze beantwoording voorafgaand aan het rondetafelgesprek nog vragen hebben, kunt u contact opnemen met de heer J.N.M. Groot.

Hoogachtend,

H.C.D. Korvinus
Inspecteur-generaal Inspectie Justitie en Veiligheid