Agentschap Telecom
Ministerie van Economische Zaken
en Klimaat

Tijdelijke commissie Digitale Toekomst
van de Tweede Kamer der Staten-Generaal
Mevrouw K.M. Buitenweg
Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Datum 10 februari 2020
Betreft Rondetafelgesprek Wettelijk kader en Toezicht d.d. 17/02/2020

Geachte mevrouw Buitenweg,

Hartelijk dank voor uw uitnodiging om deel te nemen aan het rondetafelgesprek 'Wettelijk kader en toezicht' op 17 februari a.s. In deze brief geven wij, als toezichthouder in het digitale domein, antwoord op de vragen die de commissie op voorhand heeft gesteld aan de genodigden. Op deze manier hopen wij een constructieve bijdrage te kunnen leveren aan het gesprek over het specifieke vraagstuk rondom toezicht op het terrein van digitalisering.

Agentschap Telecom (AT) waarborgt de beschikbaarheid en betrouwbaarheid van de IT- en communicatienetwerken, zodanig dat Nederland veilig verbonden is. In een digitale toekomst is alles in ons dagelijks leven *connected*. Betrouwbare communicatienetwerken zijn noodzakelijk voor de digitale toekomst van Nederland. De maatschappij verwacht dat ze altijd en overal gebruik kan maken van telecommunicatie. Agentschap Telecom ziet toe op de betrouwbaarheid van IT- en communicatienetwerken en digitale diensten, waarop onze digitale samenleving leunt.

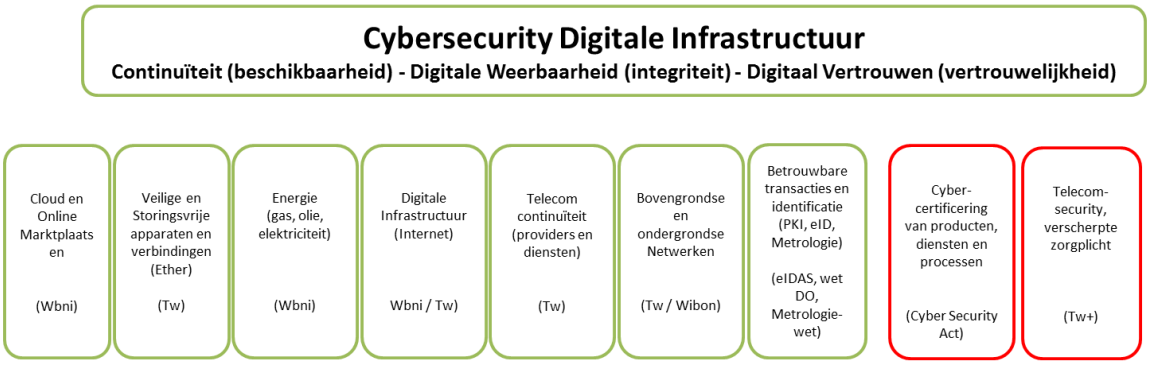
De voorwaarden voor het bestaan van hoogwaardige digitale infrastructuur zijn in onze visie drieledig:

1) **De infrastructuur is beschikbaar:** er is een uitstekende fysieke infrastructuur aanwezig, met feilloze connectiviteit op basis van glasvezel en mobiele (4G en 5G) netwerken.
2) **De werking van de infrastructuur is betrouwbaar:** de netwerken, apparatuur, verbindingen en digitale diensten zijn voldoende betrouwbaar en in staat om continu (24/7) de samenleving van digitale connectiviteit te voorzien. Inclusief betrouwbare energielevering.
3) **De samenleving heeft vertrouwen in diensten en toepassingen:** er is een rotsvast vertrouwen van de samenleving in het veilig gebruik van digitale diensten en toepassingen via de digitale infrastructuur.

Agentschap Telecom zet zich proactief in op het waarborgen van deze voorwaarden.

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?

Agentschap Telecom richt zich, vanuit de publieke waarden van de digitale samenleving, op de digitale infrastructuur. Binnen het digitale domein is het agentschap de toezichthouder op het storingsvrij gebruik en functioneren van de ether, de dekking en continuïteit van telecomnetwerken, de veiligheid van radioapparatuur (H10 Tw.), betrouwbare werking van elektronische identiteiten en handtekeningen (eIDAS verordening en eHerkenning), de cybersecurity van telecomnetwerken, energiesector, internetinfrastructuur en clouddiensten (Tw. en de Wbni). Het agentschap is daarnaast beoogd toezichthouder op de Cyber Security Act.



Betrouwbare en weerbare *digitale maatschappij*

Afbeelding 1. Overzicht huidige cybersecuritytaken AT

Meer uitgebreid in het licht van de vraagstelling: Agentschap Telecom is verantwoordelijk voor het toezicht op radioapparatuur. Dit omvat alle draadloos verbonden apparaten (waaronder IoT). De Radio Equipment Directive (RED) bevat bevoegdheden om eisen te stellen aan de veiligheid bij het op de markt komen van radioapparaten. Voor cyberveiligheid zijn deze bevoegdheden nog niet geactiveerd. Wanneer de bevoegdheden geactiveerd zijn, is Agentschap Telecom de toezichthouder.

Toezicht op het toepassen van gezichtsherkenning voor Identificatie of Authenticatiediensten vallen onder ons toezicht vanuit eIDAS en eHerkenning. Dit is een relatief nieuw vraagstuk waarvoor de standaarden waaraan we toetsen volop in ontwikkeling zijn.

Agentschap Telecom houdt daarnaast op basis van de Wet beveiliging netwerk- en informatiesystemen toezicht op (per categorie) aangewezen aanbieders van essentiële diensten (AED's) in de sectoren energie en digitale infrastructuur en op digitale dienstverleners zoals clouddiensten. Ook houdt het agentschap toezicht op de naleving van beveiligings- en meldingseisen door verleners van vertrouwensdiensten op basis van de eIDAS verordening.

Het ministerie van Economische Zaken en Klimaat heeft Agentschap Telecom gevraagd zich voor te bereiden op de rol van Nationale Cybersecuritycertificeringsautoriteit (NCCA). Dit op basis van de Europese Cyber Security Act. De uitvoeringswet is in voorbereiding bij het ministerie van Economische Zaken en Klimaat en de verwachting is dat deze medio 2021 bekrachtigd kan worden en Agentschap Telecom de rol van NCCA op zich neemt. De certificeringen die Europees verwacht worden betreffen o.a. Cloud, Common Criteria, AI en IoT.

Als bedrijven AI inzetten als technologie in de toezichtdomeinen van Agentschap Telecom, zoals ten behoeve van continuïteit en cybersecurity, dan valt dit onder ons reguliere toezicht. De wettelijke bevoegdheid hiervoor is dankzij de open normering in de wetgeving opgenomen. Dit betekent bijvoorbeeld dat een aanbieder van een essentiële dienst, die AI inzet om de continuïteit of weerbaarheid te verbeteren, moet aantonen dat dit begrepen kan worden onder het treffen van "passende maatregelen", passend bij de stand der techniek. Het juiste gebruik en de werking van de AI wordt dan door Agentschap Telecom beoordeeld.

Er zijn echter op dit moment geen mogelijkheden om generiek toezicht te houden op de werking van AI als geheel. Het gaat hier bijvoorbeeld om de (technische) invulling van aspecten zoals transparantie, veiligheid en auditeerbaarheid van algoritmes in algemene zin. Met toenemend gebruik en complexiteit kan dit in de toekomst wel nodig zijn. In die zin kan AI in de toekomst zelfs een generiek onderdeel worden van de digitale infrastructuur. Het agentschap onderzoekt dit komend jaar en gaat hierover in gesprek met andere toezichthouders.

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?

In de digitale toekomst zien we dat iedere sector gebruik maakt van digitale connectiviteit. Dit maakt dat er ook generieke vraagstukken ontstaan. Die vraagstukken zijn bijvoorbeeld al zichtbaar op het terrein van cybersecurity en privacy. Voor het vraagstuk privacy is dat geborgd door het oprichten van een specifieke toezichthouder. Ons beeld is dat voor AI en cybersecurity de sectorale kennis onmisbaar is om toezicht erop effectief in te richten.

Waar toezichtgebieden elkaar raken treedt Agentschap Telecom in contact met andere toezichthouders. Hiertoe biedt het structureel overleg van toezichthouders onder de Wbni gelegenheid. Hierin werken de toezichthouders reeds samen aan een samenhangend inspectiebeeld op cybersecurity. We hebben met diverse collega-toezichthouders samenwerkingsafspraken op domeinen waar we elkaar raken of kunnen versterken. Daarnaast neemt het agentschap deel aan de Inspectieraad, waarbij samengewerkt wordt tussen de toezichthouders ten behoeve van de informatie-uitwisseling.

Samenwerking op vraagstukken van digitalisering en veiligheid van netwerken vindt voortdurend plaats en is breder dan alleen tussen toezichthouders onderling. Denk aan samenwerking met het NCSC voor informatie-uitwisseling op

cybersecurity en samenwerking voor het toezicht op de continuïteit van 112, NL-Alert en meldkamers met de Inspectie J&V.

Daarnaast werkt Agentschap Telecom in het kader van de "Roadmap digitaal veilige hard- en software" onder voorzitterschap van het ministerie van Economische Zaken en Klimaat samen met toezichthouders zoals Autoriteit Persoonsgegevens en Autoriteit Consument en Markt.

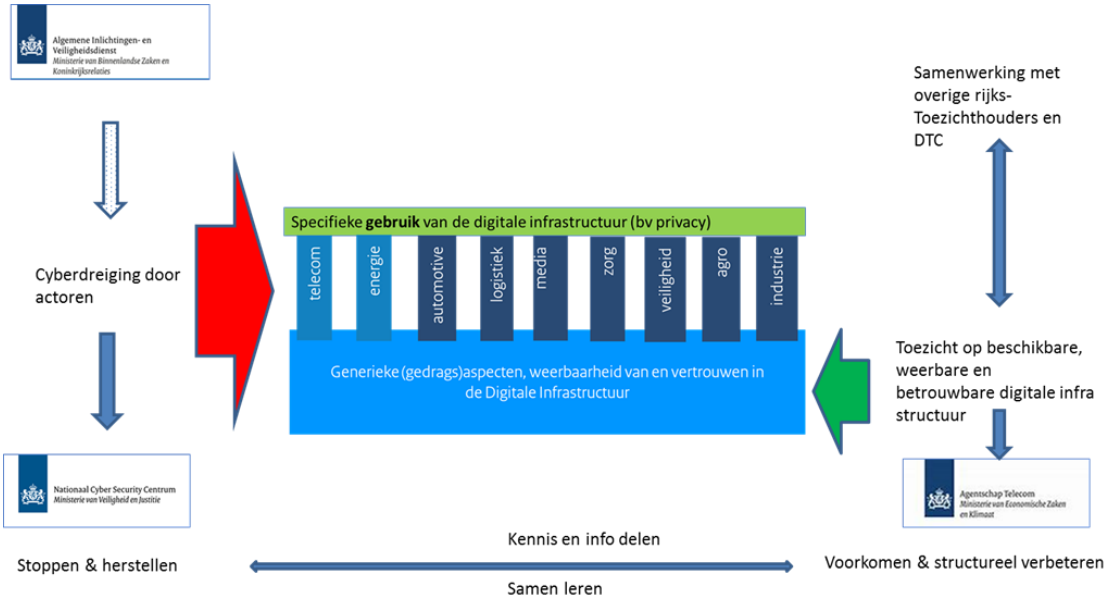
In het algemeen zien we dat, in de vraagstukken van de digitale toekomst, de werkvelden van Agentschap Telecom een grotere rol spelen in de sectorale werkvelden van andere toezichthouders en overheidsinstanties. Dit vraagt om meer samenwerking en afstemming in de brede overheidsketen.

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?

We zien zoals eerder beschreven dat bevoegdheden voor Agentschap Telecom, voor haar domeinen, in principe toereikend zijn. In het algemeen houdt het agentschap proactief toezicht gericht op het voorkomen van problemen en het structureel verbeteren bij onder toezicht gestelden. Een door Europa opgelegde uitzondering in de Wbni betreft het toezicht op de clouddiensten. Dit is nu reactief toezicht. Bij de eerste evaluatie vorig jaar met de Europese Commissie, is door Nederland aangegeven dat gezien het toenemende belang van clouddiensten dit ook proactief toezicht moet worden.

Bevoegdheden om generiek toezicht te kunnen houden op het digitale domein als geheel, of ten minste op generieke aspecten zoals bij AI, bestaan nog niet. Het kan zijn dat dit wenselijk is in de toekomst. Voor AI zou het toezicht in de toekomst bijvoorbeeld tweeledig kunnen zijn: op de AI technologie enerzijds, en op het gebruik ervan in een specifieke sector anderzijds. Het ligt in de rede dat een toezichthouder zich meer of specifieker dan anderen bezig houdt met de beoordeling van de generieke (vaak technische) werking van de AI in producten, diensten en toepassingen. Het gebruik van AI in een specifieke sector zou aan de sectorale toezichthouder moeten worden overgelaten. De aansturing met AI van een elektriciteitsnetwerk is wezenlijk anders dan beoordeling van AI in een medisch apparaat of in een zelfrijdend voertuig. Dit vraagt om een goede coördinatie tussen alle partijen. We hebben daar goede ervaringen mee onder de Wbni, waar AT als toezichthouder op de generieke digitale infrastructuur de werkgroep van toezichthouders voorzit en vanuit die rol coördineert met andere collega-overheidsinstanties, zoals het NCSC. Een thema als AI, zou in een zelfde soort verband kunnen worden opgepakt.

Het agentschap doet op dit moment onderzoek naar het gebruik van AI in onder ander telecom- en ICT-netwerken om te verkennen in hoeverre het noodzakelijk en mogelijk is om hier toezicht op te houden. Ook de Europese Commissie werkt aan een Europese benadering voor AI. Hierin is aandacht voor ethische aspecten en het juridisch kader.



Afbeelding 2. Schematische weergave rollen en samenwerking cybersecurity

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 momenteel over voldoende middelen, capaciteit en expertise? Zo nee, wat is er nodig om dat te hebben?

Ook als toezichthouder, die met veel ervaring en met jarenlange in samenwerking met industrie en onze contacten in Europees verband opgebouwde kennis, actief is in het digitale domein, is het voorbereiden op de toekomst van essentieel belang. De ontwikkelingen gaan razendsnel. Agentschap Telecom bereidt zich daarop voor met diverse instrumenten: We maken gebruik van een strategische agenda met daarop thema's als 5G, cybersecurity en AI. Daarnaast werken we met strategische personeelsplanning om de juiste competenties te waarborgen. We gebruiken een toekomst-radar waarbij we in dialoog met stakeholders de meerjarige ontwikkelingen in het digitale domein in kaart brengen. Daarnaast hanteren we een onderzoeksagenda om in een vroeg stadium onderzoek te doen naar maatschappelijke vraagstukken.

Voor de huidige taakuitvoering beschikt het agentschap over voldoende middelen, capaciteit en expertise. Bij de uitbreiding van taken is dit een randvoorwaarde. Agentschap Telecom wordt tijdig door de beleidsdepartementen betrokken bij het formuleren van deze randvoorwaarden. Een algemeen aandachtspunt is de schaarste van ICT- personeel. Dit maakt het werven en vasthouden van hooggekwalificeerd personeel lastig voor de gehele overheid. We merken wel dat er in de arbeidsmarkt veel animo is bij specialisten om zich in dit boeiende werkveld met collega's in te zetten voor het maatschappelijke belang van cyberweerbaarheid.

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?

Door digitalisering ontstaan generieke vraagstukken rondom cybersecurity, privacy en AI. Om deze vraagstukken voldoende te kunnen duiden is sectorkennis een onmisbare randvoorwaarde. Sectorale toezichthouders zullen dus ook over tien jaar een belangrijke rol spelen. Samenwerking op kennis van de nieuwe vraagstukken is daarbij van groot belang en krijgt bijvoorbeeld onder de Wbni al zijn eerste vorm. Agentschap Telecom is daarom geen voorstander van volledige centralisatie van het toezicht. De kans dat door centralisatie de aansluiting met de sectoren verloren raakt is groot.

De maatschappij heeft recht op de volle mogelijkheden die digitalisering biedt. Tegelijkertijd heeft een digitale samenleving garanties nodig, die risico's en mogelijke schadelijke gevolgen van digitalisering zoveel mogelijk voorkomen en in ieder geval beheersbaar maken. Hiervoor is zicht op die nieuwe vraagstukken nodig. Dat vraagt om een stevige en brede overheidsketen, die alle aspecten omvat en nauw samenwerkt om effectief te zijn. Een keten, met daarbinnen tenminste één overheidspartij, die het overzicht heeft over het totale speelveld van de generieke digitale infrastructuur. Een partij, die van daaruit in verbinding staat met sectorspecifieke toezichthouders en de overige organisaties in het speelveld, zoals die op het vlak van incident- en crisisbestrijding.

We verwachten daarom vanuit ons domein dat er ook in de toekomst een organisatie in Nederland nodig is, die zich richt op de digitale infrastructuur vanuit de publieke waarden van de digitale samenleving. Een organisatie, die in positie is om dit speelveld en ieders verantwoordelijkheden integraal te overzien. Een organisatie, die vanuit deskundigheid legitiem en gezaghebbend kan acteren op nieuwe maatschappelijke risico's vanuit de rol van voorkomen en structureel verbeteren. En zelfstandig kan meedenken, signaleren, agenderen en betekenisvol kan beïnvloeden op nationaal en internationaal niveau.

Net zoals digitale infrastructuur een generieke randvoorwaarde is voor de digitale samenleving, zijn er mogelijk ook andere aspecten binnen het digitale domein die gezien kunnen worden als generiek. Ook hierbij geldt dat toezicht in eerste instantie sectoraal kan worden belegd, maar dat op termijn de generieke aspecten (die gelden voor alle sectoren) bij een daartoe geëquipeerde toezichthouder belegd kunnen worden.

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

In algemene zin zien we de ontwikkeling in het toezicht naar open normen. Dit is van oudsher al het geval bij het toezicht op (radio)apparatuur, waarbij fabrikanten gebruik kunnen maken van normen om conformiteit met regelgeving aan te tonen.

Binnen de toezichtdomeinen op basis van eIDAS, de Tw. (continuïteit telecom) en de Wbni is open normering als meest passende vorm van regulering gekozen voor de dynamiek van technologische ontwikkelingen. Open normering is dynamisch,

gericht op de actuele risico's en biedt maatwerk en flexibiliteit, want het beweegt mee met de stand van zaken bij partijen in een sector. Daarmee is er blijvend een actueel toetsingskader voor de toezichthouder. In dit verband stimuleren open normen eveneens de innovatie en concurrentie binnen een sector, omdat ze structureel meer ruimte bieden voor aansluiting bij (technologische) ontwikkelingen dan gesloten normen. Op deze manier kunnen aanbieders ook bij de maatregelen die ze treffen rekening houden met de stand van de techniek. Ook in de CSA, waarvoor Agentschap Telecom beoogd toezichthouder is, is gekozen om de normering voor de veiligheid van ICT producten, diensten en processen, te harmoniseren in Europa. Om zo de door specifieke nationale normeringen veroorzaakte economische barrières weg te nemen en in de gehele Unie het niveau van beveiliging te verhogen. Onder de CSA worden in de zeer nabije toekomst Europese normenkaders van kracht voor de veiligheid van producten, diensten en processen. De eerste normenkaders worden 2021 verwacht.

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?

We hebben gesignaleerd dat er in het normenkader voor toezicht op radioapparatuur, welke IoT-apparatuur omvat, onvoldoende oog was voor de cyberveiligheid van producten. Het is van belang om Europese normen te ontwikkelen, vanwege de schaalgrootte en de concurrentiepositie van Nederland (gelijk speelveld). Om deze reden stuurt het agentschap in samenwerking met het ministerie van Economische Zaken en Klimaat op Europees niveau op het activeren van bevoegdheden en het ontwikkelen van normen voor cybersecurity voor apparatuur.

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?

In het kader van veilige netwerken en het creëren van een gelijk speelveld voor fabrikanten van cyberveilige apparatuur, is het nodig om basiseisen voor cyberveiligheid te ontwikkelen. Dit normenkader is nog in ontwikkeling. Hierbij zijn betrokken: het Europees Telecommunicatie en Standaardisatie Instituut (ETSI), de Stichting Koninklijk Nederlands Normalisatie Instituut (NEN), het ministerie van Economische Zaken en Klimaat en de Europese Unie.

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?

Het wettelijk kader biedt vooralsnog voldoende houvast en volgt de ontwikkelingen op Europees niveau. Zoals aangegeven bij de vraag hoe toezicht er over tien jaar eruit moet zien: verwacht kan worden dat in de toekomst één of meer centrale toezichthouders voor generieke aspecten van de digitale samenleving worden ingesteld. Het wettelijk kader zal daar mogelijk op aangepast

moeten worden. Belangrijker is dat er een adequaat niveau van coördinatie is tussen alle overheidsorganisaties in deze keten. De coördinatie moet ons inziens voornamelijk plaatsvinden vanuit de rol gericht op voorkomen en structureel verbeteren. Dit om een eenzijdig focus op "brandjes blussen" te voorkomen. Deze eenzijdige focus kan problemen juist verergeren in plaats van oplossen. Bijvoorbeeld, het ondoordacht verplichten van een software-patch kan een organisatie in de vitale infrastructuur juist kwetsbaarder maken voor een cyberaanval.

Hoogachtend,

Angeline van Dijk
Directeur-hoofdinspecteur
Agentschap Telecom