Toetsingscommissie
Inzet Bevoegdheden

Binnenhof 19
2513 AA Den Haag
www.tib-ivd.nl

Eerste Kamer der Staten-Generaal
t.a.v. de Voorzitter
Postbus 20017
2500 EA Den Haag

Referentienummer: BWP2231316
Den Haag, 7 december 2023

Betreft: reactie op vragen van de heer Nicolaï

Geachte heer Bruijn,

In de commissievergadering van dinsdag 21 november 2023 heeft de heer Nicolaï gevraagd of de TIB kan verduidelijken naar welke meningsverschillen tussen de toezichthouders en de diensten de Raad van State in haar advies bij de Tijdelijke wet verwijst en of er verwachtingen zijn over geschillen die ook na de inwerkingtreding van de Tijdelijke wet zullen (blijven) bestaan. Met deze brief kom ik graag aan dit verzoek tegemoet. Uiteraard ben ik bereid tot een nadere toelichting mocht daar behoefte aan zijn.

Achtergrond en inleiding
In het advies van de Raad van State wordt verwezen naar de Memorie van Toelichting bij de Tijdelijke wet. De Raad van State verwijst daarbij enkel naar de verschillende zienswijzen van de Ministers en de TIB over de wijze waarop het gerichtheidscriterium bij de inzet van kabelinterceptie moet worden ingevuld en het bijschrijven van niet-exclusieve actorinfrastructuur.

Naast de door de Raad van State benoemde verschillende zienswijzen van de Ministers en de TIB worden in de Tijdelijke wet ook andere aanpassingen voorgesteld. Voor de achtergrond daarbij is het volgende het vermelden waard. Eerder heeft de evaluatiecommissie Jones-Bos in haar evaluatie op de Wiv 2017 een aantal andere knelpunten (soms patstellingen genoemd in het rapport) in de praktijk geduid[1]. Dit betreft onder meer de waarborgen bij kabelinterceptie, de toetsing van technische risico's bij hackoperaties, de bewaartermijn en de relevantiebeoordeling bij bulkdatabestanden en de inzet van geautomatiseerde data-analyse. Ten aanzien van al deze door de evaluatiecommissie gesignaleerde knelpunten brengt de Tijdelijke wet een gewijzigd wettelijk kader, dat overigens in reikwijdte is beperkt tot onderzoeken naar landen met een offensief cyberprogramma. Daarnaast wordt met de Tijdelijke wet een eenzijdige beroepsmogelijkheid bij de Raad van State gecreëerd. Hieronder zal ik op een aantal van deze punten reflecteren.

[1] Evaluatie 2020 Wet op de Inlichtingen- en veiligheidsdiensten 2017, rapport van 20 januari 2021.

Mogelijke toekomstige geschillen

Gerichtheidscriterium en overige toezeggingen rondom kabelinterceptie

De TIB hanteert als uitleg van het gerichtheidscriterium de volgende definitie: «in hoeverre is bij verwerving sprake van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus» .[2] Het gerichtheidscriterium is na de uitslag van het raadgevend referendum in 2018 over de Wiv 2017 expliciet en voor alle bijzondere bevoegdheden van toepassing verklaard. Eerst is dat gebeurd middels een beleidsregel bij de Wiv 2017.[3] De Wiv 2017 is later, met ingang van 26 juni 2021, gewijzigd. Het gerichtheidscriterium is met deze wijziging in de Wiv 2017 onder artikel 26 lid 5 opgenomen.[4] Bij de toevoeging van dit gerichtheidsvereiste is tweeënhalf jaar geleden geen onderscheid gemaakt tussen verschillende bijzondere bevoegdheden en evenmin tussen de verkenningsfase en de productiefase van kabelinterceptie. Dit betekent dat de TIB in alle fasen van kabelinterceptie moet toetsen in hoeverre sprake is van een zo gericht mogelijke uitvoering van de interceptie.

In de Tijdelijke wet wordt in artikel 6 lid 4 een expliciet ongerichte verkenningsbevoegdheid gecreëerd om (binnen het toepassingsbereik van de Tijdelijke wet) ongerichte kabelinterceptie mogelijk te maken door artikel 26 lid 5 Wiv 2017 buiten toepassing te verklaren. Met de Tijdelijke wet wordt aldus een ongerichte verkenningsbevoegdheid gecreëerd waar die voorheen niet bestond.

Tevens heeft de minister naar aanleiding van het referendum een aantal toezeggingen gedaan rondom de filtering van streamingsdiensten.[5] Ook heeft de minister een toezegging gedaan omtrent verkeer dat oorsprong en bestemming heeft in Nederland (het zogenaamde Nederland-Nederlandverkeer).[6] Dit verkeer zou niet geïntercepteerd worden, tenzij voor *cyber defence*. Hieromtrent bevat de Tijdelijke wet geen nadere bepalingen. Wel is in de Nota naar aanleiding van het verslag opgenomen dat die waarborg uit de gedane toezegging zo gelezen dient te worden dat het vrijwel uitgesloten is dat de diensten OOG-interceptie zullen inzetten voor inlichtingen-onderzoek naar gegevens met oorsprong en bestemming Nederland, met uitzondering van de onderzoeken binnen *cyber defence*. Met andere woorden, de toezegging is niet zo bedoeld dat de interceptie van deze gegevens niet zal plaatsvinden. De waarborg zal dus niet gelden ten aanzien van de onderzoeken waar de Tijdelijke wet op ziet.

---

[2] Kamerstukken II 2018-2019, 35 242, nr. 3 (Memorie van Toelichting), p. 4-onder.
[3] Beleidsregels Wiv 2017, artikel 5.
[4] Wet van 16 juni 2021 tot wijziging van de Wet op de inlichtingen- en veiligheidsdiensten 2017, Stb 2021, 300.
[5] Kamerstukken II 2017/18, 34588, nr. 69, bijlage p. 3.
[6] Kamerstukken II 2017/18, 34588, nr. 76, p.3.

Daarbij moet nog wel worden aangetekend dat niet duidelijk is wat onder 'verkeer dat oorsprong en bestemming heeft in Nederland' zal moeten worden verstaan en wat dit in de praktijk betekent. Als twee mensen die zich beiden bevinden op Nederlands grondgebied elkaar een berichtje sturen via gmail.com, is dit dan Nederland-Nederland verkeer, of internationaal verkeer omdat het mogelijk via servers in een ander land loopt? Indien de inzet zich zou richten op server-to-server verkeer, maar de inhoud van dat verkeer feitelijk deze mailtjes bevat hoe wordt er dan tegenaan gekeken? Valt het surfen van Nederlanders vanuit Nederland naar en scrollen op websites als Instagram, YouTube, Snapchat, BeReal wel of niet hieronder? De wet maakt niet duidelijk op basis van welke concrete indicatoren dit wordt bepaald.

Delen met buitenland van ongeëvalueerde gegevens

Zoals hiervoor reeds benoemd creëert de Tijdelijke wet een expliciete wettelijke grondslag voor het ongericht verkennen ten behoeve van bulkinterceptie. Het betreffende artikel introduceert ook een grondslag voor het onder bepaalde voorwaarde delen van (ongeëvalueerde) bulkdata met buitenlandse partnerdiensten. De Wiv 2017 bevat op dit moment geen specifieke bepaling die dat mogelijk maakt.

De Raad van State heeft geadviseerd de mogelijkheid tot het delen van ongeëvalueerde gegevens afkomstig uit de bevoegdheid tot verkennen uit het wetsvoorstel te schrappen. De Raad van State heeft er op gewezen dat deze gegevens in het Nederlands wettelijk systeem uitsluitend door daartoe aangewezen functionarissen ingezien mogen worden. Verdere verwerking in het inlichtingenproces is niet toegestaan. Daarnaast wijst de Raad van State op de ernstige inbreuk op het recht op de bescherming van de persoonlijke levenssfeer die de overdracht van deze gegevens met zich brengt. Het wetsvoorstel is echter niet aangepast. De bezwaren die de Raad van State heeft genoemd blijven echter aan de orde.

Bijschrijven niet exclusieve actorinfrastructuur

Bijschrijven is het toevoegen van bijvoorbeeld een computer of server aan een al lopende toestemming om andere computers of servers te tappen of te hacken. De diensten hoeven dan dus niet opnieuw toestemming te vragen om ook die aanvullende computers of servers te tappen of te hacken, maar kunnen er meteen op inzetten.

Ten aanzien het bijschrijven maakt de TIB bij het rechtmatigheidsoordeel onderscheid tussen exclusief bij een persoon of organisatie in gebruik zijnde actorinfrastructuur en niet-exclusieve actorinfrastructuur, met andere woorden, of die computers of servers al dan niet door anderen dan het target worden gebruikt. De Wiv 2017 'koppelt' de bevoegdheid tot bijschrijven namelijk aan de persoon of organisatie waarop binnen de toestemming wordt ingezet. Voor infrastructuur die ook wordt gebruikt door anderen is door de minister in zijn destijds genomen beslissing niet zonder meer toestemming verleend.

Ter verduidelijking het volgende. Exclusieve actorinfrastructuur betreft door de actor zelf gehuurde servers van waaruit deze zijn cyberaanvallen uitvoert. Hierop komt doorgaans alleen het verkeer langs dat de actor zelf genereert voor de aansturing van de aanval of verkeer van gegevens van de slachtoffers die de actor buitmaakt.
Bij niet-exclusieve actorinfrastructuur gaat het om gedeelde servers of door de actor gehackte servers. In het eerste geval huurt de actor niet een eigen (*'dedicated'*) server, maar een gedeelde server. Actoren hacken ook servers van anderen om vanuit een dergelijke positie verder te hacken en zo (bijvoorbeeld) de herkomst van een aanval te verbergen. In een dergelijk geval heeft de legitieme gebruiker van de server of computer geen weet van het feit dat hij gehackt is en dat er vanuit diens server verdere aanvallen worden uitgevoerd. Het tappen of hacken van die gedeelde of de actor gehackte server geeft in zo'n geval al het verkeer van de andere veelal legitieme gebruikers van en naar die server ook als opbrengst. Deze opbrengst kan vervolgens worden opgeslagen en bewaard door de diensten.

De TIB heeft (los van de juridische grondslag, zie boven) geoordeeld dat het bijschrijven van niet-exclusief in gebruik zijnde actorinfrastructuur gevolgen heeft voor de weging van de proportionaliteit. Of alleen verkeer van de actor of data die door de actor is buitgemaakt wordt verworven, of ook data die op geen enkele wijze een relatie heeft met de taak van de diensten en wellicht zelfs buitengewoon gevoelig zou kunnen zijn, heeft natuurlijk betekenis. De TIB bekijkt bij de beoordeling van dergelijke verzoeken daarom vooraf of deze voldoende garanties bevatten dat de data van de overige legitieme gebruikers op geen enkele wijze ter beschikking komt in het inlichtingenproces van de diensten.

In de Tijdelijke wet is er in artikel 5 lid 2 voor gekozen deze beperking te laten vervallen. De verleende toestemming om te hacken strekt zich ook uit tot een ander geautomatiseerde werk voor zover dat in de plaats treedt of een aanvulling is op het geautomatiseerde werk waar oorspronkelijk door de minister toestemming voor is verleend, ongeacht of er ook andere legitieme gebruikers van het betreffende apparaat zijn. In de Tijdelijke wet zijn verder geen wettelijke waarborgen opgenomen ten aanzien van de legitieme gebruikers van de gedeelde of gehackte servers.

In artikel 9 lid 1 van de Tijdelijke wet wordt een soortgelijke bepaling opgenomen ten aanzien van het tappen. Ook met deze bepaling wordt het mogelijk om zonder voorafgaande toets van de TIB niet-exclusief gebruikte communicatiemiddelen te tappen.

Ten aanzien van deze bepalingen krijgt de CTIVD de bevoegdheid krijgt om op de feitelijke bijschrijving bindend toezicht te houden. Bovendien wordt expliciet geregeld dat de TIB en de CTIVD informatie kunnen uitwisselen over het toezicht dat zij hierop houden. Dat is van belang, bijvoorbeeld als de TIB een verzoek tot verlenging voorgelegd krijgt ten aanzien van kenmerken waarvan de CTIVD al heeft kunnen beoordelen of het bijschrijven rechtmatig was.

Toetsing van technische risico's bij hackoperaties

De TIB toetst technische risico's voorafgaand aan de uitvoering van een hackoperatie. Immers, voorkomen moet worden dat een aanzienlijk risico ontstaat dat als gevolg van een hackoperatie door de diensten essentiële dienstverlening stil komt te liggen of andere statelijke actoren de vaardigheden van de dienst kunnen kopiëren en vervolgens misbruiken. Om dit adequaat te kunnen doen heeft de TIB ook een technisch deskundig lid in haar commissie. De diensten hebben de toetsing van technische risico's zoals beschreven in het rapport Jones-Bos als belemmerend ervaren en vinden het niet op de praktijk van hackoperaties toegesneden.

Met de Tijdelijke wet wordt in artikel 5 lid 1 de verplichting om een omschrijving van de technische risico's op te nemen in de beslissing buiten toepassing verklaard. De TIB heeft overigens goede nota genomen van de brief van de minister d.d. 31 maart 2023 waarin benadrukt wordt dat er geen enkele intentie is om de wijze waarop de TIB thans de proportionaliteitstoets uitvoert in te perken. De aanpassing in de toelichting bij de beoordeling van technische risico's is doorgevoerd met als doel te verduidelijken waar (in de nieuwe systematiek) het domein van de TIB ophoudt en het domein van de CTIVD begint, aldus de minister.

Bulkdatasets, relevantiebeoordeling en bewaartermijn

Al sinds rapport 70 van de CTIVD, verschenen op 19 augustus 2020, pleit de CTIVD voor één bulkdataregime. Er moet volgens de CTIVD één regime gelden voor de beoordeling op relevantie van alle bulkdatasets van de diensten, onafhankelijk van de wijze waarop deze zijn verkregen. Het toezicht hierop zou vervolgens moeten plaatsvinden door middel van bindende toezicht door de CTIVD.

Met de Tijdelijke wet wordt in artikel 14 alleen een bulkdataregime voorgesteld voor bulkdatasets die zijn verkregen middels de inzet van bijzondere bevoegdheden. Hierdoor ontstaat een verschil in waarborgenniveau ten aanzien van de bescherming van fundamentele rechten van burgers op basis van de manier waarop een bulkdataset is verkregen en niet op basis van de omvang van de inbreuk op de grondrechten van burgers. Voor de TIB en CTIVD is niet begrijpelijk waarom dit onderscheid gemaakt zou moeten worden.

De Commissie Jones-Bos adviseerde in haar rapport een onderscheid te maken tussen verschillende bulkdatasets, waarbij datasets maximaal drie jaar bewaard zouden moeten kunnen worden.[7] De Raad van State adviseerde nadrukkelijk om in de wet een fatale termijn op te nemen waarbinnen bulkdatasets vernietigd moeten worden. Zij sloot daarbij aan bij de bewaartermijn voor kabelinterceptie, te weten drie jaar.[8]

---

[7] Aanbeveling 13 uit; Evaluatie 2020 Wet op de Inlichtingen- en veiligheidsdiensten 2017, rapport van 20 januari 2021.

[8] Advies Raad van State bij Nota van wijziging inzake Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, van 10 mei 2023 met kenmerk W04.23.00073/I.

De Tijdelijke wet bevat echter geen fatale bewaartermijn. Het Europees Hof voor de Rechten van de Mens heeft al eerder uitgesproken dat het wenselijk is een zo kort mogelijke bewaartermijn op te nemen in wet- en regelgeving.[9] Een ongelimiteerde bewaartermijn zou een punt kunnen vormen dat aan de orde komt bij de proportionaliteitstoets door de TIB.

Bij deze stand van zaken is overigens ook voorstelbaar dat maatschappelijke partijen dit verschil zullen aanvechten en daarin zullen betogen dat onvoldoende duidelijk beschreven is wanneer data uiteindelijk vernietigd moet worden. Een dergelijk geschil kan echter niet in de geschilprocedure bij de Raad van State ingebracht worden nu maatschappelijke partijen zoals reeds uiteengezet in de paragraaf over de beroepsmogelijkheid geen mogelijkheid hebben om daarin te participeren. Een gang via de civiele rechter, als 'restrechter' lijkt daarom een van de mogelijkheden.

Geautomatiseerde data-analyse (GDA)

De TIB en CTIVD hebben al in 2018 een rechtseenheidsbrief gestuurd over de inzet van het middel geautomatiseerde data-analyse.[10] Een van de geschilpunten die hierin speelde was dat de diensten niet uiteen konden of wilde zetten met welke andere bestanden de desbetreffende data gecombineerd zou gaan worden. Naast het feit dat dit een wettelijk vereiste is waaraan de TIB wordt geacht te toetsen, is het ook relevant om zich een beeld te kunnen vormen van de uiteindelijke inbreuk die met het middel gepaard gaat. Dit was overigens nog voordat hedendaagse *artificial intelligence*-toepassingen zich nadrukkelijk hadden aangekondigd. Inmiddels is *artificial intelligence* in staat om binnen datasets verbanden te leggen die zonder de toepassing daarvan niet zichtbaar zouden worden. Dit geldt zelfs nog meer bij het combineren van verschillende databestanden, omdat de potentiële omvang van de inbreuk op grondrechten bij de inzet van een dergelijke bevoegdheid exponentieel kan toenemen.

In de Tijdelijke Wet wordt in artikel 8 voorgesteld om de toepassing van GDA niet langer bindend vooraf te laten toetsen door de TIB. Ook hier krijgt de CTIVD de mogelijkheid om hierop bindend toezicht te houden.

Introductie van beroepsprocedure

In de Tijdelijke wet wordt een beroepsprocedure bij de Raad van State geïntroduceerd. De hierboven genoemde onderwerpen kunnen in de beroepsprocedure aan de orde komen. Het is evenwel niet uitgesloten dat er meer onderwerpen zich zullen aandienen. De beroepsmogelijkheid bij de rechter ten aanzien van een beslissing van de toezichthouder is een figuur die in het bestuursrecht vaker voorkomt.

---

[9] EHRM 25 mei 2021, Big Brother Watch t. Verenigd Koninkrijk, nrs. 58170/13 62322/14 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013, paragraaf 405 en 423.

[10] Brief van de TIB en de CTIVD van 23 november 2018 betreffende Rechtseenheid -geautomatiseerde data-analyse ex. artikel 50 Wiv 2017.

Internationaal gezien is het echter wel bijzonder dat een beroepsprocedure bij de rechter kan worden gevoerd tegen de partij die de verzoeken om inzet van bevoegdheden door de inlichtingen- en veiligheidsdiensten bindend voorafgaand moet toetsen. De TIB moet bestaan uit twee leden met tenminste zes jaar ervaring als rechter en voert onafhankelijk en effectief toezicht uit zoals vereist door het EHRM en het Hof van Justitie van de Europese Unie. In een vorm van voorafgaande rechterlijke toetsing is op deze wijze dus reeds voorzien.

Opmerking verdient nog dat het verbazing wekt dat er geen beroepsprocedure wordt voorgesteld ten aanzien van de beslissingen die nu worden genomen door de rechtbank Den Haag ten aanzien van de inzet van bijzondere bevoegdheden op advocaten en journalisten, ook niet voor zover die inzet onder het bereik van de Tijdelijke wet zou vallen.

Een opmerkelijk verschil met andere beroepsprocedure in het bestuursrecht is dat de in Tijdelijke wet voorgestelde beroepsprocedure bij de Raad van State slechts openstaat voor één partij, de minister. Andere belanghebbenden die door een beslissing mogelijk worden geraakt (degene op wie de inzet van de bevoegdheden ziet, al dan niet vertegenwoordigd door NGO's) kunnen geen beroep instellen. Dus slechts als door de TIB en CTIVD een voor de minister onwelgevallige beslissing, bijvoorbeeld ten aanzien van uitleg van de wet, wordt genomen zal die beslissing aan de Raad van State kunnen worden voorgelegd. Dit geldt echter niet voor enige andere partij. Voorstelbaar is ook dat de TIB onbedoeld een te ruime wetsinterpretatie hanteert die de ministers er niet toe zal brengen de casus aan de Raad van State voor te leggen. Ook in die situatie is er geen beroepsmogelijkheid voor andere belanghebbenden wiens belangen daardoor geraakt worden. Door deze eenzijdigheid ontstaat een zeer bijzondere situatie. Een dergelijke casus zal door de TIB of CTIVD overigens ook niet aan het EHRM kunnen worden voorgelegd omdat de TIB en CTIVD geen grondrechten als bedoeld in het Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) toekomen die een dergelijke gang naar de Europese rechter mogelijk maken.

Hoewel de diensten en de minister dat niet altijd zo zullen zien, komt het ook voor dat de TIB beslissingen neemt die (in potentie) in het voordeel zijn van de diensten, bijvoorbeeld gelet op zeer bijzondere geopolitieke omstandigheden. Hetzelfde geldt voor sommige beleidslijnen waar de TIB bij de invulling van de open normen die de huidige wet kent na ampel beraad de diensten 'het voordeel van de twijfel' heeft gegeven. Dit brengt echter de mogelijkheid met zich mee dat een dergelijke beslissing als precedent zal worden aangevoerd bij de Raad van State. De TIB beraadt zich op de mogelijke gevolgen hiervan.

Toename van onduidelijkheden

Door de Tijdelijke wet is het wettelijk kader op sommige vlakken onduidelijker geworden. Hiervan geef ik u enkele voorbeelden:

<u>Proportionaliteitstoets bij kabelinterceptie</u>

Artikel 7 van de Tijdelijke wet noemt twee aspecten die betrokken moeten worden bij de proportionaliteitstoets van de TIB. In de verschillende versies van de wet is hierover geschreven dat deze elementen zwaarwegend of zelfs het meest zwaarwegend zouden moeten worden betrokken bij de proportionaliteitstoets van de TIB. In de Tweede Kamer is een amendement aangenomen waardoor de woorden "met name" in dit artikel komen te vervallen. Voor de TIB is het een gegeven dat zij, conform Europese jurisprudentie, een volledige rechtmatigheidstoets moet uitvoeren. Daarbij hoort een volle toetsing op de gronden van noodzaak, proportionaliteit en subsidiariteit. Een proportionaliteitstoets kenmerkt zich daarbij tussen een afweging van de noodzaak van het voorgestelde middel en de inbreuk op grondrechten die het middel met zich brengt. De in het wetsvoorstel voorgestelde twee elementen bevatten nu alleen een omschrijving van de gegevensstroom die geïntercepteerd moet worden en de voorgestelde latere reductie van gegevensstromen. De TIB leest het amendement dan ook dat is betoogd om te verduidelijken dat deze twee elementen betrokken moeten worden bij de proportionaliteitstoets, naast andere elementen die hierin moeten worden betrokken, waaronder de feitelijke inbreuk die het voorgestelde middel heeft op de grondrechten van burgers. Indien de Tijdelijke wet een meer beperktere vorm van de proportionaliteitstoets zou bedoelen, ziet de TIB zich op basis van internationaal recht nog steeds gedwongen om een volledige toets op proportionaliteit te verrichten.

Proportionaliteit van kabelinterceptie

De TIB ziet dat de diensten de wens hebben om kabelinterceptie uit te voeren op een wijze die de proportionaliteit van het middel onder druk zet. Dit zou kunnen worden 'hersteld' als een zeer gerichte filtering en tijdige vernietiging van data zal plaatsvinden. Bij het uitblijven daarvan is niet ondenkbaar dat de TIB en diensten van mening blijven verschillen over wat een proportionele inzet van dit middel is in een democratische samenleving.

Proportionaliteitstoets bij hackoperaties

De TIB voert ook een volledige proportionaliteitstoets uit ten aanzien van hackoperaties door de diensten. Per brief van 31 maart 2023 hebben de toenmalig minister van BZK en de minister van Defensie uiteengezet dat de Tijdelijke wet geen beperking van de proportionaliteitstoets zal betekenen.[11] Onderdeel van deze proportionaliteitsafweging bij hackoperaties is of door de inzet van het middel inbreuken worden gemaakt op de fundamentele rechten van burger en of de inzet van het middel zwaarder weegt dan deze inbreuken. Het hacken beperkt zich overigens niet alleen tot een target, maar kan zich ook richten ook op *non targets* of derden. Ook hun belangen worden bij de beoordeling betrokken.

Conclusie

De wet geeft geen duidelijkheid wanneer sprake is van een land met een offensief cyberprogramma. Dat zou 'ad hoc' bepaald moeten worden en dus mogelijk geschillen kunnen

[11] Kamerstukken II 2022-2023, 36263, nr. 6.

opleveren. Ook bevat de Tijdelijke wet in artikel 2 een bepaling dat de diensten moeten vermelden of toepassing wordt gegeven aan de wet. Het is dus aan de diensten te kiezen of zij een verzoek om toestemming willen indienen op basis van de Tijdelijke wet of op basis van de Wiv 2017. Hierdoor ontstaat de mogelijkheid om, ook al is er sprake van inzet op een land met een offensief cyberprogramma, de Tijdelijke wet toch niet van toepassing te laten zijn. Dit zou in het slechtste geval tot gevolg kunnen hebben dat er 'geshopt' gaat worden op zoek naar de vorm die het laagste niveau van toezicht met zich meebrengt. Het zou behulpzaam zijn dat er duidelijkheid komt over dit punt.

Een gevolg van de Tijdelijke wet is dat er voor de inzet van bevoegdheden van de diensten twee verschillende regimes van toepassing zullen worden. Voor de TIB is niet direct duidelijk waarom mogelijkheden en of verschuivingen in toetsing en toezicht op de inzet van bijzondere bevoegdheden voor het ene doel niet en voor het andere doel wel zouden moeten plaatsvinden.

Op dit moment is voor de TIB niet in volle omvang te overzien of en op welke punten uitspraken van de Raad van State een of meer van de hierboven genoemde geschillen volledig zal kunnen beslechten.

Tot slot

De Tijdelijke wet geeft op een aantal vlakken veranderingen in aanloop naar de bredere herziening van de Wiv 20XX. Deze herziening verdient het om adequaat en gestructureerd te worden uitgedacht, met aandacht voor alle relevante ontwikkelingen in het werk van de diensten en de technologische en juridische ontwikkelingen. Het feit dat de toezichthouders op basis van de Tijdelijke wet met elkaar relevante informatie kunnen gaan uitwisselen is een belangrijke stap vooruit. In de herziening van de Wiv zou moeten worden bezien hoe de integratie van toezicht verder vorm kan worden gegeven. Al eerder hebben de TIB en de CTIVD aangegeven dat zij de voorkeur hebben voor het introduceren van één toezichthouder die 'end-to-end' toezicht houdt. Hierdoor ontstaat de mogelijkheid om intern en extern toezicht effectiever op elkaar af te stemmen en om zo een normatief kader voor de hele keten op te stellen. Zoals gezegd, de technologische ontwikkelingen gaan snel. Het herijken van een (techniekonafhankelijk) normatief kader voor de hele keten biedt de mogelijkheid om daarop te kunnen anticiperen. Het gaat er immers om dat de balans tussen de bescherming van grondrechten en de inbreuk op grondrechten effectief gewaarborgd blijft, nu en in de toekomst.

Met vriendelijke groet,

Anne Mieke Zwaneveld
Voorzitter Toetsingscommissie Inzet Bevoegdheden