COLLEGE VOOR
DE RECHTEN
VAN DE MENS

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (H.G.J Bruins Slot) en de minister van Defensie (K.H. Ollongren)

Onderwerp	Uw brief van	Datum
Wetgevingsadvies inzake Tijdelijke wet onderzoek AIVD en MIVD naar landen met offensief cyberprogramma	-	15 april 2022
	Uw kenmerk	Ons kenmerk
	-	2022/0026/JG/KY/HJ

Geachte minister Bruins Slot en minister Ollongren,

Het College voor de Rechten van de Mens (hierna: College) heeft met belangstelling maar ook met bezorgdheid kennisgenomen van het concept wetsvoorstel voor de Tijdelijke wet onderzoek AIVD en MIVD naar landen met een offensief cyberprogramma (hierna: de Tijdelijke wet).

Het College vraagt dringend uw aandacht voor een aantal onvolkomenheden uit het wetsvoorstel dat op 1 april jl. in consultatie is gegaan. Gezien de korte consultatietermijn behoudt het College zich het recht voor om op een later tijdstip nog aanvullend te adviseren mocht het daartoe aanleiding zien. Het College gaat hieronder op haar voornaamste zorgen, die zien op:

- de reikwijdte van het wetsvoorstel;
- de uitbreiding van de bijschrijfmogelijkheid bij de hackbevoegdheid;
- het schrappen van de fatale bewaar- en beoordelingstermijn voor bulkdatasets die zijn verworven door inzet van de hackbevoegdheid;
- de verruimde verkenningsbevoegdheid ten behoeve van kabelinterceptie en het in deze context laten vervallen van het gerichtheidscriterium;
- de invulling van het gerichtheidscriterium bij kabelinterceptie
- de informatieplicht van de toezichthouders en;
- de eenzijdige beroepsmogelijkheid bij de Afdeling Bestuursrecht van de Raad van State (ABRvS).

1. Reikwijdte van het wetsvoorstel

De reikwijdte van de tijdelijke wet zoals voorgesteld in artikel 2 lid 1 is beperkt tot onderzoeken van de inlichtingen- en veiligheidsdiensten naar landen met een

Postbus 16001
3500 DA Utrecht
Kleinesingel 1-3
3572 CG Utrecht
T 030-888 38 88
F 030-888 38 83
info@mensenrechten.nl
www.mensenrechten.nl

offensief cyberprogramma tegen Nederland of Nederlandse belangen. Het onderwerp van onderzoek bepaalt zodoende of de inzet van bevoegdheden kan plaatsvinden onder deze wet. De memorie van toelichting merkt daarover op dat aanvallen vanuit landen met een offensief cyberprogramma niet uitsluitend afkomstig zijn vanuit een inlichtingendienst of krijgsmacht van dat land, maar ook door of via bedrijven of instellingen of meer diffuse proxy-organisaties uitgevoerd worden. Het onderzoek van de AIVD en MIDV dient hier dus ook op gericht te zijn. Tevens valt uit de memorie van toelichting af te leiden dat de Tijdelijke wet ook van toepassing is op onderzoeken naar een cyberdreiging en cyberaanvallen tegen Nederland of Nederlandse belangen wanneer *verondersteld* wordt dat een bepaald land daarachter zit, maar de aanval nog niet aan dat land geattribueerd kan worden.[1]

Het bovenstaande doet vermoeden dat er in de praktijk veel situaties zullen zijn waarbij op voorhand onvoldoende duidelijk is of de Tijdelijke wet al dan niet van toepassing is. Dat geldt temeer nu ook niet wordt uitgelegd wat kwalificeert als een 'een offensief cyberprogramma'. Bij gebrek aan nadere regels rondom deze 'grijze gebieden' voorziet het College een situatie waarin mogelijk zeer brede toepassing gegeven zal worden de Tijdelijke wet. Het College acht dit onwenselijk, zeker nu deze wet een substantiële verruiming van bestaande bevoegdheden met zich meebrengt. De onduidelijkheid rondom toepassing van de Tijdelijke wet is daarnaast ook vanuit mensenrechtelijk perspectief bezien problematisch. Uit jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) volgt immers dat wetgeving die inbreuk maakt op de rechten van burgers voldoende helder afgebakend moet zijn om misbruik ervan te voorkomen.[2] Dat is des te belangrijker waar het gaat om wetgeving waarin de heimelijke inzet van bevoegdheden door inlichtingen- en veiligheidsdiensten wordt geregeld, nu het risico op willekeur en machtsmisbruik in deze context zeer groot is.[3]

Gelet op het bovenstaande adviseert het College om specifiekere regels te stellen omtrent de toepasselijkheid van de Tijdelijke wet en deze regels openbaar te maken.

2. Tijdelijke uitbreiding van de hackbevoegdheid (artikel 45 Wiv 2017)

a) Geen vermelding technische risico's

Op basis van artikel 45 lid 4 sub a van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 (Wiv 2017) moet een verzoek om toestemming voor de inzet van de hackbevoegdheid momenteel o.a. een omschrijving bevatten van de technische risico's die verbonden zijn aan de uitoefening van deze bevoegdheid.

[1] Memorie van toelichting, p. 12-13.
[2] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*) [GC], § 333.
[3] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*) [GC], § 333.

Met voorgesteld artikel 5 lid 1 van de Tijdelijke wet komt dit vereiste te vervallen. Dat betekent ook dat de TIB de technische risico's niet langer zal meewegen in haar bindende *ex ante* rechtmatigheidstoets. Hiermee gaat het wetsvoorstel verder dan de aanbevelingen uit het rapport van de Evaluatiecommissie Wiv 2017: daarin wordt aanbevolen om meer ruimte te bieden voor differentiatie in de mate van detail van de omschrijving van de technische risico's voor de *ex ante* toets door de TIB – *niet* om deze omschrijving en toets geheel te laten vervallen.[4]

Het College maakt zich zorgen over de keuze om het in artikel 45 lid 4 sub a Wiv 2017 neergelegde vereiste te laten vervallen. Proportionaliteit vormt een belangrijk onderdeel van de toets door de TIB en technische risico's zijn bij uitstek iets om mee te wegen in die proportionaliteitstoets. Immers: technische risico's kunnen zeer schadelijke (en soms onomkeerbare) gevolgen hebben voor degene wiens geautomatiseerd netwerk wordt binnengedrongen of wiens persoonsgegevens zich in dit netwerk bevinden. Het gaat hier om gevolgen die direct raken aan de mensenrechten van deze personen, waaronder het recht op eigendom (bijvoorbeeld wanneer schade wordt aangebracht aan een computer of server) en het recht op privacy (bijvoorbeeld wanneer het beveiligingssysteem zodanig wordt aangetast dat andere actoren makkelijker binnen kunnen dringen).

In aanvulling op het bovenstaande merkt het College op dat het plaatsvervangende bindende *ex durante* toezicht door de CTIVD zich niet in alle opzichten goed leent voor het voorkomen van schade ten gevolge van technische risico's. Ten eerste omdat het *ex durante* toezicht van de CTIVD – anders dan het *ex ante* toezicht door de TIB – niet neer zal komen op een honderd procent controle. Het gaat immers, zo staat in voorgesteld artikel 13 lid 1, om een *bevoegdheid* van de CTIVD die zij naar eigen inzicht kan inzetten. Ten tweede kunnen de technische risico's zich al voordoen vóór de CTIVD haar toezichtbevoegdheden aanwendt. Onomkeerbare schadelijke gevolgen die zijn ingetreden kunnen dan niet meer ongedaan gemaakt worden. Het College vraagt zich in dat kader overigens ook af wie in dat geval toestemming heeft verleend en dus verantwoordelijk gehouden kan worden voor deze (onomkeerbare) schade. Het wetsvoorstel haalt de toestemming met betrekking tot de technische risico's namelijk weg bij de verantwoordelijke minister, maar belegt deze niet ergens anders.

Gelet op het bovenstaande vindt het College de keuze om de beschrijving van de technische risico's te schrappen uit de toestemmingsaanvraag niet begrijpelijk. Dat geldt temeer nu het wetsvoorstel het laagdrempeliger maakt voor de inlichtingen- en veiligheidsdiensten om geautomatiseerde netwerken te verkennen en daarbij eventuele technische risico's te identificeren.

Het College adviseert om de beschrijving van de technische risico's verplicht

[4] Evaluatiecommissie Wiv 2017, *Evaluatie van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017,* 2020, p. 92.

onderdeel te laten van de toestemming van de minister en daarmee tevens van de rechtmatigheidstoets door de TIB.

b) Uitbreiding van de bijschrijfmogelijkheid

In artikel 45 lid 8 Wiv 2017 is bepaald dat een verleende toestemming tot het binnendringen van een geautomatiseerd werk van een persoon of organisatie voor de duur van de toestemming ook de bevoegdheid omvat om binnen te dringen in een ander geautomatiseerd werk *van* die persoon of organisatie, voor zover dat in de plaats treedt van of een aanvulling is op het geautomatiseerde werk waar oorspronkelijk de toestemming voor is verleend. Deze bevoegdheid staat bekend als de bijschrijfmogelijkheid. De TIB legt dit in de praktijk - zo blijkt uit de Memorie van Toelichting – zo uit dat het dient te gaan om een geautomatiseerd werk dat *exclusief* aan die persoon of organisatie toebehoort. Voorgesteld artikel 5 lid 2 van het wetsvoorstel brengt daar verandering in, en bepaalt dat binnen de reikwijdte van de Tijdelijke wet geen sprake hoeft te zijn van *exclusief* gebruik om te mogen bijschrijven. Gedurende de toestemmingsperiode kunnen ook geautomatiseerde werken die, behalve door de statelijke actor zelf, ook door anderen worden gebruikt of zelfs aan anderen toebehoren, worden bijgeschreven. In de praktijk betekent dit dat de AIVD en de MIVD, zonder hiervoor opnieuw toestemming te hoeven vragen, mogen binnendringen in alle geautomatiseerde netwerken waartoe de statelijke actor toegang heeft, ook als deze toegang door de statelijke actor illegaal (bijvoorbeeld door hacken) is verkregen. Het wetsvoorstel verruimt de hackbevoegdheid dus aanzienlijk.

Vanuit mensenrechtelijk perspectief is deze verruiming van de hackbevoegdheid zorgelijk. Het maakt de hackbevoegdheid onvoldoende afgebakend. Het valt op voorhand niet goed in te schatten tot welke servers een statelijke actor allemaal toegang heeft en hoeveel dit er in potentie zijn. Dat betekent dat het wetsvoorstel een onbekend (en potentieel zeer groot) aantal servers onder de oorspronkelijke toestemmingsaanvraag schaart, die bovendien aan een grote verscheidenheid van (onschuldige) organisaties en mensen kunnen toebehoren. In dit verband herinnert het College eraan dat de Evaluatiecommissie Wiv 2017 in haar rapport wijst op de bijzondere gevoeligheid van het hacken van onschuldige organisaties en partijen en aangeeft het belangrijk te vinden dat de TIB haar toetsende rol blijft vervullen op aanvragen die hierop zien.[5] Het wetsvoorstel gaat hier volledig aan voorbij, door zowel de noodzaak tot een nieuwe aanvraag als de toets door de TIB in deze context te laten vervallen.

Het een en ander betekent ook dat het voor burgers op geen enkele wijze meer valt in te schatten tot welke (soort) servers de hackbevoegdheid zich wel of niet uitstrekt en, daarmee samenhangend, of hun persoonsgegevens op enig moment mogelijk kunnen worden verworven door de inlichtingendiensten. De hackbevoegdheid voldoet daarmee niet aan de eis van voorzienbaarheid die het

[5] Evaluatiecommissie Wiv 2017, *Evaluatie van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017,* 2020, p. 93.

EHRM stelt aan nationale wetgeving. Hoewel uit de jurisprudentie van het EHRM volgt dat het vereiste van voorzienbaarheid in de context van geheime surveillance door inlichtingen- en veiligheidsdiensten anders geïnterpreteerd dient te worden dan in andere contexten, geldt ook in deze context nog altijd dat de toepasselijke wettelijke bepalingen voldoende helder omschreven moeten zijn zodat burgers een adequate inschatting kunnen maken van de omstandigheden waarin hun rechten mogelijk beperkt kunnen worden en de voorwaarden die daarvoor gelden.[6]

Dan nog het volgende. Het staat vast dat de hackbevoegdheid een verregaande inbreuk op het recht op privacy met zich meebrengt. Het wetsvoorstel verruimt de kring van personen en organisaties die aan deze inbreuk onderworpen kunnen worden aanzienlijk, terwijl het toezicht feitelijk wordt afgeschaald. Daar waar het gaat om het binnendringen van een nieuw geautomatiseerde netwerk dat aan een ander toebehoort, komt de noodzaak tot een nieuwe toestemmingsaanvraag en de daaraan gekoppelde rechtmatigheidstoets door de TIB te vervallen. Bindend *ex durante* toezicht door de CTIVD komt daarvoor zoals artikel 13 lid 1 voorstelt in de plaats, maar dit toezicht komt, zoals eerder al opgemerkt, niet neer op volledig sluitend toezicht.

Gelet op het bovenstaande adviseert het College de wetgever om te blijven vereisen dat de inlichtingen- en veiligheidsdiensten gemotiveerd toestemming vragen voor het binnendringen van een geautomatiseerd netwerk dat toebehoort aan een nieuwe derde. Het College adviseert tevens om de toetsende bevoegdheid van de TIB ten aanzien van de verleende toestemming te behouden.

Om de gewenste snelheid in het cyberdomein te bereiken, adviseert het College de wetgever om oplossingen te zoeken die minder vergaande inbreuken op de persoonlijke levenssfeer met zich meebrengen, zoals het verkorten van interne procedures rondom toestemmingsverleningen voor het bijschrijven van nieuwe derden of het gebruik maken van de spoedprocedure ex artikel 37 Wiv 2017.[7]

c) Verlengde bewaar- en beoordelingstermijn voor bulkdatasets verkregen uit hackoperaties

In veel gevallen leidt de inzet van de hackbevoegdheid tot het verwerven van bulkdatasets.[8] Bulkdatasets die verworven zijn door de inzet van de hackbevoegdheid moeten op grond van artikel 27 lid 1 Wiv 2017 binnen een jaar worden beoordeeld op relevantie, met een mogelijke eenmalige verlenging van

[6] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*) [GC], § 333.
[7] Zie hierover Evaluatiecommissie Wiv 2017, *Evaluatie van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017,* 2020, p. 93.
[8] Voorgesteld artikel 1 sub d definieert 'bulkdataset' als een omvangrijke gegevensverzameling waarvan het merendeel van de gegevens betrekking heeft op organisaties of personen die geen onderwerp van onderzoek van de diensten zijn en dat ook nooit zullen worden.

een half jaar. Gegevens die niet relevant zijn voor het onderzoek of enig ander onderzoek, moeten terstond worden vernietigd. Gegevens die na anderhalf jaar nog niet op relevantie zijn beoordeeld, moeten tevens worden vernietigd. Binnen het huidige stelsel geldt dus een fatale bewaar- en beoordelingstermijn van anderhalf jaar voor bulkdatasets die zijn verworven door de inzet van de hackbevoegdheid.

Binnen de reikwijdte van de Tijdelijke wet verdwijnt deze fatale bewaar- en beoordelingstermijn. Voorgesteld artikel 6 lid 1 en 2 biedt de mogelijkheid om de bewaartermijn voor bulkdatasets die met de hackbevoegdheid zijn verworven telkens met één jaar te verlengen, zonder maximale termijn. Daarbij geldt steeds – in afwijking van artikel 27 lid 1 Wiv 2017 – dat de gegevens dan nog niet op relevantie beoordeeld hoeven te zijn. Feitelijk betekent dit dat bulkdatasets onbeperkt bewaard kunnen blijven zonder op relevantie beoordeeld te worden. Dat geldt temeer nu uit de memorie van toelichting blijkt dat de onderbouwing voor het verzoek op verlenging zich ook kan richten op noodzaak voor onderzoeksopdrachten die niet binnen de reikwijdte van de Tijdelijke wet vallen. Een praktisch onbegrensde bewaar- en beoordelingstermijn voor databulksets is niet in lijn met artikel 8 EVRM. Het EHRM vereist immers dat de wet duidelijke beperkingen stelt op de bewaarduur, de wijze van bewaren van verzameld materiaal en de omstandigheden waarin dergelijk materiaal moet worden verwijderd en vernietigd.[9] De voorgestelde regeling, die geen fatale termijn bevat en ook geen heldere en transparante regels omtrent mogelijke redenen voor verlenging, kwalificeert niet als zo'n duidelijke wettelijke beperking.

Gelet op het bovenstaande adviseert het College de wetgever om een fatale bewaar- en beoordelingstermijn op te nemen voor bulkdatasets verkregen uit hackoperaties. Daarnaast adviseert het College om heldere, gedetailleerde en transparante regels op te stellen omtrent mogelijke redenen voor verlenging. Het toetsingskader dat bij een verzoek om verlenging gehanteerd wordt, zou openbaar moeten zijn.

3. Tijdelijke uitbreiding van de bevoegdheid tot kabelinterceptie (artikel 48 Wiv 2017)

a) Verruimde verkenningsbevoegdheid: kabelinterceptie en afschaffing van het gerichtheidscriterium

Voorgesteld artikel 7 lid 1 van de Tijdelijke wet creëert een nieuwe zelfstandige juridische grondslag voor het ter verkenning intercepteren van gegevensstromen ten behoeve van OOG-interceptie (de zogenaamde 'snapshotbevoegdheid'). Een dergelijke 'snapshotbevoegdheid' is reeds neergelegd in artikel 48 Wiv 2017, op basis waarvan de diensten aan de hand van technische en inhoudelijke kenmerken kunnen onderzoeken of de onderschepte gegevensstromen daadwerkelijk van

[9] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*) [GC], § 361.

belang zijn voor één of meerdere, concrete onderzoeksopdrachten.[10] De bestaande snapshotbevoegdheid is dus een verificatiebevoegdheid, waarmee de diensten kunnen verifiëren of de gewenste informatie zich inderdaad binnen de onderschepte gegevensstromen bevindt. De snapshotbevoegdheid uit voorgesteld artikel 7 lid 1 van de Tijdelijke wet gaat echter verder: het gaat hier om de bevoegdheid om alle gegevensstromen die over kabels gaan te intercepteren om te bepalen waar relevante informatie te vinden is. Voorgesteld artikel 7 lid 4 van de Tijdelijke wet bepaalt dat het gerichtheidscriterium ten aanzien van deze bevoegdheid vervalt. Dat betekent dat de diensten voortaan volledig ongericht een grote hoeveelheid gegevensstromen via kabels kunnen intercepteren.

De memorie van toelichting verduidelijkt dat bij de verkenning ook sprake is van bulkinterceptie. De jurisprudentie van het EHRM over bulkinterceptie is zodoende op deze bevoegdheid van toepassing.[11] Het laten vervallen van het gerichtheidscriterium bij verkenning ten behoeve van kabelinterceptie is niet in lijn met deze jurisprudentie. Daaruit volgt namelijk dat bulkinterceptie altijd geautoriseerd moet worden door een onafhankelijke toezichthouder– in Nederland de TIB – en dat deze onafhankelijke toezichthouder op zijn minst geïnformeerd moet worden over het doel van de operatie en gegevensdragers of communicatie routes die naar alle waarschijnlijkheid onderschept zullen worden.[12] Dit stelt de toezichthouder in staat om de noodzaak en proportionaliteit van de operatie te beoordelen.[13] Hieruit blijkt tevens dat gerichtheid een belangrijk onderdeel is van proportionaliteit. Het College is dan ook bezorgd dat het geheel laten vervallen van het gerichtheidscriterium het moeilijker maakt voor de TIB om de proportionaliteit en subsidiariteit van de verkenning adequaat te kunnen beoordelen.

Tot slot merkt het College nog op dat het de stellingname dat de bevoegdheid tot intercepteren ter verkenning per definitie volledig ongericht dient te zijn, zoals de memorie van toelichting impliceert, niet kan volgen. Het College accepteert dat volledige gerichtheid in deze fase van het interceptieproces wellicht niet haalbaar is, maar begrijpt niet waarom de inlichtingen- en veiligheidsdiensten niet *zo gericht mogelijk* te werk kunnen gaan. Dit wordt in de memorie van toelichting ook niet toegelicht.

Gelet op het bovenstaande adviseert het College om het gerichtheidscriterium niet te laten vervallen bij de verkenning ten behoeve van kabelinterceptie, maar waar nodig in te kaderen.

---

[10] Zie Memorie van toelichting Wiv 2017, p. 145.
[11] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*) [GC], § 352 en EHRM 25 mei 2021, nr. 35252/08 (*Centrum för Rättvisa t. Zweden*) [GC], § 266.
[12] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*), § 352.
[13] EHRM 25 mei 2021, nrs. 58170/13, 62322/14 en 24960/15 (*Big Brother Watch t. Verenigd Koninkrijk*), § 352.

b) Invulling gerichtheidscriterium bij toestemmingsaanvraag kabelinterceptie

Voorgesteld artikel 8 van de Tijdelijke wet geeft nadere invulling aan de eisen van proportionaliteit en gerichtheid ex artikel 26 lid 2 en 5 Wiv 2017 die moeten worden betrokken bij de aanvraag van toestemming voor kabelinterceptie ex artikel 48 Wiv 2017. Het wetsvoorstel en de memorie van toelichting verduidelijken echter niet of de in voorgesteld artikel 8 opgenomen aspecten *mede* of *uitsluitend* betrokken moeten worden bij deze aanvraag.

Gelet op het bovenstaande adviseert het College om § 3.3.3 van de memorie van toelichting op dit punt te verduidelijken.

4. Informatieplicht omtrent te verstrekken inlichtingen

Op basis van voorgesteld artikel 12 lid 1 van de Tijdelijke wet mogen de TIB en de afdeling toezicht van de CTIVD in het kader van hun toezichthoudende taak inlichtingen uitwisselen over hun bevindingen. Voorgesteld artikel 12 lid 2 van de Tijdelijke wet bepaalt echter dat het hoofd van de betrokken dienst over de te verstrekken inlichtingen geïnformeerd moet worden. Het College merkt op dat een dergelijke informatieplicht van de toezichthouder jegens degene op wie toezicht wordt gehouden niet alleen ongebruikelijk is, maar ook onwenselijk vanuit mensenrechtelijk perspectief. Het staat effectief toezicht in de weg. Feitelijk worden de toezichthouders hiermee namelijk verplicht om de diensten een '*heads-up*' te geven over hun toezichthoudende activiteiten.

Gelet op het bovenstaande adviseert het College om de informatieplicht uit voorgesteld artikel 12 lid 2 te schrappen.

5. Eenzijdige beroepsmogelijkheid bij de Afdeling Bestuursrechtspraak van de Raad van State

Voorgesteld artikel 14 van de Tijdelijke wet creëert een eenzijdige beroepsmogelijkheid voor de betrokken minister bij de Afdeling Bestuursrechtspraak van de Raad van State. Dit is een fundamentele wijziging ten opzichte van het bestaande toezichtsysteem op de AIVD en MIVD. De vraag is of een tijdelijke wet, waarvoor naar alle waarschijnlijkheid een spoedbehandeling bij het parlement gevraagd gaat worden, een geëigend instrument is om zulke fundamentele wijzigingen door de voeren. Naar aanleiding van de Evaluatie van de Wiv 2017 is er een omvangrijke wijziging van de Wiv 2017 in voorbereiding. De Ministers van Binnenlandse Zaken en Koninkrijksrelaties en Defensie hebben aan de Tweede Kamer toegezegd eerst een hoofdlijnennotitie met een analyse van de aanbevelingen van de Evaluatiecommissie, waaronder ook het invoeren van een rechterlijke procedure,[14] te zullen delen en bespreken, alvorens te komen tot een

[14] Kst 34588-90 Brief van de Minister van BZK en de Minister van Defensie aan de Tweede Kamer inzake Vervolgstappen wetsvoorstel tot wijziging Wiv 2017, 5 juli 2021.

wetsvoorstel tot wijziging van de Wiv 2017. Deze analyse zal het functioneren van en het evenwicht in het stelsel in brede zin beschrijven, inbegrepen het toezicht, de uitvoeringsconsequenties voor de AIVD en de MIVD, de gevolgen van de recente jurisprudentie van het EHRM alsmede het Hof van Justitie van de Europese Unie en de inwerkingtreding van Conventie 108+.[15] De Tijdelijke wet loopt hierop vooruit. Als dit wetsvoorstel wordt aangenomen, en er bij de ABRvS een afdeling wordt ingericht om uitvoering te geven aan de wet, mag het niet zo zijn dat het parlement geconfronteerd wordt met een *fait accompli* dat in de weg komt te staan aan een fundamentele discussie in het kader van de herziening van de Wiv 2017 over de inrichting van het toezichtstelsel, waaronder ook de wenselijkheid van het instellen, dan wel de inrichting van een beroepsprocedure.

Het College vindt het tevens onwenselijk dat op grond van voorgesteld artikel 14 lid 14 de uitspraken van de ABRvS per definitie niet openbaar zijn. Het College heeft begrip voor het feit dat binnen het domein van de nationale veiligheid, volledige openbaarheid niet altijd wenselijkheid en haalbaar zal zijn, maar wijst erop dat transparantie wel het uitgangspunt zou moeten zijn, met name daar waar het gaat om wetsinterpretatie.

Gelet op het bovenstaande adviseert het College de uitspraken van de ABRvS, en met name de onderdelen die zien op wetsinterpretatie, zo veel mogelijk openbaar te maken.

Ook raadt het College aan om de verduidelijken of de Procesregeling van de ABRvS onverkort van toepassing is op grond van de Tijdelijke wet. Deze verduidelijking ontbreekt in de Memorie van Toelichting.

6. Tot slot

Het voorgestelde gewijzigde toezicht kan alleen effectief zijn als hiervoor voldoende capaciteit beschikbaar is. Hiervoor zullen voldoende financiële middelen vrijgemaakt moeten worden. Het College acht het van groot belang dat deze wet pas in werking treedt als de TIB, de CTIVD en de ABRvS volledig toegerust zijn voor hun nieuwe taken.

Mochten er naar aanleiding van dit advies nog vragen zijn, dan kunt u contact opnemen met Katina Yiannakas, beleidsadviseur (k.yiannakas@mensenrechten.nl).

Met vriendelijke groet,

drs. Jacobine D. C. Geel
Voorzitter

[15] Kst 34588-90 Brief van de Minister van BZK en de Minister van Defensie aan de Tweede Kamer inzake Vervolgstappen wetsvoorstel tot wijziging Wiv 2017, 5 juli 2021.